وزارة التعليم العالي والبحث العلمي
جامعة – باتنة 1– الحاج لخضر
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية

أطروحة مقدمة لنيل شهادة دكتوراه العلوم في القانون

التخصص: قانون جنائي

إعداد الطالب:
سعيداني نعيم

إشراف الأستاذة الدكتورة:
مباركي دليلة

أعضاء لجنة المناقشة

الرقم	الاسم واللقب	الدرجة العلمية	الجامعة	الصفة
01	زرارة لخضر	أستاذ التعليم العالي	جامعة باتنة 1	رئيسا
02	دليلة مباركي	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
03	زغدود جغلول	أستاذ التعليم العالي	جامعة أم البواقي	عضوا
04	حوحو رمزي	أستاذ التعليم العالي	جامعة بسكرة	عضوا
05	سمصار محمد	أستاذ محاضر أ	جامعة باتنة 1	عضوا
06	بوحوش هشام	أستاذ محاضر أ	جامعة قسنطينة 1	عضوا

السنة الجامعية: 2021/2020م

شكر وتقدير

الحمد لله حمدا يوافي ما تزايد من النعم،والشكر له على ما أولاني من الفضل والكرم، وأن وفقني و أعانني على إتمام هذا البحث.

أشكر أستاذتي المحترمة الدكتورة مباركي دليلة التي تفضلت بالإشراف على هذه الأطروحة ولم تبخل علي ـ بتوجيهاتها ونصائحها، فلها مني كل التقدير والإحترام.

كما أتقدم بجزيل الشكر و التقدير إلى السادة أعضاء لجنة المناقشة الكرام كل باسمه ومركزه، الذين شرفوني بقبول عضوية لجنة المناقشة متحمـلين عـناء الإ طلاع على هذا البحث وتقييمه وإثـرائه وإتمام أوجه القصور فيه، ومصوبين لي أخطائي.
فجزاهم الله عني خـير جز اء.

إهداء

أهدي هذا العمل المتواضع إلى أمي وأبي أطال الله في عمرهما.

ثم إلى زوجتي وأولادي بارك الله لي فيهم جميعا.

المختصرات:

ق.أ.ج: قانون الإجراءات الجزائية

ج.ر: جريدة رسمية

LES ABREVIATIONS

Art = article.

Dall = dalloze

Dall.pén = dalloze pénale.

Gaz.du.pal= gazette du palais.

Rev.d.dr. p= Revue de droit public.

Rev.d.dr. pén= Revue de droit pénal.

Rev.int. dr. comp = Revue internationale de droit comparé.

Rev.sc.crim = Revue des sciences criminelles.

OP.CIT OUVRAGE PRECITE. Opus citatum

L.G.D.J = Librairie Generale de Droit et de Jurisprudence

PUF= Presses Universitaires de France

Coll= collections

CA= cour d'appel

Sect= section

CNIL= Commission Nationale de l'Informatique et des Libertés

مقدمة

مقدمة:

يعتبر حق الفرد في عدم إفشاء معلوماته الشخصية والاحتفاظ بكل ما يتعلق بحياته الخاصة إحدى مظاهر الحريات الأساسية التي حظيت باهتمام كبير، وتم تكريسها في معظم الوثائق الدولية والدساتير الوطنية، ذلك أن لكل فرد الحق في المحافظة على سرية حياته الخاصة وعدم جعلها عرضة لاطلاع الغير عليها، فكل إنسان له الحق في أن يترك وشأنه وأن يعيش حياة هادئة بعيدة عن العلنية، ومن ثم كان الحق في الخصوصية حقا قائما على حماية ذلك الجانب من حياة الإنسان الذي لا يرغب في اطلاع الغير عليه، أو لا يرغب أن يكون موضوعا لحديث الناس أو معرفتهم له، ويرجع هذا الإهتمام إلى ما للحق في الخصوصية من ارتباط وثيق بمسألة أخرى بعيدة الأثر في حياة الفرد في المجتمع الذي يعيش فيه، ألا وهي حريته وما يترتب عنها من صون لكرامته واحترام لآدميته.

فحياة الإنسان تقتضي أن تتسم بأسرار صميمة تنبع من ذات صاحبها، فهو لا يحيا فقط بمصالحه المادية، وإنما يلزم لحياته حقوقا لصيقة بشخصيته وملازمة لها.

وإذا كان الحق في الخصوصية هو أحد حقوق الإنسان الأساسية الذي يعبر عن حاجة هذا الأخير بأن يخلو إلى نفسه وأن يشعر بالهدوء والسكينة بعيدا عن أعين الناس ومراقبة الفضوليين، أو الإحتفاظ بأفكاره و آرائه أو علاقاته الحميمة أو وضعيته المالية أو حالته الصحية وغير ذلك وراء أستار السرية، فإنه يعاد التركيز عليه ويتضاعف الإهتمام به على نحو متعاظم في الوقت الحاضر بسبب توظيف تقنية المعلومات التي كانت السبب في نشأة مفهوم جديد للخصوصية ارتبط بأثر التقنية التكنولوجية على الحياة الخاصة، يتمثل في الحق في الخصوصية المعلوماتية، أو حق الأفراد في السيطرة على بياناتهم الشخصية في مواجهة تحديات العصر الرقمي، فهناك نوع من المعطيات يطلق عليها معطيات شخصية كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان، مثل الإسم ،العنوان، رقم الهاتف، عنوان البريد الالكتروني، الحالة الصحية، وغيرها من المعطيات التي تأخذ شكلا تلزم فيه الإلتصاق بكل شخص طبيعي معرف أو قابل للتعريف.

وقد أصبحت هذه الطائفة من المعطيات في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل الفلسفة المعلوماتية المعاصرة، سيما وأن فكرة العالم الرقمي تعد من بين الاعتبارات التي تمكنها من السير في التطور ومواكبة اهتمامات الإنسان من خلال استخدام البيانات الشخصية على مستويات مختلفة، حيث تمكن التقنية المعلوماتية عبر استخدام الحواسيب الآلية من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من طرف المؤسسات والدوائر الحكومية أو من قبل مؤسسات القطاع الخاص.

بالإضافة إلى أنه ومع التطور السريع لتكنولوجيا المعلومات والإتصالات الإلكترونية والذي صاحبه الإنخفاض الواضح في تكاليف استخدام هذه التكنولوجيا سيما مع انتشار الأنترنت، أصبح عدد البيانات الشخصية المعالجة آليا لا يحصى، وأنه ومن السهل الحصول عليها وتداولها عالميا بصورة غير محدودة خاصة مع ظهور القيمة التجارية للبيانات ذات الطابع الشخصي بعد ذلك.

فالأكيد إذن أن التطور التكنولوجي السريع في العصر الحديث كان وراء فكرة الإستعانة بالحاسبات الآلية لما لها من قدرة هائلة على تخزين وتجميع أكبر قدر من المعطيات الشخصية واسترجاعها في أقصر وقت ممكن والإحتفاظ بها لفترة طويلة من الزمن، كما يمكن لهذه الحاسبات أيضا إحصاء هذه المعطيات وتصنيفها وتوثيقها تحت موضوعات معينة يسهل البحث عنها والحصول عليها وجمعها وتخزينها ومعالجتها، وهو ما يطلق عليه الآن بنوك المعلومات.

فحديثا أصبح التقدم العلمي والتقني الهائل الذي أدى إلى تطور العقول الإلكترونية يضع تحت تصرف الدولة وأجهزتها الأمنية والهيئات العامة والخاصة حجما كبيرا من المعطيات الشخصية المتعلقة بالأفراد، تعجز الوسائل العادية والأساليب التقليدية من الوصول إليها، ومن ثم بات من السهل الحصول على هذه المعطيات المخزنة في أجهزة الكومبيوتر في ثوان وبالطريقة المطلوبة للاستعمال في أي مكان من العالم بشكل لم يكن متاحا من قبل.

ولما بدأت الأنظمة المعلوماتية الضخمة التي تملكها الدولة والمؤسسات تتطور، أصبح يخشى من الإستعمال التعسفي للبيانات المعلوماتية ذات الطابع الشخصي المخزنة في الملفات الإلكترونية والذي يشكل بدوره خطرا على الحق في الخصوصية للأشخاص الطبيعيين.

فالذي درج البعض على اعتقاده أن إفشاء المعلومات والتنصت عليها والاعتداء على حرمة الاتصالات والمراسلات وسريتها هو فقط ما يعد من صور الاعتداء على الحياة الخاصة، وهذه الصور هي التي ركزت عليها أغلب التشريعات في قوانين العقوبات، إلا أن الاعتداء على الحق في الحياة الخاصة من خلال الأنظمة المعلوماتية مفهوم أوسع وأشمل من ذلك، بل ويأخذ أبعادا وأشكالا مستحدثة، أبرزها مواجهة المخاطر المرتبطة بجمع معطياته ذات الطابع الشخصي، ومعالجتها الاستغلالية من قبل القطاعين العام والخاص،حيث يتم جمع عدد كبير من هذه المعطيات الشخصية وتخزينها من قبل الدولة أو الجهات الأمنية أو المصارف أو شركات التأمين أو الجامعات وغير ذلك من الهيئات الحكومية أو الخاصة، وغالبا ما يجهل الشخص ما يخزن عنه من معطيات شخصية، وكيفية تخزينها أو الفترة التي تخزن فيها أو الهدف من هذا التخزين، وهنا يطرح هذا الواقع بالأخص مسألة خسارة الفرد لسيطرته على معطياته الشخصية، ويزيد الأمر جسامة في الخطورة عندما ترتبط هذه المعالجات ببعض المعطيات الشخصية الحساسة كالمعتقد الديني،الإنتماء العرقي والإثني، الرأي السياسي، الحالة الصحية وغير ذلك من المعطيات الشخصية التي يؤثر الإفصاح عنها على الحياة الخاصة للشخص المعني بشكل مباشر ويتعرض لحقوقه وحرياته الأساسية.

و على هذا الأساس قد يكون الأفراد عرضة إلى جمع معطياتهم الشخصية وتخزينها على نحو غير مشروع، ويستمد هذا الجمع أو التخزين صفته غير المشروعة إما من الأساليب غير المسموح بها التي تستخدم في الحصول على هذه المعطيات،أو من طبيعة مضمونها كالمعطيات المتعلقة بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرقي للأفراد، والتي يجب أن تكون بمنأى عن الجمع والتخزين لاتصالها بالحياة الخاصة للافراد، بالإضافة إلى عدم التزام الجهة القائمة على النظام المعلوماتي بأن يتم تجميع وتخزين المعطيات الشخصية المتعلقة بالافراد لأجل هدف واضح ومحدد سلفا، وهو الأمر الذي

يمكن لأي فرد معاينة المساس به يوميا من خلال تجاوز شركات الاتصالات مثلا للهدف الذي تم من أجله تجميع ومعالجة المعطيات الشخصية لعملائها، حيث يعاني الكثير من الأفراد من تلقي رسائل الدعاية القصيرة التي تصل إلى هواتفهم النقالة دون الحصول على إذن خطي مسبق من العميل يسمح فيه باستقبال هذه الرسائل ويظهر ذلك أيضا من خلال رسائل البريد الالكتروني الدعائية التي تصل إلى الأفراد دون علم منهم كيف ومتى تم الحصول على المعطيات المتعلقة بعنوان بريدهم الالكتروني، وهذا ما نبهت إليه المحكمة الدستورية في ألمانيا حيث جاء في أحد قراراتها " أنه لا حرية رأي أو حرية اجتماع، ولا حرية مؤسسات يمكن أن تمارس كاملة ما دام الفرد غير متيقن في ظل أي ظروف ولأجل أي هدف جمعت عنه المعلومات الفردية وعولجت آليا في الحاسوب".

كما أن السماح بجمع البيانات أو المعلومات عن الأشخاص مع عدم معرفتهم لأوجه استخدامها في المستقبل يمثل أحد الأخطار التي تهدد الحياة الخاصة للأفراد، ويظهر هذا الخطر جليا من خلال بنوك المعلومات التي تنشؤها شركات التأمين والأموال والبنوك وغيرها من المؤسسات التي تقوم بجمع معلومات تتعلق بالحياة الشخصية لعملائها ثم يتم استغلالها بطريقة غير مشروعة في المستقبل، وخاصة من خلال قيام بعض هذه المؤسسات ببيع هذه المعلومات لشركات أو مؤسسات أو جهات أخرى للتربح المادي، ويعتبر تخزين معلومات شخصية خاطئة غير مطابقة للواقع وغير صحيحة أو غير دقيقة صورة أخرى من صور الإعتداء على الحياة الخاصة، فهذه المعلومات قد تترك آثارا سيئة على سيرة الإنسان وصورته، ويلحق به ضرر وأخطار كبيرة خاصة على مستقبله الوظيفي والاجتماعي.

وهذا ما يدعونا إلى القول بأن الحواسيب الإلكترونية وإن كانت أحد المظاهر الفذة للتقدم العلمي التي وفرت على الإنسان جهدا خارقا، وقدمت للبشرية خدمات جليلة، فإنه لا يمكن التغاضي عن مخاطرها الجمة على الحياة الخاصة للإنسان، حيث أصبح ميسورا بواسطتها جمع كل المعلومات الشخصية عن شخص معين مثل هويته، سنه، وضعه العائلي، حالته الصحية، مركزه العائلي أو المالي، وآرائه السياسية وغيرها من المعطيات ذات الطابع الشخصي، واستخدامها لأغراض مختلفة تماما عن الأغراض التي جمعت لأجلها، أو جمعها بطرق غير مشروعة ودون علم صاحبها بذلك.

وهو الأمر الذي أبرز الكثير من المشكلات التي تهدد الحق في الخصوصية في المجال المعلوماتي، فإذا كان الناس قد تعودوا على أن يدلوا بكثير من المعلومات على أنفسهم لأغراض معينة وهم على ثقة بأن من يحصلون عليها يستخدمونها في الأغراض المطلوبة فقط، فإن الأمر أصبح مختلفا باستخدام الحواسيب التي تجمع وتخزن في جوفها عددا هائلا من المعطيات المرتبطة بالحياة الخاصة للأشخاص، حيث نجد في عصر المعلوماتية أن المؤسسات العامة والخاصة أصبحت تعمد على تنظيم بنوك المعلومات التي تتضمن بيانات شخصية تتعلق بالأفراد، مما أدى إلى إثارة حفيظة هؤلاء صونا لحياتهم الخاصة و صونا لسريتها.

فلوقت قريب لم يكن يشكل الاعتداء على الحق في الخصوصية خطورة بالغة، لكن مع انتشار الحاسوب وتكنولوجيا المعلومات والثورة العلمية في عالم الأنترنت، أصبح من السهل اليسير تخزين كم هائل من المعطيات الشخصية، مع إمكانية نقلها وتعديلها وحذفها في زمن وجيز جدا، وهذا الأمر لا يمنع

من استعمال واستغلال هذه المعطيات بطريقة غير مشروعة، ومن ثم أصبحت المعطيات الشخصية للإنسان تستخدم كوسيلة للاعتداء على حقه في الخصوصية،

ومكمن الخطر يتمثل في أن بنوك المعلومات اليوم وما تحتوي عليه من معلومات عن الفرد، وما يخزن فيها عنه من معطيات شخصية، تشكل عنصر تضييق وتقليل من انطلاقاته وإبداعه ومشاركته في الحياة العامة، والسبب الأساسي في ذلك يرجع إلى أنه أصبح محورا لعمليات آلية مختلفة تمسه في كل جانب من جوانب حياته المتشعبة، ذلك أن الحاسوب يقوم بجمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد، وكل ذلك أصبح يشكل خطرا بشكل أو بآخر على حياة الإنسان الخاصة ويهددها، ومن ثم يصبح الفرد أسيرا للمعلومات التي تجمعها هذه الحواسيب عنه.

وإلى جانب بنوك المعلومات فإن التطورات السريعة والثورات التكنولوجية المتلاحقة كان لها آثارها وتداعياتها الهائلة على وسائل الإتصال الإلكتروني سيما شبكات الأنترنت ومواقع التواصل الإجتماعي، وهي الوسائل التي فرضت واقعا جديدا فتح آفاق التواصل والاتصال بين الناس، وبدأ نتيجة لذلك الكثير منهم بوضع بياناته الشخصية عبر مواقع الأنترنت والشبكات الاجتماعية، وهي المعطيات التي يمكن من خلال استقرائها الوصول إلى مؤشرات معلوماتية هائلة عن الشخص صاحب هذه المعطيات.

فانطلاقا من وسائل الإتصالات الرقمية ازدادت ظاهرة دفق البيانات الشخصية على الأنترنت نتيجة ازدياد عدد أجهزة الحواسيب الموصولة بها، وتعددت وسائل تخزينها بتعدد أنظمة الحوسبة السحابية، كما يتنوع استخدامها وتتنوع التطبيقات التي تهندس لكيفية الإستفادة منها لتقديم الخدمات، علما أن القسم الأكبر منها يتم جمعه دون علم الشخص صاحب هذه البيانات.

وترتيبا على ذلك بدأ العالم يشهد انطلاق الاهتمام بحماية الحياة الشخصية من مخاطر التكنولوجيا الحديثة لينطلق معه مفهوم حماية البيانات الشخصية من مخاطر المعالجة الآلية لهذه البيانات.

وتضاعفت أهمية إرساء نظام فعال للحماية وفرض إجراءات قانونية صارمة ضد إساءة استخدام البيانات الشخصية والإعتداء عليها، بالإضافة إلى ضرورة مواكبة أرقى المعايير والإلتزام بتطبيقها في مجال حماية المعطيات ذات الطابع الشخصي بمناسبة معالجتها آليا، من أجل الحفاظ على إمكانات وفرص الإفادة مما يمكن أن تقدمه التقنيات الحديثة في مجال معالجة المعطيات الشخصية.

وبالتالي بدت الحاجة ماسة إلى صياغة نصوص قانونية لوضع وتكريس المبادئ الأساسية لحماية الخصوصية المعلوماتية من خلال التنبيه إلى ضرورة الإلتزام بالاستقامة في جمع البيانات الشخصية، التصريح عن غايات معالجتها، ملائمة البيانات الشخصية المجمعة لغاية المعالجة، وكذا إعطاء أصحاب هذه المعطيات بصفتهم معنيين بالمعالجة مجموعة من الحقوق المرتبطة ارتباطا وثيقا بجوهر الحق في الخصوصية، يأتي في مقدمتها حقه في الاطلاع على المعلومات الخاصة به والوصول إليها، وأن يكون على علم بجميع البيانات المخزنة عنه، وحقه بالغاء الخاطئة منها أو تصحيحها وتعديلها إذا دعت الحاجة الى ذلك، ومن أهم الحقوق التي يتوجب صيانتها وحمايتها أيضا والتي يعاني الفرد في مجتمعاتنا بسبب غيابه

الكبير هو حماية حق الفرد في النسيان، فالمعطيات الشخصية المخزنة لا بد وأن تتلف بعد مدة محددة حتى لا تبقى شبحا يطارد الفرد أينما ذهب وفي كل زمان.

و من خلال هذه الخطوات يمكن للمشرع أن يثبت سعيه إلى وضع أسس ثابتة ومتينة تمثل سياجا منيعا لهذا الجانب البارز والمهم من جوانب حياة الإنسان الخاصة، والذي شغل بال الباحثين والفقهاء في علم القانون والاجتماع على حد سواء، فالأمر مدعاة لأن يحظى هذا الحق باهتمام المشرع على المستوى الدولي في مجال الإتفاقيات والإعلانات والمؤتمرات الدولية، وكذا على المستوى الوطني في الدساتير والقوانين الداخلية، حيث لم يقف الأمر عند الإعتراف بالحماية القانونية للحق في الخصوصية المعلوماتية على مستوى الجهود الدولية سواء العالمية أو الإقليمية والتي كان لها دور بارز في إثارة الإنتباه إلى ضرورة العمل على توفير حماية فعالة لهذا الحق، بل امتد الأمر إلى تدخل التشريع الداخلي الدستوري أو العادي.

فنتيجة لطبيعة المعطيات ذات الطابع الشخصي فإنه وعلى الرغم من حمايتها بموجب اتفاقيات دولية ودلائل أممية، فإنها تبقى عرضة لمنطق التعسف ضد هذه المعطيات خاصة إذا تمت معالجتها آليا، ويؤدي ذلك لا محالة إلى المساس بالحق في الخصوصية المعلوماتية، لذلك تم وضع قوانين ونظم من جراء مطامح تشريعية ترمي لمحو كل أثر سلبي من آثار التقنية المعلوماتية على الحق في الخصوصية.

و هو ما حصل فعلا أمام هذه المخاطر التي تواجهها المعطيات الشخصية بمناسبة معالجتها الآلية بواسطة أجهزة الحاسوب، فقد تدخلت التشريعات لتنظيم استخدام المعطيات الشخصية التي يتم الحصول عليها، حيث ظهرت قوانين ونظم مختلفة عملت على تجسيد وترجمة مقاربات مكافحة المعالجات الإستغلالية للمعطيات الشخصية وتقرير حق الفرد في السيطرة والتحكم في معطياته الشخصية على المستوى القانوني، سواء من خلال القوانين العامة التي تتضمن المبادئ الأساسية المتعلقة بحماية المعطيات ذات الطابع الشخصي، أو من خلال القوانين القطاعية التي تخص نظما معينة وتطبق على قطاعات محددة كقطاع الإتصالات، والقطاع المصرفي، وقطاع الصحة[1]... وذلك بغية التخفيف من المخاطر المتولدة عن سوء استخدام المعطيات الشخصية عند معالجتها، ومن ثم توفير الحماية القانونية لحق الأشخاص في الخصوصية المعلوماتية.

وقد كان المشرع الجزائري واحدا من هذه التشريعات عندما تدخل بتعديل دستوري سنة 2016 بموجب القانون 01/16 المؤرخ في 2016/03/06 في المادة 16 الفقرة الأخيرة التي أشارت في نصها "على أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"، ثم استحدث القانون 07/18 المؤرخ في10يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي.

لكن في الجهة المقابلة نجد أن الاعتراف بالحق في الخصوصية لا يعني مطلقا القول بأن للفرد حقوقا تفوق حقوق الجماعة، فلا ينبغي أن يغيب عن الأذهان أن حياة الفرد في المجتمع تدعو إلى إقامة نوع من التوازن بين حرية الفرد وبين نظام المجتمع وأمنه، لذلك فلا مناص من أن يخول المجتمع الحق في فرض مجموعة من الالتزامات والرقابة على الأفراد حتى ولو ترتب على ذلك تدخل في حياتهم الخاصة، ومن ثم

يكون للدولة أن تطلع على المعطيات الشخصية للأفراد لحاجتها إلى حماية نفسها من الجرائم ذات الإرتدادات السلبية على أمنها واستقرارها كالتجسس والإرهاب... فالدول عامة تحتاج إلى جمع البيانات الشخصية حتى الحساسة منها للقيام بمهامها كسلطة عامة وكمسؤولة عن الإستقرار والأمن الإجتماعيين.

أهداف الموضوع:

يركز موضوع هذه الدراسة على البحث في مفهوم جديد للحق في الخصوصية ظهر وانتشر في ظل استخدامات المعلوماتية والأنترنت للمعطيات ذات الطابع الشخصي ومعالجتها، وهو ما يسمى بالحق في الخصوصية المعلوماتية.

والهدف من دراسة موضوع الحماية القانونية للحق في الخصوصية المعلوماتية في التشريع الجزائري يكمن في تحديد مضمون هذا الحق من خلال رسم نطاقه، وجمع جوانبه وتوضيح معالمه التي كرسها المشرع الجزائري، سيما من خلال استقراء النصوص القانونية التي أقرها القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي، لإبراز الضمانات والضوابط التي تكفل حماية هذا الحق.

كما يهدف هذا البحث أيضا إلى إبراز أهم المخاطر التي يمكن أن تهدد الحق في الخصوصية انطلاقا من أثر التقنية المعلوماتية على معالجة المعطيات ذات الطابع الشخصي، فالحواسيب الآلية التي يتم الإستعانة بها في إنشاء بنوك المعلومات، لما لها من قدرة هائلة في تخزين وتجميع أكبر قدر ممكن من البيانات الشخصية واسترجاعها في أقصر وقت ممكن، والاحتفاظ بها لفترة طويلة من الزمن وتصنيف وتوثيق هذه البيانات، من شأنها أن تهدد أسرار خصوصية الأفراد وسكينتهم.

فإذا كانت التقنية المعلوماتية مجسدة في الحاسب الإلكتروني وما يستطيع أن يقوم به وفقا لبرامج معينة من جمع للبيانات الشخصية وتصنيفها وتخزينها ونقلها بعد معالجتها إلكترونيا تحتل مركز الصدارة في عصرنا الحالي، حيث يعود لها الفضل الأكبر في تسهيل عمل الحكومة ودوائرها في إدارة شؤون الأفراد، وكذلك الشأن بالنسبة للقطاع الخاص من خلال ما يطلق عليه بنوك المعلومات، بالإضافة إلى نظام المشاركة الزمنية الذي يسمح عن طريق شبكة اتصالات واسعة بالتعامل مع البيانات الشخصية مباشرة والحصول على المطلوب منها في أقصر وقت ممكن، إلا أن مقابل هذا الوجه المشرق للمعلوماتية نجدها تحمل في طياتها جانبا سلبيا يتمثل في تهديدها لأسرار الحياة الخاصة،و كذا إسهامها في ترجمة حياة الفرد بعد أن كان سابقا من الصعب على أي كان أن يكشف عنها، لكنها أصبحت مع التقنية المعلوماتية شفافة واضحة دون أي غطاء يحجبها أو يحميها.

ومن ثمة فلما كانت بنوك المعلومات هذه والمرتبطة بالتقدم التكنولوجي مدعاة للانتهاك وعرضة للاعتداءات من خلال التلاعب بالبيانات الشخصية بشتى الصور، سواء بالإستخدام الخاطئ لمثل هاته البيانات كالإفشاء غير المشروع أو دمج هذه البيانات أو حذفها أو مسحها أو التلاعب بها أو سرقتها عبر مواقع الأنترنت بفعل الإلتقاط غير المشروع لها، وتجميعها وتصنيفها ثم استخدامها بشكل غير مشروع، فإنه كان من المحتم على المشرع أن يتدخل لتنظيم طرق استخدام المعطيات الشخصية ومعالجتها ومن ثم

توفير الحماية للحق في الخصوصية، والتركيز على أهم مظهر من مظاهرها وهي الحماية الجزائية من أجل التصدي للتهديدات والاعتداءات التي يتعرض لها الحق في الخصوصية المعلوماتية.

أهمية الموضوع:

لأجل كل هذا ارتأيت أن أقدم تصور المشرع الجزائري لمسألة التنظيم التشريعي للمعالجة الآلية للمعطيات الشخصية - جوهر الحق في الخصوصية المعلوماتية - بعد أن أدرك كما أدركت كل التشريعات في العالم بأهمية حمايتها، لما لهذا الأمر من دور حاسم في بناء بيئة مواتية لتأمين ودعم الثقة في التقنية المعلوماتية، وكذا المساهمة في الخدمات الإلكترونية.

ولأن الإنسجام على المستوى القانوني حاجة ملحة في المواجهة الفعالة، كان لا بد من أن نبحث في مدى تقارب المشرع الجزائري مع غيره من التشريعات الخاصة بحماية البيانات الشخصية في إطار رصد بعض المقاربات في مسائل بعينها، سيما مع المشرع الفرنسي من جهة، ومدى انسجامه مع التوصيات المعتمدة عالميا في ذات المجال من جهة ثانية، وذلكعبر تبيان نقاط الإلتقاء والا ختلاف أينما وجدت.

أسباب اختيار الموضوع:

ورغم إدراكي لصعوبة هذا الموضوع ودقة وسعة البحث فيه لارتباطه بجانب علمي وأساليب تقنية حديثة، كاد ذلك يصرفني ويثنيني عن المضي فيه، لكن ولشعوري بأهميته ولشدة الحاجة إلى دراسته خاصة مع غياب الدراسات المتوسعة فيه منقبل باحثين جزائريين، كان الأمر دافعا حاسما لي من أجل الاستقرار على تناول هذا الجزء من الحياة الخاصة للإنسان بنصيب من البحث، وذلك بالتطرق إلى مسائل حماية الحق في الخصوصية في العصر الرقمي، وبالتالي حماية البيانات ذات الطابع الشخصي من مخاطر المعالجة الالكترونية، وهو الأمر الذي يتطلب عرضا للدواعي والأسباب التي أوجدت هذا المفهوم، وتحديدا مخاطر التقنية المعلوماتية على جزء مهم من حياة الأفراد، ثم الحماية القانونية التي وفرها لها المشرع.

ولا أحسبني أتجاوز الحقيقة حينما أعتبر أن محاولة الإستحواذ على البيانات الشخصية أصبحت مسألة ملازمة للنشاط الإجتماعي للأفراد، وأنها كانت من أهم المتغيرات التي أثرت على تحول الرؤية نحو البيانات الشخصية، حيث أصبحت مصدرا للثروة وللقوة، واحتدام التنافس للاستحواذ عليها واستخراجها ومعالجتها وتوظيفها لتحقيق أهداف محددة.

ولا غرابة إن كان الأمر على هذه الخطورة أن ينصب اهتمامنا في هذا البحث على دراسة حق الإنسان في حماية خصوصيته المعلوماتية بعد أن تصاعد تيار يعضد من قدرة الأفراد في السيطرة على بياناتهم الشخصية وهوياتهم وثقتهم في التحول الرقمي، في مقابل الإتجاه المضاد الذي كان يدعو إلى توسيع دور الدولة في السيطرة على البيانات الشخصية على المستويين التشريعي والتقني، على أساس أن فكرة الخصوصية المعلوماتية هي أول مناطق التساؤل عن أثر التقنية على الحياة الخاصة، والتي انطلقت في أجواء التطور التكنولوجي الواسع والإستخدامات المتزايدة للمعطيات ذات الطابع الشخصي وعمليات المعالجة الآلية لها، فتمس على نحو مباشر خصوصياتهم وأسرارهم وبالتالي حياتهم الشخصية بأسرها.

إشكالية البحث:

موازاة مع التحول الرقمي الذي فتح مجالات واسعة أمام إساءة استغلال المعطيات ذات الطابع الشخصي عند معالجتها، وذلك بإدلائها للغير أو استخدامها في غير الغرض الذي جمعت لأجله أو معالجتها بطرق غير مشروعة، سرعان ما نمت الحاجة إلى إيجاد الوسائل القانونية وإلى جانبها الوسائل التقنية التي تضمن الحماية الفعالة للحق في الخصوصية في العصر المعلوماتي وما أفرزه من بنوك المعطيات وشبكات الأنترنت، وإذا كان المشرع الجزائري قد استجاب لهذه المبررات واستحدث في سبيل ذلك تشريعات جديدة لمواجهة آثار وانعكاسات التقنية المعلوماتية على معالجة المعطيات ذات الطابع الشخصي من خلال القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي، فهل كانت السياسة الجزائية المتبعة من طرف المشرع من خلال هذا النص القانوني فعالة في إرسـاء نظام قانوني متكامل لحماية جزائية للحق في الخصوصية المعلوماتية؟

وإذ نحن بصدد البحث في هذه الإشكالية الجوهرية تصادفنا تساؤلات يعتبر البحث فيها أمرا تفرضه ضرورات الإجابة عن جوهر موضوع الدراسة أهمها:

- ماهي المعطيات ذات الطابع الشخصي التي تعتبر جوهر الحق في الخصوصية المعلوماتية، ويمثل الإعتداء عليها اعتداء على هذا الحق.

- ماهي المخاطر التي يمكن أن تهدد المعطيات ذات الطابع الشخصي أثناء معالجتها، وانعكاسات ذلك على صاحب هذه المعطيات باعتباره الشخص المعني بالمعالجة في انتهاك حقه في الخصوصية.

- ماهي القيود والضوابط التي اهتم المشرع بوضعها في مواجهة الأجهزة الإدارية التابعة للدولة والمؤسسات الخاصة عندما تفكر في إنشاء أنظمة معلوماتية لمعالجة معطيات ذات طابع شخصي.

- ما هي الحقوق التي منحها المشرع للشخص صاحب المعطيات الشخصية عندما تكون هذه المعطيات محل معالجة.

- ماهي استراتيجية الحماية التي كرسها المشرع في مواجهة أنشطة الإعتداء على الحق في الخصوصية في البيئة الرقمية.

- هل اكتفى المشرع بضرورة توفير الحماية التقنية والتنظيمية للمعطيات الشخصية محل المعالجة لتأمين حماية فعالة لها، أم رافقها بحماية جزائية، وماهي حدود ومؤيدات هذه الحماية الجزائية بين الإستخدام العادل للمعطيات الشخصية وبين الأفعال التي تشكل اعتداء حقيقيا عليها.

مناهج البحث:

محاولة للإلمام بكل جوانب هذا الموضوع نظرا لتشعب مسائله وارتباطه بجوانب تقنية، فقد تطلب منا الأمر الاعتماد على مناهج تتكامل فيما بينها:

المنهج التحليلي: من خلال تحليل بعض المفاهيم والغوص في جزئياتها، وطرحها بشكل من التفصيل والتشريح، سيما تحليل بعض النصوص القانونية والإستعانة بالآراء الفقهية للوصول إلى معناها الحقيقي.

- منهج وصفي: تم اعتماد المنهج الوصفي الذي يساعد في التعامل مع مشكلة البحث بطريقة واقعية وذلك من خلال وصف بعض الجزئيات والمفاهيم التي تم التطرق إليها في موضوع هذا البحث، سيما وصف بعض أشكال الانتهاكات الحاصلة على الخصوصية المعلوماتية.

-منهج مقارن: نظرا لأن هناك من الأنظمة القانونية المختلفة للدول خاصة الأوروبية منها من وضعت تشريعات تنظم مسألة حماية المعطيات ذات الطابع الشخصية المعالجة آليا، فكان لا بد من دراسة هذا الموضوع دراسة مقارنة للاستنارة بهذه التشريعات في هذا المجال، و مقارنة كيفية معالجتها لهذا الموضوع الذي يعد ذو طبيعة عالمية، وقد نال دون شك حظه من المعالجة التشريعية لدى العديد من التشريعات المقارنة مثل المشرع الفرنسي من خلال القانون 17/78 المتعلق بالمعلوماتية والملفات والحريات المؤرخ في1978/01/06 والمعدل بالقانون 801/2004 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في2004/08/06،و كذلك المشرع المغربي بموجب قانون 09/08 المؤرخ في 2009/02/18 المتعلق بحماية الأشخاص الذاتيين تجاه المعالجة المعطيات ذات الطابع الشخصي، بالإضافة إلى التوجيه الأوروبي 95/46/CE المؤرخ في 1995/10/24 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية تدفقها، واللائحة العامة رقمUE679/2016/المؤرخة في 2016/04/27 المتعلقة بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية تدفقها.

خطة البحث

وتحقيقا للهدف المقصود من هذه الدراسة تم انتهاج خطة مقسمة إلى ثلاثة فصول، نتناول في الفصل الأول الإطار المفاهيمي للحق في الخصوصية المعلوماتية حيث نعالج فيه الجوانب المفاهيمية للحق في الخصوصية عموما من حيث تعريفه وطبيعته ونطاقه في المبحث الأول، ثم في المبحث الثاني نعرج فيه على ظهور الحق في الخصوصية المعلوماتية معبرا عن تطور الحق في الخصوصية نتيجة ارتباطه بأثر التقنية المعلوماتية، ثم المخاطر التي تهدد هذا الحق.

وفيما يتعلق بالفصل الثاني وهو المعبر عن الضوابط القانونية لعمليات المعالجة الآلية للمعطيات الشخصية، من خلال تحديد الضوابط الموضوعية المقررة لمعالجة المعطيات ذات الطابع الشخصي في المبحث الأول، ثم نتناول في المبحث الثاني الضوابط الإجرائية لهذه المعالجة من حيث تبيان الإجراءات المسبقة التي يجب على كل مسؤول عن معالجة المعطيات الشخصية التقيد بها قبل البدء في عمليات المعالجة لهذه المعطيات، ثم معرفة الإلتزامات الملقاة على عاتق هذا الأخير.

أما الفصل الثالث فقد أفردناه للحماية القانونية للخصوصية المعلوماتية، من خلال تناول الحماية الإدارية التي تجسدها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في المبحث الأول، ثم

نتناول الحماية الجزائية للمعطيات ذات الطابع الشخصي، وهي إما حماية جزائية موضوعية يتم تناولها في المبحث الثاني وإما حماية جزائية إجرائية نسلط عليها الضوء في المبحث الثالث.

وفي آخر هذه الدراسة خلصنا إلى مجموعة من النتائج والاقتراحات، تم التوصل إليها انطلاقا من دراسة هذا الموضوع تم إدراجها في خاتمته.

الفصل الأول

الإطار المفاهيمي للحق في الخصوصية المعلوماتية

الفصل الأول: الإطار المفاهيمي للحق في الخصوصية المعلوماتية

إن الحق في الخصوصية عميق الجذور من الوجهة التاريخية، إذ نجد الإ شارة إليه في العديد من الديانات والمعتقدات البشرية الضاربة في عمق التاريخ، ثم أصبح قيمة قانونية محمية في المواثيق الدولية والدساتير الوطنية والقوانين الداخلية للدول، لتعلقه وارتباطه الشديد بالكر امة الآدمية، وكذلك جمعه بين الجوانب المادية والمعنوية لشخصية الانسان وعلاقته الوثيقة بالحقوق والحريات الأ خرى.

لكن مع تزايد التقنيات الحديثة، وكثرة الابتكارات التكنولوجية، زادت المخاطر على حق الانسان في الخصوصية، فأصبح الفرد عرضة لأن تجمع عنه الكثير من المعطيات الشخصية وتخزن وتعالج بواسطة الوسائل المعلوماتية، كقواعد البيانات المعلوماتية وشبكات الإتصال الالكترونية، وهي جميعا تشكل تهديدا مباشرا وجديدا على الحياة الخاصة والحريات الفردية، خاصة إذا استغلت هذه المعطيات الشخصية المجمعة لغايات وأعراض مختلفة دون رضا أصحابها الذين قد لا يكونون أصلا على علم بوجودها، وكذلك تفعل شبكات الاتصال الالكترونية التي يترك الشخص وهو بصدد استخدامها آثار ودلالات كثيرة تتصل به على شكل سجلات رقمية تتضمن تفاصيل دقيقة ذات محتوى شخصي يتصل بحياة الفرد المستخدم على الشبكة، ومن ثم كان من الضروري السعي إلى توفير الحماية اللازمة لهذه المعطيات الشخصية في مواجهة آثار التطور التقني في العصر الحديث، دراء لما يخشى عليها من الاستعمال التعسفي الذي يشكل خطرا على حق أصحابها في الخصوصية.

المبحث الأول: ماهية الحق في الخصوصية:

يعتبر حق الإنسان في الخصوصية عموما جوهر الحقوق والحريات الشخصية، ويعد الاعتراف بهذا الحق هو مجرد الكشف عنه وليس إنشاء له، كونه من الحقوق اللصيقة بالإنسان ومن ثم فهو قديم قدم هذا الإنسان، ويعد هذا الحق من أكثر الحقوق المثيرة للجدل بين فقهاء القانون منذ زمن بعيد، كون مفهومه يتبدل ويتطور باستمرار تبعا لاختلاف المفاهيم الاجتماعية والاقتصادية والثقافية والسياسية والدينية زمانا ومكانا.

فمفهوم الحق في الخصوصية يتبدل بين منطقةلأ خرى ومن مجتمع لآخر، وأنه ليس واحدا أو متشابها في القرون الوسطى والقرن العشرين، ولهذا علينا التزام أقصى درجات الحذر والموضوعية عند إخضاعه لأي تعريف.[1]

ويكاد ينعقد إجماع بين فقهاء القانون على صعوبة التوصل إلى وضع تعريف جامع مانع للحق في الخصوصية أو الحياة الخاصة*، ويرجع السبب في ذلك لاختلاف المفهوم الذي يمثل أساسا لتحديد التعريف.

[1] رامز محمد عمار، نعمت عبد الله مكي، حقوق الإنسان والحريات العامة، الطبعة الأولى، 2010، بدون دار النشر، ص 347.

* الحياة الخاصة هي كل ما يتعلق بذاتية الشخص ويؤول إليه، وبالتالي كل ما يتعلق بحياته الشخصية، ومن الناحية التوظيفية لهذا التعبير ودلالته الاصطلاحية فان الاصطلا ح المعروف في النظام القانوني الأنجلوسكسوني هو مصطلح الخصوصية privacy، في حين المصطلح السائد في النظام اللاتيني عموما والفرنسي خصوصا والذي يعبر عن ذات الحق، هو الحياة الخاصة vie privée.

فقد ظهرت الخصوصية في أنظمة قانونية كوسيلة لتحديد الخطوط الفاصلة بين حق الفرد المطلق وحق المجتمع بالتعرض لشؤونه، وفي أنظمة قانونية أخرى كانت الخصوصية هي الحرية في مواجهة كل اعتداء أو انتهاك[1].

لذلك فإن هذا التباين كان سببا وعاملا في نشوء العديد من التعريفات للحق في الخصوصية، والتي كانت إما تتوسع في تحديده إلى درجة اقترانها بالحرية عموما، وإما تعمد إلى تضييق نطاقها لتكون في إطار معنى حق العزلة والسرية وفي أن يترك الشخص وحيدا[2].

ومن ثمة فل الإ خفاق في تحديد تعريف للحق في الخصوصية أو الحياة الخاصة يتأتى من تنوع مظاهر هذه الحياة وتقلباتها وعصيانها عن أي مضمار منطقي منظم.[3]

ذلك أن الحق في الخصوصية إما أن يكون محكوما باعتبارات تتجلى في أن ثمة أشياء يشعر الفرد بالحاجة إلى الا حتفاظ بها بعيدا عن اطلاع الآخرين عليها وهذه حالة نسبية، على أساس أن نطاق الحق في الخصوصية يختلف من فرد لآخر، فما يمكن أن يشكل خصوصية لفرد ما قد لا يكون كذلك بالنسبة لفرد آخر، وذلك بحسب رغبة كل فرد في الاحتفاظ بجزء من حياته و أفكاره وانفعالاته وأنشطته الخاصة لنفسه بعيدا عن تطفل الآ خرين.[4]

ومن جانب آخر قد يرتبط الحق في الخصوصية بقواعد السلوك والأخلاق في المجتمع والتي تختلف من بلد لآخر، ومن هنا يتسع مفهوم الخصوصية ويضيق تبعا لاختلاف المجتمعات[5].

وسوف نحاول البحث في أهم الآراء الفقهية التي من خلالها حاول الفقه تعريف الحق في الخصوصية ورسم صورته وبيان مضمونه وطريقة تعيين حدوده.

المطلب الأول: مفهوم الحق في الخصوصية

في الحقيقة إن الفقه القانوني وكذا القضاء على حد سواء لم يتمكنا من رسم الحدود المنطقية للحق في الخصوصية على الرغم من وجود النصوص القانونية التي تحمي مظاهره، وكثرة الأحكام القضائية

[1] بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي، الطبعة الأولى 2009 ،ص 09.

[2] Hala kassem, « l'internaute et son droit à être laissé tranquille » Formation doctorale : Informatique et Droit mémoire D.E.A informatique et droit, Section CNU : Droit privé et sciences criminelles. 71 Sciences de l'information et de la communication. E.R.I.D. Université de Montpellier1 Année.2003p11. Disponible sur le site www.droit-tic.com

[3] نعيم مغبغب، مخاطر المعلوماتية والانترنت، المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية، لبنان، 2008، ص 94.

[4] ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة 1996، ص188.

[5] نعيم عطية، حق الأفراد في حياتهم الخاصة، مجلة إدارة قضايا الحكومة، العدد الرابع السنة الواحد والعشرون،1977 ص84

المتعلقة بحالات الاعتداء عليه، ومن ثم فإنه من الصعب تحديد أبعاد هذا الحق بصورة جلية ودقيقة، خصوصا أنه لا يزال محل نقاش.[1]

الفرع الأول: التعريف الفقهي والقضائي للحق في الخصوصية

يجد الفقه المقارن صعوبة في التوصل إلى وضع معيار محدد وحاسم يمكن على ضوئه إعطاء تعريف للحق في الخصوصية يكون صالحا للتطبيق في المجال القانوني، فقد أوردت لجنة الخبراء المنبثقة عن المجلس الأوروبي في مجال حقوق الإنسان أنه بالرجوع إلى الكتابات والدراسات المختلفة عن الحق في الخصوصية لم يتبين أنه يوجد تعريف عام ومتفق عليه سواء على مستوى التشريع أو الفقه أو القضاء.[2]

أولا التعريف الفقهي للحق في الخصوصية:

كان للفقه دور كبير في محاولة وضع تعر يف للحق في الخصوصية، سواء اللاتيني أو الأمريكي.

1) دور الفقه الفرنسي في تعريف الحق في الخصوصية: لقد لعب الفقه القانوني الفرنسي الذي يمثل النظام اللاتيني، دورا مهما في الاعتراف بالحق في الحياة الخاصة، وكان الفقهاء يطالبون دائما القضاء بمزيد من الاعتراف بالحق في الحياة الخاصة وبالتوسع في فهم معناها وبسط نطاقها.[3]

ومن أوائل الفقهاء الفرنسيين الذين تعرضوا في كتاباتهم لهذا الحق هو الفقيه بيرو Perreau الذي ذهب إلى اعتبار حقوق الشخصية والحق في الخصوصية صنوان، وذلك إثر حديثه عن حقوق الشخصية في المقال المنشور في المجلة الفصلية للقانون المدني عام 1909، حيث كتب في مقاله هذا "أن الشخص الذي يرغب في أن يعيش في هدوء وسكينة من حقه أن يفعل ذلك، وليس لأحد أن يجلبه إلى أضواء النشر دون موافقته الصريحة أو الضمنية، وأن قيام الغير بنشر أمور متعلقة بحياة الفرد الخاصة دون موافقته يعد اعتداء على حقه في الخصوصية.[4]

وفي هذا المعنى كتب الفقيه "مازو" «mazeau» معتبرا أن من بين الحقوق الشخصية التي يحميها القانون ضد أي اعتداء يقع عليها من أعضاء المجتمع الآخرين هو الحق في السلامة المعنوية، ويندرج ضمن هذا الحق، حق الفرد في حرية الفكر والوجدان وحقه في أن يعبر عن آرائه، وحقه في كتم أسراره ومحادثاته الهاتفية ومراسلاته، وحقه في منع نشر صورته[5].

كما أوضح الفقيه نيرسون nirson في رسالته التي قدمها سنة 1939 عن "حقوق الإرث العادية" تحت باب الحقوق الشخصية، أن الحق في الحياة الخاصة يقع في دائرة الحقوق الشخصية التي تشمل الإ سم

[1] علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس لبنان،2006 ص116.

[2] علي أحمد عبد الزعبي، مرجع سابق، ص 124.

[3] ممدوح خليل بحر، مرجع سابق ص121.

[4] بولين أيوب، مرجع سابق، ص52.

[5] ممدوح خليل بحر، مرجع نفسه، ص162.

والمسكن والحقوق العائلية وأسرار المهنة والشرف والسمعة،وأن للشخص الحق في أن يحتفظ بأسرار حياته الخاصة ويتعذر على العامة معرفتها إلا بإرادة صاحب الشأن[1].

وقد عرف الفقيه كاربونيي «carbonier» الحق في الحياة الخاصة بأنها "المجال السري الذي يملك الفرد فيه سلطة استبعاد أي تدخل من الغير، وهي حق الشخص في أن يترك هادئا[2].

كما اعتبر أن الحق في الحياة الخاصة هي سلطة تمنح للفرد من أجل اختيار طريقة حياته بالشكل الذي يعجبه، ويجب تبعا لذلك أن تبقى حياته الخاصة بعيدة عن المراقبة من أجل السماح له بإمكانية الاختيار.[3]

وعرفها الفقيه بادينتار «badinter» في كتابه الحق في احترام الحياة الخاصة Le droit au respect de la» «vie privée بأنها احترام الطبيعة الخاصة للشخص، والحق في الهدوء والسكينة دون تعكير لصفو حياته.

وقد ذهب الفقيه مارتن «martin» إلى اعتبار أن الحق في الحياة الخاصة والحقوق الشخصية حقان متطابقان، حين عرف الحياة الخاصة أنها الحق في الحياة الأسرية والشخصية الداخلية والروحية للشخص عندما يعيش وراء بابه المغلق، في حين ذهب جانب آخر من الفقه الفرنسي إلى ربط فكرة الحق في الحياة الخاصة بفكرة الحرية، حيث عرف في هذا الإطار الفقيه فيري «firier»الحق في الحياة الخاصة بأنها مجموعة الحالات والأعمال والآراء الصادرة عن الفرد بحرية والتي لا تربطه بأي التزام في مواجهة الآخرين.*

وقد حاول أيضا الفقيه ماليرب «Malherbe» أن يضع تعريفا للحياة الخاصة في كتابه "الحق في الحياة الخاصة" الذي نشره سنة 1967، حيث اعتبر أن حماية الحياة الخاصة للفرد هو حماية اتصالاته الخاصة ومكاتباته ومراسلاته اللاسلكية وتسجيلاته وشؤونه الصحية، وكذا حماية شرفه وحقه في اسمه وحرمة مسكنه، ومن ناحية أخرى كذلك هي حماية حياته العائلية التي تشمل المسؤولية عن نفقة الأبناء إلى وقت بلوغهم، فضلا عن الأمور التي لها تأثير على حياته الشخصية مثل الارتباطات الزوجية.[4]

2) دور الفقه الأمريكي في تعريف الحق في الخصوصية: إن من أشهر التعريفات التي برزت في هذا الصدد هو التعريف الذي جاء به المعهد الأمريكي للقانون، والذي تضمن أن كل فرد ينتهك بصورة جدية

[1] علي أحمد عبد الزعبي، مرجع نفسه، ص122

[2] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة، الطبعة الثالثة، دار النهضة العربية القاهرة، 1994، ص11

[3] أنظر في هذا المعنى: رامز محمد عامر، نعمت عبد الله مكي، مرجع سابق، ص347.

* يعتبر غالبية الفقه أن الحرية ليست شرطا لكل حياة خاصة، فهذا المسلك من شأنه الخلط بين الحياة الخاصة وأمور أخرى لا تدخل في هذه الدائرة، فقد يكون الشخص مجردا من حريته مؤقتا كالسجين الذي تفرض عليه بعض القواعد التي يلتزم باتباعها واحترامها، ومع ذلك يبقى له الحق في التمتع ببعض عناصر حياته الخاصة، ومنها حق خصوصية مراسلاته التي لا يجوز لأحد فتحها والاطلاع عليها وهي صورة تدخل في صميم خصوصيته.

[4] ممدوح خليل بحر، مرجع سابق، ص163.

وبدون وجه مشروع حق شخص آخر في رغبته بعدم وصول أموره وأحواله إلى علم الغير، وألا تكون صورته عرضة لأنظار الجمهور، يعد مسؤولا أمام المعتدى عليه.[1]

ولقد كان للمقال الذي كتبه كل من الفقيهان الأمريكيان صموئيل وارن «Samuel Warren» ولويس براندیس [*]«louis brandies» الفضل في الدفاع عن الخصوصية، أين تم وصفها بأنها الحق في أن يترك الشخص وحيدا the right to be left aloneكما كان لهذا المقال تأثير كبير في تطور هذا الحق وإقراره أمام المحاكم[2]، بل كان الأساس لمواقف قضاة المحكمة العليا عند اتجاههم لإقرار هذا الحق وقبول الدعاوي المستندة إليه[3].

وقد وافق أغلب فقهاء القانون على اعتبار أن هذا المقال يعد النص المؤسس للخصوصية، والذي ذهبت المحكمة العليا الأمريكية الىاعتماده وتوضيحه أكثر باعتبار ها أن الحق في الخصوصية هو حق كل شخص في اتخاذ قراراته في محيطه الخاص بمفرده.[4]

كما ذهب الفقيه الأمريكي كنيت كريش إلى تعريف الخصوصية بأنها الحق في الخلوة، أي حق الإنسان في حياة هادئة وأن يترك دونما إزعاج أو قلق.

ولعل الفقيه كولي Cooly هو أول من نادى بفكرة الخلوة، وهي الفكرة التي لقيت قبولا من قبل الفقه الأمريكي، إذ عرف الفقيه نيزر «Nizer» الخصوصية على أساس أنها حق الإنسان في أن يعيش بمفرده مجهولا، ومن حق الشخص أن يعيش بعيدا عن أنظار الناس وعن القيود الاجتماعية.[5]

وفي هذا الإتجاه من التعاريف الفقهية، عبر الفقيه "آلن ويستن alen wistin" عن الخصوصية في مقاله تحت عنوان privacy and Freedom عام 1967 بأنها انسحاب إرادي ومؤقت للشخص من المجتمع إلى العزلة، أو أن يعيش حالة من الإنغلاق والتحفظ وسط مجموعة أكبر، وذهب للقول أيضا أنها أي الخصوصية رغبة الأشخاص في الاختيار الحر للآلية التي يعبرون فيها عن أنفسهم ورغباتهم وتصرفاتهم للآخرين.[6]

---

[1] أحمد فتحي سرور، الحق في حرمة الحياة الخاصة، مجلة القانون والاقتصاد، العدد 54 سنة 1987 الإسكندرية، مصر، ص 45.

[*] حدث في سنة 1890 أن قامت بعض الصحف الأمريكية بنشر قصص عاطفية وإماطة اللثام عن تفاصيل شخصية بصموئيل وارين وهو محام أمريكي سابق اعتزل المحاماة وأصبح من رجال الأعمال وعن زوجته وهي ابنة أحد أعضاء مجلس الشيوخ، وأشارت هذه الصحف على وجه الخصوص إلى مسألة زواج ابنتهما، فاستغل وارين هذا الاعتداء واتجه إلى صديقه السابق لويس براندیس والذي أصبح فيما بعد من أشهر قضاة الولايات المتحدة الأمريكية، وكتبا معا مقالا في مجلة هارفرد للقانون، بعنوان "حق الحرمة الشخصية."

[2] ممدوح خليل بحر، مرجع سابق، ص146.

[3] بولين أيوب، مرجع سابق، ص51.

[4] Farid Bouguettaya la protection des données personnelles en droit communautaire, Mémoire master 02 recherche droit européen des droits de l'homme, mémoire FACULTE DE DROIT – IDEDH Université de montpellier1 Année 2006p.5.

[5] بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة المجيستر في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2017، عمان الاردن، ص12.

[6] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الاتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر 2016، ص 41.

وقد اتجه الفقيه الأمريكي ويليام بروسر william prosser في تعريفه للخصوصية إلى الابتعاد عن التعريف المجرد للخصوصية معتمدا على تعدد العناصر التي تدخل في نطاقها بناءا على القيمة العلمية لهذه العناصر، أين اعتبر أنه يمكن رفع دعوى مدنية لدفع الاعتداء الذي يقع على الحياة الخاصة في حالات أربع:

1/انتهاك أو اقتحام عزلة أو خلوة الفرد بالاعتداء على حرمة سكنه أو التنصت على محادثاته الهاتفية أو تصويره أو التأمين على حياته دون موافقته وهو ما أسماه بالتطفل.

2/الإفشاء العلني للوقائع الخاصة والماسة باحترام الشخص العادي وهو ما أسماه بنشر حقائق محرجة.

3/تشويه سمعة الشخص في نظر الآخرين كعرض صورته في معرض لصور المتهمين بعد تبرئته من جريمة أتهم بارتكابها، وهو ما أسماه بإساءة إستعمال الصورة.

4/ إستخدام إسم الفرد أو صورته أو ملامحه لكسب تجاري دون موافقته، وهو ما أسماه بالاستيلاء على بعض عناصر الشخصية.[1]

أما الفقيه الأمريكي كافيزون روثcavison ruth فقد اعتبر أن للخصوصية ثلاث عناصر هي: السرية secrecy، العزلة solitude والتخفي .anonymity

ثانيا: دور القضاء في تعريف الحق في الخصوصية:

إذا كان الفقه المقارن يجد صعوبة في التوصل إلى وضع معيار قانوني حاسم يمكن على ضوئه إعطاء الخصوصية تعريفا محددا يصلح للتطبيق في المجال القانوني، فإن القضاء من جانبه يمتنع غالبا عن إعطاء تعريف لفكرة كفكرة الحق في الخصوصية، ويكتفي بالبحث في كل مظهر من مظاهر هذه الفكرة على حدى لتوفير الحماية الكاملة دون التقيد بقواعد معينة.[2]

وقد كان للقضاء المقارن موقف متأرجح من فكرة الخصوصية تراوح بين الإنكار والإقرار، ففي مرحلة أولى أنكر القضاء البريطاني الخصوصية واتجه إلى عدم إقرارها في ظل عدم وجود نص تشريعي.*

حيث يوجد في القضاء الإنجليزي كثير من الأحكام القضائية التي تنكر الاعتراف بالحق في الخصوصية بوصفه حقا مستقلا، ومن بين أهم مبررات رفض الاعتراف بالحق في الخصوصية في إنجلترا:

- أن فكرة الخصوصية فكرة هلامية غير محددة المضمون، وهو الأمر الذي من شأنه المساس بمسائل حساسة دستورية وسياسية لها تأثيرها المشترك على سلطة الحكومة من ناحية، وفكرة الحريات الشخصية من ناحية أخرى، كما أن عدم تحديد مضمون فكرة الخصوصية يجعل من الصعوبة بما كان وضع حدود فاصلة بين ما يعد من المصالح العامة المشروعة وما يعد من الخصوصيات.[3]

---

[1] ممدوح خليل بحر، مرجع سابق، ص150، وكذلك علي أحمد عبد الزعبي، مرجع سابق، ص ص162، 163.

[2] علي أحمد عبد الزعبي، مرجع نفسه، ص118.

* القضاء الأنجلو أمريكي تحكمه قاعدة قضاء السوابق، وهي القاعدة التي تحظر على القضاء تقرير أي حل ملائم ما دامت الحالة جديدة لم تعرض عليه سابقا، وأن القضاء عند انتفاء السابقة لا يغير وجهته إلا بتدخل المشرع لإقرار هذا الحق.

[3] ممدوح خليل بحر، مرجع نفسه، ص120.

لكن عدم اعتراف القضاء الإنجليزي بالحق في الخصوصية بوصفه حقا مستقلا، لا يعني عدم توفير أي نوع من الحماية عند المساس بالخصوصية، وإنما يحاول القضاء الإنجليزي اللجوء إلى أساليب مختلفة لتوفير الحماية من خلالها، فهو يلجأ إلى بعض الأخطاء المعترف بوجودها ليرى في المساس بالحق في الحياة الخاصة واحدا من هذه الأخطاء، فهو في ذلك يعتبر المساس بالخصوصية من قبيل القذف، وتارة أخرى من قبيل التعدي على ملكية الغير، وتارة أخرى يعتبره من قبيل المضايقات وأحيانا يعتبره من قبيل الإخلال بالثقة، ومن ثم كانت حماية القضاء الإنجليزي للحياة الخاصة متناثرة الأساس القانوني على امتداد القانونين الجنائي والمدني.[1]

أما بالنسبة للقضاء الأمريكي فقد شهد تباينا في المواقف في مواجهة الخصوصية، فاتجهت أحكامه القضائية الأولى إلى عدم الاعتراف بالحق في الخصوصية نظرا لعدم وجود سابقة قضائية[2]، وكذلك انطلاقا من أن التعديل الرابع للدستور لم يقر إلا الخصوصية المادية ولم يتجاوزها إلى أبعد من ذلك[3]، وكان ذلك في الحكم الذي صدر في قضية روبرسن Roberson، أين رفضت المحكمة العليا طلب المدعية على أساس أنه لا توجد سوابق قضائية، وأن المشرع هو وحده الذي له سلطة أن يعدل القانون الذي كان معمولا به في ذلك الوقت[4].

ومع الدعوات لتطوير النصوص الدستورية عن طريق التفسير القضائي، نظر القضاء الأمريكي في مرحلة لاحقة عددا من دعاوي الخصوصية، أين توصلت المحاكم الأمريكية على إثرها إلى إقرار الحق في الخصوصية وذلك من خلال التوسع في تفسير ما جاء به التعديلين الرابع والتاسع للدستور الأمريكي في حماية نفس الإنسان وأملاكه، وتم بسط الحماية على الخصوصية من خلال هذا التفسير.*

ولقد وصف في هذا الإطار القاضي براندیس عضو المحكمة العليا في الولايات المتحدة الامريكية الحق في الخصوصية عند نظره قضية أولمستيد ضد الولايات المتحدة الامريكية، بأنه"الحق في أن يـ ، ترك المرء وشأنه، وهو من أهم الحقوق وأكثرها قيمة لدى الناس المتحضرين".[5]

---

[1] ممدوح خليل بحر، نفس المرجع ص121.

[2] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، الطبعة الثالثة 1994، ص50

[3] بولين أيوب، مرجع سابق، ص48.

[4] ممدوح خليل بحر، مرجع سابق، ص144. وتتلخص وقائع هذه القضية في أن المدعى عليهم كانوا قد استعملوا صورة المدعية لترويج منتجاتهم دون الحصول على إذنها، أين رفعت المدعية دعوى قضائية مطالبة بالحق في التعويض مرتكزة على أن هناك انتهاكا لحقها في الخصوصية وقع على حقها في ملكية صورتها.

* حكمت محكمة ميتشجان في قضية ديمي ضد روبرتس بإلزام طبيب بأن يدفع تعويض في قضية تتمثل وقائعها في أن هذا الطبيب كان قد اصطحب معه شخصا لا يمارس مهنة الطب إلى غرفة الولادة في المستشفى دون علم السيدة التي كانت في حالة وضع بحقيقة هذا الشخص، وكذلك قضية مانولا ضد ستيفيز التي ظهرت فيها إحدى الممثلات على المسرح في ملابس ضيقة بشكل فاضح مما أغرى أحد المصورين بالتقاط صور لها، فقضت محكمة نيويورك للمدعية (الممثلة) بمنع النشر لأن في ذلك اعتداء على حياتها الخاصة. أنظر ممدوح خليل بحر، مرجع سابق ص148.

[5] ممدوح خليل بحر، مرجع نفسه، ص149.

وفي نفس المعنى ذهب القاضي دوجلاس douglas عضو المحكمة العليا للقول "أن الحرية بمعناها الدستوري تنم عما هو أبعد من مجرد التحرر من كل صور التحكم والقيود غير المشروعة للحكومة، بل يجب أن تتضمن الخصوصية أيضا حق المرء في أن يترك وشأنه، وهو بداية كل الحريات".[1]

وعلى الرغم من أن القضاء الأمريكي له السبق في مجال تشييد نظرية الحق في الخصوصية، إلا أنه حدد أحوال الإعتداء على هذا الحق قبل تحديد مضمونه، فضلا على أنه لم يتضمن تحديد ماهية هذا الحق بصورة جامعة.[2]

أما عن مسيرة القضاء الفرنسي في حقل الخصوصية فنجده اعترف بالحق في الحياة الخاصة في كثير من القضايا، عندما اتجهت محكمة النقض الفرنسية إلى إقرار الخصوصية كحق عام موحد يمتد نطاقه إلى حماية الفرد من المساس بخصوصيته أيا كانت طبيعة الانتهاك أو جهته أو غرضه، ومن ثم ذهبت بعض الأحكام القضائية في فرنسا إلى اعتبار أن احترام الحياة الخاصة هو حق الشخص في تعيين حدود لما يمكن نشره عن ألفة حياته.[3]

وهنا يتضح جليا أن القضاء الفرنسي يعتد بفكرة الألفة بصفة أساسية عند تعريف فكرة الخصوصية، والألفة تعني العزلة والخلوة بكل هدوء، والإنزواء عن أنظار ومسامع الآخرين، وبعبارة أخرى هي ذلك الجزء الذي يرغب الإنسان بالاحتفاظ به مخفيا عن الآخرين.*

ومن خلال ما سبق سرده من تعريفات للحق في الخصوصية، يمكن القول أنه بالرغم من حرص كل من الفقه والقضاء المقارنين على إعطاء هذا الحق المكانة البارزة، والتي انعكست على اهتمام الدساتير والنصوص التشريعية في أغلب دول العالم على النص عليه وحمايته من الاعتداء، إلا أنه لا يزال الجدل قائما لتحديد تعريف موحد ودقيق لهذا الحق[4]، ولعل ذلك راجع لاستناده على فكرة نسبية متغيرة من حيث الزمان والمكان نتيجة لارتباطه بعادات الأفراد وتقاليدهم وأخلاقياتهم وتطورات الحياة وعوامل البيئة الثقافية، الاجتماعية، الاقتصادية والسياسية.

فمن الصعوبة بما كان وضع تعريف محدد للخصوصية أو الحياة الخاصة لكون هذه الفكرة مازالت تثير النقاش والخلاف في الفقه والقانون المقارن، وهذه الصعوبة كما أسلفنا ترجع إلى أن فكرة الحياة الخاصة هي فكرة مرنة تختلف من مجتمع إلى آخر بحسب الأخلاقيات السائدة في المجتمعات، بل وأيضا بحسب

[1] خليل بحر، مرجع نفسه، ص150.

[2] علي أحمد عبد الزعبي، مرجع سابق، ص127.

[3] مصطفى أحمد عبدالجواد حجازي، الحياة الخاصة ومسؤولية الصحفي، دراسة فقهية قضائية مقارنة في القانونين الفرنسي والمصري، دار الفكر العربي، القاهرة 2001، ص59.

* أغلب الفقه الفرنسي اعتبر الألفة من أهم عناصر الحياة الخاصة وجوهرها. لذلك فقد استخدم بعضهم حق الألفة كمرادف للحق في الخصوصية. وقد وصف الفقيه سافاتيه savatier الحياة الخاصة بأنها الحديقة المغلقة للألفة. أنظر نعيم مغبغب مخاطر المعلومات والانترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية2008، ص 22.

[4] محمد محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، الطبعة الأولى، 2005 القاهرة مصر، ص62.

الظروف الخاصة لكل شخص كونه من الناس الذين يكتمون خصوصياتهم أو أنه من أولئك الذين يجعلونها كتابا مفتوحا.[1]

الفرع الثاني: موقف التشريعات المقارنة من الحق في الخصوصية

ليس من شك في أن خصوصية الإنسان تحتاج إلى الاعتراف القانوني وتوفير الحماية لها، بحيث لا تغدو سرية الإنسان مرتعا سهلا لانتهاكات الآخرين تحقيقا لغريزة الفضول والتطفل المتأصلة في نفوس الناس، أو رغبة في تحقيق مصلحة معينة دونما مبرر لذلك، فالأسباب التي تغري الناس بالعمل على اقتحام خصوصيات الآخرين تتعدد وتتباين، وعندئذ تظهر أهمية القانون الذي ينبغي أن يوفر حماية ناجعة لهذه الخصوصية من مثل هذه التطفلات، خصوصا بعد تزايد الضغوط على مناطق الخصوصية في العصر الحديث.

وبذلك تظهر أهمية الاعتراف القانوني بالحق في الخصوصية من خلال توفير الحماية الضرورية له إزاء كل تدخل غير مشروع من شأنه الاعتداء عليه والمساس به، خاصة بعد زيادة المخاطر التي تتهدد هذا الحق نتيجة التقدم العلمي والتكنولوجي الحديث الذي كان سببا في ضرورة الإسراع بالاعتراف بهذا الحق.

والواقع أن مفهوم الخصوصية أو الحق في الحياة الخاصة في القانون المقارن لا يزال عائما بعد، ولم تتحدد أبعاده بصورة دقيقة، ففي السنوات الأخيرة قام عدد وفير من الكتاب ومن الجمعيات القانونية وكذا عدد من المنظمات الدولية بإعداد دراسات في هذا النطاق، كانت محصلتها أن انقسم القانون المقارن في تحديد مفهوم الخصوصية بين مؤيد ومعارض لظهور ما يسمى بالحق في الخصوصية.

أولا: الإتجاه المعارض للاعتراف بالحق في الخصوصية:

هناك اتجاه في القانون المقارن لا يقر بالاعتراف بالحق في الخصوصية بوصفه حقا مستقلا وهو الموقف المستقر للقانون الإنجليزي، الذي يعد على رأس النظم القانونية الحديثة التي مازالت ترفض الاعتراف بالحق في حرمة الحياة الخاصة*، وحتى القضاء الإنجليزي لم يحاول أن يخرج عن هذا المسلك العام بشأن موضوع الخصوصية، كما أن الفقه الإنجليزي لم يحاول تغذية القانون ليصبح متلائما مع التطورات التي لاحقت المجتمعات الحديثة ومست دونما شك مسألة الحق في الخصوصية لأفرادها.

وكان من أهم الحجج لرفض الاعتراف بفكرة الخصوصية أنها فكرة غير محددة يكتنفها الغموض ويصعب وضع تعريف لها، وأن طبيعة الحياة داخل المجتمعات يوجد فيها الكثير من المضايقات التي قد يتعرض لها الإنسان والتي تقتضي أن يقبل المرء قدرا من تطفل الغير على حياته الخاصة متى كان ذلك في حدود معقولة، وأنه ليس من المناسب أن يكون علاج هذه المضايقات عن طريق القانون، كما أنه من الصعوبة التمييز بين ما يدخل في نطاق الحياة الخاصة للأفراد ومن ثم يمنع على الآخرين التدخل فيه، وبين ما

[1] منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلومات السعودي، دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في العدالة الجنائية، الرياض جامعة نايف العربية للعلوم الأمنية، 2010، ص12.

* تتمثل تلك التشريعات أساسا في التشريع الإنجليزي الإيطالي والأسترالي والأمريكي القديم والمقاطعات الكندية الإنجليزية- انظر محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة أو الخصوصية دراسة مقارنة، دار النهضة العربية، القاهرة، ص20.

يدخل في نطاق الحياة العامة لهم[1]، لأن فكرة الحياة الخاصة غير محددة المعالم وعدم دقة المعيار المتعلق بنطاقها.

ومن بين الحجج أيضا أنه مقابل تمتع الفرد بوسائل العلم الحديثة وإشباع رغباته الملحة بتلك التقنيات والأساليب التكنولوجية الحديثة، فعليه أن يقبل تعرضه لانتهاكات تطال أسراره من قبل الآخرين، وهي ضريبة حتمية يدفعها الفرد مقابل استخدامه لتلك الوسائل[2]، ولا يزال القانون الإنجليزي* يرفض الاعتراف بالحق في الخصوصية بوصفه حقا مستقلا على الرغم من توقيع بريطانيا على الاتفاقية الأوروبية لحقوق الإنسان والتي تضمنت النص صراحة على احترام الحياة الخاصة.*

ثانيا: الاتجاه الذي يعترف بالحق في الخصوصية:

يعتبر أنصار الاتجاه القانوني الذي يعترف بالحق في الخصوصية وعلى رأسهم أنصار النظام القانوني اللاتيني، أن الحياة الخاصة تعد قطعة غالية من حياة الإنسان لا يمكن انتزاعها منه، و إلا فإنها تتحول إلى أداة صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بطبيعته له أسراره الشخصية ومشاعره الذاتية ولا يمكنه أن يتمتع بهذه الملامح إلا في إطار مغلق يحفظها ويضيء لها سبيل البقاء.[3]

ولقد كان من نتائج تطور الوسائل التقنية في العصر الحديث أن عملت هذه التشريعات على توفير أكبر قدر ممكن من الحماية لخصوصيات الأفراد، إلا أن هذه الحماية تختلف باختلاف التشريعات التي تأخذ بهذا المبدأ.

---

[1] منصور بن صالح السلمي، مرجع سابق، ص53.

[2] محمد الشهاوي، مرجع سابق، ص63

* هناك بعض القوانين القديمة والحديثة في إنجلترا تجعل من أنواع معينة من التطفل على الحياة الخاصة محلا للتجريم (حماية غير مباشرة)، إلا أن هذه القوانين لا تكف لبسط حماية واسعة على أوجه الحياة الخاصة. ومن بين هذه القوانين نذكر بعضا مما ساقته لجنة تقرير العدالة:

-قانون السلامة لسنة 1361 وهو القانون الذي يجرم استراق النظر من نوافذ مساكن الغير وكذا استراق السمع من وراء الجدران.

-قانون التآمر وحماية الملكية لعام 1875 وهو القانون الذي يمنع أي شخص من مراقبة أو اختلاس النظر إلى المنازل.

-قانون التلغراف اللاسلكي لعام 1949 هذا القانون الذي تنص المادة 5 منه على أن أي شخص يستخدم أي جهاز تلغراف لاسلكي بقصد الحصول على معلومات من المرسل إليه أو نائبه يكون محلا للمساءلة الجنائية أو المدنية.

-قانون مكتب البريد العام لعام 1953 هذا القانون الذي تنص المادة 66 الفقرة الأولى منه على أن الإصرار على طلب شخص بواسطة الهاتف باستمرار قد يكون مدعاة للتقاضي، حيث يصبح هذا الفعل نوعا من إثارة القلق ويتعارض مع هدوء الشخص وراحته.

-قانون البريد العام المتعلق بتنظيم الخدمات لسنة 1967 الذي ينص على تنظيم المعلومات بواسطة الكومبيوتروالذي يفرض نوعا من الإلتزام بالسرية على موظفي مكاتب البريد بالنسبة لمثل هذه المعلومات، ويقرر عقابا لكل من يفشيها. للمزيد أنظر: يوسف الشيخ يوسف، حماية الحق في حرمة الأحاديث الخاصة- دراسة مقارنة في تشريعات التنصت والحياة الخاصة، دار الفكر العربي، الطبعة الأولى، القاهرة، مصر، 1998، ص50.

* وقد عدل المشرع الإيطالي عن موقفه الذي كان يرفض فيه حماية الحق في الحياة الخاصة بوصفه حقا مستقلا من خلال إدراجه المادة 620 مكرر من قانون العقوبات الإيطالي التي تعاقب كل من سجل بجهاز أيا كان نوعه محادثة خاصة بالغير دون رضاه في مكان خاص، وكان ذلك استنادا إلى المادة 08 من الاتفاقية الأوروبية لحقوق الإنسان، أنظر حسام الدين كامل الأهواني، الحق في احترام الحق في الحياة الخاصة، الحق في الخصوصية دراسة مقارنة، دار النهضة العربية، القاهرة 1978 ص ص 11، 12.

[3] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الأول، الطبعة السادسة، دار النهضة العربية، القاهرة1996، ص 98.

1) موقف القانون الأمريكي من الحق في الخصوصية: لقد اعترف التشريع في الولايات المتحدة الأمريكية بالحق في الخصوصية للأفراد وبسط الحماية اللازمة لحياتهم الخاصة[1]، فقد كان لما توصلت إليه المحاكم الأمريكية من الإقرار و الاعتراف بالحق في الخصوصية انطلاقا من تفسير التعديلات الدستورية التي تحمي الحريات الأساسية الواجبة لازدهار المواطن، أثر بالغ الأهمية على موقف التشريع الأمريكي في تعديل موقفه إزاء الحق في الخصوصية، ذلك أن هذا الحق إلى غاية بدايات القرن 20 لم يلق أي اهتمام من قبل الفقه ولا القضاء الأمريكيين، لكن مع مرور السنوات استشعر الجميع بأهمية هذا الحق بوصفه حقا قائما بذاته، وكانت البداية أن اهتم التشريع الأمريكي ببسط حمايته على الشخص وممتلكاته، ثم اتسع مفهوم الخصوصية عنده ليصل إلى تمكين الإنسان من التمتع بحياته من جميع جوانبها ونواحيها بما فيها كيانه المعنوي وكافة الأنشطة الصادرة منه.[2]

ويظهر الاعتراف بالحق في الخصوصية في الدستور الأمريكي خاصة في التعديل الثالث والرابع والخامس، أين اتفقت هذه التعديلات الدستورية في مجملها على حماية حق الأفراد في الخصوصية ضد كل تدخل ليس له مبرر من قبل الحكومة.

وقد تجد الخصوصية تعزيزا عاما لها بمقتضى التعديل الدستوري التاسع، وهو التعديل الذي يعتبره أغلب شراح القانون الدستوري في الولايات المتحدة الأمريكية أنه كفل حماية حقيقية للحق في الخصوصية وأكد على الاهتمام الحاصل في أمريكا بهذا الحق، فقد أعد المعهد الأمريكي للقانون مشروع قانون* عن أفعال الخطأ سنة 1935 « Restatement of torts » وهو المشروع الذي ضم ما استقرت عليه المحاكم الأمريكية من تفسيرات واسعة للقانون العام وكذلك للقواعد التي أظهرها تطبيق المحاكم لمختلف القوانين*، وبالرغم من أن هذا المشروع لم يصدر كقانون إلا أنه كان له تأثير واضح على تطور التشريع الأمريكي في مجال الاعتراف بالحق في الخصوصية وحمايته[3]، كما كان له تأثير أيضا على المحاكم الأمريكية التي قابلته بارتياح شديد حيث كانت تؤسس عليه أحكامها في قبول دعاوى حماية الحق في الخصوصية.

وفي عام 1939 أقرت المدونة الأولى للأفعال الضارة انتهاك الحق في الخصوصية كأساس للمطالبة بالتعويض إذا كان التدخل في خصوصية الشخص غير معقول وعلى قدر كبير من الجسامة، وفي عام 1968 أصدر الكونغرس الأمريكي قانونا خاصا بمكافحة الجريمة في سيارات نقل الركاب والشوارع، حيث نص في الباب الثالث منه على عقوبات جزائية ضد كل من يتنصت على المحادثات الهاتفية أو تسجيل الأحاديث دون ترخيص.[4]

---

[1] محمد يحي مطر،الحق في الخصوصية في القانون الأمريكي، "بحث مقدم إلى مؤتمر الحق في حرمة الحياة الخاصة" المنعقد في الفترة من 04 إلى 06 جوان 1987، كلية الحقوق، الإسكندرية، مصر ،1987 ص17

[2] أسامة عبد الله قايد، مرجع سابق، ص16.

* يضم المعهد الأمريكي للقانون نخبة كبيرة من ثقاة القانونيين ومجموعة من رجال القضاء والمحامين.

* نصت المادة 876 من هذا المشروع على أن كل من يتعرض بغير مبرر وبشكل جدي لمصلحة الغير في حجب شؤونه الخاصة أو صورته عن الكافة يكون مسؤولا أمامه عن ذلك.

[3] ممدوح خليل بحر، مرجع سابق، ص152.

[4] حسان أحمد محمد، نحو نظرية عامة لحماية الحق في الحياة الخاصة، دار النهضة العربية، طبعة سنة 2001،القاهرة، ص272.

وفي سنة 1970صدر في الولايات المتحدة الأمريكية قانون حرية المعلومات، ثم في سنة 1974 صدر قانون الخصوصية الفدرالي الذي يتضمن إطارا قانونيا لحماية البيانات، وهو متعلق فقط بالسلطات العامة، بينما القطاع الخاص له حرية وضع معايير الخصوصية الخاصة به، وفي سنة 1977 أقرت المدونة الثانية للأفعال الضارة بصفة صريحة الحق في الخصوصية، حيث أكدت على حمايته من أي اعتداء يتعرض له عندما نصت المادة 652 من هذه المدونة على أن من يعتدي على حق شخص آخر في الخصوصية يكون مسؤولا عن الضرر الذي يصيب مصالحه نتيجة لهذا الاعتداء و الذي تتمثل صوره فيما يلي:

-التدخل في عزلة الغير أو شؤونه الخاصة.

-استخدام إسم أو صفة الغير لتحقيق مصلحة خاصة.

-إفشاء أمور متعلقة بالحياة الخاصة للغير.

-نشر أمور تشوه حقيقة الغير في نظر الناس.[1]

وبالإضافة إلى المجهود التشريعي الفدرالي فهناك مجموعة من القوانين على مستوى الولايات الأمريكية تهتم بقضايا الخصوصية.[2]

ومن الملاحظ أنه ليس هناك تحديد للخصوصية بشكل واضح ومباشر في دستور الولايات المتحدة الأمريكية، إلا أن القضاء الأمريكي تخطى العقبة الخاصة بعدم وجود سوابق قضائية أو نص تشريعي يقر الاعتراف بالحق في الخصوصية*، وعمل على التوسع في مفهوم حماية نفس الإنسان وأملاكه وبسط من خلال هذا التفسير الحماية على الحق في الحياة الخاصة.

ولعل هذا الاعتبار القضائي هو الدافع الأساسي للتشريع الأمريكي في الإعتراف بالحق في الخصوصية كحق مستقل، بالإضافة إلى اعتبارات أخرى ساهمت في التطور الذي لحق موقف القانون الأمريكي أهمها تأثر القانون الأمريكي بما كان عليه العمل في بعض الدول الأوروبية مثل فرنسا وألمانيا والتي تعترف بهذا الحق، بالإضافة إلى تأثير بعض كتابات الفقهاء الأمريكيين في مجال الخصوصية.[3]

2) **موقف القانون الفرنسي من الحق في الخصوصية:** لقد اهتم المشرع الفرنسي بالحياة الخاصة، لذلك نجده قد أصدر العديد من التشريعات التي تعترف صراحة بالحق في الحياة الخاصة.[4]

والواقع أن اهتمام المشرع الفرنسي بموضوع الحياة الخاصة يرجع إلى زمن بعيد، ففي سنة 1868 صدر قانون ينص في المادة 11 منه على توقيع عقوبة مالية (غرامة قدرها 500 فرنك فرنسي) على كل من يقوم

---

[1] خالد ميار الإدريسي، مستقبل حماية الخصوصية في عالم الانترنت، واقع مستقبل حماية الخصوصية من منظور اليونسكو، مقال منشور بموقع: www.massarate.ma أطلع عليه يوم 2019/06/10

[2] للتوسع حول الجهود التشريعية الأمريكية في مجال حماية الخصوصية أنظر: www.ncst.org اطلع عليه يوم 2018/07/09

* لجأ القضاء الأمريكي إلى طريقة فنية مفادها ضرورة التمييز بين ما إذا كانت الحالة محل النزاع مسألة جديدة لم يسبق للقضاء الفصل في مثليتها وبين تطبيق مبدأ موجود سلفا على وقائع جديدة. أنظر: ممدوح خليل بحر، مرجع سابق، ص147.

[3] أنظر في هذا المعنى ممدوح خليل بحر، مرجع سابق، ص 146.

[4] محمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، القاهرة، مصر، 2014، ص26.

بأي نشر أو أي إعلان مكتوب يكون من شأنه التشهير بالحياة الخاصة للأفراد، وفي 1881/07/29 صدر القانون الخاص بحرية الصحافة والذي منح للمواطن العادي إمكانية رفع دعوى بالقذف على الصحف عند نشرها مقالا من شأنه المساس بحياته الخاصة، لكن لم يتطرق المشرع الفرنسي في هذا القانون إلى وضع تعريف للحياة الخاصة.[1]

ولقد بقي القضاء الفرنسي ولحقبة طويلة من الزمن يضفي حماية على الحق في الحياة الخاصة استنادا إلى قواعد المسؤولية المدنية، من خلال تطبيقه لنص المادة 1382 من القانون المدني الفرنسي التي تنص على أن "كل فعل يترتب عليه ضرر للغير ملزم من يرتكبه بإصلاح هذا الضرر"، وهذا بسبب عباراتها التي جاءت عامة والتي يمكن أن تشمل تلك الأفعال التي من شأنها أن تشكل انتهاكا لخصوصيات الأفراد.[2]

وعند صدور القانون رقم 70/ 64المؤرخ في 1970/07/07 المتعلق بحماية الحقوق الفردية للمواطنين،[3] الذي عدل القانون المدني الفرنسي، أعلنت الفقرة الأولى من المادة 09 من هذا القانون في صياغتها على الحق في احترام الحياة الخاصة[4]، ووصفت الفقرة الثانية من نفس المادة التدابير التي يمكن للقاضي المدني أن يتخذها من أجل توقيف المساس بحرمة الحياة الخاصة، غير أن هذا لم يعط تعريفا أو يحدد مفهوما لمحتوى مصطلح الحياة الخاصة[5]، رغم أن هذا النص كرس بصورة واضحة لا لبس فيها نوعين من الحماية للحق في الحياة الخاصة:

الأولى: حماية وقائية تتمثل في اتخاذ تدابير ضرورية لمنع أو وقف الاعتداء على ألفة الحياة الخاصة من خلال المصادرة أو الضبط وغيرها من الإجراءات.

والثانية: حماية إصلاحية تتمثل في إمكانية المطالبة بالتعويض عن الأضرار الناتجة عن فعل الانتهاك الماس بحرمة الحياة الخاصة.[6]

---

[1] Albert Chavanne les résultats de l'audio surveillance comme preuve pénale, revue internationale de droit comparé, vol 38 n2 avril. Juin, 1986, p 749.

[2] François Rigaux, La protection de la vie privée et des autres biens de la personnalité, Revue internationale de droit comparé, Vol 43 N°2, Avril-juin 1991 p 07

[3] Loi n 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

[4] Depuis 1970, l'article 9 du code civil dispose que :

« Chacun a droit au respect de sa vie privée. Les juges peuvent sans préjudice de la réparation du dommage subi prescrire toutes mesures telles que séquestres, saisies et autres, propres à empêcher ou à faire cesser une atteinte à la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé ».

La notion de vie privée n'est pas définie par la loi. Elle a été précisée peu à peu par la jurisprudence et peut être considérée comme incluant l'état de santé, la vie sentimentale, l'image, la pratique religieuse, les relations familiales et l'intimité.

[5] نويري عبد العزيز، الحماية الجزائية للحياة الخاصة دراسة مقارنة بين القانون الجزائري والفرنسي، دار هومة للطباعة والنشر والتوزيع 2015 الجزائر، ص91.

[6] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة الطبعة الثانية، دار النهضة العربية، 2002 ص29.

وبنفس القانون أدخل المشرع الفرنسي بموجب المادة 22 تعديلا على بعض النصوص الجزائية[1] في قانون العقوبات، وهي النصوص التي تهدف إلى تجريم الاعتداءات الواقعة على حرمة الحياة الخاصة، وذلك في المواد 368، 369، 370، 371، 372 من قانون العقوبات،[2] حيث خضع قانون العقوبات الفرنسي إلى تعديل بموجب القانون رقم 684/92 مؤرخ في 1992/07/22 والذي دخل حيز التنفيذ ابتداء من 01 مارس 1994،[3]جرم من خلاله المشرع الفرنسي أفعال المساس بالحق في حرمة الحياة الخاصة في الفصل السادس من الكتاب الثاني تحت عنوان الاعتداء على الحياة الشخصية، أين خصص الجزء الأول من هذا الفصل لتجريم الأفعال الماسة بالحق في الحياة الخاصة والمتمثلة في الاعتداء على حرمة الحديث الخاص والصورة وانتهاك حرمة المسكن في المواد 1/226 إلى المواد 7/226، ثم خصص الجزء الثاني من الفصل السادس لتجريم المساس بالحق في حرمة الحياة الخاصة الناجم عن نشر مونتاج دون موافقة أو رضا صاحبه في المادة 8/226.

والملاحظ أن المشرع الفرنسي لم يحدد معنى أو مفهوم الحياة الخاصة في قانون 1970/07/27 والذي عدل بموجبه كلا من القانون المدني وقانون العقوبات في آن واحد، وحتى عند إعادة صياغته لقانون العقوبات الجديد بموجب تعديل سنة 1992، بل إننا لا نجد أي تعريف أو أي مؤشر يهتدى به لتحديد مفهوم الخصوصية حتى في عرض الأسباب الذي قدمته الحكومة أو في الأعمال التحضيرية المتمثلة في تدخلات النواب عند مناقشتهم والتصويت على مشروعي القانونين المذكورين أعلاه.[4]

والملاحظ أيضا أن الحق في الحياة الخاصة غير منصوص عليه في الدستور الفرنسي الحالي الصادر عام 1958، وبقي حقا ذا قيمة تشريعية فقط إلى أن أصدر المجلس الدستوري الفرنسي قرارا رقم 352-94 في 1995/01/18 ذكر فيه المجلس وبصفة صريحة الحق في الحياة الخاصة في مقتضيات قراره، عندما اعتبر أن الوقاية من المساس بالنظام العام خصوصا انتهاك أمن الأشخاص والأموال والبحث عن مرتكبي الجرائم هي ضرورة من أجل المحافظة على المبادئ والحقوق ذات القيمة الدستورية، ويتعين على المشرع أن يضمن التوفيق بين الأهداف ذات القيمة الدستورية وممارسة الحريات العامة المضمونة دستوريا، والتي توجد من بينها الحريات الفردية وحرية التنقل، ذلك أن عدم الإعتراف بالحق في الحياة الخاصة يمكن أن يلحق مساسا بالحرية الفردية[5]، ومن هنا انتهى الحق في الحياة الخاصة إلى الحصول على

---

[1] Loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain

[2] المادة 1/368 تجرم فعل التقاط وتسجيل الأحاديث الخاصة.

المادة 2/368 تجرم فعل التقاط الصور الخاصة.

المادة 369 تجرم فعل الاحتفاظ أو إفشاء أو استعمال التسجيلات والمستندات بأي وسيلة كانت.

المادة 370 تجرم فعل نشر المونتاج دون موافقة المجني عليه.

ويعاقب الفاعل لأي من هذه الأفعال بالحبس من شهرين إلى 06 أشهر وبالغرامة أو بإحدى هاتين العقوبتين.

[3] LOI no 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes.

[4] محمد أبو العلا عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد الصادر في 1992/07/22، دار النهضة العربية، القاهرة 2004 ص1 وما بعدها.

[5] نويري عبد العزيز، مرجع سابق، ص117.

عتراف به كقيمة دستورية من طرف القضاء الدستوري،* وحصل على الإعتراف به كقيمة دستورية من طرف القضاء الدستوري.

وبالرغم من اعتراف القضاء الدستوري بالحق في الحياة الخاصة كقيمة دستورية ينبغي على المشرع الدستوري أن يضمن التوفيق بينها وبين ممارسة الحريات العامة، إلا أنه لم يحدد مضمون هذا الحق وما المقصود به.

الفرع الثالث: موقف المشرع الجزائري من الحق في الخصوصية:

يعتبر المشرع الجزائري واحدا من بين التشريعات التي توجهت نحو الإعتراف بالحق في الخصوصية بمفهومه الشامل واعتباره حقا مستقلا شأنه في ذلك شأن المشرع الفرنسي، حينما اقتدى به في وضع حماية نوعية مباشرة لحرمة الحياة الخاصة، وهذا خلافا لبعض القوانين المقارنة التي تشير إلى الحق في الحياة الخاصة بطريقة غير مباشرة من خلال حماية سرية المراسلات والاتصالات وحرمة المسكن وغيرها من الحقوق الشخصية الأخرى، ففي نصوص هذه القوانين تجد الحياة الخاصة الحماية عندما يقع انتهاك على تلك الحقوق الشخصية الأخرى.

وقد اخذ المشرع الجزائري بتصور المشرع الفرنسي الذي يرى أن الحماية المباشرة للحق في الحياة الخاصة تعد مكملة للحماية غير المباشرة والموجودة قبلها في نصوص قانونية أخرى.[1]

ويعد الدستور في مقدمة النصوص القانونية التي اعترفت بالحق في الحياة الخاصة في التشريع الجزائري، أين عنى المشرع الدستوري من خلالها بضرورة احترام الحياة الخاصة للأفراد، وإن كان أول دستور جزائري سنة 1963[2] لم يتضمن نصا صريحا حول الحياة الخاصة، إلا أنه نص في المادة 11 منه على أن الجزائر تمنح موافقتها للإعلان العالمي لحقوق الإنسان، وهذا الاخير الذي تنص المادة 12 منه على عدم جواز تعرض أي أحد لتدخل تعسفي في حياته الخاصة، ثم جاء بعد ذلك دستور 1976[3] بنص المادة 1/49 أين استعمل المشرع مصطلح الحياة الخاصة صراحة حينما نصت هذه المادة على "أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة ولا شرفه والقانون يصونها"، وهو نفس النص الذي أورده المشرع في دستور 1989[4] في المادة 37 مع إدخال بعض التعديلات على الصياغة، والتي تنص على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه يحميها القانون"، بالإضافة إلى نص المادة 60 من نفس الدستور التي نصت على أنه: "يمارس كل مواطن جميع حرياته في إطار احترام الحقوق المعترف بها للغير في الدستور ولاسيما احترام الحق في الشرف وستر الحياة الخاصة..."

* ولقد توالت قرارات المجلس الدستوري الفرنسي التي أقر فيها بالحق في الحياة الخاصة صراحة وأوجب ضرورة حمايته، ومن ذلك القرار الصادر في 1997/04/22 الذي أكد من خلاله أن احترام الحياة الخاصة يعد أحد العناصر التي تقوم عليها الحرية الشخصية. وأن الإنكار الخطير للحق في احترام الحياة الخاصة بالنسبة للمواطنين أو الأجانب يمثل اعتداء على حريتهم الشخصية، بالإضافة إلى القرار الصادر في 1999/07/23 الذي أكد فيه على الحماية القانونية للحياة الخاصة واعتبار هذا الحق ذو قيمة دستورية.

[1] نويري عبد العزيز، مرجع سابق، ص49.

[2] دستور 63 الجريدة الرسمية رقم 64 الصادر بتاريخ 1963/09/10.

[3] دستور 76 الصادر بموجب الأمر 97/76 مؤرخ في 1979/11/22، الجريدة الرسمية عدد94، ص1307.

[4] دستور 89 المنشور بموجب المرسوم الرئاسي رقم 18/89 المؤرخ في 1989/02/28، الجريدة الرسمية العدد 09، ص234.

وفي دستور 1996[1] اهتم المشرع الدستوري أيضا بالحق في الحياة الخاصة، حيث أورد نصين الأول من خلال المادة 39 الواردة تحت عنوان الحقوق والحريات، والتي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه يحميها القانون"، والنص الثاني يتمثل في المادة 63 الواردة تحت عنوان الواجبات والتي تنص على أنه "يمارس كل واحد جميع حرياته في إطار احترام الحقوق المعترف بها للغير، لاسيما احترام الحق في الشرف وسر الحياة الخاصة..."

ثم جاء التعديل الدستوري المؤرخ في 06 مارس 2016[2] الذي اعترف من خلاله المشرع الجزائري ولأول مرة في المادة 46 منه بالخصوصية المعلوماتية، أين نص صراحة على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أما بالنسبة للتشريع العادي فإن أول نص قانوني ورد فيه مصطلح الحياة الخاصة هو المرسوم رقم 131/88 المؤرخ في 1988/07/04 الذي ينظم العلاقة بين الإدارة والمواطن، حيث نصت المادة 11 من هذا المرسوم على أنه "لا يجوز للإدارة المسيرة أن تنشر أو تسلم أية وثيقة أو أي خبر (معلومة) مهما يكن سندها في ذلك، إذا كانت الوثيقة والخبر يتصلان بحياة الفرد الخاصة أو يرتبطان بوضعيته الشخصية بصرف النظر عن أحكام المادة 10 من هذا القانون، ما لم يرخص بذلك التنظيم المعمول به أو تكون ثمة موافقة من المعني.

كما أورد المشرع الجزائري نصا قانونيا آخر تضمن عبارة الحياة الخاصة في القانون رقم 19/04 المؤرخ في 2004/12/25 المتعلق بتنصيب العمال ومراقبة التشغيل، أين نصت المادة 27 منه على أنه "يعرض إفشاء المعلومات الشخصية التي تمس الحياة الخاصة لطالب التشغيل مرتكبه لغرامة من 50.000.00 دج إلى 100.000.00 دج.

وكذلك القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أين نصت الفقرة السابعة من المادة 04 منه على ضرورة أن تكون الترتيبات التقنية الموضوعة موجهة فقط وحصريا لتجميع وتسجيل المعطيات ذات الصلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها وعدم المساس بالحياة الخاصة للغير.

والقانون رقم 01/06 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته نص كذلك في المادة 15 الواردة في باب التدابير الوقائية من الفساد على ضرورة تمكين وسائل الإعلام والجمهور من الحصول على المعلومات المتعلقة بالفساد مع مراعاة حرمة الحياة الخاصة.

ثم توالت النصوص القانونية بعد ذلك والتي تؤكد على بداية اهتمام المشرع الجزائري بنوع حديث لمفهوم الخصوصية ويتعلق الأمر بمسألة الخصوصية المعلوماتية، التي تنبثق في دلالتها على حماية المعطيات الشخصية، حيث جاء القانون 03/15 المؤرخ في 2015/02/01 المتعلق بعصرنة العدالة لينص في المادة

[1] دستور 96/ الصادر في الجريدة الرسمية رقم 76 المؤرخة في 8 ديسمبر 1996.

[2] تعديل بموجب القانون رقم 16-01 المؤرخ في 06 مارس 2016، الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016.

05 منه على وجوب أن تتواجد على التراب الوطني كل المعطيات والمعلومات ذات الطابع الشخصي التي تم جمعها من طرف مؤدي خدمات التصديق الالكتروني.

وكذلك القانون 03/16 المؤرخ في 2016/06/19 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص*.

لكن النص القانوني ذي الأهمية البالغة الذي وفر من خلاله المشرع الجزائري حماية جزائية فعلية ونوعية للقيمة المسماة الحق في الحياة الخاصة، هو القانون 23/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون العقوبات، والذي نصت فيه المادة 303 مكرر أنه "يعاقب بالحبس من شهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 100.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت".

ورغم هذه النصوص القانونية المتعددة التي صاغها المشرع بخصوص الحياة الخاصة، إلا أنه لم يضع تعريفا لهذا الحق في أي منها، ويبدو أن هذا السكوت مرده الطبيعة المعقدة لهذا المصطلح، فلا يمكن حصر هذه القيمة في تعريف واحد يغطي كل جوانبها، وذلك بسبب تعدد وتنوع الأشكال التي تغطيها هذه العبارة، فضلا على أن مفهوم الحياة الخاصة هو مفهوم نسبي، ومن ثمة فهو يختلف باختلاف الأخلاق وتطورها فما كان يعتبر خارج الحياة الخاصة في زمن ما، لم يعد اليوم كذلك ودخل في حيز الخصوصية، كما أن مسائل كانت من دقائق الحياة الخاصة أصبحت اليوم مسائل عادية، وعليه يكون من الصعب وضع تعريف واحد للحق في الخصوصية يصلح تطبيقه على الكافة وعلى مر الأزمنة.[1]

الفرع الرابع: موقف الإعلانات العالمية من الحق في الخصوصية:

ليس من شك أن تطور الحياة والتقدم التكنولوجي كان من نتائجهما أن حق الإنسان في حياته الخاصة بات مهددا، لذلك فلم يكن هذا الحق محلا لاهتمام القوانين الوطنية فحسب، بل امتد إلى اهتمام المنظمات الدولية والإقليمية الخاصة بحماية حقوق الإنسان، فالجهد الدولي لحماية الحياة الخاصة يتصل بالجهد الدولي لحماية حقوق الإنسان عموما،فالقانون الدولي لحقوق الإنسان يوفر الإ طار العالمي الذي يجب أن يقيم على ضوئه أي تدخل في حقوق الخصوصية الفردية[2]، فمجمل المواثيق الدولية المتعلقة بحقوق الإنسان تعبر عن التزام الدول باحترامها لخصوصية الأفراد، بل وقد ارتقت بعض أحكام هذه المواثيق والاتفاقيات وأصبحت قواعد عرفية مما يعني التزام الدول بها حتى ولو كانت غير موقعة عليها.

* تنص في المادة الثالثة من هذا القانون على أنه يتعين أثناء مختلف مراحل أخذ العينات البيولوجية واستعمال البصمة الوراثية احترام كرامة الأشخاص وحرمة حياتهم الخاصة وحماية معطياتهم الشخصية. وفقا لأحكام هذا القانون والتشريع الساري المفعول.

[1] أنظر في هذا المعنى نويري عبد العزيز، مرجع سابق، ص63.

[2] تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان المقدم لمجلس حقوق الإنسان الدورة السابعة والعشرون بتاريخ 2014/06/30 رقم A/HRC/27/37 بعنوان الحق في الخصوصية في العصر الرقمي Le droit à la vie privée à l'ère du numérique اطلع عليه يوم 2018/06/02 https://undocs.org/pdf?symbol=ar/A/67/53/Add.1

ولقد تعددت المواثيق والاتفاقيات والمؤتمرات الدولية التي أقرت وأكدت حق الإنسان في الخصوصية، ونعرض فيما يلي أهمها:

أولا: موقف الاتفـــاقيات الـــدولية من الحق في الخصوصية:

1)**الاتفاقيات الدولية ذات الطابع العـــالمي:** لقد كان الإعلان العالمي لحقوق الإنسان الذي أقرته الأمم المتحدة* بمثابة أول بيان دولي أساسي يؤكد احترامه لحقوق الإنسان ومن ضمنها الحق في الحياة الخاصة،[1] فقد نصت المادة 12 من هذا الإعلان على أنه لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمس شرفه وسمعته، ولكل شخص الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات.

ومن ثم فإنه يبدو واضحا أن هذا الإعلان قد تضمن مجموعة من المبادئ التي تنادي باحترام حقوق الإنسان بصفة عامة وحق الإنسان في احترام خصوصيته بصفة خاصة، وهو على هذا النحو يضفي الحماية اللازمة على الحق في الخصوصية الذي يعتبر ميزة لبني البشر من أي تدخل سافر وغير مشروع[2]، وقد كان لهذا الإعلان أثر عظيم في لفت أنظار دول العالم وشعوبه إلى ضرورة احترام حقوق الإنسان وحرياته الأساسية ومنها حقه في الخصوصية.[3]

كما أصدرت الجمعية العامة للأمم المتحدة الاتفاقية الدولية للحقوق المدنية والسياسية أو ما يسمى أيضا بالعهد الدولي للحقوق المدنية والسياسية في 1966/12/16 بالقرار رقم 2200،[4] أين تم التأكيد في هذا العهد على مجموعة من المبادئ المتعلقة بحقوق الإنسان بما فيها الحق في الخصوصية، مما يبرز الأهمية الدولية لهذا الحق.

ويعد العهد الدولي الخاص بالحقوق المدنية والسياسية تقنينا دوليا، وتطبيقا فعليا لهذا النوع من الحقوق، وذلك من خلال فرض التزامات قانونية محددة على الدول بضرورة احترام الحقوق الموجودة فيها، وهذا بخلاف الإعلان العالمي الذي يقتصر على فرض التزامات أدبية باحترام ما تناوله من قواعد

* صدر الإعلان العالمي لحقوق الإنسان بقرار الجمعية العامة للأمم المتحدة رقم 2017 المؤرخ في 1948/12/10 والذي تضمن 30 مادة تعبر في مجملها عن مجموعة من المبادئ العالمية الدولية التي تنادي باحترام حقوق الإنسان الأساسية.

[1] علي أحمد عبد الزعبي، مرجع سابق، ص38.

[2] آدم عبد البديع حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2011، ص104.

[3] طارق صديق رشيد كه ردي، حماية الحرية الشخصية في القانون الجنائي، دراسة تحليلية مقارنة، منشورات الحلبي، الطبعة الأولى، لبنان 2011 ص209.

[4] العهد الدولي الخاص بالحقوق المدنية والسياسية اعتمد وعرض للتوقيع والتصديق والانضمام بقرار الجمعية العامة 2200 (د-21) المؤرخ في كانون الأول / ديسمبر1966 وبدأ نفاذه في: 23 آذار/مارس 1976، طبقا للمادة49.

تتعلق بحقوق الإنسان[1]، وتنص هذه الاتفاقية صراحة على حق الإنسان في خصوصيته من خلال نص المادة 17 منها، والتي تنص على أنه: "لا يجوز التدخل بشكل غير قانوني أو تعسفي في خصوصيات أحد..."*

بالإضافة إلى الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية، أصدرت الجمعية العامة للأمم المتحدة في 1975/11/10 بموجب قرارها رقم 3304 (د.30) الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لمصلحة السلم وخير البشرية، فقد أوضح هذا الإعلان ضرورة التزام جميع الدول باتخاذ تدابير فعالة بما فيها التدابير التشريعية لكفالة جعل المنجزات العلمية والتكنولوجية قادرة على تأمين الاستخدام الأكمل لحقوق الإنسان لاسيما حقه في الخصوصية[2]، وكذا منع استخدام التطورات العلمية والتكنولوجية من جانب الهيئات التابعة للدول بصورة تتنافى مع ما أكده الإعلان العالمي لحقوق الإنسان والعهود الدولية الخاصة بحقوق الإنسان ذات الصلة بحماية الحق في الخصوصية.

وقد اعترف هذا الإعلان صراحة أن الحق في الخصوصية يعد أحد الحقوق الأساسية التي يكفل حمايتها في مواجهة التقدم العلمي والتكنولوجي من خلال الفقرة السادسة منه، والتي تضمنت أنه على الدول أن تتخذ تدابير تهدف إلى تمكين جميع الأفراد من الاستفادة من حسنات العلم والتكنولوجيا في مقابل حمايتهم من الآثار الضارة التي يمكن أن تترتب على سوء استخدام التطورات العلمية والتكنولوجية بما في ذلك إساءة استعمالها على نحو يمس بحقوق الفرد والجماعة، لاسيما ما يتعلق باحترام حق الخصوصية..."[3].

2) موقف الاتفاقيات الدولية ذات الطابع الإقـليمي: تعد الاتفاقيات الإقليمية قيمة كبرى في ترسيخ حقوق الإنسان عموما وحق الخصوصية بصفة خاصة ودعمه على المستوى الإقليمي في ظل النظام القانوني الدولي، إذ عنيت بإبراز حق الإنسان في حياته الخاصة واعتبرته أمرا على درجة من الأهمية.

ومن أهم الاتفاقيات الدولية الإقليمية التي تعتبر أكثر الخطوات الإيجابية في إقرار حق الخصوصية، الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية*، وكذا الاتفاقية الأمريكية لحقوق الإنسان.

2-1) موقف الاتفاقية الأوروبية لحماية حقوق الإنسان وحرياته الأساسية

لقد أقرت هذه الاتفاقية الحق في الخصوصية لجميع الأشخاص دون تفرقة سواء الموجودين على إقليم أي من الدول الأطراف أم غير الأطراف فيها، ومن ضمنهم عديموا الجنسية الذين يوجدون على إقليم

[1] ممدوح خليل بحر، مرجع سابق ص83

* تعني عبارة بشكل غير قانوني أنه لا يصح وقوع أي تدخل إلا في الحالات التي ينص عليها قانونا، وتعني عبارة "بشكل تعسفي" حماية الحق المنصوص عليه في هذه المادة لتشمل التدخل المعقول في ظل الظروف المعينة التي يحدث فيها. أنظر في هذا المعنى: أسامة مصطفى ابراهيم الخضر، العهد الدولي للحقوق المدنية والسياسية، دراسة مقارنة رسالة ماجيستير مقدمة إلى كلية الدراسات الفقهية والقانونية في جامعة آل البيت الأردن 1997 ص85.

[2] محمود إبراهيم غازي، مرجع سابق، ص192.

[3] محمود إبراهيم غازي، مرجع سابق، ص193.

* أبرمت هذه الاتفاقية في نوفمبر 1950 بمدينة روما الإيطالية تحت مظلة مجلس أوروبا، وكان عدد الدول المنظمة إلى هذا المجلس حينها 21 دولة، ودخلت حيز التنفيذ في 1953/09/03، وقد تم تعديلها بموجب البروتوكول رقم 11 من مجموعة المعاهدات الأوروبية.

الدول الأطراف في الاتفاقية[1]، وقد أكدت هذه الاتفاقية على عزم الدول الأوروبية ذات التراث المشترك من الحرية والتقاليد السياسية باتخاذ الخطوات اللازمة نحو التنفيذ الجماعي لبعض الحقوق الواردة في الإعلان العالمي لحقوق الإنسان[2]، كما أكدت على تحريم المساس بالحياة الخاصة وتقرير حق الأفراد في الخصوصية،[3]فقد نصت المادة 08 على أنه: "لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته..."، ومن ثم فإن هذا النص يعترف صراحة بأن لكل شخص الحق في احترام حقه في الخصوصية.[4]

ونظرا لكون مسألة الحق في الخصوصية باتت على جانب كبير من الأهمية وأصبحت تشغل بال المشرعين في شتى دول العالم، تم عقد مؤتمر تحت رعاية المجلس الأوروبي في 1970/09/30 بمدينة بروكسل أين تم دراسة تأثير الاتفاقية الأوروبية لحقوق الإنسان في مجال الحق في الخصوصية، وقد قدم المؤتمرون حينها العديد من البحوث بشأن حماية الحق في الخصوصية.

2-2) **موقف الاتفاقية الأمريكية لحقوق الإنسان:** ورد الحديث عن الحق في الخصوصية بنص المادة 11 من هذه الاتفاقية[5] وذلك كما يلي: "

-لكل إنسان الحق في أن يحترم شرفه وتصان كرامته.

-لا يجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو شؤون أسرته أو منزله أو مراسلاته ولا أن يتعرض لاعتداءات غير مشروعة على شرفه أو سمعته.

-لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات".

ويستفاد من النص السابق أن هذه الاتفاقية قررت حق الفرد في حماية حقه في الخصوصية استنادا على كونه إنسانا، وليس إلى كونه مواطنا في الدولة، بمعنى أن هذا الحق معترف به للمواطن والأجنبي دون تمييز بينهما[6]، كما يلاحظ أيضا أن هذه الاتفاقية شأنها شأن الاتفاقية الأوروبية لحقوق الإنسان ميزت بين حق الخصوصية والحق في الشرف والاعتبار.*

---

[1] محمود إبراهيم غازي، نفس المرجع، ص196.

[2] عبد العزيز محمد سرحان، الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، دار النهضة العربية، القاهرة، 1966، ص324 وما بعدها.

[3] عبد العظيم الجنزوري، الحماية الدولية لحقوق الإنسان وتطوير القانون الدولي، مقال منشور في مجلة مصر المعاصرة عدد 377 جويلية 1977، ص218.

[4] ممدوح خليل بحر، مرجع سابق، ص86.

[5] تم التوقيع على الاتفاقية الأمريكية لحقوق الإنسان في 1969/11/02 في مدينة سان خوزي san-jose بكوستاريكا costarica أثناء انعقاد مؤتمر حقوق الإنسان، ودخلت حيز التنفيذ بتاريخ 1978/07/18.

[6] محمود إبراهيم غازي، مرجع سابق، ص201.

* من الملاحظ أن هذه الاتفاقية قد صيغت على نمط الاتفاقية الأوروبية لحماية حقوق الإنسان فيما يتعلق بالأجهزة التي أنشأتها لضمان تطبيق نصوصها، وهما اللجنة الأمريكية لحقوق الإنسان والمحكمة الأمريكية لحقوق الإنسان، وعلى خلاف الاتفاقية الأوروبية أقرت الاتفاقية الأمريكية لحقوق الإنسان حق الأفراد في تقديم شكاوى إلى اللجنة الأمريكية لحقوق الإنسان ضد أي دولة عضو في منظمة الدول الأمريكية بغض النظر عن تصديقها على هذه الاتفاقية، أنظر المادتين 45-44 من الاتفاقية.

وما يجدر بنا الإشارة إليه في هذا المقام أنه وإن كانت المواثيق الدولية سواء ذات الطابع العالمي كالإعلان العالمي لحقوق الإنسان أو العهد الدولي للحقوق المدنية والسياسية، أو ذات الطابع الإقليمي كالاتفاقيتين الأوروبية والأمريكية لحقوق الإنسان، تقر وتعترف جميعها للإنسان بالحق في الخصوصية إلا أنه لا يوجد في أي منها تعريف لهذا الحق، فلم تتصد هذه المواثيق الدولية لتبيان المقصود بالحق في الخصوصية، وقد أفصح عن هذه المسألة صراحة التقرير المقدم من طرف لجنة الخبراء الخاصة بحقوق الإنسان للمجلس الأوروبي عند إعداد الاتفاقية الأوروبية، حيث ورد فيه أن قرارات اللجنة الأوروبية لحقوق الإنسان لا تحتوي في طياتها على البيانات الكافية التي من شأنها أن تفصح بوضوح لا لبس فيه عن مضمون فكرة الحياة الخاصة، بل إن الأعمال التحضيرية لهذه المواثيق لا تسمح بدورها على استخلاص العناصر التي يمكن بمقتضاها تعريف هذه المسألة.[1]

ويبدو من صياغة النصوص القانونية التي جاءت بها هذه المواثيق الدولية والتي تعترف من خلالها بالحق في الخصوصية أن عدم الدخول في التفاصيل بشأن تحديد مضمون هذا الحق أمر مقصود، وذلك بسبب أن المسألة تعد من المسائل التي يختلف في مضمونها من دولة إلى أخرى، وقد يترك الأمر للفقه وللقضاء في كل دولة من الدول أن يستقلا بتحديد مضمون الحق في الخصوصية على ضوء الأفكار والعادات والتقاليد ودرجة الحرية السائدة في كل دولة من الدول الأطراف في الاتفاقية.

ثانيا: دور المؤتمرات الدولية في تعريف الحق في الخصوصية:

لقد تعاظمت مكانة الحق في الخصوصية وتزايد الاهتمام به إلى درجة الارتقاء به إلى المصاف الدولي، ويرجع ذلك إلى تطور حقوق الإنسان بصفة عامة إضافة إلى الدور الذي لعبه التقدم العلمي والتطور التكنولوجي في إثارة موضوع الحق في الخصوصية والمناداة بضرورة حمايته من الانعكاسات الخطيرة التي قد تتهدده.

لذلك فإلى جانب الاتفاقيات الدولية التي اهتمت بالحق في الخصوصية، فثمة مجموعة من المؤتمرات الدولية التي عقدت أغلبها تحت مظلة الأمم المتحدة، اهتمت هي أيضا بالتصدي لهذا الحق وإقراره والحفاظ عليه في ظل التطور العلمي، وما يمكن أن يسببه من انتهاكات جسيمة على حق الإنسان في خصوصيته.

فقد انعقدت عدة مؤتمرات دولية ناقشت الحق في الخصوصية وبحثت سبل إقراره، وما يمكن أن يتعرض له هذا الحق من أخطار بسبب التطورات العلمية والتكنولوجية الحديثة والحفاظ عليه من الانتهاكات الهائلة.

ويمكن أن نجد في هذا الشأن أمثلة عن هذه المؤتمرات سواء الدولية أو الإقليمية، ونتناول أهمها كما يلي:*

[1] ممدوح خليل بحر، مرجع سابق، ص86.

* ومن المؤتمرات ذات الطابع الدولي نذكر أيضا:

1) المؤتمرات الدولية العالمية التي اهتمت بالحق في الخصوصية

ونذكر من بين أهم هذه المؤتمرات ما يايلي:

1-1) المؤتمر الدولي لحقوق الإنسان المنعقد في طهران سنة 1968:*

لقد اعتبر هذا المؤتمر أول مؤتمر دولي يجري تنظيمه على نطاق عام، لبحث مسألة حقوق الإنسان من جميع نواحيها، حيث نظر في المشكلات المتصلة بأنشطة الأمم المتحدة الرامية إلى تعزيز احترام حقوق الإنسان والحريات الأساسية، مراعيا في الوقت نفسه الفرص الجديدة التي تولدت نتيجة التقدم العلمي والتكنولوجي السريع.[1] وقد اتخذ خلال هذا المؤتمر مجموعة من القرارات الرئيسية التي تناولت مختلف نواحي حقوق الإنسان، أهمها القرار رقم 11 والذي تبناه المؤتمرون بالإجماع، ويهدف إلى حماية الحياة الخاصة للأفراد في ضوء التقدم المستمر لأجهزة التنصت والتسجيل وحماية الحياة الشخصية الإنسانية و السلامة الجسمية والعقلية أمام التقدم الهائل في علم الأحياء والطب والكيمياء الحيوية.[2] وقد تحددت رؤية هذا القرار في:

-أن الإعلان العالمي لحقوق الإنسان قد نص على عدم جواز تعرض أحد للتدخل التعسفي في حياته الخاصة.

-أن الحق في سرية الحياة الخاصة يضمن حق الفرد في ألا تنشر معلومات تتعلق بحياته الخاصة أو بشخصيته لم يكن ليكشف عنها هو نفسه بشكل شعوري.

-أن التقدم التكنولوجي قد يجعل بالإمكان انتهاك حرمة الحياة الخاصة للأفراد أو المساس بكرامتهم وبحرمة شخصيتهم عن طريق وسائل التلصص على المخابرات الهاتفية وأدوات استراق السمع الالكترونية.

-أن خصوصيات حياة الأفراد تنشر أحيانا دون إذن منهم بواسطة وسائل الإعلام، مما يشكل مساسا بحق سرية الحياة الخاصة.*

-مؤتمر مونتريال لحقوق الإنسان ما بين 14 إلى 18 أكتوبر 1968 والذي تم فيه دراسة وبحث الآثار السلبية التي يعكسها التقدم التكنولوجي ووسائل التطفل الالكتروني على الحياة الخاصة للأفراد.

-مؤتمر بروكسل المنعقد من 30 سبتمبر إلى 03 أكتوبر 1970 والذي تناول الأبحاث حول الحق في الصورة والحق في الحياة الخاصة للأفراد وسرية المعلومات والتنصت على المحادثات الهاتفية.

-المؤتمر الدولي الثاني عشر الخاص بحماية حقوق الإنسان في الإجراءات الجنائية، الذي عقدته الجمعية الدولية لقانون العقوبات في هامبورغ بألمانيا الغربية في الفترة من 16 إلى 22 سبتمبر 1979.

-المؤتمر الدولي السابع للمركز الدولي للدراسات والبحوث الاجتماعية والجنائية المنعقد بمدريد في الفترة من 03 إلى 13 أكتوبر 1984 والذي شاركت فيه 38 دولة، بالإضافة إلى الأمم المتحدة ومنظمة الشرطة الجنائية الدولية والمجلس الأوروبي وبعض المنظمات الدولية المتخصصة.

* عقد هذا المؤتمر الدولي في الفترة ما بين 22 أفريل إلى 13 ماي 1968 بالعاصمة الإيرانية طهران، تحت رعاية المنظمة الدولية للأمم المتحدة، وذلك بموجب القرار رقم 2081 الصادر في 1965/12/20 للجمعية العامة للأمم المتحدة.

[1] ممدوح خليل بحر، مرجع سابق، ص96.

[2] أحمد عبد الزعبي، مرجع سابق، ص53.

* ينظر في هذا الشأن الوثيقة النهائية للمؤتمر الدولي لحقوق الإنسان المنعقد في طهران، منشورات إدارة الإعلام بالأمانة العامة للأمم المتحدة نيويورك، 1974، ص1 وما بعدها https://www.un.org/ar/sections/about-un/secretariat/ أطلع عليه يوم: 2018/06/02

وقد أصدرت الأمم المتحدة القرار رقم 2450 لسنة 1968 بعد مشاركتها في مؤتمر طهران، عبرت فيه عن قلقها من أن التقدم العلمي والتكنولوجي بالرغم مما يمنحه من آفاق واسعة أمام التقدم الاقتصادي والاجتماعي، فإنه مع ذلك يعرض حقوق الأفراد والجماعات للخطر، لذلك فإن هذا الأمر يتطلب اهتماما متواصلا ودراسات مستمرة لحماية حقوق الإنسان وحرياته الأساسية سيما الحق في الخصوصية.

2-1) مؤتمر خبراء اليونسكو المنعقد في باريس سنة 1970: من الأسباب التي دفعت بهيأة اليونسكو إلى الاهتمام بصفة خاصة بموضوع الحق في الخصوصية هو تعقد هذا الحق وتعدد المشكلات المتصلة به، بالإضافة إلى ظهور تنازع بين الحياة الخاصة من جانب والمصلحة العامة من جانب آخر، فكان من المحتم البحث عن إيجاد العلاج الملائم لهذه المسألة وإيجاد التوازن بين مصلحة الفرد في حماية خصوصياته وحق المجتمع تجاهه.[1]

وقد أبدى المؤتمرون بشأن الحق في الخصوصية عدة ملاحظات، لعل أهمها أنه من الصعوبة بما كان تعريف جوهر الخصوصية تعريفا عالميا نظرا لكون الخصوصية مسألة نسبية ومرتبطة بالثقافة والعادات والتقاليد والمحتوى الاجتماعي والاقتصادي لكل دولة، بالإضافة إلى ملاحظات أخرى نوجز منها:

-أن الحق في الخصوصية ليس حقا مطلقا، فقد تقتضي الضرورة التضحية بقدر منه تقديرا لاعتبارات المصلحة العامة ولى بالرعاية.

-ضرورة توفير ضمانات قوية لحماية هذا الحق خصوصا بعد اتساع نطاق تدخل الدولة والتطور العلمي والتكنولوجي، مع وجود ما يسمى بالتكنوقراط (طبقة الفنيين) والبيروقراط (طبقة الموظفين الإداريين الحكوميين) والذين كثيرا ما يمتد اعتداؤهم بصورة متزايدة على الحق في الخصوصية.

2) المؤتمرات الدولية الإقليمية التي اهتمت بالحق في الخصوصية: بالإضافة إلى المؤتمرات الدولية هناك مجموعة من المؤتمرات ذات الطابع الإقليمي التي اهتمت بمسألة الخصوصية ونذكر أهمها:

2-1) على المستوى الأوروبي: نجد من أهم المؤتمرات في هذا الإطار مؤتمر دول شمال أوروبا المنعقد بستوكهولم 1967*، حيث يعد هذا المؤتمر واحدا من أهم المؤتمرات الإقليمية التي اهتمت بالحق في الخصوصية بصفة مركزة، ويظهر ذلك من خلال العديد من التوصيات التي توصل إليها هذا المؤتمر، فقد وضع تعريفا للحق في الخصوصية[2] وحدد ضوابطه، وركز على عدم جواز انتهاكه إلا بمعرفة السلطات التي يحددها القانون، بالإضافة إلى حثه على ضرورة اتخاذ الوسائل المدنية والجنائية لحماية الإنسان من حالات التعدي على حقه في الخصوصية وتقويتها أو تعديلها على النحو الذي يضمن تحقيق حماية أكثر

[1] آدم عبد البديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، دار النهضة العربية للنشر والتوزيع القاهرة، 2000، ص114.

*عقد هذا المؤتمر في الفترة ما بين 22-23 مارس عام 1967 تحت رعاية اللجنة الدولية للقانونيين، وحضره مندوبون من السويد، الدانمارك، إيسلاندا، النرويج، بريطانيا، الهند، اليابان، الولايات المتحدة الامريكية.

[2] عرف مؤتمر دول الشمال (الدول الاسكندنافية) الحق في الخصوصية بأنه حق الشخص في أن يعيش حياته وحده حرا كما يرغب مع أدنى حد من التدخل من جانب الغير، وإن كان قد وجدت تعليقات للفقه على هذا التعريف، حيث تعتبره تعريفا موسعا من شأنه أن يحدث خلطا بين الحق في الخصوصية والحرية. أنظر في هذا الشأن خليل بحر، المرجع السابق، ص185.

فعالية للحق في الخصوصية، كما أوصى المؤتمر بضرورة تحرير الشخص من التطفل على وحدته وعزلته أو الافتئات على خصوصيته عن طريق استخدام وسائل المراقبة والترصد والتجسس.*

وقد بادرت اللجنة القانونية الأوروبية المنبثقة عن هذا المؤتمر بإصدار مجموعة من التوصيات في سبيل حماية الخصوصية، و من أهم هذه التوصيات:

-ضرورة النص صراحة على عدم مشروعية التسجيل خلسة أو تصوير الأشخاص بالصور الفوتوغرافية أو الأفلام في مجال حياتهم الخاصة، أو في مواقف محرجة وعلى الأخص بصورة سريعة وغير متوقعة.

-النص على اعتبار التنصت المتعمد على المحادثات الهاتفية بين أطراف الحديث بواسطة طرف ثالث دون موافقتهما أمرا مخالفا للقانون.[1]

2-2) على مستوى الدول العربية: اهتمت الدول العربية بموضوع حقوق الإنسان عامة والحق في الخصوصية بصفة خاصة، رغم أن تجسيد هذا الاهتمام اتسم بالتعقيد والبطء الشديدين، ومن أهم المؤتمرات التي عقدت في هذا الإطار مؤتمر الإسكندرية المنعقد في الفترة ما بين 04 و 06 جوان 1987، حيث كان من أهم التوصيات التي خرج بها هذا المؤتمر ذات الصلة بالحق في الخصوصية، هو تعريفه لهذا الحق بأنه "حق كل شخص في أن يعترف الغير بكل ما يعد من خصوصياته مادية كانت أم معنوية أم تعلقت بحرياته، على أن يتحدد ذلك بمعيار الشخص العادي وفقا للعادات والتقاليد والنظام القانوني القائم في المجتمع ومبادئ الشريعة الإسلامية".*

المطلب الثاني: الطبيعة القانونية للحق في الخصوصية

إن تحديد الطبيعة القانونية للحق في الخصوصية لا تقل أهمية عن مسألة تحديد مفهوم هذا الحق، لأجل ذلك فقد انشغل بال الفقه والقضاء منذ زمن بعيد بمسألة تحديد الطبيعة القانونية للحق في الخصوصية باعتبارها تؤثر تأثيرا مباشرا في تحديد الأشخاص الذين يتمتعون به، كما تساهم في معرفة النتائج التي تتولد عن هذا الحق، مثل بيان مدى خضوعه لقواعد التقادم ومدى إمكانية التصرف فيه.

ولقد اعتنق الفقه والقضاء اتجاهات متعددة في شأن التكييف القانوني للحق في الخصوصية، فالاتجاه الأول يذهب إلى اعتبار هذا الحق من قبيل حقوق الملكية والذي مقتضاه أن الشخص يعد مالكا لهذا الحق[2]، أما الاتجاه الثاني فيرى أن الحق في الخصوصية يعد من قبيل الحقوق الشخصية الملازمة لصفة الإنسان.

---

* ممدوح خليل بحر، مرجع سابق، ص104.

[1] آدم عبد البديع، مرجع سابق، ص117.

*نذكر كذلك من المؤتمرات في الإطار العربي مؤتمر حماية حقوق الإنسان في قوانين الإ جراءات الجنائية في العالم العربي المنعقد في القاهرة في الفترة من 16 -20 ديسمبر 1989. بالإضافة كذلك إلى الميثاق العربي لحقوق الإنسان المعتمد من طرف القمة العربية السادسة عشر بتاريخ 2004/05/23 بتونس، وقد نصت المادة 17 منه على أن للحياة الخاصة حرمتها والمساس بها جريمة، وتشمل هذه الحياة الخاصة خصوصية الأسرة وحرمة المسكن وسرية المراسلات وغيرها من وسائل الاتصالات الخاصة.

[2] علي أحمد عبد الزعبي، مرجع سابق، ص143.

الفرع الأول: الحق في الخصوصية من حقوق الملكية:

لما كانت القوانين وخاصة القانون الفرنسي، لم تفصح بداية الأمر عن تحديد طبيعة الحق في الخصوصية، فقد ذهب جانب من الفقه القانوني إلى التصريح بأن للإنسان على حياته الخاصة حق الملكية، وأن الإنسان يعد مالكا لحياته الخاصة ولا يجوز الاعتداء على خصوصياته بأي شكل، وأنه يستطيع التصرف في حياته الخاصة كيفما يشاء، وقد أسس هذا الاتجاه رأيه على أساس فكرة الحق في الصورة، ثم تعمقت الفكرة فشملت الحق في الحياة الخاصة[1]، فقد كانت الفكرة السائدة آنذاك أن الإنسان له حق ملكية على جسده، وأن شكله هو جزء من هذا الجسد، وأن الصورة ما هي إلا تجسيد لهذا الشكل[2]،ومن ثمة فللإنسان حق الملكية على صورته، ويتفرع عن ذلك أن المرء يملك أن يتصرف وأن يستعمل وأن يستغل، وهي المكنات الثلاث التي يخولها حق الملكية للإنسان على جسده وصورته، كأن يضعها في الإعلانات مقابل مبلغ مالي أو يبيع مذكراته التي تتناول أغلب أسرار حياته[3]، كما لا يجوز من جهة أخرى تصوير الشخص واستغلال صورته إلا برضاه[4]، حيث يستطرد أنصار هذا الاتجاه مقررين أنه كما يجوز للإنسان أن يتصرف في ملكه فإنه يجوز له التصرف في صورته متى كانت قابلة للتداول، أي أن الشخص يبيع جزءا من نفسه، وتعد عناصر الشخصية هنا في هذه الحالة بمثابة شرائح في حق الملكية الذي هو مقرر لكل إنسان على جسمه، أي بمعنى آخر أن صاحب الحق يملك نفسه، ومن يصوره خلسة فقد سرق شكله[5]، وهذا ينصرف باعتقادهم إلى الحق في الخصوصية، فوفقا لهذا الاتجاه أنه لما كانت حياة الإنسان الخاصة ملكا له فإن ذلك يستتبع بالضرورة النظر إلى الجوانب المختلفة للشخصية بوصفها من الأمور المتفرعة عن حق الملكية.

وتأييدا لذلك فالقانون الإنجليزي يلجأ إلى الاعتداء على حق الملكية لتبرير حماية الخصوصية، حيث اعتبر الأستاذ "ديرك هيمي" المحامي العام بلندن أن الحق في الخصوصية هو بمثابة الملكية الخاصة لكل فرد وأنها ملكية جوهرية كمنزل الإنسان وملابسه[6].

ولقد كانت المحاكم الفرنسية تعترف بالحق في طلب التعويض عن أفعال الاعتداء على حرمة الحياة الخاصة استنادا إلى القواعد الخاصة بقانون الملكية، ففي هذا الصدد نجد أن محكمة السين التجارية ذهبت في حكم لها في 1963/02/26 إلى أنه "لما كان لكل شخص أن يتمتع وأن يستعمل صورته بمقتضى ماله عليها من حق ملكية مطلق، فإن أحدا غيره لا يملك مكنة التصر ف فيه دون موافقته.[7]

[1] ممدوح خليل بحر، مرجع سابق، ص311.

[2] حسام الدين الأهواني، مرجع سابق، ص141.

[3] حسام الدين الأهواني، نفس المرجع، ص142.

[4] أسامة عبد الله قايد، مرجع سابق، ص29.

[5] علي أحمد الزعبي، مرجع نفسه، ص144.

[6] محمد خليل بحر، نفس المرجع، ص314.

[7] Pascal Gourdon, L'EXCLUSIVISME AMBIVALENT DU DROIT A L'IMAGE, p 541, disponible sur le site :
https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/nzacl-yearbooks/yearbook-5,-1999/Gourden.pdf

ويبدو أن لجوء أصحاب هذا الاتجاه إلى اعتبار أن حق الخصوصية من قبيل حق الملكية مبرر عندهم على أساس أن حق الملكية هو النموذج الأمثل الذي يخول لصاحبه سلطات مطلقة من استعمال واستغلال وتصرف، ومن ثم فإن انسحاب هذه الأوصاف إلى الحق في الخصوصية سوف يعطي سلطات كبيرة لصاحب هذا الحق، علاوة على أن هذا التصور من شأنه أن يوفر حماية واسعة للحق في الخصوصية، فطالما أن الأمر يتعلق بحق ملكيته، فإن من يقع الاعتداء على حياته الخاصة يكون في مقدوره أن يطرق باب القضاء دون حاجة لإثبات الضرر استنادا إلى حق المالك على ملكه[1]، لكن مبررات أصحاب هذا الاتجاه لم تلق قبولا واستحسانا من طرف جانب آخر من الفقه، حيث كانت محلا للنقد من عدة وجوه، فإذا كان صحيحا أن كلا الحقين أي الحق في الملكية والحق في الخصوصية يحتج بهما في مواجهة الآخرين، فإن أوجه الاختلاف بينهما متعددة، فطبيعة حق الملكية هي أنه حق عيني، وأن كل حق عيني يفترض وجود صاحب الحق ومحل لكي يمارس هذا الأخير سلطاته عليه، فإذا اتحد صاحب الحق وموضوعه فإنه يستحيل حدوث ممارسة هذه السلطات، وهوما ينطبق على حق الخصوصية، ومن هنا فلا يمكن أن تكون الصورة مثلا محل ملكية طالما أنها ليست شيئا منفصلا عن صاحبها.[2]

الفرع الثاني: الحق في الخصوصية من حقوق الشخصية

تعرف الحقوق اللصيقة بالشخصية بأنها الحقوق التي تنصب على مقومات وعناصر الشخصية في مختلف مظاهرها الطبيعية والمعنوية، أين تعبر عما للشخص من سلطات مختلفة ترد على تلك العناصر والمقومات، وقد وجدت نظرية الحقوق الشخصية مكانها في الفقه عند مطلع القرن الماضي، أين ظهرت في بادئ الأمر عند الفقهاء الألمان وهم بصدد التعليق على المادة 823 من القانون المدني الألماني، والتي تنص على "أن من يعتدي عمدا أو عن طريق الإهمال على حياة شخص أو على جسده أو على صحته أو على حريته أو على ملكيته أو على أي حق آخر للشخص، يكون ملزما في مواجهته بإصلاح الضرر الذي سببه له"، أين راح الفقهاء الألمان يبحثون عن تحديد المقصود "بالحقوق الأخرى" والتي يستوجب الاعتداء عليها أو الإضرار بها، التزام المعتدي بالتعويض، وهنا ظهرت إلى جانب الحقوق الواردة في نص هذه المادة حقوق أخرى متعلقة بالشخص مثل الحق في الشرف والسمعة والحق في الاسم والصورة[3].

وتنقسم الحقوق الشخصية إلى قسمين:

الأول: وهي الحقوق الواردة على المقومات المادية للشخصية، أي تلك الحقوق التي تستهدف حماية الكيان المادي للإنسان، كالحق في سلامة الجسم، والحق في الحياة.

[1] حسام الدين الأهواني، مرجع سابق، ص143.

[2] بشاتن صفية الحماية الجزائية للحياة الخاصة، دراسة مقارنة، رسالة لنيل شهادة دكتوراه علوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2012، ص147.

[3] خليل بحر، مرجع سابق. ص316

والثاني: يشمل الحقوق التي ترمي إلى حماية المقومات والعناصر المعنوية للإنسان، مثل حق الإنسان في سمعته وشرفه واعتباره ومعتقداته وكذا مشاعره ورغباته.[1]

وبذلك يتضح أن حقوق الشخصية هي تلك الحقوق التي تكون مستوحاة من مظاهر مادية ومعنوية فردية أو اجتماعية، أي تلك الحقوق التي ترتبط بالمظهر المادي وبالجانب المعنوي للشخص.

لذلك يرى هذا الاتجاه أن الحق في الخصوصية يعتبر من الحقوق الملازمة للشخصية، ذلك أن هذه الأخيرة إنما تقررت للمحافظة على الكيان المادي والمعنوي للإنسان وتنصب على مقومات وعناصر شخصية[2]، ويؤكد فقهاء هذا الاتجاه أن الحق في الخصوصية يقع في دائرة الحقوق الشخصية وإن كان لا يشملها كلها، فكلاهما يتضمنان حق الفرد في احترام أو حماية اسمه وشرفه واعتباره ومراسلاته واتصالاته وحياته المهنية والعائلية وكل ما له تأثير على حياته الشخصية.

ويجمع الفقه الفرنسي حديثا أن الحق في الخصوصية يعد من قبيل الحقوق الشخصية، وأن أساس الحماية القانونية لهذا الحق هو ما للمرء من حق شخصي في حرمة حياته الخاصة، واعتبار الحق في الخصوصية من حقوق الشخصية يمنحه حماية وقائية من أي خطر، إذ يستطيع صاحب الحق المعتدى عليه أن يلجأ إلى القضاء بمجرد وقوع الاعتداء على حقه للمطالبة بمنع الاعتداء عليه أو بوقفه، ولا يلزمه في ذلك إثبات عنصري الخطأ و الضرر، ومن ثمة تكون الحماية القانونية أكثر فعالية مما لو ترك الأمر للقواعد العامة في المسؤولية المدنية التي لا توفر إلا الحماية اللاحقة للحق، أي لا بعد الإعتداء عليه وتولد الضرر، لذلك ففكرة حقوق الشخصية تكفل الحماية القانونية للحق في الخصوصية دون التقيد بأحكام المسؤولية المدنية،* علاوة على أنها توفر الحماية القانونية للشخص في مواجهة الكافة، إذ يستطيع الشخص أن يلزم الجميع على احترام حقه في الحياة الخاصة بعدم التحري عنها أو التجسس عليها وعدم نشر كل ما يتعلق بها ولا يحق لأحد مهما كان أن يطلع عليها إلا برضائه سلفا.[3]

والمشرع الفرنسي يكون من خلال المادة 09 من القانون المدني قد فصل في مسألة تحديد الطبيعة القانونية للحق في الخصوصية عندما قرر من خلالها أنه يعتبر حقا شخصيا، حيث نصت هذه المادة أن لكل فرد الحق في احترام حياته الخاصة، واعتبر أن أساس الحماية لهذا الحق ليس أحكام المسؤولية المدنية وإنما وجود حق شخصي يتمثل في حرمة الحياة الخاصة.

---

[1] خليل بحر، مرجع سابق، ص317

[2] مصطفى الجمال، إبراهيم سعد، النظرية العامة للقانون –الحق- منشورات الحلبي الحقوقية، بيروت بدون تاريخ نشر، ص432.

* وهذا خلافا لما ذهب اليه التشريع الأمريكي الذي يصف الاعتداء على الحق في الخصوصية خطا من الأخطاء يستوجب المسؤولية وفقا لأحكام المسؤولية عن الخطأ. أنظر في ذلك: أسامة عبد الله قايد، الحماية الجنائية للحق في الخصوصية وبنوك المعلومات دراسة مقارنة، الطبعة الثالثة، دار النهضة العربية، القاهرة 1994ص31 وكذلك شمس الدين أشرف توفيق، الصحافة والحماية الجنائية لحرمة الحياة الخاصة دراسة مقارنة، القاهرة، دار النهضة العربية، 1999، ص 30.

[3] نايل إبراهيم عيد، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية، 2000 القاهرة، ص04.

أما عن حكم المسألة في القانون الجزائري، فإن موقف المشرع الجزائري من طبيعة الحق في الخصوصية يمكن أن نستشفه صراحة من نص المادة 47 من القانون المدني[1] التي تقرر بوجود طائفة من الحقوق تسمى الحقوق الملازمة للشخصية، و أن الحق في الخصوصية يعد من ضمن هذه الحقوق، ومن ثم فإنه يتمتع بما تتمتع به تلك الحقوق من حمايةفي ظل القانون الجزائري كنتيجة قانونية مترتبة على الإ عتراف بها، حيث يكون لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة للشخصية أن يطلب وقف الاعتداء دون حاجة الى إثبات الضرر، وهو ذات الاتجاه الذي سلكه القضاء الجزائري عندما خلصت المحكمة العليا وهي بصدد الفصل في قضية (ز، خ) ضد الشركة ذات المسؤولية المحدودة (ع، أ) إلى أن نشر صورة المطعون ضده تحت عنوان مصاب بداء السكري في مجلة إشهارية للأدوية دون الحصول على موافقته الصريحة والمكتوبة يستوجب تعويض المتضرر.*

المطلب الثالث: نطاق الحق في الخصوصية

إذا تم عتراف للشخص بحقه في الخصوصية، فإن السؤال الذي يثور بعد ذلك يتعلق بالمجال الذي يمكن أن يمتد إليه هذا الحق سواء تحديد نطاق التمتع به من حيث الأشخاص، أو تحديد نطاقه من حيث المضمون، وعليه فإننا سنعمد هنا إلى بيان نطاق الحق في الخصوصية من حيث الأشخاص الذين تشملهم حمايته، وكذلك من حيث الموضوعات التي تدخل ضمن حمايته، أو ينبغي أن تمتد إليها حمايته لأنها من المسائل التي لا تنفك عن حق الإنسان في التمتع بحقه في الخصوصية على أكمل وجه، وهو ما سوف نتعرض إليه كما يلي:

الفرع الأول: الأشخاص الذين يتمتعون بالحق في الخصوصية

يمكن بلورة هذه المسألة على شكل فكرة مؤداها التساؤل عما إذا كان نطاق تطبيق الحق في الخصوصية يشمل كل شخص قانوني، أم أن نطاق تطبيق هذا الحق قاصر على الشخص الطبيعي دون الشخص المعنوي[2].

أولا: تمتع الشخص الطبيعي بالحق في الخصوصية

تم التوصل إلى أن الحق في الخصوصية ينتمي إلى طائفة الحقوق اللصيقة بالشخصية، وبناء على ذلك فإن الشخص الطبيعي يعد الحجر الأساسي في الحماية التي تقررها القوانين للحق في الخصوصية وهو

[1] تنص المادة 47 من القانون المدني: "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء والتعويض عما يكون قد لحقه من ضرر".

*ورد بأسباب القرار المذكور: حيث ثبت لقضاة المجلس أن الطاعنة نشرت صورة المطعون ضده تحت عنوان مصاب بداء السكري في مجلة إشهارية للأدوية دون الحصول على موافقته، حيث أن نشر الصورة في مجلة إشهارية يستوجب الموافقة الصريحة التي لا تتجسد إلا بموجب الكتابة، لاعتبار أن الإشهار بالصورة يشكل مساسا بحق من الحقوق الملازمة لشخصية المطعون ضده عملا بأحكام المادة 47 من القانون المدني، ويستلزم جبر الضرر الناجم عنه وفقا لما نصت عليه المادة 124 من القانون المدني. أنظر القرار رقم 575980 مؤرخ في 210/07/22 عن الغرفة المدنية بالمحكمة العليا مجلة المحكمة العليا، عدد 02، سنة 2010، ص 157 الى 160

[2] محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضمانها في مواجهة الحاسوب، دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاتها في القانون الكويتي، ذات السلاسل للطباعة والنشر، الكويت، 1992، ص64.

المخاطب بنصوصها بصرف النظر عن عنصر المصلحة في التجريم[1]، فلا خلاف بين الفقه والقضاء في أن الشخص الطبيعي يتمتع بالحق في الخصوصية، كونه نشأ ليكون ملاذا للفرد في مواجهة جميع الأمور التي تعكر صفو حياته، فالتلازم بين الحق في الخصوصية والإنسان كان هو المظهر الأساسي والصفة الدائمة في جميع مراحل تطور الحق في الخصوصية.

إذ أن حماية حقوق الإنسان كانت الدافع الأساسي لصدور القوانين المتعلقة بالحق في الخصوصية، لذلك جاءت التشريعات لتعضد هذا الاتجاه، كما هو الحال على سبيل المثال في بريطانيا، فبالرغم من أن لجنة «Lindop» عام 1978 قد أوصت بأن يعرف من يخضع لنظام المعلومات «data subject» بأنه يشمل المؤسسات والهيئات إضافة إلى الأشخاص الطبيعيين، إلا أن قانون حماية المعلومات الصادر عام 1984 وضع تعريفا ضيقا للحق في الخصوصية وقصره على الشخص الطبيعي دون المعنوي.[2]

والمبدأ أن هذا الحق مقرر لكل شخص طبيعي متواجد على إقليم الدولة بصرف النظر على جنسيته ومن ثم فإن الحماية القانونية للحق في الخصوصية مكفولة لكل من المواطن والأجنبي سواء بسواء، لذلك نعتقد أن ما ذهب إليه المشرع الدستوري في المادة 46 من الدستور الجزائري بنصها على أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة، لا يفهم منه مطلقا أن يكون محلا لحماية حقه في الخصوصية من يتمتع بالجنسية الجزائرية فقط، ولا يستبعد أبدا من تقرير هذه الحماية القانونية إذا كان الاعتداء واقعا على الحق في الخصوصية لأجنبي، وإنما تمتد هذه الحماية للمقيمين على إقليم الدولة بصرف النظر عن الكيفية التي يتواجدون بها هؤلاء في الإقليم الوطني[3]، وهو الأمر الذي تؤكده الفقرة الثالثة من نفس المادة بخصوص حماية المعطيات ذات الطابع الشخصي، عندما جاء نصها أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه، فقد ذكرت عبارة الأشخاص دونما اعتبار لجنسيتهم.

وإذا كان الشخص الطبيعي يتمتع بالحق في الخصوصية دون أي إشكال، فإن الآراء بالنسبة للشخص المعنوي تضاربت حول إدخاله في إطار الخصوصية أو عدم إدخاله، فطالما أن المشرع يذكر عبارة الأشخاص وهي تمتد غالبا لتشمل الأشخاص الطبيعيين والمعنويين على حد سواء،أصبح الأمر يثير الجدل والنقاش حول مدى تمتع الشخص المعنوي بالحق في الخصوصية.

فضلا عن ذلك يطرح تساؤل جوهري يتعلق بمدى إمكانية انتقال الحق في الخصوصية في حالة وفاة صاحبه إلى ورثته فيتوسع نطاق هذا الحق إلى هؤلاء بعد وفاته، وهي النقاط التي سوف نتعرض لها كما يلي:

[1] أحمد عبد الزعبي، مرجع سابق، ص151.

[2] محمد عبد المحسن القاطع، مرجع سابق، ص66.

[3] ينص القانون الجزائري في المادة 03 من قانون العقوبات على مبدأ الإقليمية والذي يعني أن يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية.

ثانيا: مدى تمتع الشخص المعنوي بالحق في الخصوصية.

لقد ظهر الخلاف عند الفقه حول مسألة تمتع الشخص المعنوي بالحق في الخصوصية بين مؤيد ومعارض، فالرأي الأول يعطي للشخص المعنوي الحق في التمتع بالحق في الخصوصية، أما الرأي الثاني فينكر عليه تمتعه بهذا الحق[1]، ويعود أصل الخلاف إلى التباين الحاصل سابقا حول تمتع الشخص المعنوي بالحق في الشرف والاعتبار.[2]

فالشخصية القانونية المعترف بها لتلك الجماعات حتما هي متميزة عن شخصية أعضائها، وحتى يتمتع الشخص بالحق في الشرف والاعتبار لا بد له من استقلال نفسي وجسدي لكي تكون له فضائل ورذائل، إرادة وإدراك، وهي الأمور التي لا تتوافر في الشخص المعنوي[3]، وقد طرح هذا الخلاف من جديد ولكن هذه المرة بالسؤال حول مدى تمتع الشخص المعنوي بالحق في الخصوصية*، والإجابة على هذا التساؤل تقتضي أن نتعرض للآراء التي قيلت في تأييد تمتع الشخص المعنوي بهذا الحق ثم الآراء المعارضة، وذلك كما يلي:

1) **الاتجاه المؤيد لتمتع الشخص المعنوي بالحق في الخصوصية:** يذهب أنصار هذا الاتجاه إلى أن الشخص المعنوي يتمتع بالحق في الخصوصية شأنه في ذلك شأن الشخص الطبيعي، فليس هناك ما يمنع من تمتع هذا الأخير بهذا الحق، مستندين في رأيهم إلى الحجج الآتية:

- إن استخدام مصطلح "المواطن" في كثير من دساتير وقوانين الدول عند الحديث على الحماية القانونية للحق في الخصوصية، لا يشكل عقبة في سبيل الإعتراف للشخص المعنوي بهذا الحق، ذلك أن فقه وقضاء القانون الدولي الخاص قد استقر على تمتع الشخص المعنوي بالجنسية شأنه في ذلك شأن الشخص الطبيعي، وبالتالي فإن من يتمتع بالجنسية يمكن اعتباره مواطنا سواء كان شخصا طبيعيا أم معنويا.[4]

- كما أن للشخص المعنوي حياة داخلية مستقلة ومتميزة عن حياته الخارجية وهي التي يعتبرونها حياته الخاصة، وهنا ذهب الفقه الفرنسي إلى ضرورة التفرقة بين الحياة الخاصة وألفة الحياة الخاصة la vie privée et l'intimité de la vie privée، فإذا لم يكن للشخص المعنوي ما يسمى بألفة الحياة الخاصة إلا

[1] محمد نصر محمد، حق الإنسان في حماية حياته الخاصة في القانون الدولي والتشريعات الداخلية، مكتبة القانون والاقتصاد، الرياض 2013 ص95.

[2] عبد الرحمن خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري، دراسة تأصيلية تحليلية مقارنة، مقال منشور بمجلة البحوث والدراسات العدد 12- السنة (8) 2011، كلية الحقوق، جامعة بجاية.

[3] أحمد عبد الظاهر، الحماية الجنائية لحق الشخص المعنوي في الشرف والاعتبار، دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة الطبعة الأولى، 2005، ص58.

* وقصد د المشرع الجزائري في القانون المدني الأشخاص المعنوية وهي: الدولة، الولاية، البلدية، المؤسسات العمومية ذات الطابع الإداري، الشركات المدنية والتجارية، الجمعيات، المؤسسات وكل مجموعة من أشخاص أو أموال يمنحها القانون شخصية قانونية.

[4] محمد نصر محمد، مرجع سابق، ص 97.

أنه يتمتع بحياة خاصة، وهذه الحياة تشمل سرية الأعمال الخاصة بهذا الشخص،[1] إذ يرى بعض الفقهاء أن سرية الأعمال تشكل الحياة الحميمية للمؤسسة القانونية، كما يعتبرون أيضا أنها تأتي كمظهر من مظاهر الحقوق اللصيقة بالشخصية نظرا لانسجامها مع بعض الخصائص المتعلقة بالشخصية، إذ لا تبرز بطريقة إيجابية بقدر ما تبرز بطريقة سلبية، كونها تجد تفسيرها في الموجب الملقى على عاتق كل شخص باحترام سرية الآخرين.[2]

كما أن عتراف بوجود حياة داخلية واجبة الحماية للمؤسسات يسمح للأشخاص المعنويين بالمحافظة على سرية الأعمال التي تعود إليها، لذلك نجد أن الكثير من الدول وضعت الشخص المعنوي في نطاق الحماية للحق في الخصوصية، وقد أخذ بهذا الموقف معظم الفقهاء في بلجيكا مثلما ورد في تقرير "أورنستان" المقدم إلى جمعية هنري كابيتان[3] عن سرية الحياة الخاصة في القانون البلجيكي، وقرره مشروع القانون البلجيكي الخاص بحماية الحياة الخاصة حينما ذهب إلى تجريم انتهاك سرية الأشخاص المعنوية بكافة أنواعها إذا كان الغرض من الانتهاك الإضرار بالشخص المعنوي أو الحصول على منفعة[4]، كما نجد قانون حماية المعلومات الصادر عام 1974 في بريطانيا قد تصدى لهذه المسألة من خلال تحديده للأشخاص الذين يحق لهم الاطلاع على المعلومات الخاصة بالشخص المعنوي وهي بذلك حماية غير مباشرة لخصوصية الشخص المعنوي،[5] وهو الرأي نفسه الذي اتجهت لجنة خبراء حقوق الإنسان في المجلس الأوروبي لحقوق الإنسان إلى الأخذ به عندما قررت حق الشخص المعنوي في حماية حياته الخاصة في الحدود التي تتلاءم مع ظروفه وطبيعته[6] صراحة بقولها: "أن للأشخاص القانونية والهيئات والجماعات التمتع بمثل هذا الحق"، وكان هذا الرأي الذي ذهبت إليه لجنة خبراء حقوق الإنسان بالمجلس الأوروبي نتيجة للبحث الذي أجري على مستوى الاتفاقية الأوروبية الخاصة بحماية الحق في الحياة الخاصة للإنسان والمواطن حول مدى استفادة الأشخاص المعنوية من الحماية القانونية التي يستفيد منها الأشخاص الطبيعيون، حيث اتجه الرأي إلى أنه إذا كان الشخص المعنوي يتمتع بالحق في الاسم والوطن والجنسية وكذلك حماية سمعته واعتباره، فلماذا لا يكون له الحق في الحياة الخاصة في الحدود التي تتلاءم مع ظروفه وطبيعته[7]، وقد تم التعقيب على هذه النقطة بأنه إذا كان من المنطقي أن

---

[1] Olivier GRAF, La personne morale : un non-professionnel ? THÈSE Pour obtenir le grade de DOCTEUR EN DROIT DE L'UNIVERSITÉ D'AIX-MARSEILLE Discipline : Droit Privé UNIVERSITÉ D'AIX-MARSEILLE – ÉCOLE DOCTORALE DES SCIENCES JURIDIQUES ET POLITIQUES P237

[2] نعيم مغبغب، مرجع سابق، ص133.

[3] L'Association Henri Capitant fut fondée en 1935, sous l'autorité de Henri Lucien Capitant, Professeur à la Faculté de droit de Paris, par un groupe de juristes de différents pays de langue française : Belgique, Luxembourg, Québec, Suisse, L'Association est reconnue d'utilité publique en France, par décret du Gouvernement en Conseil d'Etat en date du 12 juillet1939. Elle anime depuis 2010 la première revue bilingue consacrée aux droits de tradition civiliste. Voir le site : www.henricapitantlawreview.org visite le 09/04/2020

[4] مصطفى أحمد عبد الجواد حجازي، الحياة الخاصة ومسؤولية الصحفي، دراسة فقهية قضائية مقارنة في القانونين الفرنسي والمصري، دار الفكر العربي القاهرة 2011، ص123 ومشار إليه في التهميش رقم 01 نعيم مغبغب، مرجع سابق، ص130

[5] محمد عبد المحسن المقاطع، مرجع، سابق، ص20.

[6] يوسف الشيخ يوسف، مرجع سابق ص212.

[7] بشاتن صفية، مرجع سابق، ص157.

يتمتع الشخص المعنوي باسم وموطن وجنسية وأهلية حتى يتمكن من تحقيق الأغراض التي أنشئ من أجلها، فإنه ومع ذلك فلا يمكن أن تكون له حياة خاصة لأنها لا تتفق مع طبيعته المعنوية، فحبذا لو قدمت لجنة خبراء حقوق الإنسان بالمجلس الأوروبي مثالا لتدعيم اقتراحها لصالح الشخص المعنوي، لذلك فإنه وعلى الرغم من قيام الاتفاقية الأوروبية بنقاش حول موضوع مدى تمتع الشخص المعنوي للحق في الخصوصية، إلا أنها لم تناشد الدول الأعضاء إلى تبني تشريعات وطنية في هذا الاتجاه.[1]

2) **الإتجاه المعارض لتمتع الشخص المعنوي بالحق في الخصوصية:** يذهب أنصار هذا الاتجاه إلى أن الشخص المعنوي ليس له الحق في الخصوصية ولا يصلح أن يكون مجنيا عليه في الجرائم الماسة بهذا الحق، وأن مثل هذا الحق لا يعترف به إلا للشخص الطبيعي باعتبار أن الحق في الخصوصية يرتبط بالإنسان[2] ولا يقترن بالشخص المعنوي، وإذا ما تم التسليم بارتباط الحق في الخصوصية بالشخص المعنوي فإن ذلك سوف يشكل اعتداء على هدف وغاية المشرع التي من أجلها فرضت الحماية اللازمة للحق في الخصوصية.[3]

وقد استند أصحاب هذا الرأي إلى حجج أهمها:

-أن الحق في الخصوصية من الحقوق اللصيقة بالشخصية وهي الحقوق التي لا تثبت إلا للإنسان، ومن ثمة عدم إمكانية تمديد قواعد حماية الخصوصية للأشخاص المعنوية.

-إذا كان للشخص المعنوي حق قد يشبه الحق في الخصوصية وهو ما يطلق على تسميته الحياة الداخلية للشخص المعنوي، وهي حياة مستقلة ومتميزة عن النشاط الخارجي للشخص المعنوي ويجب احترامها، فهي تحتاج لحمايتها إلى قواعد تختلف عن قواعد الحماية التي تحكم الحق في الخصوصية، ولا تكون داخلة إلا في إطار قانون الشركات أو القوانين الأخرى التي تنظم الأحكام المتعلقة بالشخصية المعنوية.[4]

وعليه فعدم جواز الكشف عما يدخل في نطاق الحياة الداخلية للشخص المعنوي من أسرار وعدم جواز أن تكون محلا للتحري عنها، لا يدخل في نطاق الحماية القانونية للحق في الخصوصية، فمن يتجسس على الأسرار الصناعية والتجارية ومن يسجل محادثات ذات طابع تجاري أو صناعي لا يعد منتهكا للحق في الخصوصية*، على أساس أن هذا الحق يرتبط ارتباطا وثيقا بالمقومات الخاصة للشخص الطبيعي.

كما تم الاعتراض على إخضاع الأشخاص المعنوية للتمتع بالحق في الخصوصية ومد نطاق هذا الحق إليهم استنادا إلى أن القيود الواردة في قوانين الخصوصية من شأنها أن تقلل من سرعة التحرك التجاري اللازم للشركات كأشخاص معنوية[5].

---

[1] عبد المحسن المقاطع، مرجع سابق، ص70.

[2] تنص المادة 52 من الق المدني على أن "الشخص المعنوي يتمتع بما يتمتع به الشخص الطبيعي إلا ما كان منها ملازما لصفة الإنسان".

[3] محمد الشهاوي، مرجع سابق، ص145.

[4] ممدوح خليل بحر، مرجع سابق، ص325.

* يذهب بعض الفقه في فرنسا إلى أن حماية الحياة الداخلية للشخص المعنوي تتم وفقا للأحكام العامة في المسؤولية المدنية. وفي الولايات المتحدة الامريكية تتم مثل هذه الحماية عن طريق القواعد الخاصة للمنافسة غير مشروعة، وهذا ما أخذت به المحكمة العليا الأمريكية في قضية الولايات المتحدة الأمريكية ضد شركة مورثون باعتبار أن الغرض الأساسي من هذا الحق هو توفير الهدوء والسعادة الإنسانية. أنظر حسام الدين الأهواني مرجع سابق، ص161.

[5] عبد المحسن المقاطع، مرجع نفسه، ص68.

ويؤكد هذا الاتجاه الرافض لتمتع الشخص المعنوي بالحق في الحياة الخاصة جانب كبير من الفقه الفرنسي على رأسه الأستاذ raymond Lindon الذي يعد من أهم المنكرين لتمتع الشخص المعنوي بالحق في الحياة الخاصة، حينما فسر نص المادة 09 من القانون المدني بقوله أن المشرع الفرنسي قد استبعد أن يكون للشخص المعنوي الحق في الحياة الخاصة لأنه استعمل كلمة "ألفة" intimité والتي تخص الشخص الطبيعي دون سواه.

وقد أفصح القانون الفرنسي رقم 70/643 المؤرخ في 1970/07/17 المتعلق بحماية الحقوق الفردية للمواطنين[1] عن عدم إمكانية مد حماية الحياة الخاصة لتشمل الأشخاص المعنويين.

وفي أمريكا قضت المحكمة الاتحادية العليا بأنه وإن كان من حق المؤسسات أن توفر لها الحماية في مواجهة المطالبات الخاصة بإجراء التحريات عنها، إلا أن هذه المؤسسات لا يمكن أن تطالب بمساواتها في تمتعها بالحق في الخصوصية تماما كالأفراد.[2]

وعن موقف المشرع الجزائري بخصوص مسألة تمتع الشخص المعنوي بالحق في الخصوصية من عدمها، فيمكن استنتاجه من خلال ما ورد بنص المادة 39 من الدستور، والتي تنص على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصة" وقد سبق الذكر سالفا أن عبارة المواطن تطلق في الغالب على الشخص الطبيعي دون الشخص المعنوي، ومن ثم فإن المعني بحماية الحياة الخاصة بهذا النص الدستوري هو الشخص الطبيعي، فضلا عن المادة 47 من القانون المدني التي نصت على أنه "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة للشخصية أن يطلب وقف هذا الاعتداء أو التعويض..." والحق في الخصوصية هو أحد هذه الحقوق الملازمة للشخصية.

ولتأكيد هذا المعنى أصدرت المحكمة العليا قرارا بتاريخ 1996/12/25 فهرس رقم 161815 في قضية (ش م ع) ضد فريق (ب) جاء فيه أنه: من المقرر قانونا أن الشخص الاعتباري يتمتع بجميع الحقوق إلا ما كان منها ملازما لصفة الإنسان، وذلك في الحدود التي يقررها القانون"، والحق في الخصوصية هو من الحقوق الملازمة لصفة الإنسان، وعلى هذا الأساس فإنه يبدو واضحا أن التشريع والقضاء في الجزائر قد سلكا الاتجاه الرافض للاعتراف بالحق في الخصوصية للشخص المعنوي.

ثالثا: مدى انتقال الحق في الخصوصية إلى الورثة

إن من الخصائص التي تتميز بها الحقوق اللصيقة بالشخصية* والتي يكيف الفقه أن الحق في الخصوصية يعد واحدا منها، أنها حقوق مطلقة يحتج بها على الجميع، وهي حقوق لا تقبل الحجز عليها أو التصرف فيها للغير لأنها حقوق غير مالية، كما لا تسقط بعدم الاستعمال مهما طال الزمن، فضلا عن

[1] Loi n°70-643 du 17 juillet 1970 TENDANT A RENFORCER LA GARANTIE DES DROITS INDIVIDUELS DES CITOYENS JORF du 19 juillet 1970 page 675.

[2] عبد المحسن المقاطع، مرجع سابق، ص68.

* تطلق هذه التسمية على حقوق الشخصية وذلك تأكيدا على أن هذه الحقوق ما هي إلا ترجمة قانونية للشخص، وأنها تتصل بالشخصية الإنسانية اتصالا وثيقا يصعب على الفرد أن يعيش بدونها، وقد عرفت الحقوق الشخصية بأنها تلك الحقوق التي تثبت للفرد باعتباره إنسانا، وهي تستهدف حماية كيانه ومقوماته سواء من الناحية المادية أو من الناحية المعنوية. أنظر في هذا الإطار محمد طه البشير، غني حسون طه، الحقوق العينية القسم الأول والثاني،الحقوق العينية الأصلية والحقوق العينية التبعية، الدار الجامعية للطباعة والنشر، بغداد 2017، ص43.

كون هذه الحقوق لا تنتقل إلى الورثة بعد وفاة صاحبها كقاعدة عامة*، فهل تنطبق هذه الخاصية الأخيرة على الحق في الخصوصية، أي بعبارة أخرى هل ينقضي حق الخصوصية بوفاة صاحبه وينشأ للورثة حق شخصي جديد أم أن هذا الحق قابل للانتقال إلى الورثة بعد وفاة صاحبه كاستثناء عن القاعدة.

لقد ثار النقاش والجدل حول هذه المسألة في الفقه المقارن، فأدى أن ظهر نتيجة لذلك اتجاهان، الاتجاه الأول يرى أن حق الخصوصية ينتهي بوفاة صاحبه، وأما الاتجاه الثاني فيرى بانتقال حق الخصوصية إلى الورثة.

1)الاتجاه الأول: انقضاء الحق في الخصوصية بالوفاة: يذهب أنصار هذا الاتجاه إلى تأسيس موقفهم بعدم انتقال الحق في الخصوصية إلى ورثة صاحب هذا الحق المتوفي على أنه طالما أن الحق في الخصوصية يعتبر من الحقوق اللصيقة بالشخصية فإنه يزول وينقضي بزوال الشخصية نفسها، ولا يقبل الانتقال إلى الورثة، ذلك أن الحق في الخصوصية لا يحمي إلا الأحياء فقط ولا يستفيد منه الأموات، بل تعد الوفاة عقبة مادية تحول دون انتقال هذا الحق إلى الورثة.

فالوظيفة الأساسية لهذا الحق تكمن في حماية الشخصية وهو ما لا يكون له محل إلا في حياة صاحبه، حيث يرى أصحاب هذا الرأي، أنه بعد وفاة الشخص لا تكون حياته الخاصة في عوز لحماية لأنها اختفت باختفاء شخص صاحبها، والقول بغير ذلك يعني الخلط بين أمرين متمايزين هما الحق في الحياة الخاصة الذي يختفي بمجرد موت صاحبه والحق في الشرف والاعتبار[1]. وعلى هذا الأساس يكون للورثة إذا ما تضرروا من نشر خصوصيات المتوفي أن يرفعوا دعوى أساسها حماية شرف واعتبار هذا الأخير وليس لحماية خصوصيته[2]، فمن غير المقبول حسب هذا الاتجاه،اعتبار الورثة امتدادا لشخصية المتوفي، كما لا يعتبر وجودهم استمرارا لها، فإن كانت هذه الفكرة تصلح في مجال تفسير كيفية انتقال أموال المتوفي لورثته وكذلك في مجال إعمال قاعدة لا تركة إلا بعد سداد الديون، فإنه لا يجوز التوسع فيها والأخذ بها في مجال الحقوق اللصيقة بالشخصية.

وإذا ما تضرر ورثة المتوفي من نشر خصوصيات هذا الأخير كان لهم الحق في الدفاع باسمهم الشخصي وليس باسم المتوفي عن عدم المساس بمشاعرهم تجاه المتوفي لما لهم من مصلحة معنوية وعاطفية تجاهه.[3]

وتأييدا لذلك فقد أكدت محكمة النقض الفرنسية هذا الاتجاه عندما قضت بأن الحق في رفع دعوى لحماية الحق في الحياة الخاصة ينتهي بوفاة الشخص المعني، فهو الوحيد الذي يملك هذا الحق[4]، إلا أنه

* ترد بعض الاستثناءات على هذه القواعد كانتقال الحق الأدبي للمؤلف بالوفاة إلى ورثته، انتقال الحق في التعويض عن الضرر المعنوي إلى الورثة شريطة أن يكون هذا الضرر ناشئا عن موت المصاب نتيجة الفعل الضار.

[1] Kayser PIERRE, le droit de la personnalité aspects théoriques et pratiques, revue, trim, droit. civil. p 497 . Voir aussi Jean-Luc Chenaux, Le droit de la Personnalité Face aux Medias Internationaux étude de droit international prive compare, Librairie Droze Genève, 1990, p 26

[2] أحمد عبد الزعبي، مرجع سابق، ص161.

[3] حسام الدين الأهواني، مرجع سابق، ص161.

[4] أحمد عبد الزعبي، مرجع نفسه، ص162.

بإمكان الورثة متابعة الدعوى المرفوعة من طرف المورث صاحب الحق قبل وفاته، لأن هذا يدل على رغبته في حماية حقه، أما إذا لم يرفع المتوفي الدعوى قبل وفاته فلا يمكن لورثته رفع دعوى للمطالبة بحماية حقه في الخصوصية، كما أقر القضاء الفرنسي أيضا حق الورثة في المطالبة بالتعويض عن الضرر الذي أصاب مشاعرهم جراء نشر خصوصيات مورثهم.[1]

وهو الاتجاه نفسه الذي أخذت به المحاكم الأمريكية عندما قررت في العديد من أحكامها أن الحق في الخصوصية لا يحمي إلا الأحياء ولا يستطيع الورثة رفع دعوى لحماية هذا الحق باسم المتوفي بعد وفاته.[2] ذلك أن الدعاوى الشخصية في القانون الأمريكي تسقط بالوفاة.

ونشير إلى أننا لم نجد في قضائنا قرارات للمحكمة العليا يمكن أن نستدل بها في هذا الإطار.

2)الاتجاه الثاني: انتقال الحق في الخصوصية إلى الورثة: من المعلوم أن وفاة الشخص يترتب عليها العديد من الآثار القانونية والتي من أهمها أن جميع حقوقه تؤول إلى ورثته، والمراد بالحقوق في هذا الشأن هي الحقوق المالية ولا يشمل ذلك الحقوق الشخصية، لأنها لا تدخل في ذمة المتوفي المالية، كما أن هذه الحقوق تدور مع الشخصية وجودا وعدما، مما يعني أنها تنقضي بنهاية الشخصية، وبالتالي فالقاعدة أنه لا يمكن نقل حقوق الشخصية إلى الورثة وأنها تنقضي بموت صاحبها، ويتجسد ذلك بشكل خاص في مجال الحق في سلامة كيان الإنسان المادي، أما فيما يخص سلامة الكيان المعنوي* فإن الفقه يتجه إلى التوسيع في مسألة انتقال الحقوق التي تتعلق بهذا الكيان إلى الورثة، كما هو الشأن في خصوصيات المتوفي وشرفه، وذلك لتأكيد حماية هذه الحقوق من طرف الورثة[3].

لذلك يرى أصحاب هذا الاتجاه أنه لا يجب أن يؤاخذ مبدأ عدم انتقال الحقوق اللصيقة بالشخصية إلى الورثة على إطلاقه، فهناك بعض الحقوق رغم كونها من الحقوق الشخصية كالحق الأدبي للمؤلف[4] والحق في الشرف والاعتبار*، إلا أنها قابلة للانتقال إلى الورثة بعد وفاة صاحبها، واعتبروا أن الحق في الخصوصية من بين هذه الحقوق، وذلك انطلاقا من فكرة الإرث المعنوي، والتي تعني أن المصالح المعنوية للشخص تستمر في الوجود بعد الوفاة ولا بد أن يتواجد من يتولى حمايتها، لذلك يجب أن تنتقل إلى الورثة لتأكيد هذه الحماية إلى ما بعد الوفاة.

---

[1] قرار محكمة باريس في 1998/02/24 مأخوذ من:

Recueil Dalloz 1998 p255, Disponible sur le site : www.dalloz-revues .fr

[2] حسام الدين الأهواني، مرجع سابق، ص170.

* تنطوي الشخصية على مقومات مادية وهي الكيان المادي للفرد، وكذلك على مقومات معنوية هي الشرف والاعتبار والكرامة، السمعة، المعتقدات، الأفكار، الحق في السرية والمتعلقة بالحياة الخاصة التي من حق صاحبها أن تظل محجوبة عن العلانية مصونة من التدخل والاستطلاع، بالإضافة إلى حق الشخص على ما يبتكره من أفكار وهو ما يعرف بحق المؤلف droit d'auteur

[3] حسام الدين الأهواني، مرجع نفسه، ص158.

[4] حسام الدين الأهواني، مرجع نفسه، ص178.

* أقر المشرع في نص المادة 26 من الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة أنه تمارس الحقوق المنصوص عليها في هذا القانون من قبل ورثة مؤلف المصنف بعد وفاته.

وتقوم فكرة الإرث المعنوي l'héritage moral على أن هناك تضامنا عائليا بين المورث وورثته، وهي تعبر عن قيمة معنوية يجب أن تكون أساس انتقال الحق في الخصوصية إلى الورثة، بالإضافة إلى ذلك فإن ضرورات احترام الموتى وذكراهم توجب حماية خصوصياتهم بعد الوفاة.*

أما عن موقف المشرع الجزائري من مسألة انتقال الحق في الخصوصية إلى الورثة فإننا نرى أنه أخذ بإمكانية انتقال هذا الحق إلى الورثة، وذلك من خلال إعطائه لورثة الشخص الذي تتم معالجة معطياته الشخصية الحق في تصحيح المعطيات الشخصية لمورثهم لدى الجهة التي تقوم بمعالجة هذه المعطيات إذا كانت غير صحيحة، وهو ما سوف نتطرق إليه بالتفصيل في حينه.

الفرع الثاني: نطاق الحق في الخصوصية من حيث المضمون:

نقصد بنطاق الحق في الخصوصية من حيث المضمون تلك القيم التي يحميها هذا الحق ضد التدخل الخارجي من الغير، وهو ما يقودنا طبعا للتساؤل حول ماهية الموضوعات التي تدخل ضمن الحماية القانونية المقررة للحق في الخصوصية، هل كل ما يتصل بالشخص من معلومات يعتبر بالضرورة مما يندرج تحت الحماية التي تعطي للشخص وفقا للحق في الخصوصية، أم أن هناك أمورا لا تدخل ضمن الحماية الموضوعية للحق في الخصوصية حتى وإن ارتبطت بالإنسان؟[1]

لقد عمل الفقه والقضاء المقارن جاهدا نحو وضع قائمة للقيم والعناصر التي تغطيها هذه الفكرة، كما هو الشأن بالنسبة للفقه الفرنسي على سبيل المثال، عندما حاول فريق من الفقهاء الفرنسيين أن يضعوا قائمة بالحالات التي تدخل ضمن نطاق الحق في الحياة الخاصة، فذكروا الحياة العائلية، الحياة المهنية، الحق في الصورة، كشف الراتب، الحق في الاسم، الحق في النسيان[2] ،كما أضاف جانب آخر المعتقدات الدينية للشخص واعتبرت من المسائل التي تدخل ضمن نطاق الحق في الخصوصية ويجب حمايتها ضد تطفل الآخرين[3]، كما اعتبر القضاء الفرنسي أن الحالة الصحية للشخص وما يتعلق بالرعاية الطبية التي يتلقاها تعد أيضا من نطاق الحق في الخصوصية، وأن الكشف عن الحالة الصحية له دون إذنه غير جائز ويعد مساسا بالحق في الخصوصية لصاحبه، إلا في الحالات التي يجوز فيها ذلك قانونا، بالإضافة كذلك إلى الآراء السياسية التي يعتنقها الشخص، فقد ذهبت بعض المحاكم الفرنسية إلى اعتبارها من ضمن المسائل التي تتعلق بالخصوصية[4]، كما اعتبر القضاء الفرنسي أيضا أن الكشف عن العنوان الشخصي والرقم الهاتفي للشخص وكذلك الذمة المالية دون علم صاحبها يعد من قبيل المساس بخصوصيته، فقد

* أقر المشرع الجزائري بهذا المعنى بموجب القانون العضوي رقم 15/12 المؤرخ في12 جانفي 2012 المتعلق بالإعلام في المادة 111 أنه "للورثة حق الر د للدفاع عن أمواتهم في حالة الاعتداء على حقوقهم وتعرضهم لاتهامات كاذبة من شأنها المساس بشرفهم أو سمعتهم".

[1] عبد المحسن المقاطع، مرجع سابق، ص72.

[2] عبد الرحمان بن جيلالي، جريمة الانتهاك الالكتروني لحرمة الحياة الخاصة، مقال منشور على الموقع:www.platform.almanhal.com أطلع عليه يوم: 2020/01/14

[3] علي أحمد عبد الزعبي، مرجع سابق، ص170.

[4] أسامة عبد الله قايد، مرجع سابق، ص24.

قضي أن نشر مقدار الضريبة المفروضة على الشخص يجعل من السهل معرفة حجم ثروته ومن ثم يعد ذلك مساسا بخصوصيته[1].

وإذا رجعنا إلى كتابات القانونيين الأمريكيين نجدهم يركزون على تعداد بعض القيم التي يغطيها الحق في الخصوصية والتي تحدد نطاقه الموضوعي، ومن أشهر التقسيمات التي تحدد عناصر الحق في الخصوصية في الفقه الأمريكي مال قال به ويليم بروسر[2] وتتمثل هذه العناصر في:

-اقتحام عزلة الشخص وخلوته.

-إفشاء وقائع الشخص أو صورته بدون وجه حق.

-استعمال اسم الشخص أو صورته بدون وجه حق.

وتؤكد المادة 652 من المدونة الثانية للأفعال الضارة في الولايات المتحدة الامريكية الصادرة عام 1977 تقريبا هذا التعداد لعناصر الحق في الخصوصية، من خلال نصها على "أنه يتمثل الاعتداء على الحق في الخصوصية فيما يلي:

-التدخل في عزلة الغير أو شؤونه الخاصة.

-استخدام اسم أو صفة الغير لتحقيق مصلحة خاصة.

-إفشاء أمور متعلقة بالحياة الخاصة للغير.

-نشر أمور كاذبة تشوه حقيقة الغير في نظر الناس".*

إن محاولة حصر عناصر الحق في الخصوصية وبيان الأمور والمواضيع التي تدخل في نطاقه وفق التعداد السابق يمكن أن يوصف بالقصور، ولعل السبب في ذلك يرجع إلى أن الخصوصية يختلف مداها وأبعادها باختلاف المجتمعات والأنظمة السياسية التي تحكمها، كما تختلف باختلاف الأزمنة والتقاليد والأعراف والثقافات التي تسود حتى في المجتمع الواحد، ومن ثم يكون التعداد لعناصر الحق في الخصوصية في مجتمع ما ناقصا لأنه لا يأخذ بعين الاعتبار كل المسائل التي تدخل ضمن نطاق الحق في الخصوصية، ويكون هذا التعداد نفسه واسعا لدرجة القول أنه يضم مسائل عامة ليست من مقتضيات

[1] حسام الدين الأهواني، مرجع سابق، ص62.

[2] CRS Report prepared for Members and committees Data Protection Law: An Overview. Congressional research service march25.2019, p03 https://crsreports.congress.gov/product/pdf/R/R4563.اطلع عليه يوم: 2020/01/14

*كما ذهب جانب آخر من الفقهاء الأمريكيين إلى تبني تقسيم مشابه لهذا التقسيم ومنهم الأستاذ بيني beany في كتابه the right to privacy and american law أين اعتبر أن الحق في الخصوصية يحمي الشخص ضد:

1-التدخل أو التطفل بأي طريقة كانت في حياة الشخص وأنشطته.

2-الحصول أو الكشف عن معلومات تتعلق بالشخص.

3-إستعمال عناصر شخصيته مثل الاسم والصورة دون إذنه.

الخصوصية في مجتمع آخر[1]. بالإضافة إلى أن صور الحق في الخصوصية في ازدياد مستمر نتيجة سوء استخدام التطور في علوم التكنولوجيا المعلوماتية، والتي قد تفرز صورا لم يكن قد سبق تعدادها مما يسبب انتهاكا لحق الإنسان في خصوصيته.[2]

وعلى الرغم من ذلك فإن الفقه آثر انتهاج طريق الحصر والتعداد للعناصر المشكلة للحق في الخصوصية، كبديل عن محاولة إيجاد تعريف لهذا الحق، وذلك إدراكا منه لصعوبة التوصل إلى معيار قانوني حاسم يتحدد به مدلول هذا الحق.

وسوف نركز على العناصر المهمة والتي لها مساس مباشر بخصوصية الإنسان، وتندرج تحت مضلة الحماية المستندة إلى الحق في الخصوصية، وذلك كما يلي:

أولا: عناصر الخصوصية المتعلقة بالكيان المادي للإنسان

هناك مجموعة من العناصر التي تكون الحق في الخصوصية المادية تستوجب الحماية القانونية المقررة لهذا الحق، وهي لا تثير خلافا في الفقه والقضاء وتعد ركائز أساسية لهذا الحق، وتشكل هذه العناصر ما يعرف بالخصوصية المادية، ولقد ساد لوقت طويل أن المقصود من الحق في الخصوصية هو احترام الخصوصية المادية للإنسان، وهذا الفهم يوفر الحماية القانونية للإنسان في مواجهة التدخل والاعتداء الذي يتخذ صورة اعتداء مادي على الإنسان نفسه أو على ملكه[3].

1) **حرمة المسكن والمكان الخاص:** تعتبر حرمة المسكن من أهم عناصر الحق في الخصوصية، وهو أمر بديهي، ذلك أن مسكن الشخص يعتبر بمثابة مستودع لخصوصياته وأسراره ومحل سكينته التي ينشد فيها عزلته بعيدا عن أعين ومسامع الآخرين، ويتحرر من القيود التي تكبله في الحياة الاجتماعية ويعيش في خلوته.[4]

إن مدلول المسكن يتحدد بكل مكان يقيم فيه الشخص بصفة دائمة أو مؤقتة، وعلى هذا ساس يعرف المشرع الجزائري المسكن في المادة 355 من قانون العقوبات بأنه كل مبنى أو دار أو غرفة أو خيمة أو كشك ولو متنقل متى كان معدا للسكن وإن لم يكن مسكونا، وكافة توابع المسكن مثل الأحواش وحظائر الدواجن ومخازن الغلال والإسطبلات والمباني التي توجد بداخلها مهما كان استعمالها حتى ولو كانت محاطة بسياج خاص، وكذلك عرف القانون المدني الفرنسي المسكن في المادة 102 بأنه "المكان الأساسي لإقامة الشخص الذي يمارس فيه حقوقه المدنية ".[5]

[1] محمود عبد الرحمن محمد، مرجع سابق، ص144.

[2] احمد عبد الزعبي، مرجع سابق، ص170.

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص17.

[4] محمود عبد الرحمن محمد، مرجع سابق، ص200.

[5] Article 102Modifié par art. 46de la loi n2014-366 du 24 mars 2014 Le domicile de tout Français, quant à l'exercice de ses droits civils, est au lieu où il a son principal établissement. Le lieu d'exercice des droits civils.

في حين يذهب قانون العقوبات الفرنسي[1] إلى تعريف السكن بمدلول أوسع من القانون المدني دلالة، باعتبار أن السكن يشمل كل مكان يستخدمه الفرد مقرا خاصا له[2]. كما ذهب القضاء الفرنسي إلى تعريف السكن بأنه المكان الذي يحق للشخص قانونا أن يشغله.[3]

ويعرف القانون الأمريكي المسكن بأنه المكان الذي يأوي إليه الشخص عادة ويختاره لمعيشته.[4]

وقد ذهب الفقه أيضا إلى تعريف المسكن بأنه المكان الذي يحتفظ فيه الشخص بأسراره بعيدا عن بصر وسمع الآخرين، وينطلق الإنسان داخله دون قيود ويستطيع أن يخلو بنفسه فيه[5].

كما يعتبر المسكن في نظر الفقه وحتى القانون أيضا أنه المكان المخصص للاستعمال كسكن، سواء أكان مخصصا بطبيعته لذلك الاستعمالن أم لم يكن مخصصا للسكن ولكنه مسكون بالفعل.[6]

لأجل ذلك تمتد الحماية القانونية المقررة لحرمة المسكن لتشمل كل مكان خاص للإقامة، أو كل مكان يزاول فيه الشخص نشاطه الصناعي أو التجاري مثل غرف النزلاء في الفنادق، المستشفيات ومكاتب المحامين وعيادات الأطباء، كما يعد مسكنا أيضا القوارب والسفن مادام بها من يقطنها وتتمتع بما يتمتع به السكن من حرمة.

ونظرا لاعتبار المسكن جوهر وأساس ممارسة الإنسان لحياته الخاصة، وكذا مستودع خصوصياته وأسراره، فقد تكفلت الدساتير في أغلب الدول بضرورة إحاطته بالضمانات القانونية التي تكفل احترامه.*

كما تجرم التشريعات الجنائية وتعاقب على انتهاك حرمة السكن، فقانون العقوبات الجزائري يعاقب في المادة 295 كل من يدخل فجأة أو خدعة أو يقتحم منزل مواطن، بالإضافة إلى نص المادة 135 من قانون العقوبات التي تنص على معاقبة كل موظف في السلك الإداري أو القضائي وكل ضابط شرطة وكل قائد أو أحد رجال القوة العمومية دخل بصفته المذكورة منزل أحد المواطنين بغير رضاه وفي غير الحالات المقررة

---

[1] أنظر المادة 226-4 والمادة 432-8 من قانون العقوبات الفرنسي، بالإضافة إلى ورود تعريف للمسكن في قانون هندسة وتنظيم وبناء المدن الفرنسي code de l'urbanisme

[2] علي أحمد عبد الزعبي، مرجع سابق، ص172.

[3] Cour de cassation chambre criminelle du 26 février 1963 N° de pourvoi : 62-90653

"ATTENDU, EN EFFET, QUE LE TERME DE DOMICILE NE SIGNIFIE PAS SEULEMENT LE LIEU OU UNE PERSONNE A SON PRINCIPAL ETABLISSEMENT, MAIS ENCORE, COMME EN L'ESPECE, LE LIEU OU, QU'ELLE Y HABITE OU NON, ELLE A LE DROIT DE SE DIRE CHEZ ELLE, QUEL QUE SOIT LE TITRE JURIDIQUE DE SON OCCUPATION ET L'AFFECTATION DONNEE AUX LOCAUX ET QUE LA VIOLENCE RESULTE DE L'EMPLOI, POUR S'INTRODUIRE AU DOMICILE D'AUTRUI ET CONTRE SON GRE, D'UNE CLE AUTRE QUE CELLE QUI, UTILISEE SANS FRAUDE, Y DONNE NORMALEMENT ACCES."

[4] ممدوح خليل بحر، مرجع سابق، ص267.

[5] محمد الشهاوي، مرجع سابق، ص43.

[6] عبد المهيمن بكر سالم، القسم الخاص في قانون العقوبات، جرائم الاعتداء على الأشخاص والأموال، دار النهضة العربية، القاهرة، 1976، ص425.

* ينص الدستور الجزائري "تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه. ولا تفتيش إلا بأمر مكتوب من السلطة القضائية المختصة"

-التعديل الرابع للدستور الأمريكي "للأفراد حق الحرمة في أشخاصهم ومساكنهم وأوراقهم وممتلكاتهم الشخصية، يجب ألا تنتهك بصورة غير مشروعة بتفتيشها أو ضبطها..."

-الدستور المصري "للمساكن حرمة، فلا يجوز دخولها أو تفتيشها إلا بأمر قضائي مسبب وفقا لأحكام القانون"

في القانون وبغير الإجراءات المنصوص عليها فيه، كذلك المادة 184 من قانون العقوبات الفرنسي تعاقب كل من يدخل من رجال الشرطة أو الموظفين العموميين أو رجال الضبط القضائي مسكن مواطن بوجه غير شرعي وبدون موافقته وبغير مراعاة للإجراءات التي نص عليها القانون". ووفقا للمادة 373 من قانون العقوبات المصري فإنه يعاقب كل من دخل بيتا مسكونا أو معد للسكن أو في أحد ملحقاته أو في محل معد لحفظ المال ولم يخرج منه بناء على تكليف ممن له الحق في ذلك، وكذلك إذا وقعت جريمة الدخول غير القانوني للمسكن من جانب أحد الموظفين أو المستخدمين أو أي شخص مكلف بخدمة عامة اعتمادا على وظيفته.

ويدخل في إطار حماية حرمة المسكن حق الشخص في عدم الإفصاح عن عنوان مسكنه،فقد درجت المحاكم مرارا على الحكم بأن عنوان مساكن الأفراد يندرج في دائرة الحياة الخاصة وأن نشر عنوان مسكن أو محل إقامة فرد ما من دون الحصول على إذن من صاحب العلاقة، يعتبر مساسا بحياته الخاصة[1]، كما قضي في فرنسا أنه لا يمكن إلزام محطة تلفزيونية بتزويد الغير عنوان أحد الممثلين بغية استدعائه إلى المحكمة، طالما أن هذه المعلومة تتعلق بالحياة الخاصة.[2]

كما يدخل ضمن المساس بحرمة المسكن ومن ثم المساس بحق الشخص في خصوصيته، تصوير المسكن بشكل يسمح بالتعرف عليه، ويختلف الوضع بالنسبة للصور سواء أتم التقاطها خارج السكن أم داخله، لأن هذه الصور تسمح على الأقل بتحديد موقع السكن أو تدل على هوية صاحبه، وانطلاقا من هذه الفكرة قررت محكمة باريس الكبرى أن المسكن ينتمي إلى دائرة الحياة الخاصة وأن نشر صور لمسكن أحد الممثلات يعتبر اعتداء على الحياة الخاصة.[3]

هذا وتتوقف خصوصية السكن ويخرج من نطاق الحق في الخصوصية إذا ما سمح صاحبه للجمهور بأن يرتاد مسكنه، وبالتالي لا يتمتع هذا المسكن بالحرمة التي أعطاها له القانون طالما انتفت عنه خصوصيته بإرادة صاحبه بأن سمح للجمهور بغير تمييز بالتردد عليه[4]، وقد قضت في هذا الإطار محكمة النقض المصرية أنه مادام الحكم أثبت أن المتهم قد أعد غرفتين في منزله للعب القمار ووضع فيها موائد وصف حولها الكراسي، واعتاد الناس دخول هذا المنزل دون تمييز بينهم، فإن هذا يجعل من منزله محلا عاما يغشاه الجمهور بلا تفريق بينهم ويسمح للضبطية الدخول إليه دون حاجة لإذن من النيابة.[5]

---

[1] **Tribunal de grande instance de Paris Réfère ordonnance. du 22 janvier 1996 https://www.legipresse.com**

. « La divulgation non autorisée par voie de presse de l'adresse de maurice papon constituait une atteinte à l'intimité de sa vie privée »

[2] TGI paris, ord. Réf 29 jan 1991 : gaz pal 1991. p 222

[3]. Cour de cassation chambre civile2 N° de pourvoi : 87-10463 le 29 juin 1988 : gaz Pal, 4 déc 1988, p 7, note ph Berain la cour de cassation avait accepté le pourvoi formé à l'encontre d'un arrét rendu le 27 octobre 1986, par la cour de paris au motif qu'il n'a pas précisé en quoi la publication de la photographie portait atteinte à la vie privée de la victime. Alors qu'actuellement il est généralement jugé que « la publication sans autorisation de l'image de la propriété ou réside une actrice célèbre constitue une atteinte à la vie privée » voir aussi Bulletin des arrêts des chambres civiles disponible sur le site https://www.courdecassation.fr/publications_26/bulletin_arrets_chambres_civiles_2711/ visite le : 20/01/2020

[4] محمود عبد الرحمن محمد، مرجع سابق، ص 203.

[5] نقض 17 مارس 1953، مجموعة أحكام النقض المصرية، رواق الجمل متوفر على الرابط:

والملاحظ أن خصوصية المسكن لا تقتصر على صاحبه، بل تمتد لتشمل جميع المقيمين معه في مسكنه سواء كانوا أفراد أسرته، أو خدمه، أو ضيوفه، ولا فرق في هذا الشأن بين مواطنين وأجانب.

أما عن فكرة المكان الخاص*، فهي أعم وأشمل من فكرة المسكن وهذا ما يبدو جليا من خلال ما ذهب إليه الفقه في تعريف المكان الخاص على أساس أنه كل مكان مغلق أو محدد عن المجال الخارجي الذي يحيط به، ولا يسمح للخارجين عنه بالدخول إليه إلا بإذن مالكه، أو من يستعمله لمزاولة نشاط معين من أنشطته الفردية لغرض الإنتفاع به[1]، أو كما عرفه الفقيه سافيني بأنه المكان الذي يستخدم كإطار للحياة الخاصة وليس من حق الغير أن يدخله دون رضا صاحبه، أو هو المكان المغلق الذي لا يسمح للغير بدخوله أو يتوقف دخوله على إذن صادر ممن يملكه أو ممن له الحق في استعماله أو الانتفاع به،[2] وهذا كنتيجة لتعدد أوجه الأنشطة التي يمارسها الإنسان في العصر الحالي والتي لا تمارس كلها في المساكن، فالمسكن لا تمارس فيه سوى تلك الأمور المتعلقة بالحياة الخاصة، ومن هنا تدعو الحاجة إلى حماية تلك الأنشطة الأخرى في كل مكان تمارس فيه والتي لم تعد تقتصر على المسكن بمفهومه الضيق[3]، وحماية المشرع للمكان الخاص تمتد لتشمل كل من يمكث فيه بصرف النظر عما إذا كان هذا الشخص مالكا أو مستأجرا أو زائرا أو موجودا فيه بصورة عرضية.

ومن هنا يبدو أن تحديد ماهية المكان الخاص أمر لا يخلو من بعض الصعوبات، فقد تم تعريفه أيضا أنه المكان المغلق الذي لا يمكن أن تتسرب إليه نظرات الناس من الخارج، أو أن يلجه الغير دون الحصول على إذن صاحبه، كمااعتبر أيضا المكان الخاص بأنه كل مكان لا تنسحب عليه صفة العموم، لأجل هذا ذهب بعض الفقهاء إلى تعريفه انطلاقا من تحديد وتوضيح المقصود بالمكان العام، ويقصد بالمكان العام كل مكان يسهل ارتياده من قبل الجمهور، و هو ينقسم إلى ثلاث أنواع: الأماكن العامة بطبيعتها وهي الأماكن التي يرتادها الجمهور بحرية وقد أعدت لذلك منذ إنشائها مثل الميادين والشوارع والحدائق العمومية... الأماكن العامة بالتخصيص وهي الأ ماكن التي يرتادها الجمهور في أوقات محددة، وتعتبر هذه الأماكن عامة فقط خلال الأوقات التي يسمح فيها للجمهور بارتيادها وتعد أماكن خاصة فيما عدا هذه الأوقات مثل دور السينما ودور العبادة... ثم الأماكن العامة بالمصادفة وهي أماكن خاصة بأصلها ويكون أمر ارتيادها مقصورا على أفراد أو طوائف معينة، إلا أنه يباح للجمهور ارتيادها بصفة عارضة.

2) **حرمـة جسم الإنسان:** تعتبر حرمة جسم الإنسان وسلامته من أهم الحقوق التي يتمتع بها الفرد، ولم يتفق الفقه القانوني سواء المدني أو الجنائي على تعريف محدد ومنضبط للحق في سلامة جسم الإنسان،

---

https://ahmedazimelgamel.blogspot.com/p/blog-page_26.html اطلع عليه يوم : 2020/01/20

* لقد انقسم الفقه إلى اتجاهين: الأول يرى أن مفهوم السكن يشمل المكان الخاص، باعتبار أن الحماية القانونية لا تقتصر على المسكن بل تشمل كل مكان خاص وحرمة السكن بمدلوله الواسع تتوقف على استمرار حالة الخصوصية. في حين يذهب الاتجاه الثاني إلى أن المكان الخاص لا يدخل في مفهوم المسكن فإذا كان المسكن مكانا خاصا فليس كل مكان خاص مسكنا.

[1] حامد راشد، الحماية الجنائية للحق في حرمة السكن، دراسة مقارنة، رسالة دكتوراه كليه الحقوق جامعة القاهرة 1987، ص131.

[2] مصطفى مجدي هرجة، جرائم السب القذف والبلاغ الكاذب، المكتبة القانونية للنشر والتوزيع، الطبعة الثالثة دون بلد النشر، دون تاريخ النشر ص110.

[3] علي أحمد الزعبي، مرجع سابق، ص 174.

فسادت اتجاهات مختلفة حول مضمون وجوهر هذا الحق[1]، والواقع أن تفسير هذا التفاوت في الإهتمام بهذه المسألة بين الفقه الجنائي والفقه المدني مرده إلى أن الكيان المادي للإنسان لم يكن مثارا لاهتمام القواعد التنظيمية في القانون المدني، باعتباره قانون الأموال والمعاملات، كما أن مناقشتهم لمضمون الحق في سلامة الجسد يكون باعتباره إحدى الصور البارزة لطائفة الحقوق اللصيقة بالشخصية*، وبالتالي فإنه يخضع للقواعد العامة التي تحكم هذه الأخيرة[2]، أما عند إرجاء المسألة إلى الفقه الجنائي فنجدها قد استأثرت باهتمام كبير ودراسة مسهبة على اعتبار أن الحق في سلامة جسم الإنسان يعد الركن المادي في جرائم الإعتداء على الأشخاص[3]، وقد اختلفت آراء الفقه في معرفة ما إذا كانت حرمة جسم الإنسان تدخل في نطاق الحق في الخصوصية أم لا إلى اتجاهين:

الإتجاه الأول يرى أن حرمة جسم الإنسان ليست من عناصر الحق في الخصوصية على أساس أن سلامة الجسم وحق الخصوصية هما مظهران من مظاهر الحرية الفردية، بالإضافة إلى أن سلامة جسم الإنسان تستهدف المحافظة على الحياة ذاتها، في حين أن حماية الحق في الخصوصية لا يحمي إلا جانبا من جوانب الحياة فقط، ومن ثم فحسب هذا الإتجاه أن ما يقوله البعض من أن حرمة جسم الإنسان تدخل في نطاق الحق في الخصوصية أمر ينطوي على خلط بين الحرية الفردية بصفة عامة والحق في الخصوصية.[4]

في حين يرى أنصار الإتجاه الثاني أن حرمة جسم الإنسان يعد من صميم عناصر الحق في الخصوصية، وهو الاتجاه الذي أخذت به قرارات مؤتمر البلدان الإسكندنافية المنعقدة في 15 ماي 1967، وكذلك الندوة الدولية للإتفاقية الأوروبية الخاصة بحقوق الإنسان المنعقدة في بروكسل عام 1970[5]، ويذهب العديد من فقهاء هذا الإتجاه إلى اعتبار أن المساس بحق الإنسان في خصوصيته من خلال الإعتداء على جسمه لا يعني الإعتداء على الكيان المادي للشخص فقط، بل على حياته الخاصة من خلال جسمه، مثل إخضاع الشخص لفحوصات طبية أو نفسية دون موافقته*، أو إجراء أي تفتيش على جسم الإنسان من شأنه المساس بخصوصيته.

---

[1] حبيبة سيف سالم الراشدي، النظام القانوني لحماية جسم الانسان، رسالة لنيل درجة الدكتوراه كلية الحقوق جامعة عين شمس، قسم القانون المدني، سنة 2005، ص 25.

* نص القانون الفرنسي رقم 94/653 المتعلق باحترام جسم الانسان الصادر في 29 جويلية 1994 صراحة على عدم جواز اعتبار حق الإنسان على جسمه حقا ماليا حيث تنص المادة 1/16 على أنه لا يجوز أن يكون الجسم البشري محلا لحق مالي Loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain) disponible sur le site www.legifrance.gouv.fr

[2] محمود نجيب حسني، الحق في سلامة الجسم ومدى الحماية التي يكفلها له قانون العقوبات، مجلة القانون والاقتصاد، العدد الثالث، السنة التاسعة والعشرون، سبتمبر1959 رقم 6 -7 ص 542.

[3] فتوح عبد الله الشاذلي، جرائم الاعتداء على الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية 2002، ص132.

[4] ممدوح خليل بحر، مرجع سابق، ص263.

[5] ممدوح خليل بحر، مرجع نفسه، ص263.

* تنص المادة 44 من المرسوم التنفيذي رقم 276/92 المؤرخ في 1992/07/06 جريدة رسمية عدد 52 سنة 92 المتضمن مدونة أخلاقيات الطب.
Décret exécutif N°92-276 du 06-07-1992 portant sur le Code de Déontologie Médical

على أنه يخضع كل عمل طبي فيه خطر جدي على المريض، لموافقة المريض موافقة حرة ومتبصرة..."

ثانيا: عناصر الخصوصية المتعلقة بالكيان المعنوي للإنسان:

إن المنطق الأساسي الذي يركن إليه في بيان معنى الخصوصية المتصل بمفهومها المعنوي يرتبط ارتباطا وثيقا في فهم طبيعة الإنسان نفسه، فالقانون في حمايته لحق الإنسان في خصوصيته يجب أن يمتد ليشمل في نطاقه جميع شؤونه سواء كانت مادية محسوسة أم معنوية غير مدركة للغير.[1]

وقد أوضحت الحياة المدنية للإنسان أن جوانبها المادية لا تشكل سوى جزء من أسباب الألم والفرح التي تمر بالإنسان، لذلك فإن أمورا أخرى كالأفكار، والمحادثات والأحاسيس والمشاعر تستلزم اعترافا وحماية قانونيتين، وهو الأمر الذي استقر عليه قضاء المحكمة الاتحادية العليا في الولايات المتحدة الامريكية في قضية أدت إلى تغيير الفهم المادي لمعنى الخصوصية، وذلك حينما قررت في هذه القضية أن التعديل الرابع للدستور الأمريكي يحمي الخصوصية بمعنى السرية وليس فقط حماية الخصوصية ضد الانتهاكات المادية، وقد تبعه قرار آخر عندما فصلت ذات المحكمة عام 1967 في قضية katzv. united states أين تجاوزت فيه المعنى المادي للخصوصية المحمية بالتعديل الرابع، ليصل إلى معنى جديد يحمي حالة الخصوصية بحد ذاتها، أي بمعنى الإنعزالية*، ومن هذا المنطلق ذهب الفقه إلى توضيح هذا المعنى للخصوصية من خلال إعطاء أمثلة عن ذلك، مقررا أن الحق في الخصوصية المعنوية يكون بارزا عندما يكون هدف المعتدي ملاحقة ملفات الأشخاص المرضية أو الوظيفية أو محادثاتهم الهاتفية... وفي جميع الحالات التي يكون فيها انتهاك للخصوصية بمعنى السرية والانعزالية.

ويمكن بيان أهم تلك العناصر التي تدخل في إطار الخصوصية بمفهومها المعنوي وهي الحياة العاطفية والزوجية والعائلية، الحالة الصحية والرعاية الطبية، المحادثات الهاتفية والمراسلات الالكترونية، الذمة المالية، الآراء السياسية والمعتقدات الدينية، رقم هاتف الإنسان وبريده الالكتروني، إسمه وصورته وحياته الوظيفية والمهنية، وهي عناصر ليست جامعة لكل جوانب الخصوصية ببعدها المعنوي وليست مانعة من دخول غيرها فيها، كما أنها ليست جميعها محل اتفاق من جانب الفقه والقضاء،[2] ولعل هذا ما جعل القضاء الأمريكي يقيم معيارا موضوعيا بناء عليه ووفقا له تتحدد حالة الخصوصية للفرد بغض النظر عن المكان الذي يتواجد فيه، وهذا المعيار هو "توقع الإنسان بأنه فيما يقوم به من أعمال إنما تحيطه خصوصية بنيت على أسباب معقولة، وقياس هذا التوقع ومدى توافره يتم وفق معيار الرجل العادي، وسوف نحاول أن نتطرق لأهم هذه العناصر كما يلي:

1) **الحق في الصورة:** تعد الصورة عبارة عن تصوير لشخص في موقف معين ودائما تمثل صاحبها، وبالتالي يكون لصاحب الصورة وحده الحق في الاستئثار بنشرها أو توزيعها بحسب رغبته الشخصية، وهو

[1] عبد المحاسن المقاطع، مرجع سابق، ص18.

* في هذه القضية قررت المحكمة بأن المقصود بالحماية التي قررها التعديل الرابع للدستور الأمريكي ليست للمكان فقط وإنما هي حماية الأشخاص، وعليه فإن أي تجسس على ما يحاول الشخص أن يجعله من خصوصياته وأسراره، يعتبر انتهاكا لحقه في الخصوصية، وإن حدث مثل هذا التجسس (التنصت) في مكان عام فلا محل للاحتجاج هنا بحرمة المكان أو الانتهاك المادي وذلك لحرمة خصوصية الأشخاص أنفسهم باعتبارها أمورا لصيقة بذواتهم. أنظر: عبد المحسن المقاطع، مرجع سابق، ص20.

[2] عبد الرؤوف المهدي، الجوانب الإجرائية لحماية الحق في الحياة الخاصة، بحث مقدم إلى مؤتمر الحق في الحياة الخاصة، المنعقد بكلية الحقوق جامعة الإسكندرية 1987 ص36.

الذي يقدر ويقرر مدى ملائمة نشر الصورة أو توزيعها من عدمه، حتى ولو كان شخص آخر (رسام أو مصور) هو الذي التقط له هذه الصورة.[1]

كما تعد الصورة انعكاسا لشخصية الإنسان في مظهرها المعنوي لأنها تعكس مشاعره وأحاسيسه ورغباته، فهي المرآة المعبرة في كثير من الأحيان عما يخفيه الإنسان بداخله[2]، وعليه ترتبط الصورة بشخص الإنسان ارتباطا وثيقا، وقد عرفت الصورة أيضا بأنها ذلك التجسيد الحقيقي لمشاعر الإنسان وأحاسيسه، حيث تظهر بصمات الأحداث التي يمر بها على ملامح وجهه، وهو ما يفسر الارتباط الوثيق بين الإنسان وصورته[3]، لذلك تكمن أهميتها في القيمة المعنوية التي تتمتع بها في تحديد هوية الأشخاص والكشف عنهم ومن هنا تأتي قيمتها وضرورة حمايتها.

وعلى هذا الاساس فقد نادى الفقه بضرورة تدخل التشريعات وكذلك القضاء لحماية صورة الإنسان، وبناء على ذلك ظهرت فكرة الحق في الصورة، فقد قررت أغلب التشريعات اعتبار الحق في الصورة من ضمن الحقوق الملازمة للشخصية، وأن حمايته تندرج ضمن الحماية المقررة لحماية الكيان المعنوي للإنسان، لذلك فقد استقر القضاء الفرنسي على أن للإنسان حق على صورته، وأن هذا الحق ليس حقا في الملكية لأن الإنسان ليس مجرد شيء يباع ويشترى، ولا يمكن أن يكون محلا لأحد الحقوق العينية، فصورة الإنسان لا يمكن أن تنشئ له غير حق من حقوق الشخصية التي يتمتع بها، ورغم اختلاف الفقه نوعا ما حول أسس تبرير حماية هذا الحق، هل على أساس الملكية، أم على أساس حماية الشخصية، إلا أن التحليل الذي بات كلاسيكيا يفضل تأسيس الحق في الصورة على أساس أنه حق من حقوق الشخصية.[4]

ويقصد بالحق في الصورة سلطة الشخص في الإعتراض على أن تؤخذ له صورة أو أن يرسم له رسم بغير موافقته الصريحة أو الضمنية،وكذلك حقه في الإعتراض على نشر صورته أو توزيعها على الجمهور[5]، ومن ثمة فإن هذا الحق يخول صاحبه سلطة الإعتراض على التقاط صورة له وعلى عرضها، وكذا سلطة عتراض على نشرها، وأن أي اعتداء على أي من هذه الأمور يعد مساسا بالكيان المعنوي للإنسان، ويترتب على ذلك امتناع الكافة بالتصرف أو الإستغلال أو النشر أو الإستعمال للصورة دون إذن صاحبها.

وما يهمنا في هذه المسألة هو الإشكالية القانونية التي طرحت بخصوص الإرتباط الوثيق للحق في الصورة بالحق في الخصوصية، فهل يعد حق الإنسان في صورته مظهرا من مظاهر الحق في الخصوصية أو عنصرا من عناصره أم أنه حق مستقل بذاته؟

---

[1] نبيل فزيع فرج، الحماية الجنائية للحق في الصورة في القانون المصري، رسالة للحصول على درجة ماجستير في الحقوق، جامعة القاهرة، الدراسات العليا 2015-2016 ص32.

[2] أحمد عبد الزعبي، مرجع سابق، ص176.

[3] محمد حسناوي شويع، جعفر كاظم جبر الوزاني ونعيم كاظم جبر الوزاني، نحو نظام قانوني لمسؤولية الصحفي المدنية عن عرض صور ضحايا الجريمة، مجلة مركز دراسات الكوفة، جامعة الكوفة، العراق العدد 07 سنة 2008، ص206.

[4] Malaurie Philippe et Laurent Aynés, Droit des personnes La protection des mineurs et des majeurs, L.G.D.J 10e édition 08/2018, p122.

[5] جلال علي العدوي، رمضان أبو السعود، الحقوق وغيرها من المراكز القانونية، منشأة المعارف، الإسكندرية 1996ص342.

لقد انقسم الفقه حول مدى اعتبار الحق في الصورة عنصرا من عناصر الحق في الخصوصية إلى ثلاث اتجاهات:

الإتجاه الأول: يرى أنصاره أن الحق في الصورة يعتبر أحد مظاهر الحق في الخصوصية، فصورة الشخص ليست سوى أحد مقومات خصوصيته وأكثر العناصر قدسية[1]، على أساس أن التقاط صورة للشخص معناه أخذ جزء من ذاته[2]، وبالتالي فإن الاعتداء على صورة الشخص يعد اعتداء على خصوصيته، باعتبارها مظهرا من مظاهر الخصوصية شأنها في ذلك شأن حياته العاطفية أو العائلية، فالفعل الواحد من أفعال الإ عتداء يشكل مساسا بالحق في الصورة وبالحق في الخصوصية في آن واحد.[3]

وقد ذهب بعض الفقهاء الذين حاولوا تعريف الحق في الخصوصية عن طريق تعداد الحالات التي تعد من قبيل هذا الحق، عندما ذكروا أن الحق في الصورة يمثل واحدا من العناصر المكونة للحق في الخصوصية[4]، وفي ذلك يقول كايزر: "أن الحق في الصورة يستهدف دائما حماية الحق في الحياة الخاصة، ليس فقط إذا تعلقت الصورة بهذه الحياة وإنما أيضا في الحالة التي ترسم الصورة فيها ملامح الشخص نظرا لأن هذه الملامح هي التي تكشف عن شخصية المرء.[5]

كما أكد أنصار هذا الإتجاه بالقول أن انتهاك الحق في الصورة ينطوي غالبا على إخلال بحرمة الحق في الخصوصية، بل إن الاعتداء على الحق في الصورة هو الذي يعطي المساس بالحق في الخصوصية صفة عتداء الفاضح الذي لا يمكن التسامح فيه.[6]

وقد استدل أصحاب هذا الرأي بقضية الممثلة الشهيرة "بريجيب باردو" والتي كان قد تم تصويرها عن بعد عن طريق آلة تصوير مقربة وهي شبه عارية بحديقة منزلها، أين قضي بأن مثل هذا التصوير يعد اعتداء على خصوصيتها.[7]

لذلك فإنه وحسب هذا الإتجاه يعد الحق في الصورة واحدا من مظاهر الحياة الخاصة، وأن الشخص يستطيع استنادا إلى حقه في احترام خصوصيته أن يرفع دعوى ضد من يلتقط صورته أو ينشرها دون رضاه.[8]

---

[1]. Cécile DESCHANEL .LE DROIT PATRIMONIAL À L'IMAGE. ÉMERGENCE D'UN NOUVEAU DROIT VOISIN DU DROIT D'AUTEUR. Thèse de doctorat en droit privé. ACADÉMIE AIX-MARSEILLE UNIVERSITÉ D'AVIGNON ET DES PAYS DE VAUCLUSE. Faculté de droit .Décembre 2017, P37.

[2] محمد الشهاوي، مرجع سابق، ص202.

[3] مصطفى أحمد حجازي، مرجع سابق، ص82.

[4] خليل بحر، مرجع سابق، ص271.

[5] Irma ARNOUX, les droits de l être humain sur son corps et les droits de la personnalité. Presse universitaire de Bordeaux. Pessac 2003p165

[6]. Raymond Lindon, La création prétorienne en matière de droits de la personnalité et son incidence sur la notion de famille. In: Revue internationale de droit comparé. Vol. 27 N°1, Janvier-mars 1975. pp. 283-286 ; https://www.persee.fr/doc/ridc_0035-3337_1975_num_27_1_16342

[7] اندريه برتران، نيكولا فتوش، الحق في الحياة الخاصة والحق في الصورة، المنشورات الحقوقية، صادر، الطبعة الأولى، دون سنة النشر، ص 206.

[8] محمود عبد الرحمن محمود، مرجع سابق، ص233.

وقد تبنى المشرع الجزائري هذا الاتجاه من خلال نص المادة 303 مكرر من قانون العقوبات التي جاءت عباراتها صريحة عندما اعتبرت أن من يقوم بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص* بغير إذن صاحبها أو رضاه يعد مساسا بحرمة الحياة الخاصة أو الحق في الخصوصية، ومن ثم فإن المشرع الجزائري صنف الحق في الصورة ضمن عناصر الحق في الخصوصية، واعتبر أن القيام بفعل الإلتقاط أو التسجيل أو النقل لصورة الإنسان من الأفعال الماسة بالحق في الخصوصية.

وكذلك المشرع الفرنسي قد جرم بنص المادة 226-1 من قانون العقوبات الجديد لسنة 1992 كل من يتعدى عمدا على الحياة الخاصة للآخرين، وذلك عن طريق تسجيل أو نقل بأي جهاز صورة شخص آخر أخذت في مكان خاص ودون رضاه،[1]

والمشرع المصري هو أيضا يعترف بحق الإنسان في صورته ويعتبره من عناصر الحق في الخصوصية، حيث تنص المادة 309 من قانون العقوبات المصري على أنه يعاقب كل من اعتدى على حرمة الحياة الخاصة (الخصوصية) للمواطنين وذلك بأن ارتكب أحد الأفعال التالية في غير الأحوال المصرح بها قانونا أو بغير رضا المجني عليه: –التقط أو نقل بجهاز من الأجهز ة أي كان نوعها صورة شخص في مكان خاص".

ولقد اعترف القضاء في كثير من القضايا بالحق في الخصوصية استنادا على الحق في الصورة، فالقضاء الفرنسي مثلا أدان إحدى الصحف الفرنسية على خلفية التقاطها صورا لإحدى الممثلات وهي على فراش الموت، وقرر عدم جواز ذلك لأنه يعد من قبيل المساس بحياتها الخاصة[2]، وكذلك القضاء الأمريكي عندما اعتبرت محاكم نيويورك أن ما قام به أحد المصورين من التقاط لصور ممثلة وهي على خشبة المسرح بألبسة خفيفة يعد اعتداء على الحق في الحياة الخاصة، ومنعته من نشر هذه الصور.

وتعتبر المحكمة العليا في الجزائر أن الإشهار بالصورة في غياب الموافقة الصريحة والمكتوبة يعد مساسا بحق من الحقوق الملازمة للشخصية.

---

* إن المشرع الجزائري لا يحمي حق الشخص في الصورة إلا إذا كان موجودا في مكان خاص، وهو ما ورد بنص المادة 303 مكرر، فيفترض أن صورة المجني عليه قد التقطت أو نقلت وهو في مكان خاص، أي أن يكون المجني عليه في حالة خصوصية وفي وضع يلتزم فيه قدرا من الخلوة والبعد عن الناس، ويبدو أن نص 303 مكرر مأخوذ نصها من نص المادة 226 قانون العقوبات الفرنسي الجديد الصادر بموجب قانون 1992 الذي ألغى المادة 368 من قانون 1970، والتي كانت تشترط أن يتم التصنت ونقل الحديث وكذا الصورة عندما يكون المجني عليه متواجد في مكان خاص. ولما صدر قانون 1992 ألغى شرط المكان الخاص بالنسبة للحديث، في حين ظل الشرط قائما بالنسبة للصورة، ولعل ما يعزز اعتقادنا في اشتراط المشرع لفكرة المكان الخاص إذا تعلق الأمر بالتقاط الصور وتخليه عنها في التقاط الأحاديث هو ما ورد في نص المادة 65 مكرر 5 من ق ا ج التي تسمح باتخاذ الترتيبات التقنية بعد إذن الجهات القضائية المختصة من أجل التقاط وتثبيت وتسجيل الكلام المتفوه به من طرف شخص أو عدة أشخاص بصفة سرية ودون موافقتهم يتواجدون في أماكن خاصة أو عمومية، بينما هذه الترتيبات يمكن اتخاذها بعد إذن الجهات القضائية المختصة من أجل التقاط صور مع شخص أو عدة أشخاص عندما يتواجدون في مكان خاص، وهو ما يبدو كذلك جليا في نص المادة 06 من المرسوم 208/15 المؤرخ في 22 أوت 2015 الذي يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره، التي تؤكد صراحة أن تنصيب كاميرات المراقبة في الأماكن العامة والمفتوحة للجمهور لا يخضع لرخصة إدارية مسبقة.

[1] Artcle 226-1 "Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé".

[2] اندريه برتران، نيكولا فتوش، مرجع سابق، ص232.

أما الاتجاه الثاني فيرى عكس ذلك، حيث يذهب أنصاره إلى أن الحق في الصورة هو حق مستقل ومتميز عن الحق في الخصوصية وليس عنصرا من عناصره، فهو إن كان من الحقوق اللصيقة بالشخصية، إلا أنه منفصل عن الحق في الخصوصية، حيث صرح الفقيه برنار بارنيه أن الاجتهاد يعترف اليوم بوجود "الحق في الصورة" وبتمتعه باستقلالية تامة ضمن إطار الحقوق الشخصية[1]، فحسب هذا الاتجاه إذا ما التقطت صورة لشخص ما وتم نشرها بشكل يسيء له ويقلل من وضعه، اعتبر ذلك اعتداء على حقه في الصورة، وليس اعتداء على حقه في الخصوصية، فهذا الحق الأخير لا يلحقه أي ضرر من التقاط الصورة[2]، ولذلك يجب عدم الخلط بينهما، بل وقد ذهب بعض الفقهاء من أنصار هذا الاتجاه إلى القول بأنه لا يوجد أي علاقة بين الحق في الصورة والحق في الخصوصية، على أساس أن نشر صورة شخص ما يمكن أن يكون محلا للمجازاة حتى ولو لم تكن هذه الصورة قد أخذت أثناء ممارسته لحياته الخاصة، ويكون الجزاء حينئذ أساسه هو انتهاك الحق في الصورة وليس الإعتداء على الحق في الخصوصية، لأن هذا الأخير لم يلحقه أي أذى في هذه الحالة[3]، وإذا كان الإعتداء على الحق في الصورة يصاحبه غالبا اعتداء على الحق في الخصوصية، فإن ذلك لا يعني أبدا الخلط بين الحقين، بل إن للإنسان الإعتراض على تصويره حتى ولو كان ذلك لا يمثل اعتداء على خصوصيته، بمعنى أن هذا الحق يخول للشخص سلطة الإعتراض على تصويره ليس فقط أثناء ممارسته لحياته الخاصة، بل أيضا أثناء ممارسته لحياته العامة، بل ويخوله هذا الحق سلطة الإعتراض على نشر صورته حتى ولو كان هذا النشر لا يمثل أي اعتداء على حياته الخاصة.[4]

كما وقد ذهب جانب من أنصار هذا الاتجاه لتبرير هذا الموقف أن التقاط صورة لشخص في مكان عام يشكل مساسا بالحق في الصورة وليس اعتداء على الخصوصية التي لا تتوفر في المكان العام، وقد أخذ بهذه الفكرة القضاء الفرنسي عندما قضى بعدم مشروعية التقاط صورة ونشرها لإحدى السيدات أثناء اشتراكها في مظاهرة في الطريق العام، كون تلك الصورة تظهر المرأة بشكل متميز عن المنظر العام الذي التقطت فيه، واعتبر الحكم القضائي في هذه القضية أن المصور قد أتى عملا غير مشروع يعد بمثابة انتهاك للحق في الصورة، لذلك فقد قيل بأن تصوير الشخص أثناء ممارسته حياته العامة جائز على أساس توافر رضاه المفترض، ولا يعني ذلك أن استعمال الصورة التي التقطت له في مثل هذه الظروف مباح في جميع الأحوال، إذ يجب أن يكون هذا الاستعمال في حدود الرضا المفترض فإن جاوز الاستعمال هذه الحدود، كان اعتداء على حقه في الصورة، وليس على حقه في الخصوصية.[5]

فضلا عن ذلك فإن الشخص قد لا يستطيع أن يدفع بوقوع اعتداء على خصوصيته لمجرد نشر واستخدام صورته، فالصورة التي تؤخذ لشخص ما بصفة عرضية دون علمه ودون قصد المصور إذ

---

[1] Beignier Bernard, Le droit de la personnalité, coll « que sais je » n°2703. Presses Universitaires de France - PUF 1992. P 62

[2] Nerson Roger, distinction du droit à l'image et du droit au respet de la vie privée, revue. tim. Droit. Civil 1971 p364.

[3] ممدوح خليل بحر، مرجع سابق، ص272.

[4] محمود عبد الرحمن محمد، مرجع سابق، ص 234.

[5] Nerson Roger. La protection de la vie privée en droit positif français, In: Revue internationale de droit comparé. Vol. 23 N°4, Octobre-décembre 1971. pp. 737-764, https://www.persee.fr/doc/ridc_0035-3337_1971_num_23_4_16099

يكون ذلك الشخص جزءا من الموضوع المراد تصويره، ففي هذه الحالة لا يشترط الإذن ولا يعتبر المصور قد انتهك حق الخصوصية، فالصورة المأخوذة في مكان عام والتي تكون متعلقة بالحياة العامة للشخص لا تنطوي على اعتداء على الحق في الخصوصية.[1]

و يرى البعض من أنصار هذا الاتجاه أن الحق في الصورة يحمي العنصر المادي من الشخصية،[2] في حين يحمي الحق في الخصوصية العنصر المعنوي منها[3]، لكن قوبل هذا التبرير بعدم القبول لدى الفقه القانوني ذلك أن الحق في الصورة هو أيضا يحمي الكيان المعنوي للإنسان*، مضيفا بعضهم أيضا فرقا آخر بين الحق في الصورة والحق في الخصوصية يجعل من الأول مستقلا عن الثاني وهو أن الحق في الصورة له طابع مالي ينتقل إلى الورثة خاصة بالنسبة للشخصيات العامة، مثلما ذهب إليه القضاء الفرنسي في قضية اللاعب المشهور إيريك كونتونا، حيث اعتبرت المحكمة أن له حقا استئثاريا على صورته ولا يمكن استنساخها وبيعها دون إذنه[4]، بينما الحق في الخصوصية يعد من الحقوق اللصيقة بالشخصية.

ويرى اتجاه ثالث إلى أن للحق في الصورة طبيعة مزدوجة، فقد يكون أحيانا حقا قائما بذاته ومستقلا عن الحق في الخصوصية، وقد يكون في أحيان أخرى عنصرا من عناصرها[5]، فمتى تعلقت الصورة الملتقطة للشخص بحالته العائلية أو الصحية أو العاطفية وتم التقاطها في مكان خاص دون موافقته أو رضاه بنشرها اعتبر ذلك مساسا بالحق في الخصوصية، ويكون هو أساس عدم المشروعية في هذه الحالة، أما إذا تم التقاط ونشر صورة لشخص في مكان عام علنيا دون أي مساس بإحدى جوانب حياته الخاصة ولكن كان ذلك دون إذنه ولا موافقته اعتبر ذلك مساسا بالحق في الصورة بصفته حقا مستقلا بذاته، ومن ثم الإستناد إلى هذا الحق لتوفير الحماية المنشودة في هذا الشأن[6]، ويبدو أن أنصار هذا الاتجاه بهذا الموقف يريدون إسباغ حماية فعالة على الحق في الصورة،فإذا كان صحيحا القول بأن الإعتداء على الصورة بالتقاطها أو نشرها غالبا ما يستتبع الإعتداء على الحق في الخصوصية لصاحب الصورة، فإن الواقع يدلنا على أن الشخص قد لا يستطيع الإدعاء بوقوع اعتداء على حقه في الخصوصية بالرغم من التقاط صورته أو نشرها دون إذنه، فلو لم يتم اعتبار أن الحق في الصورة حق مستقل لصيق بشخص صاحبه لما أمكن لهذا الأخير المطالبة بحماية القانون،لعدم استطاعته إثبات الإعتداء على حقه في الخصوصية.[7]

---

[1] اندريه برتران، نقولا فتوش مرجع سابق، ص 244.

[2] مصطفى أحمد عبد الجواد حجازي، مرجع سابق، ص90.

[3] حسام الدين الأهواني، مرجع سابق، ص165.

* اعتبر المشرع المصري في قانون حماية المؤلف رقم 354 لسنة 1954 المعدل بالقانون رقم 38 لسنة 1992 المنشور في الجريدة الرسمية العدد 23 لسنة 1992 أن الحق في الصورة حق من حقوق المؤلف وهو بذلك حق مستقل تماما عن الحق في الخصوصية.

[4] Tribunal de grande instance. Nantérre 1 ère chambre.civ.6 avril 1996. Gazette du Palais1995, p 285.

[5] مصطفى أحمدعبدالجواد حجازي، نفس المرجع، ص،92.

[6] Jacques Ravanas, la protection des personnes contre la réalisation et la publication de leurs images, Revue internationale de droit comparé, Vol. 31 N°1, Janvier-mars 1979. pp. 246-249.

[7] محمود عبد الرحمن محمد، مرجع سابق، ص، 237.

وهذا ما دفع الفقه الفرنسي مؤخرا بأن أصبح الحق في الصورة عنده يقترب أكثر من المقاربة الأمريكية التي تتضمن عنصرين منفصلين هما:

- الحق في الطمأنينة القريب جدا من الحق في الخصوصية right of privacy

- الحق في الشخصية الذي يحفظ لكل شخص حق استثمار صورته الخاصة تجاريا، وهو بالتالي شبيه بالحق في الإعلان.

ونستخلص مما سبق ذكره حقيقة الصلة الوثيقة بين الحق في الصورة والحق في الخصوصية، وأن المساس بالحق في الصورة غالبا ما يعد مساسا بالحق في الخصوصية بوصف الصورة مظهرا من مظاهر الحق في الخصوصية.

2)**الحق في سرية الإتصالات الخاصة والمكالمات الهاتفية الشخصية:** تعد سرية حديث المرء مع غيره من الأمور التي ترتبط بكيان الشخص، وذلك لما تتضمنه هذه الأحاديث من دقائق الأسرار وما تفصح به عما يلج في النفوس من خبايا، ففي هذه المحادثات يثق المتحدث بشخص المتحدث إليه ويطمئن إليه، فيطلق لنفسه العنان ويهمس إليه بخفاياه دون حرج أو خوف من سماع الغير، معتقدا أنه في مأمن من استراق السمع.

ومصطلح الإتصالات الخاصة يصلح لتغطية المحادثات المباشرة بين شخصين أو أكثر أيا كانت وسيلته،[1] كما يقصد بالاتصالات الشخصية المسموعة تلك المحادثات التي يمكن سماعها من قبل الغير سواء بالأذن أو باستعمال الأجهزة التقنية[2]، كما يقصد بها أيضا كل صوت له دلالة معينة صادر من شخص ما، أو متبادل بين شخصين أو أكثر أيا كانت اللغة المستعملة في ذلك، كما عرفت أيضا أنها كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار المترابطة، فإذا كان هذا الصوت فاقد الدلالة على أي تعبير كالهمهمة والصيحات فلا يعد حديثا، ومن ثم لا يصلح أن يكون موضوعا للحماية ضد التعدي على سرية الإتصالات الخاصة.[3]

ومن المستقر عليه لدى الفقه القانوني أن لكل إنسان الحق في التمتع بالحرية في إجراء أحاديث خاصة في وسائل الإتصال المختلفة، لذلك اعتبرت المحادثات التي تتم عبر الإتصالات الهاتفية وكذلك عبر الوسائل التي أفرزتها التكنولوجيا من وسائل تقنية حديثة للتواصل الكترونيا، من عناصر الحق في الخصوصية، نظرا لما يتم من خلالها من تبادل للمعلومات والأسرار والأفكار المتعلقة بأشخاص طرفي المكالمة أو الحديث

[1] محمود أحمد طه، التنصت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، دار الفكر والقانون للنشر والتوزيع، المنصورة مصر، 2018، ص21.

[2] محمد علي السالم عياد الحلبي، ضمانات الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن، الطبعة الأولى، منشورات ذات السلاسل 1986 الكويت، ص132.

[3] محمد زكي أبو عامر. "قانون العقوبات القسم الخاص"، دار المطبوعات الجامعية، الإسكندرية، مصر 1977، ص680.

دون حذر أو حيطة بعيدا عن شبهة التنصت وبمأمن من استراق السمع، ومن ثم كان لازما أن يتدخل المشرع الجنائي لإضفاء الحماية على هذه المكالمات حفاظا على خصوصية الأشخاص.[1]

وترتيبا على ذلك فإن المقصود بالحق في خصوصية الإتصالات هو حق الشخص في عدم الإعتداء على اتصالاته ومحادثاته الشخصية التي يجريها بواسطة استخدام جهاز الهاتف أو أي تقنية أخرى تمكنه من ذلك، سواء كان ذلك الإعتداء بالتنصت أو المراقبة أو التسجيل*، وذلك في غير الأحوال التي يجيزها القانون.[2]

لذا كان من الواجب كفالة حق الإنسان في المحافظة على أسراره وأحاديثه، لأنها أكثر الأمور ارتباطا بشخصيته، فالإحساس بالأمن الشخصي الذي يستولي على المرء وهو بصدد القيام باتصالات خاصة ومحادثات شخصية هو ضمان هام لممارسة الحق في الخصوصية، إذ ينبسط المتحدث مع الطرف الآخر ويبوح له بأسراره وهو في أتم الإطمئنان لعدم وجود دخيل يتنصت دون وجه حق على هذا الحديث الخاص.[3]

وقد ميز الفقه بين نوعين من المحادثات والإتصالات الخاصة، فإما أن تكون مباشرة وهي تلك المحادثات التي تتم بين الأفراد مباشرة أي دون وجود جهاز ناقل للحديث للطرف الآخر، وهذا النوع من المحادثات كما يعبر عنه بعض الفقهاء أنه لصيق بحرمة المسكن والمكان الخاص، وأن تسجيله يعد انتهاكا واعتداء على حق الفرد في خلوته[4]، أما النوع الثاني وهو المحادثات غير المباشرة، وهي التي يتم تبادلها عبر وسائل الإتصال الحديثة السلكية واللاسلكية.

ومن مجرد التنصت على هذه المحادثات والإتصلات يتحقق الإعتداء على الحق في الخصوصية دون حاجة إلى إقامة الدليل على أن المكالمة كانت تتضمن وقائع متصلة بالحياة الخاصة، وكذلك بصرف النظر تماما عن مكان المكالمة عاما أو خاصا[5]، لذلك فقد اتجه بعض الفقه إلى القول أن الشخص يتمتع بالحق في خصوصية محادثاته واتصالاته دون النظر إلى مضمونها وما إذا كانت تتضمن أسرارا بين طرفي المكالمة من عدمه، بل يتمتع الشخص بهذا الحق حتى ولو كانت المكالمة عادية ولم تتعرض لأية أمور شخصية

[1] محمد محمد الشهاوي، مرجع سابق، ص15.

* يعد التنصت والإلتقاط والتسجيل والنقل هي العناصر المكونة للركن المادي في جريمة المساس بخصوصية الاتصالات، فالتنصت هو الاستماع سرا بوسيلة أيا كان نوعها إلى كلام له صفة الخصوصية أو السرية صادر من شخص دون رضاه، والتقاط المكالمات أو الأحاديث هو الحصول على ما جرى من كلام بين الأشخاص أو ما تفوه به الفرد سرا ودون علم صاحب الشأن وبأي تقنية كانت، أما التسجيل فيعني حفظ الأحاديث على جهاز معد لذلك بقصد إعادة الاستماع إليه فيما بعد، أما النقل فيقصد به أن يتم نقل الحديث والمكالمة التي تم الإستماع إليها أو تسجيلها من المكان الذي تم فيه الإستماع أو التسجيل إلى مكان آخر غيره وذلك بأي تقنية كانت.

[2] سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، مذكرة لنيل شهادة الماجيستار، جامعة نايف العربية للعلوم الأمنية السعودية، كلية الدراسات العليا قسم العدالة الجنائية، 2005 ص225.

[3] عمار عباس الحسيني، التصوير المرئي والتسجيل الصوتي وحجيتهما في الاثبات الجنائي، دراسة مقارنة في التشريعات واجتهادات الفقه والقضاء الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، القاهرة،2017، ص280.

[4] ممدوح خليل بحر، مرجع سابق، ص283.

[5] حسام الدين كامل الأهواني، مرجع سابق، ص69.

تتعلق بحياته الخاصة أو عناصرها، كما لو كانت المكالمة لمجرد تبادل التهنئة بين طرفيها بشأن مناسبة دينية أو رسمية معينة.[1]

وإذا كانت مسألة المساس بخصوصية الإتصالات والمحادثات الشخصية مطروحة منذ زمن، فإنها تعود مجددا للطرح وبحدة بسبب التقدم التكنولوجي الذي أفرز تقنيات عالية لها القدرة على التصنت واستقطاب المحادثات عن بعد، فالتطور التقني الهائل في أجهزة التصنت على وسائل الإتصالات أدى إلى ازدياد احتمالات تهديد الحق في الخصوصية بالإعتداء على سرية المكالمات والإتصالات من خلال استراق السمع ورصد المكالمات وتسجيلها دون موافقة أصحابها، ومن ثمة أصبحت الأحاديث التي يجنح المرء إلى إحاطتها بالكتمان والسرية ولا يدلي بها إلا لمن ائتمنه ووثق به عارية و مكشوفة أمام قدرة تلك الأجهزة التقنية الحديثة على التقاطها وتسجيلها دون أن يشعر بها أحد.[2]

وهو الأمر الذي دفع المشرع إلى التدخل لكفالة الحماية لحق الشخص في خصوصية اتصالاته ومحادثاته الخاصة، وقد فعل ذلك المشرع الجزائري من خلال المادة 46 من الدستور التي جاء في مفهوم نصها بأن سرية الإتصالات الخاصة بكل أشكالها مضمونة، وأنه لا يجوز بأي شكل المساس بهذا الحق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم، و تكريسا لهذا النص الدستوري عمد المشرع الجزائري إلى إحاطة الإتصالات الشخصية والمحادثات الخاصة بأقوى صور الحماية القانونية وأكثرها فعالية وهي الحماية الجزائية، فقد نصت المادة 303 مكرر من قانون العقوبات[3] على أنه "يعاقب بالحبس والغرامة كل شخص تعمد القيام بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه"، وأضافت المادة 303 مكرر 01 من نفس القانون معاقبة كل شخص يحتفظ أو يضع في متناول الجمهور أو الغير أو يستخدم التسجيلات المتحصل عليها والمتعلقة بالمكالمات أو الأحاديث الخاصة أو السرية.

وبذلك يبدو جليا أنه إذا قام الغير باستراق السمع (الإلتقاط) أو بتسجيل المكالمات والأحاديث الخاصة أو إذا قام بنقلها إلى مكان آخر، كنا أمام انتهاك للحق في الخصوصية، والمقصود بالغير هنا من كان خارج طرفي الحديث أو المكالمة أيا كانت صفته شخصا عاديا أو موظفا.[4]

وفي التشريع المقارن نجد أن المشرع الفرنسي قد كان له السبق في إصدار تشريع خاص يستهدف توفير الحماية الجنائية لحق الإنسان في سرية اتصالاته الشخصية، وذلك من خلال النصوص المستحدثة بالقانون الصادر في 1970/07/17،[5] حيث أضاف المشرع الفرنسي 05 مواد إلى قانون العقوبات وهي المواد

[1] محمد نور الدين، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية – دراسة تحليلية نقدية للقانونين الكويتي والإماراتي- دراسات علوم الشريعة والقانون الجامعة الأردنية، المجلد 43، ملحق الرابع سنة 2016، ص 1689.

[2] أحمد فتحي سرور، مراقبة المكالمات التلفونية، المجلة الجنائية القومية مارس 1963، ص43.

[3] أنظر القانون رقم 23/06 المؤرخ في 2006/12/20 المعدل والمتمم للأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات.

[4] محمود أحمد طه، مرجع سابق، ص46.

[5] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens. Disponible sur le site :https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT

368 إلى 372 التي تعاقب على الاعتداءات الماسة بحرمة وسرية الإتصالات والأحاديث[1] دون رضا أصحابها حال تواجدهم في أماكن خاصة، لكن فريقا كبيرا من الفقه نحا باللائمة على المشرع الفرنسي حينما ربط حماية سرية وخصوصية الاتصالات بالمكان الخاص، إذ كان من الواجب عليه أن يحمي الأحاديث متى كانت لها السمة الشخصية دون التفات إلى طبيعة المكان الذي صدرت فيه.

وعلى إثر هذه الانتقادات التي أبداها الفقه ألغى المشرع الفرنسي هذا القانون بموجب قانون 1992 وتجاوز من خلاله فكرة المكان الخاص* عندما يتعلق الأمر بالأفعال الماسة بخصوصية وسرية الاتصالات، حيث نصت المادة 1/226 على معاقبة كل من يعتدي عمدا بأي وسيلة كانت على ألفة الحياة الخاصة للآخرين بالتصنت أو بالتسجيل أو بالنقل دون موافقة صاحب الشأن كلاما صادرا وله صفة الخصوصية والسرية.[2]

وفي التشريع الأمريكي نجده يعاقب طبقا لقانون مراقبة السيارات العامة وأمن الطرقات الصادر عام 1968 كل شخص يقوم بالتصنت عن عمد على أي اتصال شفهي أو تلفوني أو يكلف شخصا للقيام بذلك، بالإضافة إلى قانون الإتصالات الإتحادي الذي يجرم صراحة التصنت والتسجيل الخاص وعدم إباحته، كما أن قانون حرمة خصوصية الإتصالات الإلكترونية لعام 1986 مد الحماية للاتصالات الإلكترونية، حتى ولو لم تكن محمولة بواسطة موجات صوتية.[3]

والجدير بالذكر أن الحماية الجزائية الموضوعية من خلال تجريم أفعال التصنت أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية لا تكف في حد ذاتها لتوفير الحماية الجزائية الكافية التي من شأنها الحيلولة أو الحد من ظاهرة التعدي على الخصوصية، إذ لا بد من أن يتسع نطاق هذه الحماية لتشمل

[1] تنص المادة 368 من قانون العقوبات الفرنسي على أنه "يعاقب بالحبس من شهرين إلى سنة وبالغرامة أو بإحدى هاتين العقوبتين كل شخص يعتدي على حرمة الحياة الخاصة للغير، وذلك بأن يستمع أو يسجل أو ينقل بواسطة أحد الأجهزة أيا كانت نوعية المحادثات التي تمت في مكان خاص دون رضا المتحدث".

* لقد اقترح في الأعمال التحضيرية التي سبقت التصويت على قانون 1970/07/17 أن تستبدل فكرة المكان الخاص lieu privé بتعبير حالة الخصوصية « en privé » لكن قوبل هذا الاقتراح بالرفض، لذلك جرت المحاكم الفرنسية قبل تعديل قانون العقوبات في أحكامها على هذا المعنى، حينما اعتبرت محكمة باريس الكبرى في حكمها الصادر في 07 نوفمبر 1975 أنه يعد اعتداء على الحق في الحياة الخاصة التسجيل خلسة بجهاز تصنت وضع في إحدى الصيدليات للتجسس على إحدى العاملات فيها، وأعرضت المحكمة عن الدفع الذي تمسكت به صاحبة الصيدلية والذي مؤداه أن الصيدلية تعتبر في ساعات العمل مكانا عاما لا خاصا، مؤكدة (المحكمة) أن الجهاز الموضوع في الصيدلية يكون معدا للتسجيل ليس فقط أثناء افتتاح الصيدلية وإنما أيضا قبل افتتاحها للجمهور وبعد إغلاقها، كما أن الجهاز يسجل ليس فقط المحادثات التي تجرى في الصيدلية ولكن يسجل أيضا الأحاديث التي ينطق بها في الغرفة الخاصة للسكن وهذه تعتبر أماكن خاصة. كما يأخذ القانون الإنجليزي بفكرة المكان الخاص وذلك للتمييز بين المحادثات الخاصة والمحادثات العامة، كما ينبغي أن يكون المكان الخاص الذي يقع عليه الإعتداء مملوكا للشخص أو في حيازته، ذلك أن القانون الإنجليزي يعتبر أن انتهاك خصوصية المحادثات التي تتم في المكان الخاص هو انتهاك لخصوصية المكان ذاته. وقد أفضى هذا المذهب إلى تضييق الحماية الواجب توفيرها للحق في الخصوصية، فمن يزور شخصا في بيته لا يكون محلا للحماية من قبل المشرع الإنجليزي في هذه الحالة لأنه ليس بمالك ولا بحائز، فإذا تم التسجيل عليه وعلى صاحب المسكن فإن من يستفيد من الحماية هو فقط صاحب المسكن.

[2] Lartcle226-1/1dispose qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, Volontairement de porter atteinte à l'intimité de la vie privée d'autrui : 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titreprivé ou confidentiel

[3] محمود أحمد طه، مرجع سابق، ص68.

الحماية الإجرائية والتي من شأنها إجهاض أي نتيجة قانونية قد يتصور الجاني أنه بإمكانه الاستفادة من ذلك التعدي[1]، لأجل ذلك ثار جدل فقهي وكذا في القانون المقارن حول مشروعية مراقبة المحادثات الخاصة ومدى التعويل على الدليل المستمد منها بوصفه أداة إثبات في المسائل الجزائية.

ففي مقابل القاعدة العامة التي تقضي بعدم مشروعية التصنت على المحادثات الخاصة بكافة أشكالها وأنواعها، هناك استثناء على هذه القاعدة يقتضي إباحة التقاط وتسجيل المحادثات الشخصية وذلك بغية كشف الجرائم وضبط مرتكبيها[2]،وتكمن مبررات إقرار هذا الإستثناء في أن التجريم المطلق لهذه الأفعال من شأنه إعاقة السلطات في البحث عن الحقيقة، ومن ثم يتعذر عليها كشف الجريمة وضبط مرتكبيها وإنزال العقاب بالجناة، وذلك في إطار محاولة المواءمة بين مصلحة المجتمع في توقيع العقاب على الجاني ومصلحة الأفراد في المحافظة على مكنون أسرارهم وحقهم في سرية اتصالاتهم الشخصية، لذلك لا يجب المبالغة في احترام هذا الحق إذا كانت صيانته هذه من شأنها أن تؤدي إلى ضياع حقوق الغير المجني عليهم، أو من شأنها أن تتعارض مع مصلحة المجتمع في وقاية نفسه من الأخطار الكامنة في أشخاص ذوي خطورة إجرامية تؤدي إلى المساس بأمنه واستقراره.[3]

وقد أخذ المشرع الجزائري في قانون الإجراءات الجزائية هذه المسألة بالحسبان عندما نصت المادة 65 مكرر05 على جواز وضع ترتيبات تقنية من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة دون حاجة إلى موافقتهم، وذلك إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم معينة على سبيل الحصر وهي:

-جرائم المخدرات.

-الجرائم المنظمة العابرة للحدود الوطنية.

-الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

-جرائم تبييض الأموال.

جرائم الإرهاب.

-الجرائم المتعلقة بالتشريع الخاص بالصرف.

-جرائم الفساد.

ونعتقد أنه حتى مراقبة المحادثات الهاتفية التي تقررت إستثناء، تعد ذات خطر على الحق في الخصوصية، ذلك أنه فضلا عن كونها تتم دون علم الشخص المراقب وكذا تتبع وسماع وتسجيل أدق

[1] أسامة عبد الله قايد، حقوق وضمانات المشتبه فيه في مرحلة الاستدلالات دراسة مقارنة. دار النهضة العربية 1992. ص306.

[2] سعيد أمجد الزهاوي، التعسف في استعمال حق الملكية في الشريعة والقانون، دار الاتحاد العربي للطباعة، الطبعة الأولى القاهرة 1975، ص29.

[3] محمود أحمد طه. مرجع سابق، ص70.

أسرار حياته الخاصة التي يفضي بها بشكل تلقائي إلى من يتحدث معهم، فإنها أيضا تمتد إلى معرفة أسرار أشخاص آخرين أبرياء لمجرد اتصالهم عن طريق الهاتف بالشخص الموضوع تحت المراقبة.

ورغم ما تحمله المراقبة على المحادثات الشخصية من خطورة على الحق في الخصوصية فإن أغلب التشريعات المقارنة ذهبت إلى عدم إنكار دور هذا الإجراء وأهميته في إطار التحقيقات الإبتدائية والقضائية لمكافحة الجرائم خاصة الخطيرة منها، شريطة إحاطتها بمجموعة من الضمانات القانونية تفاديا للتعسف والمساس بخصوصية الأشخاص، وتحقيق التوازن بين حق الأفراد في حياتهم الخاصة وحق المجتمع في مكافحة الجريمة.

لأجل ذلك تتوقف إمكانية اللجوء إلى هذه الإجراءات والتي تعد في أصلها مساسا بخصوصية المكالمات والأحاديث الشخصية على ضرورة الإذن من الجهة القضائية المختصة، وهي إما وكيل الجمهورية أو قاضي التحقيق حسب الحالة لمدة أقصاها أربعة أشهر قابلة للتجديد مرة واحدة فقط لتفادي التعسف فيها.

أما في فرنسا فقد انشغل الفقه في وقت سابق بمدى مشروعية مراقبة المكالمات الهاتفية وتسجيلها في ظل غياب نص قانوني واضح، لذلك وعلى إثر الإنتقاد الموجه لفرنسا من طرف المحكمة الأوروبية لحقوق الإنسان حول عدم وجود قانون ينظم موضوع التصنت على المحادثات الشخصية والمكالمات الهاتفية، واعتبار ذلك يشكل خرقا للمادة 08 من الاتفاقية الأوروبية لحقوق الإنسان،[1] استجابت فرنسا من خلال إصدار القانون رقم 646/91 المؤرخ في 1991/07/10[2] والذي من خلاله يمكن إباحة التصنت على المحادثات والمكالمات الشخصية في حالتين:

1-التصنت القضائي بموجب أمر من قاضي التحقيق.

2-التصنت الإداري أو التصنت الأمني والذي تقتضيه ضرورات أمنية في إطار مكافحة التجسس والإرهاب.

3) الحق في خصوصية المراسلات: يقصد بالمراسلات كافة الرسائل المكتوبة سواء تلك المرسلة عن طريق البريد أو بواسطة شخص يقوم بنقل تلك الرسائل، كما ينصرف هذا المعنى أيضا إلى البرقيات[3]، وقد عرف البعض المراسلات بأنها الخطابات والطرود والبرقيات التي توجد لدى مكاتب البريد أيا كانت الطريقة التي ترسل بها، سواء كانت داخل مظروف مغلق أو مفتوح طالما أراد مرسلها عدم إطلاع غير المرسل إليه عليها.[4]

[1] Naut Pol, Chevallier Jean-Yves. II - Procédure pénale. In: Revue juridique de l'Ouest, 1994-3. pp. 407-410 ; https://www.persee.fr/doc/juro_0990-1027_1994_num_7_3_2168.

[2]. Loi n°91-646du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications Jorf n° 162 du 13 juillet 1991 page 9161.

[3] أحمد فتحي سرور، مرجع سابق، ص578.

[4] شريف بدوي. أسباب بطلان الضبط والتفتيش، دار الثقافة للطباعة والنشر، القاهرة 1989، ص260.

وقد عرف المشرع الجزائري المراسلات في قانون البريد والإتصالات الإلكترونية[1] بأنها "كل اتصال مجسد في شكل كتابي على دعامة مادية مهما كانت طبيعتها، يتم إيصاله وتسليمه إلى العنوان المبين من طرف المرسل نفسه أو بطلب منه".

ومن خلال هذا التعريف يبدو واضحا أن المشرع الجزائري قد انحاز إلى جانب الإتجاه الفقهي الذي تبنى معنى ضيقا في تعريفه للمراسلات، إذ قصرها على الرسائل المكتوبة دون سواها من المراسلات الأخرى التي يتم التخاطب فيها بوسائل شفهية.

وقد وجد هذا الاتجاه تأييدا في بعض الدساتير ومنها الدستور الجزائري والذي ورد في نص المادة 46 منه على أن سرية المراسلات مضمونة ولا يجوز المساس بها بأي شكل دون أمر من السلطة القضائية.

في حين ذهب اتجاه آخر من الفقه إلى تبني تعريف واسع للمراسلات، عندما وسع من نطاقها لتشمل كافة الرسائل المكتوبة وكذا الهاتفية[2]، فقد فسر البعض من الفقه المحادثات بوصفها رسائل شفوية وأن التنصتات الهاتفية هي نوع من الإ طلاع على الرسائل، لكن هذا الرأي قوبل بالنقد لافتقاره إلى الأساس السليم، إذ لا يمكن القول أن المكالمات الهاتفية تعد رسالة شأنها في ذلك شأن الخطابات المكتوبة، طالما أنها لا تتمتع بهذه الصفة المادية للمراسلات بل هي أقوال شفوية.[3]

لكن ما يجب الإشارة إليه أنه وفي ظل التطور التكنولوجي وما أفرزه من تقنيات حديثة أصبحت المراسلات الخاصة تتخذ أشكالا وأنواعا متعددة في العصر الحديث، إذ لم تعد تقتصر على المراسلات المكتوبة فقط ولم تقتصر وسائل إرسالها عبر البريد أو الفاكس فقط، بل أصبحت تأخذ شكلا إلكترونيا وترسل كذلك إلكترونيا، لذلك فقد أدرجها المشرع الجزائري ضمن مفهوم الإتصالات الإلكترونية، والتي يقصد بها حسبه أنها كل تراسل أو إرسال أو استقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.*

وعلى هذا الأساس قد تتخذ المراسلات شكلا إلكترونيا، حيث تكتب الرسالة بجهاز الكمبيوتر ثم تبعث إلى المرسل إليه عن طريق العنوان البريدي على شبكة الأنترنت، ويعرف هذا النوع من الرسائل بالبريد الالكتروني e-mail وقد تكون الرسائل بواسطة الهاتف الثابت، حيث يقوم المتصل في حالة عدم وجود من

[1] أنظر الفقرة 16 من المادة 09 من القانون 04/18 المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، جريدة رسمية العدد 27.

[2] عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، الجزء الأول، مطبعة المعارف بغداد، الطبعة الأولى 1974، ص350.

[3] حسن علي حسن السمني، شرعية الأدلة المستمدة من الوسائل العلمية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة 1983، ص411.

* أنظر المادة 10 من القانون 04/18 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. جريدة رسمية العدد 27 ، وكذلك المادة 02 من القانون 04/09 المؤرخ في 05 اوت 2009 جريدة رسمية عدد 47 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي عرفت الإتصالات الإلكترونية على أنها "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية" وهو نفس المعنى الذي أخذت به المادة 07 من القانون 04/14 المؤرخ في 24فيفري 2014 جريدة رسمية عدد 16 المتعلق بالنشاط السمعي البصري في تعريفها للاتصالات على أساس أنها كل إرسال أو بث أو استقبال للعلامات أو الإشارات أو الكتابات أو الصور أو الأصوات أو المعلومات مهما تكن طبيعتها بواسطة الأنظمة السلكية أو الراديوية أو البصرية أو غيرها من الأنظمة الكهرومغناطيسية.

يرد على الهاتف بتسجيل رسالة صوتية تخزن في جهاز الهاتف، وهناك نوع يرسل بواسطة الهاتف النقال وعادة ما تسمى بالرسائل القصيرة sms messages.

وتنوع أشكال المراسلات ووسائل إرسالها لا يخرجها من طابعها العام باعتبارها ترجمة مادية لأفكار شخصية أو آراء خاصة، لا يجوز لغير مصدرها ولمن توجه إليه الإطلاع عليها، سواء تعلقت بالمرسل أو بالمرسل إليه أو بالغير، لأنها تعد بمثابة محادثات شخصية تجسدت في صورة مراسلة[1]، وإذا قام أحد الأشخاص بالإطلاع عليها فإنه يعد منتهكا لحرمة الخصوصية، ذلك أن هذه الرسالة قد تتضمن أسرارا أو أمورا تتعلق بخصوصيات طرفي الرسالة فلا يجوز للغير الإطلاع عليها.[2]

وبهذا المفهوم تعد المراسلات مظهرا من مظاهر الحق في الخصوصية، وأن انتهاك سرية هذه المراسلات يعني اعتداء على خصوصية الأفراد لما قد تتضمنه هذه المراسلات من أمور تتعلق بمعتقدات دينية أو أفكار سياسية[3]، فمقتضى هذا الحق أنه لا يجوز لغير مصدر المراسلات ومن توجه إليه الإطلاع على سريتها بغض النظر عن مضمونها، أي حتى ولو لم يتعلق مضمونها بالحياة الخاصة للمرسل أو المرسل إليه.

وهذا على عكس ما دفع به البعض قائلا أن الحماية المقررة لسرية المراسلات لا تدخل في المبدأ العام المتعلق بحرمة الحياة الخاصة، ويحتجون في ذلك بمقولة أن مضمون الخطاب أو الرسالة المرسلة لا يتعلق في كل الأحوال وبصفة دائمة بالحياة الخاصة للمرسل أو المرسل إليه، لكن هذه الحجة مردود عليها على أساس أن من يقوم بفض المراسلة والإطلاع عليها لن يكون في مقدوره أن يتعرف على مضمون الخطاب ومدى تعلقه بالحياة الخاصةللمرسل أو للمرسل إليه إلا بفض الرسالة والإطلاع على محتوياتها، ومن ثم كان من اللازم منع مثل هذا العمل أصلا واعتبار مرتكبه معتديا على سرية المراسلات ومن ثم على الحق في الخصوصية.[4]

ونظرا للأهمية التي تتمتع بها سرية المراسلات واعتبارها عنصرا أساسيا من عناصر الحق في الخصوصية، فقد أجمعت كافة التشريعات على احترامها ورصدت العقوبات الرادعة بحق من ينتهك حرمتها كونها تعد مستودعا مهما لأسرار وخصوصيات الإنسان.[5]

وتطبيقا لهذا المبدأ فقد أشارت معظم دول العالم في دساتيرها إلى حرمة وسرية المراسلات وعدم جواز الاعتداء عليها، و أن عدم النص عليها من قبل بعض الدساتير لا يعني أن هذه الأخيرة لا تجد نفسها في حاجة إلى النص عليها، نظرا لأن هذه الحقوق تستمد أصلها من القانون الطبيعي نفسه، فمما لا شك فيه أن الحماية الدستورية تعد من أقوى الضمانات القانونية لحماية هذا الحق، إذ ترفعه من الحقوق العادية إلى الحريات العامة التي يكفلها الدستور للأفراد[6]، والدستور الجزائري إحدى الدساتير التي

[1] محمود عبد الرحمن محمد، مرجع سابق، ص212.

[2] محمد الشهاوي، مرجع سابق، ص17.

[3] طارق صديق رشيد كه ردى، مرجع سابق، ص228.

[4] ممدوح خليل بحر، مرجع سابق، ص286.

[5] رافع خضر صالح، الحق في الحياة الخاصة وضماناته في مواجهات استخدامات الكومبيوتر، رسالة ماجستير جامعة بغداد ،1993، ص24.

[6] محمود أحمد طه، مرجع سابق، ص59.

تضمنت النص على هذا الحق كما سبق الإشارة إلى ذلك من خلال المادة 46 منه، والتي نصت صراحة أن سرية المراسلات مضمونة وأنه لا يجوز المساس بها بأي شكل دون أمر من السلطة القضائية.

ومن الدساتير الأوروبية التي أقرت حق الإنسان في الخصوصية المتعلقة بسرية مراسلاته الخاصة، الدستور الإيطالي حيث نصت المادة 15 منه على أن حرية وسرية الرسالة مضمونة لا تنتهك ولا يجوز تقييدها، ونصت المادة 36من الدستور السويسري على حماية سرية المراسلات، وفي دستور ألمانيا المعدل سنة 1956 تم النص على أن سرية المراسلات البريدية والمواصلات الهاتفية مصونة ولا يجوز أن تفرض عليها قيود إلا بمقتضى القانون[1]، أما بالنسبة لفرنسا فلم ينص دستورها على حماية حق الإنسان في سرية مراسلاته الخاصة، رغم أن بعضا من الفقهاء الفرنسيين قد ذهبوا إلى تفسير الحرية الفردية التي قرر المجلس الدستوري في 1977/01/02 دستوريتها بأنها تتسع لتشمل حرمة الحياة الخاصة، والتي بدورها تتسع لتشمل الحق في سرية المراسلات الخاصة.[2]

وتطبيقا لنصوص تلك الدساتير فقد استجاب المشرع في جميع تلك الدول بسن القوانين العادية التي تحمي الحق في سرية المراسلات بشكل تفصيلي، وغالبا ما نجد تلك النصوص التي تحمي الحق في سرية المراسلات في قانون العقوبات وفي قانون البريد، وأحيانا كذلك في القانون المدني والقوانين المنظمة لحقوق المؤلف.

وترتيبا على ذلك فقد نصت المادة 303 من قانون العقوبات على معاقبة كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية، كما نصت المادة 137 من نفس القانون على معاقبة كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها، كما تعاقب نفس المادة أيضا كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها، ثم توضحت الحماية وتكرست من خلال القانون 04/18 الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية،[3] حيث نصت المادة 164 منه على معاقبة كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو عن طريق الإتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها.

وكذلك تنص المادة 165 من نفس القانون على معاقبة كل متعامل للبريد أو الإتصالات الإلكترونية يقوم بفتح أو تحويل أو تخريب البريد، أو يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الإتصالات الإلكترونية.

---

[1] سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة رسالة مقدمة استكمالا لنيل درجة الماجستير في العدالة الجنائية، تخصص سياسة جنائية الرياض 2005 ص148.

[2] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، بحث مقدم إلى مؤتمر الحق في الحياة الخاصة بالإسكندرية 1987 ص25.

[3] القانون 04/18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية المؤرخ في 10 ماي 2018، جريدة رسمية عدد 27.

وفي فرنسا فقد جرم المشرع الفرنسي الأفعال التي تشكل مساسا بسرية المراسلات في المواد 226-1، 226-15 من قانون العقوبات الفرنسي.

ومن التطبيقات القضائية في مجال حماية خصوصية المراسلات ما قضت به محكمة النقض الفرنسية من خلال القرار المؤرخ في 1991/07/11 الذي ورد فيه أنه إذا كان من حق الوكيل الخاص أن يتسلم الرسائل الخاصة بالموكل وأن يتولى الرد عليها، فإن ذلك ينصرف فقط إلى الرسائل المتعلقة بأعماله ولا يمتد إلى رسائله الشخصية، فإذا تجاوز هذا الحد ووسع نطاق رقابته ليشمل تلك الأخيرة فإنه يكون بذلك قد انتهك خصوصية موكله[1]، بل إن القضاء الفرنسي قد ذهب إلى أبعد من ذلك في إطار توسيع دائرة الحماية القانونية لخصوصية المراسلات حينما اعتبر أن واقعة تصوير العبارات المذكورة على ظرف الخطاب أو المراسلة أثناء إرسالها انتهاكا لمبدأ سرية المراسلات[2]، ومما لا شك فيه أن رسائل البريد الالكتروني عندما يتوفر فيها عنصري الخصوصية، أي العنصر الموضوعي والمتعلق بمضمون الرسالة بمعنى أن تكون الرسالة ذات طابع شخصي وخاص فيما تخبر به، وكذا العنصر الشخصي والمقصود به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة، فإن هذه الرسائل تعد من المراسلات الخاصة، إذ لا أهمية لوسيلة نقل الرسالة، وهذا ما ذهب إليه الفقه القانوني رغم عدم وجود نص قانوني يعتبر البريد الالكتروني من المراسلات الخاصة[3]، وهذا ما أكد عليه القضاء الفرنسي حيث اعتبر هذا الأخير أن الاعتداء على سرية البريد الالكتروني يعد مساسا بالحق في الخصوصية، وذلك بناء على النصوص القانونية التي تجرم المساس بسرية المراسلات[4]، ومن ذلك ما قضت به المحكمة الكبرى بباريس عندما قررت أن البريد الالكتروني المرسل من شخص إلى شخص آخر يعد من المراسلات الخاصة، لأنه ينقل مضمون المراسلات والخطابات من شخص لآخر على المستوى الفردي، مؤكدة في حكمها أن التقنين الجنائي لا يحمي فقط الرسائل المسلمة عن طريق البريد العادي بل حتى الواردة عبر شبكة الانترنت*، لذلك فالمؤكد حاليا أن البريد الإلكتروني يعد من المراسلات الخاصة في شكل إلكتروني، ومجرد الدخول إليه هو تعد على الحق في الخصوصية، وقد أكد القضاء الفرنسي ذلك عندما أدانت محكمة جنح باريس في 2000/11/02 مسؤولين بإحدى المدارس العامة لقيامهم باعتراض ومراقبة رسائل البريد الإلكتروني لأحد الطلاب، واعتبرتها من المراسلات الخاصة التي لا يجوز انتهاكها إلا

[1] محمود عبد الرحمن محمد، مرجع سابق، ص213.

[2] ممدوح خليل العاني، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة، 1983، ص250.

[3] عبد الهادي فوزي العوضي- الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة ،2005 ص108.

[4] صلاح محمد أحمد دياب، الحماية القانونية للحياة الخاصة للعامل وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب الحديثة وشتات للنشر والبرمجيات، مصر 2010، الطبعة الأولى، ص208.

* يقصد بالبريد الإلكتروني نقل الرسائل أو الملفات بين الحواسيب، وغالبا ما يتم هذا باستخدام مخزن وطريقة نقل معينة أو طريقة إرسال النصوص إلكترونيا من حاسوب مركزي أو نهاية طرفية إلى نهاية أخرى، أما إجرائيا فالبريد الالكتروني هو كل رسالة أيا كان شكلها نصية أو صوتية أو مصحوبة بصور أو أصوات يتم إرسالها عبر شبكة عامة للاتصالات، ويتم تخزينها على أحد خوادم هذه الشبكة أو المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعادتها، ومن الناحية القانونية فقد تم تعريفه بأنه مكنة التبادل غير المتزامن للرسائل بين أجهزة الحاسب الآلي. وقد عرف التشريع الفرنسي البريد الالكتروني في القانون المتعلق بالاقتصاد الرقمي، كما عرفه التشريع الأمريكي بالقانون المتعلق بخصوصية الإتصالات الإلكترونية. أنظر عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الالكتروني، دراسة تأصيلية مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2010 ص22.

بنص قانوني يبيح ذلك*، حيث قضت المحكمة صراحة بأن إرسال رسالة إلكترونية من شخص لآخر يشكل مراسلة خاصة تخضع لأحكام القانون رقم 91/646 المؤرخ في 10 جويلية 1991 الخاص بالإتصالات عن بعد[1]، وكذلك أقرت محكمة استئناف باريس في حكمها الصادر في2001/12/17 و "أكدته أيضا محكمة النقض أن الرسائل الإلكترونية الشخصية التي يرسلها العامل أو يستقبلها على الحاسب الخاص برب العمل، تدخل في نطاق حياة العامل الخاصة، وعليه يحظر الإطلاع عليها أو المساس بسريتها.[2]

وبالإضافة إلى هذه الأحكام القضائية، فإن المجلس الدستوري الفرنسي قرر في 2004/07/10 أن تعريف البريد الإلكتروني الوارد في المادة الأولى من قانون الثقة في الاقتصاد الرقمي ما هو إلا تعريف فني ليس من شأنه تقييد أو تعديل فكرة الرسالة الخاصة وسرية المراسلات الثابتة للبريد الالكتروني.[3]

ولقد اتجه الفقه إلى القول بأن عدم جواز الكشف عن محتوى المراسلات أو المساس بخصوصيتها مرتبط بالحق في الملكية والحق في الحياة الخاصة، فأما حق الملكية فهو الحق الذي يتمتع به المرسل إليه من وقت تسلمه للرسالة، فيكون له وحده حفظ كيانها المادي، وله على مضمونها حق الملكية الأدبية والفنية، ويكون للمرسل إليه بمقتضى هذا الحق أيضا الإنتفاع بهذه الرسائل والتصرف فيها، إلا أن كل ذلك منوط بقيد مهم يتمثل في عدم المساس بالحياة الخاصة للمرسل أو غيره[4]، وأما الحق الثاني وهو الحق في الخصوصية والذي يتولد عنه مجموعة من الإلتزامات تتمثل في أنه:

1-لا يجوز للمرسل إليه أن ينشر محتويات الرسالة التي تتعلق بالحياة الخاصة للمرسل إلا بموافقته، ذلك أن هذا الأخير هو وحده من يملك خصوصيته.

2-لا يجوز للمرسل الذي حرر الرسالة التي تتضمن معلومات تتعلق بالحياة الخاصة للمرسل إليه والتي هي معروفة له وفق علاقته الخاصة به أن ينشر محتويات هذه الرسالة، إلا بموافقة المرسل إليه، لكونه هو وحده صاحب الحق في أسرار حياته الخاصة.

3-لا يجوز للمرسل أو المرسل إليه نشر محتوى مراسلة تتعلق بالحياة الخاصة للغير إلا بموافقته، لأن هذا الأخير هو وحده صاحب الحق في أسرار حياته الخاصة.[5]

---

* ملخص وقائع هذا الحكم أن طالبا بإحدى المدارس الفرنسية بباريس وضع تحت المراقبة من قبل إدارة المدرسة لشكها في أنه يقوم بأعمال قرصنة، وأنه يستخدم بريده الإلكتروني على نحو شاذ وبطريقة غير مألوفة، وقد لاحظت اللجنة التي تم تنصيبها لمراقبة الطالب أن 90% من رسائله تمتاز بالخصوصية والبعض منها ينطوي على تشهير بالمدرسة، وعليه رفضت المدرسة إعادة قيد الطالب بها في العام التالي، وعليه تقدم هذا الأخير بدعوى ضد المدرسة متهما إياها بانتهاك سرية بريده الالكتروني، وتمسكت المدرسة في مواجهة ذلك بأن سرية المراسلات لا تنطبق على رسائل البريد الالكتروني.

[1] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques(

[2] Cour d'appel de paris (CAP) 11ème chambre, Arrêt du 17 décembre 2001disponible sur le site :

https://www.legalis.net/jurisprudences/cour-dappel-de-paris-11eme-chambre-arret-du-17-decembre-2001.

[3] نشوى رأفت إبراهيم، الحماية القانونية لخصوصية مراسلات البريد الالكتروني، بحث مقدم بكلية الحقوق جامعة المنصورة، مصر، ص7.

[4] أحمد فتحي سرور، الوسيط في الإجراءات الجنائية، مرجع سابق، ص409.

[5] سليمان بن عبد الله بن سليمان العجلان، مرجع سابق، ص104.

4-لا يجوز للغير الذي بحوزته رسالة يتضمن محتواها معلومات تتعلق بالحياة الخاصة للمرسل أو المرسل إليه أن ينشر مضمون هذه الرسالة إلا بموافقة صاحب الشأن، لأن هذا الأخير هو وحده صاحب الحق في أسرار حياته الخاصة.[1]

ومع ذلك فإن الحق في خصوصية المراسلات ليس حقا مطلقا، إذ ترد عليه استثناءات تمليها الضرورة، ففي ظروف وحالات استثنائية يجوز التضحية بهذا الحق من أجل المصلحة العامة.*

فمعظم الدساتير التي تكفل الحق في حرمة المراسلات لا تجعل منه حقا مطلقا وإنما تجيز المساس به في أحوال معينة، مع التأكيد في نفس الوقت على أن يكون ذلك وفق قيود وضوابط وذلك لمنع التوسع والتعسف، بل بالقدر الذي تسمح به نصوص القانون التي تجيز الإطلاع على مضمون المراسلات.[2]

وقد تبنت كثير من الدول في قوانينها جواز الإطلاع على الرسائل كحالة استثنائية لضرورة الحفاظ على أمن الدولة أو الكشف عن الجرائم، ففي قانون الإجراءات الجزائية نصت المادة 65 مكرر5 على أنه يجوز لوكيل الجمهورية أو لقاضي التحقيق أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية، وذلك إذا كان هذا الإجراء ضروريا للتحري عن جرائم معينة[3]، كما يجيز القانون رقم 04/05 المؤرخ في06 فيفري 2005 المتضمن تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين في المادة 73 منه لمدير المؤسسة العقابية مراقبة كل المراسلات الصادرة أو الواردة للمحبوسين ما عدا المراسلات الموجهة من المحبوس إلى محاميه أو التي يوجهها هذا الأخير إليه، ولا يتم فتحها لأي عذر كان[4]، ونفس الشيء بالنسبة للمراسلات الموجهة من المحبوس إلى السلطات القضائية والإدارية والوطنية.

وفي فرنسا نظم المشرع الفرنسي حالات الخروج على مبدأ سرية المراسلات الخاصة في المادة الأولى من القانون الصادر في 1991/07/10 المتعلق بحالتي الإعتراض القضائي والإعتراض الإداري، فأما الإعتراض القضائي فيكون لغرض تحقيق نوع من التوازن بين حق الأفراد في الخصوصية والسرية وحق المجتمع في مكافحة الجريمة بوسائل فعالة[5]، لذلك فلا يمكن اللجوء إليه إلا بترخيص من السلطة القضائية المتمثلة في قاضي التحقيق، كما يشترط أن تكون العقوبة المقررة قانونا للجريمة محل التحقيق هي الحبس لمدة لا

[1] آدم عبد البديع آدم، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون، دار نهضة مصر للطباعة والنشر، القاهرة، 2000 ص 212. وقد طبق القضاء الفرنسي حرمة المراسلات الخاصة المتعلقة بأي من الزوجين، فلا يجوز لأحدهما فتح الرسائل المرسلة إلى الآخر أو إفشاء مضمونها، لأنه وبالرغم من حياتهما المشتركة والاختلاط الجزئي بين حقهما في الألفة فإن لكل منهما حياته الخاصة التي ينفرد بها وأسراره الذاتية التي يستقل بها، حتى وإن كانت في حدود ضيقة. أنظر في هذا المعنى محمد محمود عبد الرحمن، مرجع سابق، ص214.

* وهذا ما جاء واضحا في نص المادة 2/8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لسنة 1950 فقد نصت على أنه:"لا يجوز للسلطة العامة أن تتعرض لممارسة الحق في خصوصية المراسلات إلا وفقا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي.

[2] سليمان بن عبد الله بن سليمان العجلان، مرجع سابق، ص167.

[3] المادة 65 مكرر 05 من قانون الإجراءات الجزائية المعدل بموجب القانون رقم 22/06 المؤرخ في 2006/12/20.

[4] تنص المادة 217 من قانون الإجراءات الجزائية "ألا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه"

[5] براهيم بن داود، أشرف شعت، الإطلاع على البريد الالكتروني بين متطلبات النظام العام والحق في سرية المراسلة، مقال منشور بمجلة دفاتر السياسة والقانون العدد 16 جانفي 2017، كلية القانون جامعة الغرير، دبي الإمارات العربية المتحدة، ص38.

تقل عن سنتين، أما الإعتراض الإداري للمراسلات فيسمح باللجوء إليه بصفة استثنائية لغرض البحث عن معلومات تهم الأمن القومي والمحافظة على عناصر النظام العام ومنع الجريمة بشتى أنواعها.*

وفي كل الأحوال يجب ألا يغيب عن الأذهان أن الأصل هو حماية حق الإنسان في خصوصية مراسلاته، لكن أبيح المساس بهذا الحق لضرورات تقتضيها حماية أمن الدولة ونظامها العام، لذا يجب أن تقدر هذه الضرورة بقدرها، كما يجب على كل من وصل إلى علمه شيء من أسرار تلك المراسلات بحكم طبيعة عمله ألا يفشي شيئا من ذلك.

4) **الحــق في الاسم:** تنص المادة 28 من القانون المدني على أنه يجب أن يكون لكل شخص لقب و إسم فأكثر، ولقب الشخص يلحق أولاده،* وإسم الشخص هو وسيلة تعيينه وتمييزه عن غيره من أفراد المجتمع، وهو يتكون من الإسم الشخصي الذي يطلق على المولود عند ولادته ويميزه عن سائر أفراد أسرته، ثم اللقب وهو الإسم العائلي الخاص بالعائلة التي ينتمي إليها الشخص، ويشترك فيه كافة أفراد هذه الأسرة.*

وقد اعتبر الفقه أن إسم الشخص مرتبط ارتباطا وثيقا بحالته، لذلك فإنه لا يجوز التصرف فيه كما لا يسقط بالتقادم، وتظهر أهمية للإسم في كونه يساهم في تكوين علاقة محددة بين الشخص و إسمه تؤدي ضمن حدود معايير معينة إلى إعطاء حق مانع عليه، خاصة وأن اختياره في الأساس لا يكون إلا من أجل تمييز الشخص المسمى به عن غيره من الأشخاص، الأمر الذي يبيح القول أن لكل شخص امتيازا على إسمه يقابله حقه في الدفاع عنه ومنع الإعتداء عليه.

هذا وقد احتدم الخلاف بشأن الطبيعة القانونية للاسم وما يتفرع عن تلك الطبيعة من خصائص*، وما يهمنا في هذا الصدد هو معرفة ما إذا كان اسم الشخص يعتبر عنصرا من عناصر الحق في الخصوصية، أم كونه مجرد حق من الحقوق اللصيقة بالشخصية.[1]

---

* ولمنع إمكانية التعسف في اللجوء إلى هذا الإجراء، وضع المشرع ضمانات لحماية الحق في الخصوصية في مواجهة هذا النوع من الإعتراض، فنص في المادة 13 من نفس القانون على إنشاء لجنة وطنية لمراقبة الإعتراض الإداري ومنحها سلطة التوصية في حالة الإعتراضات غير المشروعة، ولذلك يجب إخطارها بكل قرارات الإعتراض.

* المبدأ أن يتبع المولود بحكم النسب لقب أبيه، إلا أن بعض الدول بدأت تتراجع عن ذلك في قوانينها، ففي فرنسا مثلا صدر القانون رقم 02/304 المؤرخ في 2002/03/04 المتعلق بقواعد انتقال الإسم العائلي المعدل للقانون المدني الفرنسي، أين تنص المادة 311-21 منه على أنه يختار الأبوين إعطاء المولود إسم الأب أو الأم أو الإسمين معا. LOI n° 2002-304 du 4 mars 2002 relative au nom de famille JORF du 5 mars 2002 page 4159 « lorsque la filiation d'un enfant est établie à l'égard de ses deux parents ces derniers choisissent le nom de famille que lui est dévolu soit le nom de père soit le nom de la mère soit les deux noms accolés... »

* وقد يتخذ الإنسان لنفسه إسما يختلف عن إسمه الشخصي يدعى الاسم المستعار وكثيرا ما يشيع استعمال هذا الإسم بين الناس، وغالبا ما يكون هذا الإسم هو أساس شهرة الشخص.

* تكون حماية الإسم أكثر أو أقل شدة طبقا لاختلاف النظر للطبيعة القانونية هذا الحق، وعليه فقد اختلفت النظريات في تحديد الطبيعة القانونية لحق الشخص على إسمه:

النظرية الأولى: يرى أصحابها أن حق الشخص على إسمه هو حق ملكية وينتج عن ذلك أن الشخص يستطيع أن يواجه أي اعتداء للغير على إسمه دون أن يكون مضطرا لإثبات الضرر الذي يلحق به جراء ذلك الاعتداء، وذلك انطلاقا من أن أي إعتداء على حق الملكية يجب منعه

لقد انقسم الفقه في نظر هذه المسألة إلى فريقين أو اتجاهين:

يرى الاتجاه الأول أنه لما كان الحق في الحياة الخاصة يعني أن يعيش الشخص حياته الخاصة في هدوء وسكينة وكما يشاء بعيدا عن تدخل الأخيرين إلا في أضيق الحدود، فإنه من المنطقي اعتبار إسمه داخلا في نطاق الحق في الخصوصية، ومن ثمة فإنه لا يجوز الكشف عنه دون إذنه، وقد انظم القضاء في فرنسا إلى هذا الإتجاه في بعض أحكامه، عندما قضت محكمة باريس في 1970/02/15 بأن الكشف عن الاسم الحقيقي لأحد الفنانين الذي كان يمارس حياته الفنية تحت إسم مستعار حرصا منه على الفصل بين حياته الخاصة وحياته الفنية، يعد اعتداء على خصوصياته، وذلك على اعتبار أن مثل هذا الفعل من شأنه أن يعكر صفو سكينة وألفة حياته الخاصة.*

لكن التشريع الأمريكي يشترط لاعتبار أن استخدام إسم الشخص دون موافقته إعتداء على حقه في خصوصيته، أن يكون هذا الإستخدام بهدف تحقيق غرض معين، خاصة الدعاية والإتجار، فإذا لم يثبت توافر مثل هذا الشرط في استخدام الإسم من الغير دون موافقة صاحب الشأن فإنه يكون مباحا، فقد ورد في الفقرة (ب) من المادة 652 من المدونة الثانية للأفعال الضارة أنه من يستغل إسم أو صفة شخص آخر لاستخدامه الخاص أو لفائدته، يكون مسؤولا نحو إعتدائه على خصوصيته، وكأن القانون الأمريكي لم يعتبر إسم الشخص من خصوصياته إلا بتوافر شرطين هما[2]:

-أن يكون استخدام سم يفيد من خلال السياق أن المقصود منه شخص معين لا غيره، وعليه فلا يستطيع شخص أن يدعي انتهاك حقه في الخصوصية لمجرد أن إسما مثل إسمه قد ذكر في إحدى الروايات، بل لابد من أن يثبت فضلا عن ذلك، أن المقصود بالإسم المذكور يخص شخصه هو وليس شخصا آخر.

-أن يكون المقصود من استخدام إسم الغير الحصول على فائدة شخصية، وتشترط بعض التشريعات في الولايات المتحدة الامريكية أن تكون هذه الفائدة ذات طبيعة مالية.

وإزالته، وهو ما أكده القضاء الفرنسي في أن لكل فرد من أفراد العائلة حق الإعتراض على استعمال إسمه من قبل الغير ومنع ذلك تماما كما يحق لأي مالك أن يعترض على استعمال غيره لشيء من أشيائه التي يملكها وأن يمنع ذلك دون اشتراط وقوع الضرر.

النظرية الثانية: يرى أصحابها أن حق الشخص على إسمه ليس إلا طريقة إدارية لتمييز الناس أو التعريف بكل واحد منهم، فالإسم عندهم أشبه ما يكون بلوحة إدارية أو رقم مميز يعطى للشخص وفي هذه الحالة على الذي يقيم الدعوى لرفع الإعتداء على إسمه يكلف بإثبات وقوع الضرر من أجل تحقيق شرط المصلحة. أنظر في هذا الموضوع محمد العبد الله، مقال منشور على موقع الصحيفة القانونية www.jle.gov.sy (اطلع عليه يوم 2019/05/01 على الساعة 10:05)

[1] محمود عبد الرحمن محمد. مرجع سابق، ص 226.

* ورد في حيثيات الحكم:

La révélition au public du vrai nom de l'intéressé, n'est pas une atteinte au droit au nom patronymique, mais une atteinte à l'intimité.

ومن أهم وقائع هذه القضية هو قيام إحدى المجلات بالإفصاح عن الاسم الحقيقي لأحد الممثلين ورقم هاتفه وعنوانه على نحو تمكن من خلاله الجمهور من ملاحقته والتطفل على خصوصياته محمود عبد الرحمن محمد. مرجع سابق، ص226.

[2] محمد ثامر، الحماية القانونية والقضائية لحق الانسان في الخصوصية، مقال منشور في مجلة الحوار المتمدن، عدد 4797 ماي 2015، متوفر على الموقع http://www.ahewar.org/debat/show.art.asp?aid=466748&r : أطلع عليه يوم 2020/05/05

أما الإتجاه الثاني فيذهب إلى اعتبار أن إسم الشخص لا يدخل في نطاق الحق في الخصوصية ولا يعد من قبيل عناصره، فحسب أنصار هذا الإتجاه أن للإنسان حق على إسمه وهو أحد الحقوق اللصيقة بشخصه ولا يدخل في إطار حقه في حياته الخاصة، بل هو متميز عنه وهذا لفقدانه صفة السرية التي تتصف بها عناصر الحق في الخصوصية، فإسم الشخص وسيلة لتفريده وتمييزه عن غيره وهو بذلك يتسم بقدر كبير من العلنية و من ثم فكشفه للغير لا يعد اعتداء عليه عكس خصوصيات الشخص التي يحرص على إخفائها.[1]

فالإعتداء على الإ سم حسب هذا الإتجاه لا يكون بكشفه وإنما بالخلط بينه وبين غيره من الأسماء وانتحاله من قبل الغير أو استخدامه على نحو يضر بحامله*.

وقد اعتبر بعض أنصار هذا الإتجاه أن الحالات التي ذهب فيها القضاء الفرنسي إلى اعتبار الإ سم من عناصر الحياة الخاصة، كشف لنا أنها حالات تختلف عن تلك التي يحميها الحق في الإ سم، فهذا الأخير يحمي الفرد ضد انتحال إسمه أو استخدامه على نحو يدفع إلى عدم تمييزه عن غيره أو إثارة المنازعات في الاسم.[2]

ويمكن القول أن المشرع الجزائري يتفق وهذا الإتجاه الثاني الذي يذهب إلى عدم اعتبار الاسم من عناصر الحق في الخصوصية، فما يفهم من نص المادة 48 من القانون المدني التي تقضي بأن كل من نازعه الغير في استعمال إسمه من دون مبرر، ومن انتحل الغير إسمه له أن يطلب إيقافهذا الإ عتداء أو التعويض، فالمشرع الجزائري اعتبر الإ سم من ضمن الحقوق الواردة على مقومات الشخصية وعناصرها في علاقات الأفراد بعضهم ببعض،وبالتالي يكون الهدف من هذا المعنى هو حماية حقوق الشخصية والتي يعد الإ سم واحدا منها وليس من عناصر الحق في الخصوصية.

لكن يمكن في حالات معينة أن تتحقق العلاقة بين الحق في الاسم والحق في الخصوصية، من خلال شكل أو طبيعة عتداء، وكذا الحالة التي يتم الإعتداء عليها، فالكشف عن الإ سم في بعض الحالات كنشر أسماء الراسبين في الإ متحان أو أسماء المفلسين في التجارة وغيرها من المواقف التي تزعج الشخص في راحته وألفته وهدوئه وتسبب له حرجا داخل مجتمعه، يؤدي حتما إلى المساس بحق ذلك الشخص بحقه في الخصوصية[3]، وهو المعنى الذي أكده القضاء الأمريكي في قضية السيدة التي تم عرض فلم عن حياتها وكشف فيه عن شخصيتها من خلال استعمال اسمها الحقيقي، أين علل القضاء حكمه في أن نشر قضية السيدة لا يؤدي في حد ذاته إلى مسؤولية المنتج،ولكن استعمال الإ سم الحقيقي للسيدة في ظل وقائع هذا الفيلم، و هو ما يعتبر مساسا بحقها في الخصوصية.[4]

---

[1] محمود عبد الرحمن محمد، مرجع سابق، ص227.

* تطرق المشرع الجزائري إلى الحماية الجزائية للاسم في القسم الثامن من الفصل السابع من الباب الثالث في قانون العقوبات تحت عنوان انتحال الوظائف والألقاب والأسماء وإساءة استعمالها في المواد 248، 249.

[2] ممدوح خليل بحر، مرجع سابق، ص295.

[3] حسام الدين الأهواني، مرجع سابق، ص71.

[4] حسام الدين الأهواني، نفس المرجع، ص79.

كما اعتبر المشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10جوان 2018 أن عناصر الهوية للشخص تدخل ضمن المعطيات ذات الطابع الشخصي التي تعد الأساس الذي تقوم عليه الخصوصية المعلوماتية، ولا شك أن سم يعد عنصرا من عناصر الهوية،وعلى ذلك فإنه لا يعد الإ عتداء على حق الشخص في اسمه إعتداء على حق من حقوق الشخصية فقط، بل في حالات أخرى يمكن أن يشكل ذلك اعتداء على الحق في الخصوصية،ويجد الحق في الإ سم في هذه الحالة حمايته ضمن الحماية القانونية للحق في الخصوصية.

ومن هذا المنطلق فقد اعتبر البعض أن الحق في حماية البيانات الشخصية يرد على كل المعلومات التي من شأنها تحديد الشخص وجعله قابلا للتعرف عليه وذلك بالرجوع إلى مظاهر شخصيته المتعلقة بهويته،[1]وتعد المعطيات الاسمية أهم العناصر المكونة لهوية الشخص، وهو المعنى الذي نجده موضحا في نص المادة 35 من المرسوم التشريعي المتعلق بالمنظومة الإحصائية حينما نصت على أنه يمنع نشر أي معلومات اسمية أو إحصائية قد تسمح بالتعرف على الأشخاص..."[2].

5) الحق في خصوصية الحالة الصحية: تعد الحالة الصحية للإنسان وتاريخه المرضي والأمراض التي يعاني أو عانى منها وكذا أسبابها وجميع ما يتعلق بحالته الصحية والأدوية التي يتناولها والعلاجات التي يخضع لها عنصرا من عناصر الحق في الخصوصية، وهذا بسبب أن الحالة الصحية والرعاية الطبية التي تقدم له تعد من الأمور الخاصة والتي غالبا ما يرغب الأشخاص في عدم كشفها[3]، فمما لا شك فيه أن حالة الشخص الصحية تعد من الأمور الخاصة به والتي يفضل الجميع إخفاءها عن الكافة، بل قد تؤدي أحيانا الحالة الصحية للشخص والإصابة بالمرض إلى الإنسحاب من الحياة العامة، نظرا لما يكون عليه من حالة جسمية ومعنوية صعبة، لذا فمن باب أولى لا يجوز نشر أو إذاعة خبر المرض الذي أصابه، ولا تصويره وهو على فراش المرض إلا بعد موافقته، لأنه حينئذ يكون في أمس الحاجة إلى الهدوء والسكينة بعيدا عن أي تطفل أو إزعاج.

وفي فرنسا فإنه وبعد صدور قانون 1970 المتعلق بدعم ضمان الحقوق الفردية للمواطن المشار إليه سابقا، أصبح بلا أدنى منازع اعتبار مسألة الإفشاء للأحوال الصحية للشخص تمثل مصدرا خطيرا للاعتداء على الخصوصية، ذلك أن طبيعة الأعمال الطبية والجراحية تسمح بالكشف عن خبايا جسد المريض وعوراته من أجل علاجه.

والسر الطبي يشمل كل المعلومات والحقائق التي يطلع عليها الطبيب بحكم عمله وعلاقته بالمريض، سواء أدلى له بها هذا الأخير أو توصل إلى معرفتها من خلال التشخيص الذي يقوم به*، وعليه فإن تدخل المشرع

[1] Meulders-Klein Marie-Thérèse. Vie privée, vie familiale et droits de l'homme. In: Revue internationale de droit comparé. Vol. 44 N°4, Octobre-décembre 1992. pp. 767-794 https://www.persee.fr/doc/ridc_0035-3337_1992_num_44_4_4572.

[2] مرسوم تشريعي رقم 01/94 مؤرخ في 1994/01/15 يتعلق بالمنظومة الإحصائية. جريدة رسمية رقم 94/03.

[3] علي عبود جعفر، جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2013، ص399.

* وقد عرف قانون الصحة رقم 11/18 المؤرخ في 02جويلية 2018، جريدة رسمية عدد 46 السر الطبي بأنه جميع المعلومات التي علم بها مهنيو الصحة، وعرفته المادة 37 من مدونة أخلاقيات الطب بأنه كل ما يراه الطبيب ويسمعه أو يفهمه أو كل ما يؤتمن عليه خلال أدائه لمهمته.

لتجريم الأفعال التي تشكل إفشاء السر الطبي هو بمثابة ترقية للثقة التي ينبغي أن يتحلى بها الطبيب ومن في حكمه وكذا حماية لخصوصية المريض في آن واحد.

فمهنة الطب تعد من أكثر المهن المتصلة اتصالا مباشرا بالأسرار المتعلقة بأدق تفاصيل الحياة الشخصية للمريض والتي قد ينعكس البوح بها سلبا على خصوصيته وكرامته الإنسانية، لذلك فلقد اعتبر السر الطبي أكثر قدسية واحتراما على أساس أن حياة الإنسان هي أغلى ما يملكه، وعليه يجب أن تحاط صحة الإنسان بسرية تامة.[1]

وتجاوبا مع هذا السياق فإن السر المهني الطبي أصبح يتخذ طابعا خاصا اهتمت به التشريعات الحديثة، بعد أن انقلب الإلتزام به من تقاليد مهنية إلى التزام قانوني يتحمله كل من تسنى له الإطلاع بحكم عمله على أسرار المرضى والتي تكون في مجملها معلومات صحية عن المريض، وتتكون المعلومات الصحية من الوثائق وصور الأشعة والتقارير الخاصة بالمريض والفحوصات والتحاليل وكل الشهادات التي يدون فيها الطبيب ما توصل إليه من معلومات وملاحظات والعلاج المقترح للمريض ومتابعة حالته الصحية والتطورات الحاصلة له، كما يندرج ضمن المعلومات الصحية للمريض أيضا كل المعلومات التي من شأنها الكشف عن عيوبه وأمراضه وحالته النفسية والعقلية وكل ما يتعلق بالفحوص التمهيدية والتكميلية وتشخيص المرض والعلاج اللازم له.[2]

ولقد خص المشرع الجزائري السر الطبي بأحكام خاصة في كل من قانون العقوبات[3]، وقانون حماية الصحة وترقيتها[4]، وكذا مدونة أخلاقيات مهنة الطب.[5]

ففي قانون العقوبات نصت المادة 301 على معاقبة الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة على أسرار أدلي بها إليهم أفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاؤها.

وفي قانون الصحة فقد نصت المادة 24 أنه لكل شخص الحق في احترام حياته الخاصة وسر المعلومات الطبية المتعلقة به.

وفي مدونة أخلاقيات الطب نصت المادة 36 على أنه يشترط في كل طبيب أو جراح أسنان أن يحتفظ بالسر المهني المفروض لصالح المريض إلا إذا نص القانون على خلاف ذلك.

---

[1] حسن زرداني، حماية السر المهني الطبي، مقال منشور على موقعwww.platform.almanhal.com اطلع عليه يوم 2019/05/02 على الساعة 15:10.

[2] محمد رايس، مسؤولية الأطباء المدينة عن إفشاء السر المهني في ضوء القانون الجزائري، مجلة العلوم الاقتصادية والقانونية، جامعة دمشق سوريا المجلد 25 العدد 01 2009 ص252. أنظر كذلك بومدان عبد القادر، المسؤولية الجزائية للطبيب عن إفشاء السر المهني، مذكرة لنيل شهادة الماجستير، كلية الحقوق جامعة مولود معمري تيزي وزو الجزائر، السنة الجامعية 2010-2011، ص65.

[3] ورد نص المادة 301 في القسم الخامس من الفصل الأول من الباب الثاني تحت عنوان الاعتداء على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار.

[4] قانون 11/18 المؤرخ في 02 جويلية، المتعلق بالصحة وترقيتها. جريدة رسمية عدد 46.

[5] مرسوم تنفيذي رقم 276/92 مؤرخ في 1992/07/06 يتضمن مدونات أخلاق الطب.

وفي فرنسا صدر قانون يتعلق بقوائم الأبحاث الصحية، والذي لا يسمح لغير الأطباء بالإطلاع على هذه المعلومات حرصا على سريتها.[1]

وترتيبا على ذلك فإنه يبدو جليا مدى اتفاق القوانين على وجوب حماية الحياة الصحية للمريض، وذلك لاعتبارها من صميم حرمة الحياة الخاصة التي لا يجوز للغير التطفل أو الإطلاع عليها دون موافقة صاحب الشأن فيها، حيث شددت التشريعات على اعتبار الحالة الصحية للشخص حقا دستوريا مقررا من أجل حماية الحق في الخصوصية للفرد بما تحويه من أسرار، وبحسبانها من خبايا الشخص وإحدى دقائق حياته الخاصة، بما يترتب عليه ضرورة احترام حق المريض في الإ حتفاظ بسره والتزام الطبيب أو من اؤتمن على سره الطبي بعدم إفشاء ذلك السر.[2]

الفرع الثالث: إتساع نطاق الحق في الخصوصية

إن المنطق الأساسي الذي يركن إليه في بيان معنى الخصوصية يرتبط ارتباطا وثيقا في فهم طبيعة الإنسان نفسه، فالإنسان في شؤونه الخاصة وأحواله المنزوية عن الناس وكراهيته اطلاعهم عليها، لا يساوره القلق فقط في شأن جانب منها إنما في جميع شؤونه سواء كانت مادية أو معنوية.[3]

ولقد ساهمت النقاشات الفقهية والقضائية بشأن الحق في الخصوصية حول ما يمكن أن ينطوي عليه من معان إلى توسيع نطاق هذا الحق، ليشمل فضلا عن معناه المرتبط بالخصوصية المادية والمعنوية معنا آخر للخصوصية ينظر إليه بمفهوم واسع من أجل حماية مصالح الأفراد، وذلك بأن يبقوا جميع المعلومات المرتبطة بهم بعيدة عن متناول المتطفلين.

فمن اليقين أنه وبمجرد أن حظي الإنسان بمنزله الخاص وتوزعت الملكيات بين الأفراد، نشأ التفكير بحماية هذا الحصن الخاص من المعتدين، وحينها بدأ ظهور الحق في الخصوصية لحماية محل مادي أو في مواجهة سلوكيات مادية، ثم لم يلبث أن امتد الحق لحماية الجوانب المعنوية للشخص، لينتقل أخيرا إلى موضعه الطبيعي كحق عام يكفل حماية الفرد من أي انتهاك لخصوصيته.[4]

وبالتالي لم يعد الحق في الخصوصية يتعلق فقط بحماية الفرد من التعرض للمساس بممتلكاته، فتكون ذات محتوى مادي فقط تحمي الإنسان من أي انتهاك مادي يطال حرمة جسده أو حرمة مسكنه، ولا ينطوي أيضا فقط إلى جانب البعد المادي على بعد معنوي يتصل بحق الفرد في حماية كرامته وكشف أسراره وحمايته من أنشطة التجسس والتنصت على مكالماته وأحاديثه ومراقبة مراسلاته... بل لقد أصبح الحق في الخصوصية حقا عاما يحمي الفرد من كل تعدٍ أو انتهاك أيا كانت طبيعته أو مصدره، فيمتد بذلك لحماية معطيات الفرد الخاصة ويمنع وصول المعلومات الخاصة به إلى الغير.[5]

---

[1] Décret n° 95/682 du 09 mai 1995 modifié le décret n° 78/78 du 17 juillet 1978. Relatif à la recherche sur la santé publique.

[2] محمد عبد المحسن المقاطع، مرجع سابق، ص88.

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص88.

[4] بولين أنطونيوس أيوب، مرجع سابق، ص8.

[5] بولين أنطونيوس أيوب، نفس المرجع، بتصرف، ص36.

فالملاحظ أن غالبية الدساتير الحديثة قد تضمنت نصوصا صريحة بشأن حماية الحق في الخصوصية ببعديه المادي والمعنوي، وأن عددا منها تضمن أيضا بالإضافة إلى ذلك نصوصا بشأن حماية الحق في البيانات الشخصية والوصول إليها وإدارتها[1].

ففي فرنسا مثلا نجد أن التشريع الفرنسي التقليدي كان قد جرم صور التعدي على الأمور التي تدخل في نطاق الحياة الخاصة كالأمور المتعلقة بالشرف والاعتبار، حرمة المسكن والمراسلات والمحادثات، لكن الفقه الفرنسي حاول وضع قائمة موسعة بالحالات والأمور التي تتعلق بالحياة الخاصة للأفراد، وقد تبنى القضاء الموقف الذي ذهب إليه هذا الجانب من الفقه.

وكأثر للجدل القضائي والفقهي اتجه المشرع الفرنسي إلى سن تشريع وسع من نطاق الحماية القانونية للحق في الخصوصية من خلال حماية جمع ومعالجة البيانات الشخصية، كمفهوم مستقل عن بقية مفاهيم الخصوصية وتحديدا التدخل المادي.

وتكريسا لمنطق التوسع في نطاق مفهوم الحق في الخصوصية وعدم ربطه فقط بالخصوصية المادية التي تقوم في جوهرها على فكرة العزلة، أو بالخصوصية المعنوية التي تقوم هي أيضا في جوهرها على فكرة الحق في السرية، فقد ذهب بعض الفقه إلى القول أن للخصوصية وجه آخر وهو الوجه الإعلامي والذي مقتضاه ألا تكون المعلومات الخاصة بالفرد محلا للإعلام بالنسبة للغير، وهو الأمر الذي يستتبع عدم استخدام الآخرين معلومات تتعلق بالحياة الخاصة للفرد، وهي من هذا الوجه يسميها البعض بالخصوصية الإعلامية.[2]

المبحث الثاني: التطور الحديث لمفهوم الحق في الخصوصية

لقد عرفت الخصوصية وفق تطورها التاريخي ثلاث محطات رئيسية تختصر رحلتها بين الماضي والحاضر وتعكس تطور مفاهيمها، فبعد الإعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الإعتداء المادي على حياتهم وممتلكاتهم أو ما يعرف بالخصوصية المادية، انطوت الخصوصية في مرحلة لاحقة على حماية القيم والعناصر المعنوية للشخص والتي عرفت بالخصوصية المعنوية.

وفي نطاق آخر ارتبطت فيه الخصوصية بالتطور التكنولوجي المعاصر فأدى إلى ميلاد مفهوم جديد للخصوصية تمثل في الخصوصية المعلوماتية، والتي تقوم على حق الأفراد في حماية بياناتهم الشخصية والسيطرة عليها في ظل تحديات العصر الرقمي.[3]

ولقد شهد النصف الثاني من القرن الحالي اهتماما منقطع النظير من قبل الفقه والقضاء والقانون المقارن بشأن موضوع الحق في الخصوصية، وهو أمر ترك بصمات واضحة في تطور المقصود من هذا الحق، وظهور مفاهيم جديدة له تتناسب مع الظروف التي استلزمت الإهتمام به ودراسته، فما كان هذا

[1] محمود إبراهيم غازي، مرجع سابق، ص78.

[2] أنظر في هذا المعنى: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، الطبعة الاولى، أسيوط مصر 1992، ص176-178.

[3] بولين أنطونيوس أيوب، مرجع سابق، ص54.

الحق ليفرض نفسه على القانونيين ليقوموا بدراسته وبحثه وتطوير مفاهيمه، لولا أنه ارتبط بأمر لا مفر للإنسان من مواجهته اليوم وهو التطور التكنولوجي المعاصر.[1]

وعلى هذا الأساس يرى جانب من الفقه أن الحق في الخصوصية الذي نتحدث عنه في عصر وسائل تقنية المعلومات الحديثة والعالم الرقمي هو ذو محتوى مغاير، ذلك أن خصوصيات الأفراد وأسرارهم ومعلوماتهم الشخصية أصبحت بداخل الأجهزة الإلكترونية وشبكات المعلومات.[2]

فبعد أن أفرز التطور التكنولوجي في مرحلة سابقة ما اصطلح عليه بتكنولوجيا الإتصالات ظهر في مرحلة لاحقة ما أصبح يعرف حاليا بتكنولوجيا المعلومات أو عصر المعلومات، وهذا التطور هو الذي أوجد الحاجة لتطوير مبادئ ومفاهيم قانونية كثيرة تتجاوب معه، ومن أهم المسائل التي كانت أوفر حظا في التصدي لها من بين المسائل المتصلة بالكمبيوتر هو الحق في الخصوصية وحمايته، خاصة مع ظهور ما اصطلح على تسميته ببنوك المعلومات[3]، والتي قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه كبنوك المعلومات القانونية مثلا، أو قد تكون شاملة لمختلف الشؤون والقطاعات، وقد تكون مهيأة للاستخدام على المستوى الوطني العام أو المستخدمة على نحو خاص، كمراكز المعطيات وبنوك معلومات المؤسسات المالية.[4]

المطلب الأول: نشأة فكرة الحق في الخصوصية المعلوماتية

في الحقيقة أن للخصوصية وفق تطورها التاريخي ثلاث محطات رئيسية تختصر رحلتها بين الماضي والحاضر وتعكس حركة التاريخ في تطور وتبدل مفهوم الخصوصية، إلى أن تبلورت فكرة خصوصية المعلومات في العصر الرقمي.

---

[1] نعيم مغبغب، مخاطر المعلوماتية والانترنت، المخاطر على الحياة الخاصة وحمايتها في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية بيروت لبنان، 2008، ص126.

[2] عوده يوسف سليمان، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة، مقال منشور على الموقع الالكتروني https://www.iasj.net/iasj?func=fulltext&aId=142830 كلية الرافدين الجامعة. أطلع عليه يوم2019/09/11

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص24.

وحسب الجمعية الفرنسية للتقييس (afnor) Association française de normalisation abrégée Afnor ' يعتبر بنك المعلومات مجموعة من المعلومات أو البيانات المتعلقة بميدان محدد من المعارف المنظمة لكي تلبي احتياجات المستعملين والتي ظهرت نتيجة التقدم التكنولوجي في مجالات استخدام الآلية لتخزين المعلومات واسترجاعها. أنظر للتفصيل أكثر إبراهيم عامر قنديلجي، إيمان ناضل السمرائي، تكنولوجيات المعلومات وتطبيقاتها، مؤسسة الوراق للنشر والتوزيع 2002، الطبعة ولى - عمان الاردن، ص191.

[4] محمود إبراهيم غازي، مرجع سابق، ص235.

كما يقصد بمصطلح بنوك المعلومات أيضا تكوين قاعدة بيانات تفيد موضوعا معينا يهدف لخدمة غرض معين، وتتم معالجة هذه البيانات بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، ويكون بذلك بنكا للمعلومات المالية، المعلومات القانونية، المعلومات الطبية، السياسية والعسكرية، كما عرفت أيضا بأنها مجموعة المعلومات التي يتم معالجتها إلكترونيا وذلك من أجل بثها عبر شبكة المعلومات، بحيث يمكن للمشترك الوصول إليها من خلال ربط جهازه بشبكة المعلومات. كما عرف قانون الملكية الفكرية الفرنسي رقم 250/91 المؤرخ في 10 جانفي 1994 بنك المعلومات أنه عملية جمع لمؤلفات أدبية أو فنية أو موسيقية أو لبرامج الحاسب الآلي أو لأي بيانات أخرى كالنصوص والأصوات والوثائق والأرقام والوقائع يجري ترتيبها وتنسيقها وتخزينها بطريقة منظمة ومنهجية، ويمكن الوصول إليها واسترجاع المعلومات منها بالوسائل المعلوماتية أو بأي وسيلة أخرى.

فالمحطة الأولى كان الاعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الإعتداء على الكيان المادي في حياتهم، وهي ما تعرف بالخصوصية المادية.

والثانية انطوت الخصوصية فيها على حماية القيم والعناصر المعنوية للشخص، وهي ما يعرف بالخصوصية المعنوية.

وأما المحطة الثالثة، ففي نطاقها ولد مفهوم جديد للخصوصية ارتبط ارتباطا وثيقا بأثر التقنية على الحياة الخاصة، تمثل في خصوصية المعلومات، أو حق الأفراد في حماية البيانات الشخصية والسيطرة عليها في ظل تحديات العصر الرقمي.

لذلك فقد ارتبطت ولادة مفهوم خصوصية المعلومات بالخوف والخشية من مخاطر التقنية وأثرها على النظام القانوني ومسائله في سياق حماية الأفراد من مخاطر التقنية التي تتهدد حياتهم الخاصة، فظهرت خصوصية المعلومات بشكل واضح في الستينات أين انطلق خلالها التوجه نحو التطور التكنولوجي الواسع، وأجواء الإستخدامات المتزايدة للحوسبة وإنشاء بنوك المعلومات وعمليات المعالجة الآلية للبيانات.[1]

ولقد انعكست آثار التطور التكنولوجي المذهل الذي تحقق في هذا القرن بشكل واسع على حقوق الأفراد وحرياتهم المختلفة، ولعل التأثير الذي تركه على حقهم في حماية حياتهم الخاصة كان أبرز من غيره،بعد أن أصبحت بيانات الأفراد الخاصة يتم الإحتفاظ بها في بنوك للبيانات والمعلومات، مما يجعلها عرضة للعديد من الإنتهاكات والإعتداءات عبر وسائل تقنية المعلومات الحديثة، ومن ثم يمكن لأي شخص الولوج إليها والحصول على ما يريد منها[2]، ومن هنا كان لابد من أن يتأثر مفهوم الحق في الخصوصية بذلك، وعليه فقد قيل بأن الحق في الخصوصية في الوقت المعاصر يجب أن يفهم على أنه يشمل في حمايته أيضا معنى خصوصية المعلومات[3]، وهو الأمر الذي ألقى بضلاله على موجة التشريعات التي انطلقت منذ السبعينات والتي عرفت بتشريعات حماية البيانات أو حماية الخصوصية من مخاطر تقنية المعلومات[4]، حيث استوجبت هذه التشريعات وضع قواعد معينة تحكم جمع ومعالجة البيانات الشخصية.[5]

وسوف نتطرق في هذا المطلب إلى نشأة فكرة الخصوصية المعلوماتية لدى الفقه ثم لدى التشريعات المقارنة وذلك كما يلي:

[1] مروة زين العابدين صالح، مرجع سابق، ص41.

[2] أسامة عبد الله قايد، مرجع سابق، ص48.

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص24.

[4] بولين أنطونيوس أيوب، مرجع سابق، ص55.

[5] علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2013 لبنان، ص403.

الفرع الأول: نشأة مفهوم الخصوصية المعلوماتية في الدراسات الفقهية

إن الدراسات الفقهية التي اهتمت بالخصوصية في ضوء التطورات التقنية محدودة جدا، فقد انطلقت مثل هذه الدراسات في نهاية الستينات وبداية السبعينات من القرن الماضي والتي شهدت لأول مرة شارة إلى موضوع خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية.[1]

ولعل الفضل في توجيه الانتباه لمفهوم الخصوصية المعلوماتية خلال هذه الفترة يعزى إلى الفقهين الأمريكيين:[2]

-Alin Wistin في كتابه الخصوصية والحرية privacy and freedom سنة 1967

-Miller(ميلر) في كتابه الإعتداء على الخصوصيةthe assault on privacy 1971

فكلاهما قدم تعريفا لمفهوم خصوصية المعلومات، فوفقا لـ "ويستن" فإن الخصوصية المعلوماتية تعني حق الفرد في تحديد متى وكيف و إلى أي مدى تصل معلوماته الشخصية إ خرين، في حين جاء تعريف ميلر أكثر عمقا عندما عرف الخصوصية المعلوماتية بأنها "قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم"[3]، كما نجد في هذا الإطار بعد تجاوز فكرة تحديد المعنى و تأصيله كتاب قواعد الحياة الخاصة والر قابة العامة private lives and public surveillance لمؤلفه رولي (rule) عام 1973 الذي استعرض من خلاله على نحو شامل ومعمق مسائل جمع واستخدام البيانات الشخصية كوسيلة للسيطرة الاجتماعية، وتضمن تفاصيل حالات تطبيقية ودراسية لعدد من الهيئات القطاعية وما تقوم به من جمع للبيانات الشخصية،ووسائل جمعها ومن له الحق في الوصول إليها وكيف تستخدم، وكيف يؤثر هذا الإستخدام على صاحب البيانات.[4]

ولقد توجهت خلاصة هذه الدراسات الأكاديمية خلال هذه الفترة إلى التأكيد على أنه مما لا شك فيه أن استخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد قد خلف آثارا إيجابية عريضة لا أحد يستطيع إنكارها، خاصة في مجال تنظيم الدولة لشؤون الأفراد الإقتصادية والإجتماعية والعلمية وغيرها، إلا أنه وفي المقابل يجب التعامل مع هذه البيانات الشخصية من حيث مفهومها كحق لصاحبها من أجل منع إساءة استخدام الحكومة لهذه البيانات التي يصار معالجتها آليا أو الكترونيا، ومن ثم تقييد استخدامها وفق القانون فقط[5]، لذلك فقد برز اهتمام عام بالحفاظ على البيانات الشخصية كخطوة ضرورية للحفاظ على الحق في الخصوصية المعلوماتية، حيث

[1] بولين أنطونيوس أيوب، نفس المرجع، ص56.

[2] مروة زين العابدين، مرجع نفسه، ص41، 42.

[3] يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية وحماية البيانات في العصر الرقمي، منشورات اتحاد المصارف العربية، بيروت، الطبعة الأولى 2002، ص 61.

[4] مروة زين العابدين، مرجع سابق، ص42.

[5] مروة زين العابدين نفس المرجع، ص43.

يعتبر الإقرار بحمايتها إقرارا بحق الشخص في الحفاظ على خصوصيته[1]، ومن أبرز ما قيل في هذا الجانب ما قرره الفقيه الأستاذ Frosini Vittorio "فروزيني فيتوريو" في مؤتمر روما عام 1987 بأنه لا وجود اليوم لحرية رفض إعطاء المعلومات المتصلة بالبيانات الشخصية، ولكن بدلا من ذلك فإن الحرية استقرت في القدرة على السيطرة على البيانات الشخصية التي أدخلت في برنامج الحاسب الآلي، وهو الأمر الذي يترتب عليه العديد من الحقوق التي تعتبر مهمة ومستمرة التوالد مادام أن كل واحد منها يحقق السيطرة على المعلومات، فهناك الحق في الوصول إلى بنوك المعلومات، الحق في التأكد من سلامة المعلومات، الحق في تحديثها وتصحيحها، الحق في سرية المعلومات الحساسة ثم الحق في السماح بنشرها، وهذه الحقوق كلها تشكل اليوم ما يسمى بالحق في الخصوصية بمفهومه الجديد.[2]

ثم بدأ الفقه يبرز جهده حول مسألة الخصوصية المعلوماتية، حيث شهد عام 1994 إعداد دراسات واسعة بشأن المسائل المتصلة بالخصوصية وحقوق الإنسان عالميا في ضوء التطورات التقنية الحديثة، ومن أهمها الدراسة التي أعدها الأستاذ "جيروم مشال" Jerome Michael في مؤلفه الخصوصية وحقوق الإنسان:

Privacy and humain rights: an international and comparative study with special reference to developements in information technology.

والذي قام من خلاله المؤلف بتقييم المحتوى الإجتماعي والسياسي والثقافي الذي تضمنته تشريعات الخصوصية وحماية البيانات الشخصية، مستعرضا الصعوبات والتباينات الثقافية في استخدام اصطلاح الخصوصية المعلوماتية واختلاف المفهوم القانوني لهذا المصطلح بين النظم القانونية المختلفة للخصوصية عموما.[3]

ونظرا لكون معنى الخصوصية المعلوماتية لا ينفك في فهمه عن التأثيرات المختلفة التي تتركها الحاسبات الآلية عليه من خلال ما تقوم به من العمليات المختلفة لمعالجة المعطيات الشخصية، فإنها تشكل في غالب الأحيان تهديدا لحياة الأفراد الخاصة وتعدٍ في أحايين أخرى بل و من أسباب تعكير صفائها، لذلك نجد الأستاذDavid Burnham ذهب إلى حد أن نبه في كتابه "ظهور دولة الكمبيوتر" إلى أن خطر الحاسبات الآلية لم يعد قاصرا على تجميع وتذكر المعلومات، وإنما له القدرة على تحديد الأشخاص ومعرفة تحركاتهم، فالقدرة الخيالية التي وصل إليها الحاسوب في تجميع المعلومات المختلفة عن الفرد في كل تحرك من تحركاته أو أي تصرف من التصرفات التي يقوم بها، تجعلهذا الأخير أسيرا للمعلومات التي جمعها عنه هذا الجهاز،* وهنا قال جانب من الفقه بأن المعلومات التي يمكن أن تتسرب عن الفرد من

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى،2018 بيروت، لبنان،ص 23.

[2] عبد المحسن المقاطع، مرجع سابق، ص111.

[3] بولين أيوب، مرجع سابق، ص58.

* وخير مثال يضرب في هذا الشأن للتدليل على هذه المسألة هو الشخص الذي يقوم بالحجز في شركة طيران للسفر إلى وجهة ما لقضاء إجازته، ثم يقوم بسحب مبلغ مالي من بنكه بواسطة بطاقة السحب الآلي، وخلال تلك الفترة يحتاج لمبالغ مالية في أوقات مختلفة فيقوم باستعمال بطاقة الائتمان لقضاء بعض حاجاته الشرائية، فإن الخلاصة التي ستجتمع لدى كمبيوتر شركة بطاقة الائتمان، عبارة عن معلومات مذهلة بما

خلال الحاسب الآلي من شأنها أن تفقده حريته تدريجيا حتى تنتهي، فالحرية على حد تشبيههم بمالها من ضمانات مثل وعاء الماء فإذا ما وجد به ثقب تتسرب منه المعلومات الشخصية، وستنتهي الحرية كما هو الحال بالنسبة للماء المتسرب من ذلك الوعاء المثقوب.[1]

وقد أكد الفقه على ضرورة الإعتراف بالحق في الخصوصية المعلوماتية سواء كان يتضمن عددا من الحقوق أم أنه حق موحد، وذلك في مواجهة الثورة غير المتوقعة والتي لم تكن في الحسبان نتيجة التطور التكنولوجي السريع الذي أدى الى خلل في المجتمع من خلال المساس بالحياة الخاصة لأفراده، بعد ما أصبح تحليل البيانات المتبادلة عن الأفراد يتم بواسطة الكمبيوتر، وأضحى الإنسان بالنتيجة مكشوفا أمام هذا الكومبيوتر، والمعلومات الشخصية التي يمكن جمعها عنه لا تترك له أية زاوية يمكنه الاختباء وراءها.[2]

لذلك فأمام هذه المخاطر تعالت صيحات العديد من الفقهاء محذرة من آثارها على الحياة الخاصة للإنسان و أن حق الإنزواء والتستر والعزلة الذي كان مكسبا له سيصبح دون معنى ولا مغزى بعد أن أصبح من الممكن تجميع المعلومات الخاصة به في نظم المعلومات الآلية التي تنشئها الدولة والأجهزة التابعة لها أو المؤسسات التابعة للقطاع الخاص.

لذلك حرص الفقه القانوني على التأكيد أن الإدارة وهي تملك الكمبيوترات قد تصبح على درجة بالغة من القوة، بحيث تحبس الخصوصية داخل حدود ضيقة، وتكيف حياة الفرد وأسرته بهذه الأجهزة في اللحظة التي يكون لها في ذلك مصلحة إقتصادية أو إجتماعية، ويصبح بذلك الإنسان معاملا كالأرقام بكمبيوتر مسلوب الإرادة، ويصبح بذلك أن ما يهدد الجنس البشري ليس حربا نووية بل جهاز كومبيوتر مستقل.[3]

الفرع الثاني: الإعتراف التشريعي بالحق في الخصوصية المعلوماتية

إدراكا لخطورة العمليات التي يجريها الحاسب الآلي على المعطيات المتوافرة في ذاكرته، قامت العديد من الدول سيما الأوروبية منها بسن العديد من التشريعات لحماية هذه المعطيات، وذلك بمنع استخدام وحفظ ومعالجة أو توزيع المعطيات الشخصية بواسطة الحاسب الآلي دون ترخيص سواء حدث ذلك عمدا أو بطريق الخطأ[4]، فقد تأثرت حركة حماية الحق في الخصوصية المعلوماتية على المستوى القانوني منذ بروزه بتطور تقنية المعلومات وكذا الإتصالات مع بدء مكننة الإدارات الرسمية والمؤسسات الخاصة وظهور إمكانية تحديد هوية الشخص من خلال رقم تعريفي أو هوية رقمية موحدة، وهذا الأمر أدى إلى إثارة هواجس لدى الأفراد تتعلق بالمساس بخصوصيتهم، مما استدعى تحرك المشرع لدى كثير من الدول لإقرار حماية الخصوصية المعلوماتية في مواجهة الأثر التكنولوجي عليها.

يكفي للإحاطة بشؤون الفرد المختلفة، من ذلك مثلا نوع الطيران الذي تم السفر به، تاريخ الحجز، مكان قضاء الإجازة، نوع المشتريات التي اقتناها المحال التجارية التي تعامل معها إلى غير ذلك من المعلومات الخاصة به. أنظر مروة زين العادين، مرجع سابق، ص379.

[1] عبد المحسن المقاطع، نفس المرجع، ص51.

[2] نعيم مغبغب، مرجع سابق، ص162.

[3] محمود إبراهيم غازي، مرجع سابق، ص281.

[4] عبد المحسن المقاطع، مرجع سابق، ص51.

وبذلك كانت حماية مظاهر الخصوصية المعلوماتية محل موجة تشريعية انطلقت منذ السبعينات من القرن الماضيوهي التشريعات التي عر ِفت بتشريعات حماية الخصوصية المعلوماتية أو حماية البيانات من مخاطر تقنية المعلومات، وقد استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة[1]، وقد برز في هذا الإطار مسميات مختلفة للقوانين الجديدة مثل قانون حماية البيانات الشخصية، أو قانون حماية الخصوصية المعلوماتية.

فمنذ مطلع السبعينات من القرن الماضي بدأت دول العالم تتبنى قوانين حماية الخصوصية إما عن طريق القوانين الشمولية التي تعترف بالحق وتقر المبادئ الأساسية وتقدم الإطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات من خلال حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة، أو عن طريق حزمة قوانين قطاعية تتعلق بالبيانات في قطاعات معينة كالبيانات الصحية أو المالية وغيرها.[2]

وتعتبر أول معالجة تشريعية في ميدان حماية الخصوصية المعلوماتية على الرغم من كونها ليست قانونا متكاملا باعتبار أنه ليس قانون دولة، كان عام 1970 في ولاية هاس بألمانيا land of Hesse، لكن تعد دولة السويد أول دولة تضع قانونا وطنيا تقود من خلاله موجة التشريع في هذا المجال عام 1973 وهو قانون تنظيم سجلات الكومبيوتر وحماية البيانات.[3]

ثم صدر في فرنسا م ِسايرة لموجة تشريعات حماية الخصوصية من مخاطر التقنية قانون ٌ خاص لحماية البيانات المعالجة آليا في عام 1978 بموجب القانون رقم 17/78 الصادر بتاريخ 06 جانفي 1978 المتعلق بتكنولوجيا المعلومات والملفات والحريات، وهو القانون الذي حصل بشأنه عدة تعديلات[4] بغية التوافق مع مقررات الإتحاد الأوروبي في هذا الحقل، وقد كان أهمها القانون رقم 04/801 المؤرخ في 2004/08/06 والمتعلق بحماية الأشخاص الطبيعيين تجاه المعالجة الآلية للمعطيات الشخصية[5]، والذي حددت المادة الأولى منه الهدف من المعلوماتية على أنها خدمة لكل مواطن، واعتبرت أن إطار تطويرها يجب أن يتم عبر قنوات التعاون الدولي، مع الإلتزام بالإمتناع عن استخدامها في التعرض للهوية الإنسانية أو لحقوق

[1] بولين أيوب، مرجع سابق، ص 61.

[2] مروة زين العابدين، مرجع سابق، ص112.

[3] علي جعفر، مرجع سابق، ص403.

[4] أهم هذه التعديلات:

-القانون رقم 227/88 المؤرخ في 11 مارس 1988.

-القانون رقم 1336/92 المؤرخ في 16 ديسمبر 1992

-القانون رقم 548/94 المؤرخ في 02 جويلية 1994

-القانون رقم 641/99 المؤرخ في 27 جويلية 1999.

- القانون رقم 239/2003 المؤرخ في 19 مارس 2003

- القانون رقم 2006/64 المؤرخ في 23 جانفي 2006

- القانون رقم 344/2014 المؤرخ في 07 مارس 2014

- القانون رقم 1547/2016 المؤرخ في 18 نوفمبر 2016

- القانون رقم 55/2017 المؤرخ في 20 جانفي 2017

[5] Loi 2004/801 du 06 aout 2004 relative à la protection des personnes physiques à l'egard des traitements de données à caractère personnel.

الإنسان أو الحياة الخاصة أو الحريات العامة والفردية، كما أقر هذا القانون حق كل شخص في اتخاذ القرار للسيطرة على استخدامات بياناته الشخصية بحسب أحكام هذا القانون.[1]

ولعل المخاوف التي أثارها المشروع الوطني الفرنسي الذي عر ف بالنظام الآلي للملفات الإدارية، ودليل الأفراد المعروف اختصارا ب safari[2] الذي يهدف إلى تحديد هوية كل مواطن من خلال تقاطع الملفات الموجودة في كافة الإدارات الفرنسية، كانت هي الدافع الأساسي لإقرار قوانين حماية الأشخاص الطبيعيين من المعالجة الآلية للبيانات الشخصية.[3]

وفي الولايات المتحدة الأمريكية اتجه النظام القانوني الأمريكي إلى سن جملة تشريعات قطاعية[4] تتصل في جزء منها بتطبيقات حماية الخصوصية المعلوماتية، فالولايات المتحدة الأمريكية لم تعرف تشريعا عاما لحماية البيانات الشخصية من مخاطر التقنية المعلوماتية كما هو الشأن في الدول الأوروبية، فقد شرعت حزمة من القوانين على أساس الإستخدام العادل للبيانات الشخصية، فكان أول هذه القوانين عام 1970، أين قامت إدارة الصحة والتعليم بالولايات المتحدة الأمريكية بطرح ٍ يعتمد على جملة من المبادئ الأساسية في حماية البيانات الشخصية ومنها مثلا:

-أن يكون جمع البيانات لغرض محدد.

-لا يجوز التصريح بالبيانات الشخصية التي يتم الحصول عليها لأي فرد أو مؤسسة إلا برضا صاحب البيانات أو بسند قانوني.

-ضرورة وجود آلية تمكن الأفراد من مراجعة بياناتهم الشخصية لضمان الدقة، بالإضافة إلى ضرورة مسح البيانات الشخصية في حالة انتهاء الغرض من تجميعها.

بالإضافة إلى قانون الخصوصية لعام 1974 المتعلق بحماية البيانات الشخصية الذي عالج هذه المسألة في القطاع العام فقط، من خلال التطرق الى تنظيم الممارسات العادلة لجمع وحماية ونشر و استخدام البيانات الشخصية التي تحفظ في سجلات دوائر الحكومة الفدرالية، حيث يمكن استخراج معلومات باستخدام إسم الشخص أو أي أداة تعريفية عنه كرقم هويته أو سجله الطبي، وقد منع هذا القانون كشف بيانات شخص معين دون الحصول على موافقته الخطية، ما عدا الحالات المحددة قانونا و التي

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص48.

[2] Safari : système automatisé pour les fichiers administratifs et les répertoires des individus

[3] منى الأشقر جبور، محمود جبور، مرجع نفسه، ص46.

[4] وعلى سبيل المثال نجد قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة لسنة 1996.

Health insurence portability and accomtability act

وقانون حماية خصوصية الأطفال على الانترنت لسنة 1998

Childrens online privacy protection act

قانون الخصوصية الشخصية على الانترنت لسنة online personal privacy act 2001

وقانون المعاملات الائتمانية العادلة والدقيقة لسنة fair accurate credit transactions act 2003

قانون تحديث قانون الخصوصية لمواكبة عصر المعلومات لسنة The privacy act modernization for the information age act 2011

ترتبط ارتباطا وثيقا بحاجة الإدارة الى إرساء الإستقرار الإجتماعي و الإقتصادي و الصحي و الأمني في البلاد، وكان الهدف الأساسي لهذا القانون حسب ما نصت عليه المادة الأولى منه هو إرساء التوازن بين حق الدولة في جمع البيانات الشخصية و حق الفرد في حماية بياناته الخاصة من التدخل غير المشروع للدولة، و الذي يمكن أن ينتج عن كشف هذه البيانات و إساءة استخدامها في وقت ازداد فيه استخدام الإدارة لتقنيات معالجة البيانات الشخصية، وقد تم سن هذا القانون استجابة للمخاوف حول الكيفية التي يمكن أن يؤثر بها إنشاء واستخدام قواعد البيانات آليا على خصوصية الأفراد، لذلك فقد طالب هذا القانون الوكالات الحكومية أن تعرض على الأفراد أي سجلات تحتفظ بها عنهم، بالإضافة إلى مطالبتها باتباع مبادئ معينة يطلق عليها الممارسات العادلة للمعلومات عند عملية جمع ومعالجة البيانات الشخصية، كما دعا هذا القانون أيضا إلى إنشاء مفوضية دراسة حماية الخصوصية privacy protection study commission والتي تكون لها سلطة تقديم توصيات متعلقة بتنفيذ وتفعيل القانون.[1]

وفي بريطانيا صدر قانون حماية البيانات عام 1984« the data protection act » الذي عدل في العام 1998[2]، أين أقام كلا هذين القانونين مبادئ حماية البيانات الخاصة والتعامل معها، ومما جاء في هذا القانون أن أي شخص يقوم بالتعامل بمثل هذه المعلومات آليا، أو من يؤدي هذه العمليات مثل مستخدمي الكومبيوترات أو من يؤدي خدمات خاصة بالعمليات الآلية يجب عليه أن يلتزم بالشروط التي قررها القانون، ويعد هذا القانون التشريع الرئيس الذي ينظم حماية البيانات الشخصية في بريطانيا، على الرغم من أنه لا يشير إلى الخصوصية، إلا أنه قد تم سنه ليجعل من التشريع البريطاني متوافقا مع توجيهات الإرشاد الأوروبي لحماية البيانات الشخصية الصادر عن الاتحاد الأوروبي سنة 1995[3]، و الذي يطالب الدول الأعضاء بحماية حق الخصوصية المتعلق بمعالجة البيانات الشخصية على وجه الخصوص، لذلك فقد تضمن مجموعة من المبادئ كونت الغرض منه، وهو حماية خصوصية الأفراد والتأكد من أن البيانات التي تخصهم لا يتم معالجتها دون معرفتهم، وأنه قد تم معالجتها بموافقتهم متى كان ذلك ممكنا، كما تلت هذا القانون مجموعة من قوانين جديدة أوجبت تطوير مفهوم الخصوصية، كقانون حرية الوصول إلى المعلومات لسنة 1998 والذي تم استبداله بعد ذلك بموجب قانون حماية البيانات لسنة 2018 Data Protection Act (DPA 2018) المؤرخ في 2018/05/23 حيث يعمد هذا القانون إلى تنظيم عملية جمع البيانات الشخصية وتخزينها واستخدامها بشكل أكثر صرامة.[4]

ويعود هذا الإهتمام الذي أولته الدول الأوروبية والدول الغربية عامة بحماية البيانات الشخصية كأحد مظاهر الحق في الخصوصية في الأساس إلى الخوف من جمع هذه البيانات ومعالجتها بشكل مؤذٍ يساهم

[1] مروة زين العابدين، مرجع سابق، ص214.

[2] حل قانون 1998 محل قانون حماية البيانات لعام 1984 وقانون الوصول إلى الملفات الشخصية لعام 1987 وجاء منفذا لتوجيه الاتحاد الأوروبي لحماية البيانات لعام 1995.

[3] DIRECTIVE 95/46/CE DU PARLEMENT EUROPEEN ET DU CONSEIL du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données Journal officiel des Communautés européennes N° L 281 /31.

[4] مروة زين العابدين، مرجع سابق، ص46.

في تدخل الدولة بشكل غير مبرر في الحياة الخاصة لأفرادها[1]، ولقد اعتمدت هذه الدول في إقرارها لتشريعات الخصوصية المعلوماتية على التوجيه الأوروبي لعام 1995، والذي تميز بإلزامه للدول الأوروبية بإدماجه ضمن تشريعاتها في فترة أقصاها نهاية أكتوبر 1998، ومن ثم كان هو السبب في موجة تشريعية جديدة، وكذا موجة تعديل التدابير التشريعية القائمة في مختلف دول أوروبا، كما أثر ذلك على عشرات الدول الأخرى في العالم من خارج أوروبا، والتي وجدت في هذه التجربة الناضجة لحماية البيانات الشخصية نموذجا هاديا لها.[2]

أما على مستوى التشريعات العربية فعديدة هي الدول التي كرست وأقرت حماية الحق في الخصوصية في دساتيرها، ويعد الدستور التونسي لسنة 2014[3] السباق بالتفرد في ذكر المعطيات الشخصية كأحد العناصر التي يجب الحفاظ عليها في إطار الحق في الخصوصية عموما إلى جانب خصوصية المسكن وسرية الاتصالات والمراسلات.[4]ويبدو واضحا أيضا أسبقية المشرع التونسي لباقي التشريعات العربية الأخرى في تنظيمه وحمايته لخصوصية المعلوماتية، حينما أصدر قانونا أساسيا سنة 2004 يتعلق بحماية المعطيات الشخصية[5] تضمن النص في مادته الأولى أنه لكل شخص الحق في حماية المعطيات الشخصية المتعلقة بحماية حياته الخاصة باعتبارها من الحقوق الأساسية المضمونة بالدستور.

وفي المغرب تم التكريس التشريعي لمسألة الخصوصية المعلوماتية من خلال القانون رقم 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[6].

وفي قطر نجد أن القانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية المؤرخ في 2016/11/13 نص في مادته الثالثة أنه لكل فرد الحق في حماية خصوصية بياناته الشخصية.

وفي لبنان صدر قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي[7] ، الذي تضمن في الباب الخامس منه بعنوان حماية البيانات ذات الطابع الشخصي، الأحكام المتعلقة بالمعالجات الآلية وغير الآلية للبيانات ذات الطابع الشخصي.

وعلى غرار التشريعات العربية السابق ذكرها وأخرى لم نذكرها، فإن المشرع الجزائري قد لحق بركب هذه التشريعات، ولم يعد ينظر إلى الخصوصية من زاوية بعدها المادي فقط، بل أيضا يتعامل معها ببعدها غير المادي، واعترف بالخصوصية المعلوماتية من خلال التعديل الدستوري المؤرخ في 06 مارس 2016 بنص المادة 46 من الدستور، لينص من خلالها على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص23.

[2] مروة زين العابدين، مرجع نفسه، ص112

[3] تنص المادة 24 من الدستور التونسي المؤرخ في 17 جانفي 2014 على "تحمي الدولة الحياة الخاصة وحرمة المسكن وسرية المراسلات والاتصالات والمعطيات الشخصية"

[4] منى الأشقر جبور، محمود جبور، مرجع نفسه، ص26

[5] القانون الأساسي عدد 63 بتاريخ 27 جويلية 2004 يتعلق بحماية المعطيات الشخصية

Loi organique n°63 du 27 juillet 2004 portant sur la protection des donneés à caractère personnel

[6] الصادر تنفيذه بالظهير الشريف رقم 15-09-1 المؤرخ في 18 فيفري 2009 الجريدة الرسمية العدد 57110 بتاريخ 23 فيفري 2009

[7] قانون رقم 18/81 المؤرخ في 2018/10/10، جريدة رسمية عدد 45 بتاريخ 2018/10/18متوفر على الموقعhttps//www.lp.gov.lb :

ذات الطابع الشخصي ويعتبرها حقا أساسيا يضمنه القانون ويعاقب على انتهاكه، وتحقيقا لهذا النص الدستوري وسدا للفراغ التشريعي في هذا المجال صدر القانون رقم 07/18 بتاريخ 10 جويلية 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث يهدف هذا القانون إلى وضع إطار قانوني يحدد نظام معالجة المعطيات ذات الطابع الشخصي والتصدي للآثار المترتبة عن التطور السريع لتكنولوجيات الإعلام و الإتصال على الحياة الخاصة وحريات الأشخاص، بتحديد المبادئ الواجب احترامها أثناء جمع ومعالجة وحفظ البيانات الشخصية وقواعد استعمال هذه البيانات وكذا حقوق الأشخاص الذين تم جمع بياناتهم، وهذا من خلال تبني القواعد العالمية المعمول بها في هذا المجال. وحسب ما ورد في عرض الأسباب لمشروع هذا القانون يظهر جليا أنه قانون ذو مرجعية دولية، سيما المادة 17 من العهد الدولي المتعلق بالحقوق المدنية والسياسية المصادق عليه في الجمعية العامة للأمم المتحدة في 16 ديسمبر 1966 والذي انضمت إليه الجزائر سنة 1989بموجب المرسوم الرئاسي ر قم 67/89 المؤرخ في 16 ماي 1989.

وما تجدر الإشارة إليه في هذا الشأن أن المشرع الجزائري نجده يعترف بالمعطيات الشخصية قبل النص عليها دستوريا، وقبل صدور هذا القانون الإطار 07/18 المذكور أعلاه، وهذا ما وجدناه في بعض النصوص القانونية المتفرقة التي تتعلق بقطاعات مختلفة تضمنت في طياتها الحديث عن ضرورة احترام المعطيات الشخصية، ولعل أول نص قانوني نصادفه في المنظومة التشريعية الجزائرية تطرق صراحة لحماية المعطيات الخاصة للأفراد هو نص المادة 11 من المرسوم 131/88 المنظم للعلاقات بين الإدارة والمواطن، حيث تنص على أنه لا يجوز للإدارة المسيرة أن تنشر أو تسلم أية وثيقة أو أي خبر[1] مهما يكن سندها في ذلك، إذا كانت الوثيقة أو الخبر يتصلان بحياة الفرد الخاصة أو يرتبطان بوضعيته الشخصية ما لم يرخص بذلك التنظيم المعمول به أو تكون ثمة موافقة من المعني*، بالإضافة إلى نصوص تشريعية أخرى نذكر منها على سبيل المثال لا الحصر:

- القانون رقم 19/04 المتعلق بتنصيب العمال ومراقبة التشغيل الذي تعاقب المادة 27 منه من يقوم بإفشاء المعلومات الشخصية التي تمس بالحياة الخاصة لطالب التشغيل إلى عقوبة جزائية".[2]

- المرسوم التشريعي رقم 01/94 المتعلق بالمنظومة الإحصائية، والذي تنص المادة 03 منه على أنه لا يحق للمصلحة المؤتمنة أن تكشف أو تنشر المعلومات الفردية الواردة في الإستمارات التي تتضمن التسجيل الإحصائي ولها علاقة بالحياة الشخصية والعائلية وعلى العموم الوقائع والتصرفات الخصوصية[3].

[1] المقصود بكلمة أي خبر أي "معلومة" فقد ورد بالنص الفرنسي كلمة information

* المرسوم 131/88 مؤرخ في 04 جويلية 1988 ينظم العلاقات بين الإدارة والمواطن، جريدة رسمية رقم 1013 بتاريخ 06 جويلية 1988،من النصوص القانونية الأولى أيضا التي تحدثت عن حماية أية معلومات ذات صلة بالحياة الخاصة.نجد القانون رقم 09/88 المؤرخ في 26 جانفي 1988 المتعلق بالأرشيف الوطني، والذي تنص المادة 10 الفقرة 02 منه على أنه من أجل حماية السيادة الوطنية والنظام العام وشرف العائلات فإنه لا يجوز الإطلاع على الوثائق المتعلقة بالقضايا المطروحة أمام القضاء ولها صلة بالحياة الخاصة للأفراد، وكذلك الوثائق التي تحتوي على معلومات فردية ذات طابع طبي لاسيما الملفات التي تخص حياة الأفراد الخاصة إلا بعد انقضاء أجل 100 سنة ابتداء من تاريخ ميلاد الشخص.

[2] القانون 19/04 مؤرخ في 25 ديسمبر 2004 يتعلق بتنصيب العمال ومراقبة التشغيل الجريدة الرسمية عدد 83 مؤرخ في 26 ديسمبر 2004.

[3] أنظر المرسوم التشريعي رقم 01/94 المؤرخ في 15 جانفي 1997، يتعلق بالمنظومة الإحصائية جريدة رسمية عدد 03 بتاريخ 16 جانفي 1994.

- القانون المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص[1]،حيث تنص المادة 03 على أنه يتعين أثناء مختلف مراحل أخذ العينات البيولوجية واستعمال البصمة الوراثية احترام كرامة الأشخاص وحرمة حياتهم الخاصة وحماية معطياتهم الشخصية، وتعاقب المادة 18 من نفس القانون كل من يفشي المعطيات المسجلة في القاعدة الوطنية للبصمات الوراثية وهي عبارة عن معطيات شخصية حسب نص المادة 12.[2]

- القانون المتعلق بالتجارة الالكترونية[3]، حيث تلزم المادة 26 منه المورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي، ويشكل ملفات الزبائن ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية كما يجب عليه:

*الحصول على موافقة المستهلكين الاكترونيين قبل جمع البيانات الشخصية.

*ضمان أمن نظم المعلومات وسرية البيانات.

* تحديد كيفيات تخزين المعطيات ذات الطابع الشخصي وتأمينها وفقا للتشريع والتنظيم المعمول بهما.

- القانون المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، حيث تفرض المادة 97 أن يخضع إنشاء واستغلال شبكات الإتصالات الإلكترونية المفتوحة للجمهور وتقديم خدمات الإتصالات للجمهور إلى احترام شروط خصوصية البيانات والمعلومات التي يتم إيصالها بواسطة شبكات الإتصال، وكذا شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي.[4]

- القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[5]، حيث تنص المادة 04 من في فقرتها الرابعة أن الترتيبات التقنية التي يتم وضعها من أجل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، تكون موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من هذه الأفعال ومكافحتها، وذلك دون المساس بالحياة الخاصة للغير.

[1] أنظر القانون رقم 03/16 المؤرخ في 19جويلية 2016 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، الجريدة الرسمية عدد 37 بتاريخ 22 جويلية 2016.

[2] تنص المادة 12 من القانون المذكور أعلاه "يجب أن ترفق المعطيات الوراثية عند تسجيلها في القاعدة الوطنية للبصمات الوراثية بالبيانات الخاصة المتعلقة بما يأتي:

-هوية صاحب البصمة الوراثية إذا كان معروفا.

-تاريخ ومكان الوقائع وطبيعة الجريمة المرتكبة.

[3] قانون رقم 05/18 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الالكترونية، أنظر الجريدة الرسمية عدد 28 مؤرخة في 16 ماي 2018.

[4] قانون رقم 04/18 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، جريدة رسمية عدد 28 مؤرخة في 16 ماي 2018.

[5]قانون 04/09 مؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ج رعدد 47.

- القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، حيث نصت لمادة 05 منه على أنه يجب أن تتواجد على التراب الوطني كل البيانات والمعلومات ذات الطابع الشخصي التي تم جمعها من طرف مؤدي خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق أو سلطات التصديق الإلكتروني.[1]

بالإضافة إلى هذه القوانين نجد كذلك الإتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي المبرمة بين الجزائر وفرنسا، والتي أشارت كذلك في المادة 23 منها على حماية المعطيات الشخصية التي تمثل الخصوصية المعلوماتية.[2]

لقد اعترف المشرع الجزائري بمفهوم الخصوصية المعلوماتية عن طريق تبنيه لحزمة قوانين قطاعية أشارت في نصوصها إلى ضرورة احترام وحماية البيانات الخاصة في قطاعات معينة، كالبيانات الصحية أو المالية أو بيانات الأحوال المدنية وغيرها، إلى أن وصل به المطاف إلى تبني قانون شمولي يعترف بالحق ويقرر المبادئ الأساسية ويقدم الإطار القانوني الموضوعي والإجرائي لحماية الخصوصية المعلوماتية التي تتصل بالأفراد وبحياتهم الخاصة، وهو القانون رقم 07/18 المؤرخ في 10 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.*

الفرع الثالث: إعتراف الصكوك الدولية بمبادئ حماية الخصوصية المعلوماتية

يتصل الجهد الدولي لحماية الخصوصية المعلوماتية بجهده في حماية الحق في الخصوصية عموما، ضد أي اعتداء بغض النظر عن طبيعته، وقد تبلورت هذه الجهود مؤخرا بعد انتشار تكنولوجيا المعلومات في إطار خاص يتعلق بحماية الحياة الخاصة من أخطار المعالجة الآلية للبيانات الشخصية من نظم الكومبيوتر وبنوك المعلومات.

---

[1] القانون رقم 04/15 مؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج ر عدد 06 مؤرخة في 2015/02/10.

[2] تم التوقيع على هذه الاتفاقية في باريس بتاريخ 05 أكتوبر سنة 2016 وتم التصديق عليها بموجب المرسوم الرئاسي رقم 73/18 المؤرخ في 25 فيفري 2018 وقد نصت المادة 23 على ما يلي:

1/لا يجوز استعمال المعطيات الشخصية التي تم إرسالها من طرف إلى آخر بغرض تنفيذ طلب التعاون من قبل الطرف الذي تلقى هذه المعطيات، إلا للأغراض التالية:

-الإجراءات التي تطبق فيها هذه الإتفاقية.

-الإجراءات القضائية والإدارية.

-إذا تعلق الأمر بمواجهة تهديد مباشر وجدي يستهدف الأمن العام.

2/لا يجوز استعمال هذه المعطيات لأغراض أخرى بما في ذلك نقلها فيما بعد إلى دولة أخرى أو منظمة دولية إلا بعد موافقة الطرف الذي قدم هذه المعطيات أو عند الإقتضاء الموافقة المسبقة للشخص المعني.

3/للشخص المعني بنقل معطياته الشخصية تطبيقا لهذه الاتفاقية الحق في الطعن في حالة خرق هذه المعطيات.

4/يتخذ كل طرف جميع الإحتياطات اللازمة للحفاظ على سلامة المعطيات المرسلة تطبيقا لهذه الاتفاقية، لاسيما منعها من التعرض للتحريف، أو التلف أو الإطلاع عليها من الغير غير المرخص لهم.

* هناك دول تعمد إلى سن قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام والخاص، مع وجود هيئة لضمان التواؤم مع القوانين الأخرى وتطبيقها، وهو النموذج الشائع كما هو الحال في دول الإتحاد الأوروبي، ويسمى نموذج القوانين الشاملة، وثمة دول تعتمد نموذج القوانين القطاعية وهي التي تتعلق بقطاع معين، حيث تتجنب سن تشريع عام لحماية الخصوصية وتفضل إصدار قوانين معينة تحكم قطاعات بعينها، وفي مثل هذه الحالة فإن إنفاذ القواعد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل. أنظر مروة زين العابدين صالح، مرجع سابق، ص151.

فالتزايد المستمر لاستخدام وسائل التقنية العالية في ميدان جمع ومعالجة البيانات الشخصية من قبل الدولة أو القطاع الخاص غير من موضوع المصلحة المحمية، حيث بدأ الإنتقال من حماية الحياة الخاصة إلى الإهتمام أكثر بحماية البيانات الشخصية باعتبارها الجزء المعنوي من الحياة الخاصة، وفي هذا المناخ تضافرت الجهود الدولية في وضع إطار قانوني لحماية الإنسان من تأثير المعلوماتية على خصوصيته.[1]

ولعل بدايات هذه الجهود ظهر من خلال المؤتمرات الأكاديمية المتخصصة بمسائل حقوق الإنسان والخصوصية، فقد انعقدت عدة مؤتمرات دولية لبحث موضوع الحق في الخصوصية وما يتعرض له من أخطار بسبب التطورات العلمية والتكنولوجية الحديثة، وأصدرت عدة توصيات تتعلق بحماية هذا الحق.[2]

ومن أهم هذه المؤتمرات، مؤتمر ستوكهولم لسنة 1967 الني أصدر إعلانا اعتبر فيه أن خصوصية المعطيات هي عبارة عن مزيج من حقوق الأفراد من خلال التوازن بين الحق في الوصول للمعلومات والتنظيم الإداري لملفات الكومبيوتر[3]، وكذلك المؤتمر الدولي لحقوق الإنسان الذي انعقد في طهران في الفترة من 22 أفريل إلى 13 ماي من عام 1968، والذي كان له الأهمية البالغة في توجيه الإهتمام بمسائل حماية البيانات والخصوصية من مخاطر التقنية[4]، حيث تناول المشكلات المرتبطة بأنشطة الأمم المتحدة التي تهدف إلى تأكيد احترام حقوق الإنسان وحرياته الأساسية، واضعا في الإعتبار الظروف التي طرأت وتولدت بسبب التقدم العلمي والتكنولوجي[5]، بالإضافة أيضا إلى مؤتمر مونتريال بكندا الذي انعقد لدراسة مدى تأثير التكنولوجيا الحديثة على حق الفرد في خصوصيته، حيث أوصى هذا المؤتمر بضرورة العناية بالأخطار التي تهدد الحياة الخاصة نتيجة التطورات العلمية، كما انعقد في الفترة من 19 إلى 23 جانفي من سنة 1970 مؤتمر باريس، الذي ضم خبراء هيئة اليونسكو التابعة للأمم المتحدة لدراسة الحق في الحياة الخاصة، وذلك بسبب تعقد المشكلات المتصلة بها، وكذا وجود تعارض أحيانا بين الحفاظ على الحياة الخاصة للفرد من جانب، وتحقيق المصلحة العامة للمجتمع من جانب آخر، لاسيما بعد اتساع نطاق تدخل الدولة وكذا ما طرأ من تطور علمي وتكنولوجي.[6]

وكنتيجة لهذه الدراسات فقد حصل اهتمام من طرف العديد من المنظمات الدولية بهذه المسألة من خلال تطويرها لأنشطة مختلفة في حقل حماية الخصوصية المعلوماتية، وذلك بهدف تنظيم حماية المعطيات الخاصة وتنظيم تدفق وانتقال هذه المعطيات، ومن ثمة بدأ حرص المجتمع الدولي على توفير

---

[1] بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، المجلة العربية للعلوم ونشر الأبحاث، المجلد الثاني العدد الخامس 04 جوان 2016، رقم البحث A17316، ص43.

[2] محمود عبد الرحمن محمد، مرجع سابق، ص88.

[3] عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية 2003، ص191.

[4] بولين أنطونيوس أيوب، مرجع سابق، ص64.

[5] وقد أوصى هذا المؤتمر من بين ما أوصى به احترام الحياة الخاصة للإنسان في ضوء الإنجازات التي تحققت في تقنيات التسجيل وضرورة إقامة التوازن بين التقدم العلمي والتكنولوجي وبين رقي الإنسان الفكري والثقافي والأخلاقي.

[6] محمود عبد الرحمن محمد، مرجع سابق، ص90.

الحماية للمعلومات والمعطيات بمختلف أنواعها، وتبنى في سبيل ذلك عددا من الإتفاقيات والقرارات الدولية.[1]

ولعل الجزء الأكبر من هذا الجهد أ ، نجز من قبل منظمة التعاون الإقتصادي والتنمية، مجلس أوروبا، الإتحاد الأوروبي، الأمم المتحدة ومنظمة التجارة العالمية.[2]

ومحاولة لإبراز دور الجهود الدولية في الإ عتراف بالحق في الخصوصية المعلوماتية نتطرق إلى دور المنظمات الدولية في حماية الخصوصية المعلوماتية ثم الى دور الهيئات الإقليمية.

أولا: دور المنظمات الدولية في حماية الخصوصية في مجال المعلوماتية

1) الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر عن منظمة التعاون الاقتصادي والتنمية OECD :* لعبت منظمة التعاون الإقتصادي والتنمية منذ منتصف السبعينات من القرن الماضي دورا أساسيا فيتعزيز احترام الحق في الخصوصية المعلوماتية كقيمة أساسية وشرط ٍ لضمان التدفق الحر للبيانات الشخصية عبر الحدود، فمنذ سنة 1978 بدأت هذه المنظمة في وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات، ومحاولة لإبراز دور الجهود الدولية في الإ عتراف بالحق في الخصوصية المعلوماتية، ثم إلى دور الهيئات الإقليمية.[3]

وقد تم تبني هذه القواعد من طرف مجلس المنظمة، أين تم إعداد سنة 1980 دليلا إرشاديا تحت عنوان حماية الحياة الخاصة وتدفق البيانات الشخصية عبر الحدود، تضمن مجموعة من القواعد تشكل ضمانة للمعلومات والبيانات الشخصية المعالجة إلكترونيا في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر[4]، ولا تعد هذه القواعد إلزامية وإنما مجرد إرشادات وتوصيات تمت التوصية للأعضاء بالالتزام بها، واعتبارها قواعد ذات طابع توجيهي للخطوات التي ينبغي اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية في مجال الخصوصية المعلوماتية، واعتبار هذا الأمر من مصلحة الدول الأعضاء، والتوفيق بين القيم الأساسية التي يمكن أن تتعارض كالحق في الخصوصية والإنسياب للمعلومات.

ومن أهم التوجيهات الرئيسية المتعلقة بحماية البيانات الخاصة التي جاء بها هذا الدليل:[5]

---

[1] محمد كمال محمد الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دراسة مقارنة دار الفكر والقانون، المنصورة مصر 2017، ص189.

[2] مروة زين العابدين، مرجع سابق ص297

* تضم هذه المنظمة organization for economic cooperation في عضويتها 29 دولة وهي: أستراليا، النمسا، بلجيكا، كندا. جمهورية التشيك. الدنمارك. فلندا. فرنسا. ألمانيا. اليونان. هنغاريا. ايسلندا. إرلندا. إيطاليا. اليابان كوريا الجنوبية، لوكسمبورغ، المكسيك، هولندا، النرويج، بولندا، البرتغال، إسبانيا، السويد، سويسرا، تركيا، بريطانيا، والولايات المتحدة الأمريكية. غرضها الرئيسي هو تحقيق أعلى مستويات النمو الإقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص51.

[4] محمد كمال محمود الدسوقي، مرجع سابق، ص189.

[5] مروة زين العابدين، مرجع سابق، ص298.

-مشروعية جمع البيانات من خلال تحديد وحصر عمليات جمعها، والإقتصار على طبيعة البيانات الشخصية وتحديدها، وذلك بشكل يوفر الضمان على أن الحصول على هذه البيانات يتم بطريقة وأساليب مشروعة ونزيهة.

-تحديد الغرض من جمع البيانات واستخدامها، وذلك فقط للغرض الذي جمعت من أجله، وأن تكون في نطاق الحدود الضرورية لتحقيق هذا الغرض.

-توفير وسائل حماية أمن المعلومات وضمان سريتها.

-الحق في المشاركة والمساءلة، ومقتضى ذلك أن يكون للأشخاص المعنيين الحق في الحصول والتعرف على البيانات التي تخصهم ومراقبة مدى صحتها.

ولقد اعتبر مجلس المنظمة أن التدفق الحر للبيانات الشخصية عبر الحدود من العوامل المساهمة في النمو الإقتصادي والإجتماعي بما يفرض على الدول الأعضاء الإهتمام بضمان حماية هذه البيانات الشخصية والحياة الخاصة والحريات الفردية في إطار قانوني وتنظيمات منسجمة، تمنع إعاقة حركة تدفق البيانات عبر الحدود.[1]

والظاهر أن هذا الدليل قد لعب دورا أساسيا في التأثير على اتجاه العديد من الدول الأوروبية ودفعها إلى إقرار تشريعات وطنية في حقل الخصوصية المعلوماتية.

ولقد تأكد اهتمام هذه المنظمة بشكل عملي بحماية الخصوصية المعلوماتية ونقل وتدفق البيانات الشخصية من خلال وضعها لمجموعة من القواعد الإرشادية، والتي تتمتع بالصبغة الإلزامية للعاملين سواء في نطاق القطاع الخاص أو القطاع العام، بحيث يمتد نطاق هذه القواعد للبيانات المتعلقة بالأشخاص الطبيعيين في القطاعين الحكومي والخاص، وتشمل البيانات المعالجة آليا وكذا المعدة يدويا، وتتكون هذه الإرشادات من ثماني مبادئ تتمثل في[2]:

1-تعيين حدود التجميع، من خلال فرض قيود على تجميع البيانات الشخصية، حيث تحدد البيانات التي يتم التحصل عليها بطرق وأساليب مشروعة ونزيهة، مع توفر العلم والرضا بموضوع تجميع هذه البيانات من أصحاب الشأن.

2-تعيين الغرض، حيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورا ومقيدا ومحددا سلفا.

[1] يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنيت، الجزء الأول، منشورات اتحاد المصارف العربية الطبعة الأولى، بيروت، 2002، ص26-27.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي، دراسة معمقة في مكافحة جرائم التقنية الحديثة، دار النهضة العربية، الطبعة الأولى 2009 القاهرة، ص 626.

3-تحديد نوعية البيانات حيث يتوجب أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله، فضلا عن كونها دقيقة وكاملة ومعينة.

4تعيين حدود الإستخدام وهو مبدأ يقتضي عدم نشر البيانات الشخصية وإفشائها من غير المصرح لهم بذلك إلا بموافقة صاحب البيانات أو بناء على نص قانوني.

5-ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة لحماية البيانات الشخصية.

6-مبدأ حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم ومراقبة مدى صحتها.

7-مبدأ مساءلة الأشخاص والجهات المرخص لهم بالوصول والإطلاع على البيانات ذات الصفة الخاصة.

2) دليل الجمعية العامة للأمم المتحدة رقم 95/45 المتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية: لم تكن مسألة حماية الخصوصية المعلوماتية غائبة عن اهتمامات الأمم المتحدة وذلك من خلال تبني الجمعية العامة التابعة للأمم المتحدة دليلا لتنظيم استخدام المعالجة الآلية للبيانات الشخصية.[1]

والذي صدر على شكل قرار بتاريخ 1990/12/14 تضمن مجموعة من المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحواسيب الإلكترونية كتوصيات للدول الأعضاء لتضمينها في التدابير التشريعية في مجال حماية الخصوصية المعلوماتية، وهي تقريبا نفس المبادئ المقررة لدى منظمة التعاون الاقتصادي والتنمية، ومن أهم هذه المبادئ التي جاء بها هذا القرار نذكر:[2]

-مبدأ المشروعية والنزاهة في جمع المعلومات المتعلقة بالأشخاص وعدم استخدامها لأغراض مخالفة لمقاصد ميثاق الأمم المتحدة.

-مبدأ الصحة الذي يلتزم بمقتضاه المسؤول عن إعداد ملفات البيانات أو المسؤول عن حفظها بالتحقق من دقة البيانات المسجلة وملاءمتها.

-مبدأ تحديد الغاية من إنشاء الملف الذي يتضمن البيانات الشخصية، والتي يجب أن تكون محددة ومشروعة ومعلنة قبل إنشائه، حتى يتسنى إعمال الرقابة على أن البيانات الشخصية المذكورة أنها لا تستخدم أو تفشى لغايات لا تتفق مع الغايات المحددة دون موافقة الشخص المعني.

-مبدأ وصول الأشخاص المعنيين إلى الملفات الشخصية عنهم، وهو المبدأ الذي يقر حق الشخص أن يعرف ما إذا كانت تجري معالجة آلية لمعلومات شخصية تتعلق به وأن يعترض بخطر بذلك.

-مبدأ الأمن والذي يتضمن التزام الدولة اتخاذ التدابير الملائمة لحماية البيانات الشخصية من اطلاع الغير عليها بغير إذن، أو استخدام البيانات بشكل غير آمن.

[1] مفوضية الأمم المتحدة لحقوق الانسان مجموعة، صكوك دولية لحقوق الانسان في مجال إقامة العدل. منشورات الأمم المتحدة ،2004 ص294.
https://www.ohchr.org/Documents/Publications/training11Add1ar.pdf

[2] منى الأشقر جبور، محمود الأشقر، مرجع سابق، ص 54.

والملاحظ أن هذه المبادئ تكاد تكون متطابقة مع القواعد التي تضمنها الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر عن منظمة التعاون الاقتصادي والتنمية المشار إليه، من حيث نطاق تطبيق هذه المبادئ، إذ تطبق على جميع المعطيات ذات الطابع الشخصي سواء الواردة في الملفات العامة أو الخاصة وسواء المعالجة آليا أو يدويا.[1]

وقد دعا هذا القرار إلى ضرورة إنشاء سلطة رقابة تتولى الإشراف على احترام المبادئ السالفة الذكر وكيفية تطبيقها[2].

3) قرار الجمعية العامة للأمم المتحدة بشأن الحق في الخصوصية في العصر الرقمي: نظرا لتضخم بواعث القلق الذي أعربت عنه الدول الأعضاء في الأمم المتحدة وغيرها من الجهات ذات المصلحة إزاء الأثر السلبي الذي يمكن أن يطال الخصوصية بسبب الإستعمال غير المشروع للمعلوماتية في سياق المراقبة الداخلية والخارجية و إعتراض الإتصالات الرقمية وجمع البيانات الشخصية، فقد اعتمدت الجمعية العامة للأمم المتحدة في شهر ديسمبر من سنة 2013 القرار رقم 167/68 بشأن الخصوصية في العصر الرقمي*، والذي أكدت من خلاله الجمعية العامة على أن حقوق الأشخاص الموجودة خارج الفضاء الإلكتروني يجب أن تحظى أيضا بالحماية في هذا الفضاء.* ويدعو هذا القرار في البند الرابع منه جميع الدول إلى تنفيذ الإجراءات التالية:

-احترام وحماية الحق في الخصوصية في سياق الإتصالات الرقمية.

-إعادة النظر في الإجراءات والممارسات والتشريعات المتعلقة بمراقبة الإتصالات واعتراض و جمع البيانات الشخصية، وذلك بهدف الحفاظ على الحق في الخصوصية.[3]

واستنادا إلى هذا القرار فتحت المفوضية السامية لحقوق الإنسان مشاورة في 27 فيفري 2014، وجهت في إطارها استبيانا إلى الدول الأعضاء عن طريق بعثاتها الدائمة في جنيف ونيويورك والمنظمات الدولية والإقليمية والمؤسسات الوطنية لحقوق الإنسان والمنظمات غير الحكومية، ودعت المفوضية في بيانها الدول إلى تقديم إسهامات بشأن القضايا والمواضيع التي تناولتها الجمعية العامة في قرارها 167/68، وقد

[1] محمد كمال محمود الدسوقي، مرجع سابق، ص191.

[2] منى الأشقر جبور، محمود جبور، مرجع سابق، ص54.

* شارك في تقديم هذا القرار 57 دولة عضوا، وقد طلبت الجمعية العامة فيه من مفوضية الأمم المتحدة السامية لحقوق الإنسان أن تقدم إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين تقريرا عن حماية الخصوصية وتعزيزها في سياق جمع البيانات الشخصية.

* التقرير السنوي لمفوضية الأمم المتحدة السامية لحقوق الإنسان، مجلس حقوق الإنسان الدورة السابعة والعشرون، الحق في الخصوصية في العصر الرقمي، 30 جوان 2014 The right to privacy in the digital age , Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 متوفر على الموقع www.ohch.org

[3] Voir la Résolution adoptée par l'Assemblée générale le 18 décembre 2013 [sur la base du rapport de la Troisième Commission (A/68/456/Add.2)] 68/167. Le droit à la vie privée à l'ère du numérique Soixante-huitième session A/RES/68/167 disponible sur le site www.undocs.org

وردت الإسهامات من 29 دولة عضوا من جميع المناطق ومن 05 منظمات دولية، وثلاث مؤسسات وطنية لحقوق الإنسان، و16 منظمة غير حكومية.

وأشارت العديد من هذه الإسهامات بالتفصيل إلى الأطر التشريعية الوطنية القائمة وإلى تدابير أخرى اتخذت لضمان احترام الخصوصية في العصر الرقمي وحمايتها.

ثانيا: دور الهيئات الإقليمية في الإعتراف بالحق في الخصوصية المعلوماتية

لقد كان للهيئات والمنظمات الإقليمية حضور قوي إلى جانب المنظمات الدولية في مجال الإعتراف بالخصوصية المعلوماتية وإرساء الحماية لها، ولعل من أبرز هذه الجهود الإقليمية كان على المستوى الأوروبي لانطوائها على جهود هامة في مجال حماية البيانات الشخصية وكذلك تشكيلها نموذجا لكثير من دول العالم في هذا المجال.

فالدول الأوروبية سيما الغربية منها تحديدا كان لها السبق في مجال التشريعات الخاصة بالجرائم المعلوماتية وحماية البيانات والمعلومات المعالجة آليا، بحكم كونها أحد منابع ثورة المعلومات التي انطلقت إلى باقي دول العالم، وأمام مخاطر وتحديات تلك التقنية الحديثة كان لزاما على تلك الدول أن تتخذ من التشريعات درعا واقيا لها ولمؤسساتها وأفرادها لصد تلك المخاطر[1]، ومن أبرز تلك الجهود نذكر ما يلي:

1) إتفاقية المجلس الأوروبي بشأن حماية الأشخاص في مواجهة المعالجة الآلية للبيانات الشخصية:

لعب مجلس أوروبا والذي هو في الأصل معني بحقوق الإنسان دورا كبيرا في إفراد ووضع إتفاقية عالمية بشأن حماية الخصوصية المعلوماتية[2]، حيث تبنت لجنة وزراء من مجلس أوربا التي أنيط بها معالجة موضوع الخصوصية إتفاقية حماية الأشخاص في نطاق المعالجة الآلية للبيانات الشخصية.[*]

Convention for the protection of individuals with regard to automatic processing of personal data

تضمنت هذه الاتفاقية مجموعة من المبادئ تمثل الحد الأدنى لمعايير حماية الخصوصية المعلوماتية المتعين على الدول الأطراف تضمينها في التدابير التشريعية والقوانين التي تصيغها، حيث نصت المادة الرابعة منها على أن تقوم كل دولة طرف باتخاذ التدابير الضرورية لتفعيل المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي.

[1] محمد كمال محمود الدسوقي، مرجع سابق، ص195.

[2] بن قارة مصطفى عائشة، مرجع سابق، ص44.

[*] أبرمت هذه الاتفاقية في 1981/01/28 بمدينة ستراسبورغ بفرنسا وأصبحت نافذة بتاريخ 1985/10/01 وقد وقعت عليها 31 دولة صادق منها 21 دولة، وحملت الرقم 108. كما وقعت على هذه الاتفاقية دول أخرى غير أعضاء في الإتحاد الأوروبي كتونس والمغرب، الأرجنتين المكسيك، الأرغواي، بوركينافاسو... وتعتبر هذه الإتفاقية في أغراضها ومبناها امتدادا للقرارين الصادرين عن المجلس الأوروبي عامي 1973-1974 إضافة إلى مجموعة التوصيات القطاعية، لكن الجديد فيها ما تضمنته حول قواعد نقل البيانات خارج الحدود.

تهدف هذه الإتفاقية حسب نص المادة الأولى منها إلى ضمان إحترام الحقوق والحريات الأساسية لكل شخص طبيعي كيفما كانت جنسيته أو مكان إقامته، وخاصة حقه في حياة خاصة تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي الخاصة به.[1]

وقد نصت المادة 05 من هذه الإتفاقية على أن الحماية تشمل المعطيات ذات الطابع الشخصي التي تم تحصيلها ومعالجتها بطريقة نزيهة ومشروعة، بالإضافة إلى أنها مسجلة لغايات محددة ومشروعة والتي لا يتم استعمالها بشكل يتعارض مع هذه الغايات.[2]

تتكون اتفاقية مجلس أوروبا من ثلاث أجزاء رئيسية، تمثل المبادئ الأساسية والقواعد الخاصة بشأن تدفق المعطيات خارج الحدود، وقد شكل الفصل الثاني منها الذي تضمن القواعد والمبادئ الأساسية لحماية المعطيات الشخصية الجزء الرئيسي من هذه الإتفاقية، كما يلاحظ أن جوهر هذه المبادئ يكمن في إعطاء المعطيات الشخصية في كافة الدول التي تطبق فيها الإتفاقية حدا أدنى من الحماية في مواجهة عمليات المعالجة الآلية للبيانات الشخصية، وبتطبيق هذه المبادئ فإن الدول الأطراف تتجه نحو حظر قيود نقل البيانات وتدفقها وتتجنب إمكانية أن يتعارض حق حرية المعلومة مع نظام الحماية الواجب للبيانات الشخصية.

والملاحظ أنه على خلاف توصيات منظمة التعاون الإقتصادي والتنمية، فإن هذه الإتفاقية ملزمة للأعضاء المتعاقدين، فقد طلب البرلمان الأوروبي من الإتحاد الأوروبي دفع الدول الأعضاء إلى توقيع هذه الاتفاقية، والذي بدوره أصدر بتاريخ 29-07-1981 توصية للدول الأعضاء يحثهم بضرورة التوقيع عليها.[3]

هذا وقد بذل مجلس أوروبا جهودا إضافية في هذا الحقل من خلال لجنة الخبراء العاملة في حقل حماية المعطيات والتي أصدرت سلسلة من الأدلة التوجيهية المعتمدة على الإتفاقية المذكورة تتعلق بحماية قواعد المعلومات الطبية المؤتمنة، وقواعد المعلومات الخاصة المتعلقة بالأنشطة الطبية والإحصاءات، وقواعد المعلومات الخاصة لأغراض التسويق، وقواعد المعلومات الخاصة بأغراض الضمان الاجتماعي، وكذلك لأغراض الضبطية[4] والبيانات الجنائية، وقواعد المعلومات الخاصة بأغراض التوظيف وخدمات الإتصال.[5]

والأكيد في هذه الإتفاقية من خلال ما ورد في ديباجتها هو تعبير الدول الأعضاء في مجلس أوروبا الموقعة عن رغبتها في توسيع حماية الحقوق والحريات الأساسية لكل فرد لتشمل الحق في احترام الحياة الخاصة،

---

[1] تنص المادة الأولى: تهدف هذه الاتفاقية إلى ضمان احترام الحقوق والحريات الأساسية لكل شخص طبيعي كيفما كانت جنسيته أو مكان اقامته وخاصة حقه في حياة خاصة تجاه المعالجة الالية للمعطيات ذات الطابع الشخصي الخاصة به وذلك ضمن المنطقة الترابية لكل طرف.

[2] أنظر نص الإتفاقية منشور باللغة العربية على موقع http//rm.coe.int

[3] منى جبور الأشقر، محمود الأشقر، مرجع سابق، ص55.

[4] Voir : LA RECOMMANDATION N° R (87) 15 DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES VISANT À RÉGLEMENTER L'UTILISATION DE DONNÉES À CARACTÈRE PERSONNEL DANS LE SECTEUR DE LA POLICE (adoptée par le Comité des Ministres le 17 septembre 1987, lors de la 410e réunion des Délégués des Ministres) disponible sur le site : https://eur-lex.europa.eu/legal-content. Visite le 26/05/2020.

[5] مروة زين العابدين، مرجع سابق، ص302.

آخذة بعين الإعتبار كثافة التداول عبر الحدود للمعطيات ذات الطابع الشخصي المعالجة آليا، وفي نفس الوقت إقرارها لضرورة التوفيق بين القيم الأساسية لاحترام الحق في الخصوصية وحرية تداول المعلومات.

2) إتفاقية المجلس الأوروبي بشأن مكافحة الجرائم المعلوماتية:[1] تهدف هذه الإتفاقية بشكل عام إلى حماية المجتمع الأوروبي من الجريمة المعلوماتية عن طريق التعاون الدولي، حيث كرست مبدأ السرية في عملية تبادل المعلومات الدولية بين الأطراف[2]، وقد جسدت هذه الإتفاقية الجهود التي بذلها المجلس الأوروبي للتصدي ومكافحة الجرائم المعلوماتية و التي شكلت تحديا خطيرا وتهديدا حقيقيا لمصالح الدول والمؤسسات والأفراد، ووفقا لما جاء في ديباجة هذه الاتفاقية، فقد حرصت الدول الموقعة من جانبها على ضرورة ضمان وجود توازن ملائم بين مصالح تنفيذ القانون واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا عام 1950 بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 بشأن الحقوق المدنية والسياسية، والمعاهدات الدولية الأخرى واجبة التطبيق بشأن حقوق الإنسان التي تؤكد على حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير وتلقي ونقل المعلومات والأفكار في شتى المجالات بغض النظر عن الحدود والحقوق المتعلقة باحترام الخصوصية.[3]

فقد اعتبرت مسألة حماية الأفراد إزاء المعالجة الآلية للبيانات الشخصية من أهم المواضيع التي أخذت بعين الإعتبار عند توقيع هذه الإتفاقية، بعد تأكيدها في ديباجتها على إدراك الدول حاجتها في الحرص على الحق في حماية البيانات الشخصية وفقا لاتفاقية مجلس أوروبا الموقعة عام 1981.

وقد تضمن الفصل الأول من هذه الإتفاقية النص على الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم تحت عنوان الجرائم التي تمس خصوصية وتجانس وتوافر بيانات الكمبيوتر ومنظوماته، ومن الجرائم المنصوص عليها في هذا الشأن، جرائم الوصول والإعتراض غير المشروع على نظام معلوماتي، التعدي على البيانات عن طريق إتلافها أو تغييبها أو محوها أو إفسادها أو تغييرها بدون وجه حق.[4]

3) التوجيه الأوروبي 46/95 المتعلق بحماية الأشخاص الطبيعيين في مواجهة المعالجة الآلية للمعطيات ذات الطابع الشخصي وحرية تدفق المعطيات :

إهتم الاتحاد الأوروبي هو الآخر بموضوع الخصوصية المعلوماتية في نفس اللحظة التي طرحت فيها مسألة هتمام بحقوق الإنسان على المستوى العالمي منذ سبعينات القرن الماضي، لذلك فقد أولى جهود عديدة من أجل توحيد القواعد المقررة لحماية الخصوصية المعلوماتية وذلك ابتداءا من عام 1976، حيث أصدر الإتحاد الأوروبي تعليمات في 1976/04/08 تتعلق بحماية الأفراد من أنشطة التقييم الآلي للبيانات، ثم

[1] تحمل هذه الاتفاقية رقم 185 أبرمت في 2001/11/23 بمدينة بودابست عاصمة المجر، وقد تم التوقيع عليها من قبل الدول الأعضاء في مجلس أوروبا. أنظر موقع مجلس أوروبا مجموعة المعاهدات الأوروبية www.conventions.coe.int ودخلت حيز التنفيذ في 2004/06/01 ويمكن لأي دولة في العالم الإنضمام إلى هذه الإتفاقية إذا رغبت في ذلك.

[2] بولين أيوب، مرجع سابق، ص326.

[3] انظر دباجة الاتفاقية متوفرة على الموقع www.rmcoe.int/budapest-convetion اطلع عليه يوم 2020/05/26

[4] محمد كمال محمود الدسوقي، مرجع سابق، ص197.

تعليمات في 1979/05/08 تتعلق بحماية الأفراد من مواجهة التطوير التقني لمعالجة البيانات،[1] بالإضافة الى إصداره بتاريخ 1981/07/29 توصية للدول الأعضاء بضرورة الإلتزام بتوقيع إتفاقية مجلس أوروبا السابق الإشارة إليها.

وفي تطور ملحوظ بالنسبة لمستويات الحماية التي وفرها الإتحاد الأوروبي للخصوصية المعلوماتية صدر الدليل الأوروبي بشأن حماية الأفراد فيما يتصل بمعالجة البيانات ذات الطابع الشخصي وحرية انتقالها المؤرخ في 24 أكتوبر 1995، والذي دخل حيز التنفيذ في 25 أكتوبر 1998.

وقد حظي هذا الدليل بأهمية بالغة وذلك لصدوره عن البرلمان والمجلس الأوروبيين معا، وكذا انطلاقه من جهود المفوضية الأوروبية لحقوق الإنسان[2]، حيث أن هذه الأخيرة كانت مهتمة بالتباين الحاصل في تشريعات حماية البيانات الذي اعتبرته أن من شأنه إعاقة التدفق الحر للبيانات داخل إقليم الإتحاد الأوروبي[3]، ذلك أن البيئة التشريعية المركبة والمعقدة في الإتحاد الأوروبي (التي تتألف من 28 تشريعا وطنيا لحماية البيانات الشخصية) لم تعد ملائمة لحركة التطور السريعة في تكنولوجيا المعلومات، إضافة إلى الحاجة لمواكبة الإلتزامات والموجبات التي تفرضها حماية الخصوصية المعلوماتية، لذلك قررت المفوضية الأوروبية لحقوق الإنسان التقدم باقتراح لتوفيق قانون حماية البيانات داخل الاتحاد الأوروبي.[4]

لقد احتوى هذا التوجيه[5] على عدد من المبادئ الأساسية في مجال حماية المعطيات ذات الطابع الشخصي والتي يتوجب على الدول الأعضاء الإلتزام بها، وكذلك على أي شخص يقوم بمعالجة البيانات الشخصية أن يلتزم بها، وأهمها أن:

-يتم معالجة البيانات الشخصية بشكل عادل وقانوني.

-يتم معالجتها لأغراض محدودة.

-تكون المعالجة مناسبة وغير مفرط فيها.

لا يتم الإحتفاظ بها فترة أطول مما هو ضروري.

-يتم نقلها فقط إلى الدول التي تتوافر لديها الحماية المناسبة.

ويلاحظ أن هذا التوجيه الأوروبي جاءت مبادئ الحماية المقررة للخصوصية المعلوماتية فيه أوسع وأكثر شمولية من المبادئ التي تضمنتها المدونات السابقة، حيث تضمن بالإضافة إلى المبادئ التي جاء بها دليل

[1] عائشة بن قارة، مرجع سابق، ص44.

[2] بولين أنطونيوس أيوب، مرجع سابق، ص321.

[3] مروة زين العابدين، مرجع سابق، ص140.

[4] منى الأشقر جبور، ومحمود جبور، مرجع سابق، ص54.

[5] Derective 95/46/CE du parlement européen et de conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'egard du traitement des données à caractère personnel et à la libre circulation de ces données. Journal officiel n° L281 du 31/11/1995.

منظمة التعاون الاقتصادي والتنمية السابق ذكرها، قواعد أساسية خاصة بالبيانات الحساسة، وحقوق صاحب البيانات تجاه البيانات التجارية وغيرها.[1]

ولقد قامت جميع الدول الأعضاء في الإتحاد الأوروبي بإعداد تشريعات متسقة مع هذا التوجيه، أو قامت بتكييف قوانينها القائمة مع أحكامه*، ويعد التوجيه الأوروبي لسنة 1995 من أهم التوجيهات الصادرة عن الإتحاد الأوروبي في حقل الخصوصية المعلوماتية، ذلك لأنه أخذ في الإعتبار ضرورة التوسع في تفسير مصطلح المعالجة، بحيث تشمل التجميع والتسجيل والإضافة وغيرها من الأنشطة الإلكترونية التي تنصب على المعطيات ذات الطابع الشخصي، وبصفة عامة جعل البيانات متوافرة بأي شكل، كما اعتد هذا التوجيه بحرية حركة البيانات بحيث تكون لها ذات الحرية التي تكون عليها حركة تداول السلع والخدمات.[2]

4) الدليل الأوروبي 66/97 المتعلق بالمعالجة الآلية للمعطيات ذات الطابع الشخصي وحماية الحياة الخاصة في قطاع الإتصالات:[3]

يتعلق هذا الدليل حسب نص المادة الأولى منه بتنسيق أحكام قوانين الدول الأعضاء لضمان مستوى متكافئ من الإنسجام فيما يخص حماية الحقوق والحريات الأساسية في جانبها المتعلق بالحق في الخصوصية، لاسيما البيانات الشخصية في قطاع الإتصالات السلكية واللاسلكية، وتعد أحكام هذا التوجيه موضحة ومكملة لأحكام التوجيه 95/46 عند التطرق إلى مسألة الخصوصية المعلوماتية في قطاع الإتصالات، بدليل أن هذا التوجيه قد استهل في حيثيات ديباجته بالتأكيد على أحكام التوجيه 95/46 والتذكير بمطالبة هذا الأخير في أحكامه الدول الأعضاء بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات ذات الطابع الشخصي، وذلك بغرض ضمان حرية تنقل البيانات الشخصية في المجتمع.[4]

---

[1] بولين أنطونيوس أيوب، مرجع سابق، ص321.

* يلاحظ أن فرنسا رغم كونها أحد الدول الخمسة عشر في الإتحاد الأوروبي والتي كانت ملزمة بتطبيق قانون الإتحاد الأوروبي 95/46/CE قبل شهر أكتوبر، إلا أنها تأخرت في إدخال هذا الإرشاد المذكور في نظامها القانوني، حيث أنها لم تقم بذلك رغم إعلانها منذ شهر فيفري 1998 بأنها كلفت المجلس الإستشاري الحكومي بوضع قانون يتلاءم مع القانون الأوروبي الملزم. فرغم التعديلات التي لحقت قانون 1978 إلا أن فرنسا لم تقم بتطبيق هذا الارشاد بكل التزاماته المقررة فيه، وهو الأمر الذي استدعى أن تكون من بين الدول الخمسة التي أقامت عليها اللجنة الأوروبية دعوى أمام محكمة العدل الأوروبية عام 2000.

[2] أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد للنشر والتوزيع، الطبعة الأولى 2014، الرياض العربية السعودية، ص839.

[3] Directive 97/66/CE du parlement européen et du conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications. Journal officiel n° L024 du 30/01/1998

[4] Considérant que la directive 95/46/CE du parlement européen et de conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'egard du traitement des données à caractère personnel et à la libre circulation de ces données requiert que les états membres protègent les droits et les libertés des personnes physiques a l'egard du traitement des données à caractère personnel, et notament le droit au respect de leur vie privée, afin d'assurer le libre circulation des données à caractère personnel dans la communauté.

لقد تضمن هذا الدليل مجموعة من المبادئ تركز في مجملها على تحديد المتطلبات الجديدة لحماية البيانات الشخصية، بعد أن تم إدخال تقنيات رقمية متقدمة وجديدة في شبكات الإتصالات العامة.[1]

وقد تضمن هذا الدليل الجديد توسيعا لنطاق الحماية للأفراد فيما يتعلق بمعطياتهم الشخصية، كما تضمن قواعد بشأن التقنيات الحديثة وطوائفها الجديدة، وكذلك أضاف تعريفات جديدة للمراسلات والبيانات المنقولة وموقع البيانات وغيرها، وكل ذلك بقصد توسيع نطاق حماية الخصوصية والسيطرة على كافة أنواع البيانات المعالجة.[2]

5) الدليل الأوروبي 2002/58 حول الخصوصية ضمن إطار شبكة الاتصالات الالكترونية[3]

صدر هذا الدليل بتاريخ 2002/07/12 ووضع موضع التنفيذ في 2002/08/01 على أن يتم التوقيع عليه من قبل دول الإتحاد الأوروبي في مهلة أقصاها 2003/10/31، وتلتزم هذه الدول الموقعة بنقل أحكامه إلى قوانينها الداخلية، وقد تضمن هذا الدليل عدة مواضيع أبرزها ما يتعلق بالبيانات الشخصية المعالجة خلال عملية الإتصال بأي شبكة اتصال الكترونية[4]، وقد عالج هذا الدليل تقنيات إتصال وبرامج إلكترونية قد تشكل خطرا جديا على الحق في الخصوصية مثل:

*cookies وهي عبارة عن برامج ترسلها مواقع الواب التي يزورها مستخدموا الشبكة في شكل ملفات نصية، وتستقر في الحاسبات الآلية لهؤلاء المستخدمين وتقبع بداخلها لتعود مجددا إلى الموقع الذي انطلقت منه محملة بمعلومات حول زوار هذا الموقع (كعنوان البريد الالكتروني، الإسم، رقم بطاقة ئتمان...) عند اتصال المستخدم مجددا بالشبكة.

*برامج التنصت web bugs أيضا اعتبرها الدليل من التقنيات التي يمكن أن تشكل خطرا على الحياة الخاصة لمستخدم شبكة الإتصالات الإلكترونية، حيث يمكنها أن تخزن الكثير من المعلومات المتعلقة بالحياة الخاصة للأفراد ومن ثم استعمالها لغايات غير مشروعة، خاصة إذا ما تم تجميعها دون موافقة الأشخاص المعنيين، كما هو الحال مثلا بالنسبة للبريد الدعائي الإلكتروني المكثفSPAMMING حيث اعتبره الدليل غير مسموح به إلا في حالة الموافقة الصريحة من المعني، وهذا الأمر يتعلق كثيرا بالتجارة الالكترونية.[5]

---

[1] Farid bouguettaya, la protection des données personnelles en droit communautaire. Mémoire master 2 recherche droit européen des droits de l'homme. Université de Montpellier 1 faculté de droit EDEDH 2006 p13

[2] بولين أيوب، مرجع سابق، ص325.

[3] DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002, Concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) Journal officiel des Communautés européennes L 201/37.

[4] بولين أيوب، مرجع نفسه، ص 328.

[5] Larticle 13 dispose que : « L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».

كما تطرق هذا الدليل إلى مخاطر الهاتف النقال على الحق في الخصوصية، حيث يمكن لشبكة الإتصالات أن تعالج أو تخزن بيانات شخصية تسمح بتحديد مكان أو هوية المتصل، لذلك فقد ألزم هذا الدليل أنه لا يمكن معالجة البيانات المتعلقة بها إلا في حالة موافقة المتعاقد الصريحة.

وقد توقف هذا التوجيه أيضا عند مسألة الدليل الهاتفي وأثره على الحق في الخصوصية، معتبرا أنه لا يمكن وضع إسم المشترك فيه إلا إذا وافق هذا الأخير صراحة، مع إعطائه حق الوصول إليه وتصحيح المعلومات المتعلقة به.

6) اللائحة العامة لحماية البيانات « GDPR »[1] هي عبارة عن مجموعة من القواعد والمبادئ التي تتعلق بالخصوصية المعلوماتية، تم وضعها من طرف الإتحاد الأوروبي في 2016/04/14 لتحل محل التوجيه الإرشادي رقم 95/46/CE الصادر عن البرلمان الأوروبي في 24 أكتوبر 1995 والذي سبق الإشارة إليه، وتعرف هذه اللائحة أيضا بالنظام الأوروبي العام لحماية البيانات، إذ يعد هذا النظام التغيير الأكثر أهمية في تنظيم خصوصية البيانات خلال 20 عاما الأخيرة في أوروبا، وهو أحد الأنظمة التي سنها الإتحاد الأوروبي من أجل حماية الخصوصية المعلوماتية للأفراد المقيمين فوق أراضي الإتحاد الأوروبي، وهذا ما يفهم من نص المادة الأولى منه التي حددت الهدف والغرض من أحكامه، وهو إرساء أحكام خاصة بحماية البيانات الشخصية للأفراد الطبيعيين في مواجهة المعالجة الرقمية من جهة، وأحكام خاصة بالتدفق الحر للبيانات من جهة ثانية، ضمن إطار احترام الأفراد وحقوقهم الأساسية التي تقرها مواثيق حقوق الإنسان الدولية والإقليمية.[2]

وقد دخل هذا التشريع الأوروبي الموحد حول حماية البيانات الشخصية حيز التنفيذ في 25 ماي 2018 تحت عنوان "القواعد العامة لحماية البيانات، وهو يهدف إلى تحقيق الإنسجام بين قوانين الدول الأوروبية الخاصة بحماية البيانات عبر توحيد التشريع بما يخدم تعزيز الشفافية لدعم حقوق الأفراد ونمو الاقتصاد الرقمي،[3] كما يستجيب هذا التشريع لحاجة مركزية وهي بناء الثقة والأمان في الفضاء السيبراني من جهة ومواكبة التطورات المتسارعة في مجال تقنية المعلومات من جهة أخرى.

لذلك فقد أدخلت هذه القواعد الأوروبية الجديدة تغييرات عميقة وجذرية إلى البيئة القانونية لحماية البيانات الشخصية، عبر إرسائها نظاما صارما يرتكز على حقوق الإنسان الأساسية، وعلى تحديات العالم

[1] General data Protection Regulation

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données Journal officiel de l'Union européenne L 119/1

[2] Article premier **Objet et objectifs** 1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

2.Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.

3.La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص55.

الرقمي، وفي سبيل ذلك فقد فرض هذا النظام الأوروبي على الشركات والإدارات الحكومية والمنظمات بجميع أشكالها القانونية، والتي تقدم خدمات لمواطنين أوروبيين أو لمقيمين في الإتحاد الأوروبي وتقوم بجمع بياناتهم الشخصية وتعالجها في سبيل هذه الغايات، قواعد جديدة من أجل حماية البيانات الشخصية لهؤلاء، بحيث يتيح هذا التشريع لصاحب البيانات الشخصية فرصة استعادة السيطرة عليها، ويفتح أمامه المجال واسعا لمتابعة ما ينشر منها، وما يتم تبادله أو الوصول إليه.

ومن الجديد الذي جاء به هذا التشريع أن قواعده تختلف عن القواعد الإرشادية التي كانت معتمدة منذ عام 1995، وذلك بكونها تتمتع بقوة القانون دون الحاجة إلى إصدار قوانين وطنية لإعطائها القوة التنفيذية، أو الحاجة لوضع تشريع وطني يتناسب معها، حيث تنص المادة 99 من هذه اللائحة أن نصوصها تدخل حيز السريان في جميع الدول الأعضاء بعد انقضاء 20 يوما على نشرها في الجريدة الرسمية للاتحاد الأوروبي.[1]

8) الإتفاقية الأوروبية الأمريكية لحماية خصوصية البيانات: تم في شهر أوت 2016 الإعلان عن توصل الإتحاد الأوروبي والولايات المتحدة الأمريكية إلى اتفاق يعد إطارا جديدا لتنظيم البيانات الشخصية وحمايتها عبر الأطلسي، أطلق عليه درع الخصوصية[2]، وكان ذلك بطلب من هيئة الإشراف الأوروبية على حماية البيانات، بضرورة إدخال تعديلات كبيرة على عملية تداول البيانات بين الإتحاد الأوروبي والولايات المتحدة الأمريكية، ويعد هذا الإتفاق الجديد بديلا للاتفاقية المعروفة باتفاقية الملاذ الآمن للبيانات safe harbor agreement المتعلقة بحماية البيانات الشخصية التي يتم تبادلها بين أجهزة الشرطة والسلطات القضائية في إطار التحقيقات، وكذا بين الشركات وجهات إنفاذ القانون لكل من الإتحاد الأوروبي والولايات المتحدة الأمريكية وذلك في إطار مكافحة الإرهاب،* حيث فتحت ذريعة مواجهة حرب المعلومات وحماية المجتمع الأمريكي من الإرهاب الإلكتروني أمام وكالة التحقيقات الفدرالية والمخابرات المركزية الأمريكية المجال لتطبيق نظم تتبع وملاحقة وتنصت على اتصالات الأنترنت والبريد الإلكتروني، أهمها نظام « carnivore » وهو الوضع الذي دفع الإتحاد الأوروبي إلى التساؤل عن مدى توفر الحماية للبيانات الشخصية المنقولة من أوروبا إلى الولايات المتحدة الأمريكية، وعن مدى جواز السماح للشركات الأوروبية تبادل ونقل البيانات الشخصية الى الولايات المتحدة الأمريكية في ظل التخوف من إهدار نظم التتبع

[1] Art 99 : « le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au journal officiel de l'union européenne Il est applicable à partir du 25 mai 2018, le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout état membre. »

[2] L'accord publié au JOCE du 25 aout 2000

* أكدت محكمة العدل الأوروبية في 2015/10/06 أن اتفاقية الملاذ الآمن لتبادل البيانات بين الاتحاد الأوروبي والولايات المتحدة الأمريكية لا تضمن حماية كافية للبيانات الشخصية لمواطني الاتحاد الأوروبي، وذلك على خلفية أعمال التجسس الأمريكية المتكررة على أوروبا، وقد كان هذا الحكم بمناسبة القضية التي رفعها الناشط النمساوي ماكس شيرمز ضد هيأة حماية المعلومات الإيرلندية بعد أن رفضت شكواه بشأن ممارسات شركة فايس بوك حول تخزين بيانات المستخدم في الولايات المتحدة الأمريكية، كما طالب البرلمان الأوروبي بتعليق العمل بهذه الاتفاقية على لسان كلود مورايس رئيس لجنة الحريات المدنية والعدل في البرلمان الأوروبي الذي صرح أن نظام اتفاقية الملاذ الآمن الذي ينظم نقل البيانات الشخصية الأوروبية إلى أمريكا لا يقدم حماية للبيانات الشخصية للأوروبيين.

والملاحقة الأمريكية لقواعد حماية الخصوصية المعلوماتية للمواطنين الأوروبيين، وكذلك إهدار فعالية هيئات الخصوصية التابعة لدول الاتحاد.[1]

لذلك فقد اعتبرت أوروبا على لسان مفوضة العدل في الاتحاد الأوروبي "فيراجوروفا" أن هذا الإتفاق الجديد يعد صفقة جديدة في مجال حماية الحقوق الأساسية للأوروبيين عند نقل بياناتهم الشخصية إلى الشركات الأمريكية، ويسمح للشركات الأمريكية بتلقي البيانات الشخصية من الشركات الأوروبية ضمن مستويات حماية جرى الإتفاق عليها، خاصة بعد التزام الولايات المتحدة الأمريكية بإخضاع عملية اطلاع السلطات العامة فيها على تلك البيانات لأهداف الأمن القومي لقيود وآليات محددة الضمانات والرقابة، كما تعد هذه الاتفاقية آلية قانونية لضمان حماية البيانات الشخصية التابعة لمواطني الإتحاد الأوروبي عندما يتم نقلها خارجه، كما اعتبرت الولايات المتحدة الأمريكية من جانبها من خلال وزير التجارة أن هذا الإتفاق من شأنه تعزيز حماية الخصوصية المعلوماتية، كما يقدم تحسينات مهمة في إطار الشفافية بشأن استخدام البيانات الشخصية.[2]

9) إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي[3]

تعتمد هذه الاتفاقية إطارا قانونيا للأمن في الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، كما تهدف إلى محاولة تحديد الأهداف والتوجيهات الرئيسية لمجتمع المعلومات في إفريقيا، وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيات المعلومات والإتصالات للدول الأعضاء والمجموعات الإقتصادية الإقليمية، وقد اعتبرت هذه الاتفاقية أن انضمام الدول الأعضاء في الإتحاد الإفريقي يعتبر بمثابة تجديد تمسكها بالحريات الأساسية وحقوق الإنسان والشعوب الواردة في الإعلانات والاتفاقيات المعتمدة في الإطار الإفريقي والأمم المتحدة، باعتبارها تنشئ أطارا معياريا حول الأمن في الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، يراعي احترام حقوق المواطنين الأساسية المكفولة بموجب النصوص الأساسية للقانون المحلي وكذلك بموجب الاتفاقيات والمعاهدات الدولية بحقوق الإنسان، لا سيما الميثاق الإفريقي لحقوق الإنسان والشعوب.

واعتبارا لذلك فإن استقراء نصوص هذه الاتفاقية يوحي بوجود سعي إلى تحديد قواعد الأمن الضرورية لإنشاء فضاء رقمي موثوق به في المعاملات الالكترونية وحماية المعطيات ذات الطابع الشخصي، من خلال إيجاد قواعد قانونية تحمي المعطيات ذات الطابع الشخصي وأنظمة المعلومات، وفي ذلك استجابة للاحتياجات المتمثلة في وضع تشريعات متناسقة في مجال الأمن الإلكتروني بالدول الأعضاء في الإتحاد الإفريقي، مستهدفة أن تضع كل دولة طرق آلية قادرة على مكافحة الانتهاكات للخصوصية، والتي قد تنشؤ عن جمع ومعالجة ونقل وتخزين واستخدام بيانات ذات طابع شخصي، مع ضرورة التزام أي مؤسسة عند

[1] منى الأشقر، محمود الأشقر، مرجع سابق، ص103.

[2] جريدة الشرق الأوسط، مقال بعنوان أوروبا وأمريكا تراجعان اتفاق درع الخصوصية لحماية البيانات، منشور يوم 18 اكتوبر2018 عدد رقم 14569 متوفر على الرابط https://aawsat.com/home/article/1431311

[3] أبرمت في مالابو، غينيا الإستوائية، بتاريخ 27 جوان 2014 متوفرة على الرابط. www.au.imt/ أطلع عليه يوم 2020/05/26.

معالجتها لهذه المعطيات احترام الحريات والحقوق الأساسية للأفراد، مع الأخذ بعين الاعتبار في نفس الوقت مصالح هاته المؤسسات مراعاة لأفضل الممارسات المعترف بها على الصعيد الدولي.

وهو الأمر الذي وقفت على تأكيده دباجة هاته الاتفاقية عندما اعتبرت أن حماية البيانات ذات الطابع الشخصي والحياة الخاصة عموما تشكل تحديا رئيسيا لمجتمع المعلومات بالنسبة للسلطات الحكومية والأطراف المعنية الأخرى على حد سواء، وأن هذه الحماية تقتضي توازنا بين استخدام تكنولوجيا المعلومات وحماية الحياة الخاصة للمواطنين في نشاطاتهم اليومية أو المهنية مع ضمان حرية تداول المعلومات، كما تحرص الدول على إنشاء سلطة إدارية تتكفل بتوفير هذه الحماية للمعطيات الشخصية.

ولذلك نجد أن هذه الاتفاقية اعتبرت من أهم آليات الحماية للخصوصية المعلوماتية، هي الحماية الجزائية سواء من حيث القانون الجزائي الموضوعي بالدعوة إلى وضع سياسات لاعتماد جرائم جديدة خاصة بالاعتداء على المعطيات ذات الطابع الشخصي ومواءمة نظام العقوبات الموجود فعليا في الدول الأعضاء مع المناخ التكنولوجي في العصر الحديث وبيئة تكنولوجيا المعلومات والاتصالات، أو من حيث القانون الجزائي الإجرائي من خلال تحديد الآليات لتكييف الإجراءات التي تكون مناسبة للبحث والتحري عن الجريمة ذات الطبيعة المعلوماتية.

وعلى المستوى العربي فإن القانون الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، الذي اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 495 د 19 بتاريخ 2003/10/08 والمعتمد كذلك من طرف مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 د 21 في سنة 2004حث ّ على المعاقبة على مجموعة من صور السلوك الإجرامي التي تمس الحق في الخصوصية بواسطة نظام معلوماتي، وهو ما نصت عليه المادة 16من هذا القانون، حيث تنص على أنه "كل من اعتدى على أي من المبادئ أو القيم الدينية أو الأسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها يعاقب بالحبس مدة لا تقل عن..."

كما نصت المادة 08 من مشروع القانون المذكور على معاقبة كل من تنصت أو التقط أو اعترض عمدا بدون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.[1]

والتالي اعتبر هذا المشروع الإسترشادي أن حقيقة التعدي على الحق في الخصوصية بوسائل معلوماتية أمر وارد، لذلك عاقب على أي فعل بوسيلة معلوماتية من شأنه انتهاك حرمة الخصوصية، وترك للمشرع الوطني لكل دولة أن يفصل في هذه المسألة عند التصدي لها.

بالاضافة إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 أين أبدت الدول العربية الموقعة حسب ما ورد في ديباجة هذه الإتفاقية رغبتها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وذلك اقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص677.

المعلومات، مع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، لذلك فقد نصت المادة الرابعة عشرة منها على تجريم الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

المطلب الثاني: مفهوم الخصوصية المعلوماتية

لقد شهدت نهاية الستينات من القرن الماضي انطلاق الإهتمام بحماية الحياة الخاصة من مخاطر التكنولوجية المعلوماتية الحديثة، حيث تمكن هذه التقنيات الحديثة من تخزين واسترجاع وتحليل كميات هائلة من المعطيات الشخصية، والتي تم تجميعها من طرف المؤسسات والدوائر الحكومية، وكذا من قبل الشركات الخاصة[1]، وهو الأمر الذي انطلق معه مفهوم حماية المعطيات الشخصية من مخاطر المعالجة الآلية، وأثير بذلك لأول مرة وبشكل متزايد مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية.

لقد مر التطور التكنولوجي المعاصر بمرحلتين أساسيتين هما مرحلة تكنولوجيا الإتصالات الإلكترونية ومرحلة تكنولوجيا المعلومات، وعلى الرغم من الفوائد الكبيرة التي حملها معه هذا التطور التكنولوجي، والتي لا يمكن إنكارها في تسيير شؤون المجتمع ومواجهة متطلباته نظرا لغزارة المعلومات المتدفقة والقدرة على تخزينها ومعالجتها واسترجاعها، إلا أنه ظهرت معه آثار سلبية ناجمة عن سوء استخدام الحواسيب، مما أثار مشاكل عديدة نالت حظا وافرا من دراسات الباحثين، ومن أهم المشاكل المتصلة بالحاسوب والتي تم التصدي لها وتطوير مفاهيمها هو الحق في الخصوصية في مجال المعلوماتية، خاصة مع ظهور ما اصطلح على تسميته ببنوك المعلومات[2]، فهذه الأخيرة أي بنوك المعلومات تقوم بتكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، وذلك من خلال معالجة المعطيات ذات الطابع الشخصي بواسطة أجهزة الكمبيوتر، لإخراجها بعد ذلك في صورة معلومات تفيد مستخدمين مختلفين بعد عمليات الحوسبة المختلفة من تسجيل وتصنيف ومعالجة لهذه المعطيات[3]، إذ أضحت الحواسيب مستودعات رقمية لبياناتنا الشخصية، وأضحت قواعد البيانات هذه مصطلحا مألوفا منذ ثمانينات القرن المنصرم في القوانين الوضعية لكثير من الدول،وكذلك في مفاهيم الفقه القانوني وجديرة بالحماية القانونية.[4]

[1] محمود إبراهيم غازي، مرجع سابق، ص276.

[2] علي أحمد عبد الزعبي، مرجع سابق، ص296.

[3] أسامة عبد الله قايد، مرجع سابق، ص48.

[4] سوزان عدنان، إنتهاك حرمة الحياة الخاصة عبر الانترنت، مقال منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث 2013، ص423.

فمن المبادئ الأساسية أن تخزين المعطيات الشخصية في الحواسيب لا يعني أن هذه المعطيات قد انتقلت من الخصوصية إلى العلانية، كما أن رضا أصحابها بالتجميع والتخزين لا يعني حرية تداولها ونقلها إلى الكافة.[1]

ومن جهة أخرى فإن ظهور الأنترنت وشيوع استخدامها في كافة مجالات الحياة تقريبا، أدى كذلك إلى نماء التوجه نحو جمع البيانات المتوفرة في العالم الحقيقي باعتبارها تصبح أكثر سهولة في بيئة الأنترنت من حيث القدرة على الوصول إليها وأكثر ملاءمة للتبويب من خلال تقنيات الكومبيوتر، وتصبح كذلك أسهل للتبادل في ضوء وسائل تبادل المعلومات بكل أشكالها التي أتاحتها الأنترنت وبرمجيات التصفح والتبادل والنقل.[2]

وبالرغم من أن وسائل التواصل الحديثة والمتمثلة في شبكة الأنترنت ساعدت على سهولة وسرعة التبادل الإلكتروني للبيانات، فإن ذلك لا يعني ترك البيانات الشخصية التي قدمها أصحابها طوعا أو كرها للحصول على الخدمة المعلوماتية عرضة للمتطفلين hackers أو المخربين crackers دون رقيب، أو استخدامها من قبل من قام بتجميعها في غير الغرض الذي قدمت من أجله، وذلك لأهمية وسرية هذه البيانات بالنسبة للأشخاص المتعلقة بهم.

الفرع الأول: تعريف الخصوصية المعلوماتية

إنه من الصعب الوقوف على تعريف موحد لمفهوم الخصوصية المعلوماتية، إلا أن الفضل في توجيه نتباه لمفهوم الخصوصية المعلوماتية يـ ٍ عزى إلى مؤلفين أمريكيين، الأول كتاب الخصوصية والحرية privacy and freedom لمؤلفه alan westin عام 1967 والثاني كتاب عتداء على الخصوصية the assault on privacy لمؤلفه miller "ميلر"، فقد عرف ويستن الخصوصية المعلوماتية بأنها "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم إلى الغير"، في حين عرفها ميلر والذي جاء تعريفه لها أكثر شمولية وعمقا حينما عرف الخصوصية المعلوماتية بأنها "قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم".[3]

ومن ثم برز هذا المفهوم خاصة مع التدخل المتزايد للحكومات وحتى الخواص في إنشاء بنوك المعلومات، وأصبح الفرد مجموعة من البيانات المتعددة والتي يمكن تجميعها من أجل تكوين معرفة حقيقية عنه، وأصبح الحق في حماية البيانات أو المعطيات الشخصية من المظاهر الرئيسية للحق في الخصوصية في

[1] عمر أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، طبعة سنة 2000 القاهرة، ص155. وكذلك محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثالث 2009، عمان الاردن، ص62.

[2] طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الانترنت، دراسة مقارنة، مذكرة ماجستير قانون جنائي، كلية الحقوق، جامعة بسكرة 2007/2006، ص82.

[3] بولين انطونيوس أيوب، مرجع سابق، ص56

مجال المعلوماتية، خاصة أمام ما فرضته تكنولوجيا المعلوماتية من سهولة الحصول عليها وبساطة الإطلاع والكشف عنها بطرق مميزة ومثيرة للانتباه.[1]

ومن أهم التعريفات التي ساقها الفقه للخصوصية المعلوماتية انطلاقا من هذا المفهوم، "أنها قدرة الأفراد في السيطرة على معلوماتهم الشخصية وحرصهم أن تضل في سرية"، أو هي "حق الفرد في أن يقرر متى وكيف وإلى أي مدى يمكن تبادل المعلومات التي تخصه مع الآخرين"، أو هي "رغبة الشخص في التحكم أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية".[2]

كما عرفت أيضا على أنها "قدرة الشخص على التحكم في سرية بياناته ومعلوماته الشخصية والتحكم كذلك فيمن يمكنهم الوصول إلى هذه المعلومات، سواء كانوا أفرادا آخرين أو حكومات أو حواسيب"، كما عرفها البعض الآخر بأنها "حق الأفراد في أن يحددوا لأنفسهم متى وكيف و إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين، وبأن يضبطوا عملية جمع المعلومات الشخصية عنهم، وكيفية معالجتها آليا وحفظها وتوزيعها واستخدامها في صنع القرار الخاص بهم أو المؤثر فيهم"[3].

يبدو واضحا من هذه التعاريف العديدة أن الحفاظ على حق الشخص في خصوصيته المعلوماتية يقوم بالأساس على حماية البيانات الشخصية له، إذ لا يمكن التفريق بين حماية البيانات الشخصية والحق في الخصوصية المعلوماتية، فهذه الأخيرة تعني بشكل أساسي المحافظة على السرية ومنع التدخل فيما يعتبر حميمية الشخص وأسراره عبر حماية بعض البيانات ذات الطابع الشخصي، بشكل يمنع انتشار المعلومات التي تكشف عن الحياة الخاصة أو تجعلها عرضة للإنكشاف عند عملية جمع المعطيات وتخزينها ومعالجتها[4] استنادا إلى مبدأ النزاهة والأمانة في التعامل بالمعطيات.

وهو الأمر الذي أكده التقرير الذي جاء به الأمين العام للأمم المتحدة الذي شمل دراسة المشاكل المتعلقة بحقوق الإنسان الناجمة عن التطور العلمي والتكنولوجي، لاسيما اعتداء الحاسب الآلي على الحياة الخاصة معتبرا أن هذا الأخير يعد من أدوات المراقبة، و أنها من أخطر التهديدات على الحرية الشخصية في الوقت الحاضر، وتتمثل الحرية الشخصية في سهولة إعداد البيانات والمعلومات وقدرة اختزالها وسرعة استخدامها واستعادتها، فالحاصل أن هناك نوعا من البيانات تعتبر معلومات خاصة كونها تتعلق بالشخص ذاته،وتنتمي إلى كيانه كإنسان مثل الإ سم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي إذن معلومات تأخذ شكل بيانات تلزم الإلتصاق بكل شخص طبيعي، وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل فلسفة المعلوماتية المعاصرة، سيما وأن

[1] A. Michael Froomkin, The death of privacy. Stanford law review; vol 52 may 2000 p1468 disponible sur le site: http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf

[2] فهد عبد العزيز سعيد، دور تقنية المعلومات في حماية خصوصية البيانات، مركز التميز لأمن المعلومات، المقالات العالمية، جامعة الملك سعود الرياض 2010، ص02

[3] سوزان عدنان، مرجع سابق، ص433.

[4] منى الأشقر جبور، محمود جبور، مرجع سابق، ص22.

فكرة العالم الرقمي لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات، ومن هنا ظهر ما يعرف بالخصوصية المعلوماتية.

وعليه يمكننا القول إذن أن الخصوصية المعلوماتية هي حماية البيانات الشخصية، لكن الخصوصية ليست هي حماية البيانات ذلك أن هذه الأخيرةهي فرع من الخصوصية تتعلق بمواجهة الإعتداءات على البيانات الشخصية، وتنظم الحق في حماية هذه البيانات وسيطرة صاحبها عليها في مواجهة القوى الرقابية المحتملة لأنظمة الكومبيوتر من خلال وضع قواعد معينة تحكم جمع ومعالجة البيانات الشخصية في عصر المعلوماتية[1]، وبالتالي فإن هناك ترادفا بوجه عام قائم ما بين اصطلاح الخصوصية المعلوماتية وحماية البيانات الشخصية وليس بين الخصوصية وحماية البيانات.

أما عن شيوع استخدام اصطلاح الخصوصية منفردا دون إلحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات الشخصية، فهو أمر يرجع إلى أن تعبير الخصوصية شاع بهذا الوقع في ظل تزايد مخاطر التقنية إلى حد ارتباطها بهذهالمخاطر في الإستخدام، وكأنه ينحصر في نطاقها وبيئتها ذلك أن أشد ما يمكن أن يمثل تغولا ً على هذا الحق وانتهاكا له هو الوسائل التقنية ومخاطر المعالجة الآلية للبيانات الشخصية.[2]

وبهذا يمكننا القول أن الفقه قد ساهم في إثارة مسائل نظام خصوصية المعلومات وتوضيح ملامحه، في ظل التطورات الحاصلة في مجال تقنية المعلومات، وتحديدا إنشاء بنوك المعلومات وإجراء عمليات المعالجة والتحليل للبيانات الشخصية بواسطة الكومبيوتر.

ومن الدراسات الواسعة بشأن المسائل المتصلة بالخصوصية المعلوماتية مثلا، تلك الدراسة التي أعدها البروفيسور ميشال جوناتون michael jonathon بعنوان الخصوصية وحقوق الإنسان privacy and human rights» تحت إشراف اليونسكو، حيث قام هذا الأخير بتقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالميا، مستعرضا الصعوبات والتباينات الثقافية في استخدام مصطلح الخصوصية واختلاف المفهوم القانوني له بين النظم القانونية المختلفة*، موضحا في هذا الصدد أن المفهوم الذي قامت على أساسه تشريعات شمولية في حماية البيانات

[1] مروة زين العابدين، مرجع سابق، ص49.

[2] منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية 2013، ص5.

* أوضحت الدراسة في إطار المفهوم القانوني للخصوصية ثلاث مواقف:

أولا: موقف مؤتمر دول الشمال الأوروبي: ويتضمن المبادئ الناتجة عن لقاء الخبراء القانونيين في ستوكهولم عام 1967 والذي نتج عنه إعلان غير ملزم حول معنى الحق في الخصوصية وهي المبادئ نفسها التي قام عليها فيما بعد أول تشريع شمولي لحماية البيانات وهو القانون السويدي لعام 1973.

ثانيا: موقف القانون المدني اللاتيني، وهو المفهوم الذي يتقارب مع الموقف الأمريكي والذي يقوم على توسيع القواعد الدستورية والمبادئ العامة لحماية طائفة من الحقوق كالحق في الخصوصية من أنشطة الرقابة الحكومية متى توافر للفرد اعتراف مقبول بخصوصيته.

ثالثا: موقف نظام القانون العام الأنجلوأمريكي والذي يطبق مبادئ الحماية وفق الحالات الفردية، مثل القوانين في بريطانيا التي تمثل بوضوح هذا النظام، حيث لم يرد صراحة مبدأ حماية الخصوصية في قانون حماية البيانات البريطاني لعام 1998 وسابقه لعام 1984، فكلاهما لا يقيمان مفهوم مبدأ حماية الخصوصية صراحة وإن كانا ينظمان مبادئ حماية البيانات الخاصة والتعامل معها.

الشخصية يقوم على اعتبار خصوصية المعلومات مزيجا من مكنات أو حقوق الأفراد من خلال التوازن بين الحق في الوصول إلى المعلومات والتنظيمات الإدارية لملفات الكمبيوتر.

A combinaition of legal remedy available to the individual through rights of access and the administrative regulation of computerized records

ومن خلاصة هذه الدراسات الأكاديمية، فإنه قد جرى التعامل مع الخصوصية من حيث مفهومها كحق لمنع إساءة استخدام الحكومة والإدارات وحتى الشركات الخاصة للبيانات الشخصية التي يصار إليها معالجتها آليا أو الكترونيا، أو تقييد استخدامها وفقا للقانون فقط[1].

وعلى هذا الأساس يمكن القول أنه إذا كان الحق في الخصوصية بمفهومه التقليدي يعني حق الفرد في أن يقرر بنفسه متى وإلى أي حد يمكن للغير أن يطلع على شؤونه الخاصة كما سبق أن تم إيراده في هذا الإطار، فإن هذا الحق في إطار الإعتداءات التي تطال الحياة الخاصة بواسطة التقنيات المعلوماتية الحديثة أصبح يعني حق الفرد في أن يقرر بنفسه متى وكيف وإلى أي مدى يمكن أن تصل بياناته الشخصية إلى الآخرين.[2]

وهنا يبرز وبكل وضوح أن الحق في حماية البيانات أو المعطيات الشخصية يعد أحد عناصر الحق في الخصوصية بوجه عام إلى جانب العناصر التقليدية الأخرى لهذا الحق.

الفرع الثاني: طبيعة المعطيات الشخصية المتعلقة بالخصوصية المعلوماتية

يثور التساؤل في هذا الصدد حول ماهية البيانات التي يشكل المساس بها تعريضا لخصوصية الأفراد في إطار مجتمع المعلومات الإلكترونية للانتهاك، بمعنى آخر هل كل معلومة يتم تخزينها ومعالجتها أو تداولها عبر قواعد البيانات وشبكة الأنترنت تثير مسألة الخصوصية الشخصية في المجال المعلوماتي[3]، وعليه فالسؤال الذي نحن في صدده هو البحث عن الموضوعات التي تدخل ضمن الحماية القانونية المقررة للحق في الخصوصية المعلوماتية، فهل كل ما اتصل بالشخص من معلومات يعتبر بالضرورة مما يندرج تحت الحماية التي تعطى للشخص وفقا للحق في الخصوصية المعلوماتية؟ أم أن هناك أمورا لا تدخل ضمنها وإن ارتبطت بالإنسان.

يذهب الفقه القانوني إلى اعتبار أن البيانات المجهولة وهي التي لا تدل على من تتعلق به لا تثير أية صعوبات، ذلك أن المجهول لا خصوصية له، لكن الأمر يدق في حالة المساس بالبيانات المتعلقة بأشخاص معرفين أو من شأنها أن تسمح بالتعرف عليهم بطريقة مباشرة أو غير مباشرة،[4]وهي ما يعرف بالبيانات سمية أو المعطيات ذات الطابع الشخصي، أو المعطيات الشخصية، والملاحظ أن البيانات أو المعطيات لا

[1] بولين أيوب، مرجع سابق، ص57.

[2] محمد حسين منصور، المسؤولية الإلكترونية، الطبعة الأولى، منشأة المعارف الإسكندرية، مصر 2006، ص59.

[3] محمد أمين الشوابكة، مرجع سابق، ص62.

[4] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتبكة عبر الأنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، الطبعة الأولى دار النهضة العربية، القاهرة 1999، ص43.

تكون شخصية إلا لكونها ملتصقة بشخص بعينه، فالإستلاء على البيان لا يمثل خرقا في حد ذاته إلا إذا كان مرتبطا بشخص معين.

والملاحظ أيضا أن الشخص محل البيانات قد يكون معرفا أو قابلا للتعريف، وأن تلك البيانات أو المعطيات تكون في استخدامها من أجل تعريف الشخص سواء منفردة أو مدمجة مع بيانات أخرى.

كما تم الإقرار كذلك في هذا الصدد بعدم ضرورة توثيق البيانات حتى تعتبر بيانات شخصية وتشملها الحماية القانونية، بل يكفي لضمان هذه الحماية أن تكون البيانات ملتصقة بشخص بعينه، فعينات التحاليل الطبية التي تسحب من جسم إنسان معين قد تتغير نتائج هذه التحاليل من مرة إلى أخرى، ومن ثمة فهي معلومات غير موثقة، ولكنها تعد بيانات شخصية، والإعتداء عليها بالاستيلاء أو النشر دون رضا صاحبها يدخل تحت مظلة حماية البيانات الشخصية.[1]

لذلك ومن هذا المنطلق أوضحت لجنة «lindop» (lindop committees) الإنجليزية بأن البيانات الشخصية يمكن أن تعتبر أي معلومات تتصل بأي شخص خاضع لنظام المعلوماتية ويمكن التعرف عليه من خلالها أو يمكن أن تؤدي إلى معرفته، بما في ذلك المعلومات التي يمكن أن يعرف بواسطتها، وهو الرأي الذي ذهبت إليه لجنة justice الإنجليزية أيضا عندما أشارت إلى أن التطفل على الخصوصية المعلوماتية يشمل الاستخدام غير المصرح به أو الكشف لما هو من البيانات السرية أو حتى نشر حقائق إذا كانت تتصل بشخصية الإنسان.[2]

فطبيعة البيانات المكونة للخصوصية المعلوماتية إذن هي نوع من المعلومات يطلق عليها المعلومات الشخصية، كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان، مثل الإسم، العنوان، رقم الهاتف وغيرها من المعلومات التي تأخذ شكل بيانات تلزم الإلتصاق بكل شخص طبيعي معرف أو قابل للتعريف.

وقد يحصل أن يشترك أكثر من شخص في بيان شخصي واحد، وهو أمر لا يخرجها من دائرة البيانات الشخصية، فعنوان السكن الذي تقطنه أسرة يعتبر بيانا شخصيا مشتركا لجميع أفرادها، كما تعد التقارير الطبية من البيانات الشخصية للشخص المعني بها وتدخل ضمن تعريف البيانات الشخصية وبالتالي تشملها الحماية القانونية، وهي في الوقت ذاتهتعتبر من البيانات الشخصية للطبيب، حيث أنه يعبر عن رأيه في شخص آخر، وبالتالي فإن التعدي على التقارير الطبية يعد انتهاكا للبيانات الشخصية للشخص المعالـ ـج المعني بهذه التقارير، والبيانات الشخصية للطبيب على حد سواء، كما تظل أيضا المعلومات مصنفة أنها بيانات شخصية حتى وإن أصبحت متاحة للعامة عن طريق التنازل طواعية من الشخص صاحب هذه البيانات، فمن يتقدم لملئ استمارات يضع فيها بياناته الشخصية للحصول على خدمة، فهنا يتنازل الشخص عن مجموعة من البيانات الشخصية نظير تلقيه تلك الخدمة، ويكون من حق مقدم الخدمة استغلال هذه البيانات بالبحث أو التسجيل في حدود الخدمة المقدمة، دون أن يعد هذا التنازل سببا لنزع الحماية عن هذه البيانات الشخصية المفصح عنها، والحال كذلك لا يعتبر الرضا

[1] مروة زين العابدين، مرجع سابق، ص72.

[2] محمد عبد المحسن المقاطع، مرجع سابق، ص74.

بإعطاء بيانات شخصية لأحد المواقع عبر شبكة الأنترنت رضاء بتداول هذه البيانات وإخراجها عن طابعها الشخصي.

وبالتالي فإن المعلومات قد تكون ذاتية أو موضوعية وكلاهما غالبا ما تتعلق بالحياة العامة للأفراد، لكن المعلومات الشخصية المخزنة في بنوك المعلومات هي التي تمس بالحق في الخصوصية المعلوماتية.

ومن هذا المنطلق يفترض بأي مسؤول عن معالجة البيانات والذي يحاول تحديد ما إذا كانت هذه البياناتشخصية، أن ينتبه إلى قدرتها على التعريف بالشخص الطبيعي الذي تعود إليه.

وترتبط صحة الجواب هنا حول اعتبار البيانات شخصية أم لا بمدى شمولية نظرة المسؤول عن المعالجة ومعرفته بالمعالجات التي تتم على البيانات، إضافة إلى قدرته على تصور وتوقع إمكانات سوء الإستخدام، وهو الأمر الذي يمكن أن ينتج عن التحول عن أهداف المعالجة وغايتها، وهذا ما يجعل تحديد البيانات الشخصية أمرا صعبا يفترض جهدا ملحوظا من قبل المعنيين بالمعالجة، سيما في ظل تقنيات البيانات الضخمة التي تتيح معالجة كميات هائلة من البيانات لاستخراج القيمة المضافة، وهو ما يزيد الأمور تعقيدا من ناحية تحديد البيانات الشخصية.[1]

كما نشير هنا أيضا إلى ذهاب البعض في تحديد نطاق البيانات الشخصية المتعلقة بالأفراد إلى استعمال معيار آخر، وهو تمييزها عن البيانات العامة، فقد عرف هذا الإتجاه البيانات الشخصية بأنها تلك البيانات غير العامة أو التي لا تتعلق بالشخص، وأن كل بيان شخصي هو ذلك البيان الذي لا يدخل في نطاق الإطار العام، ومن ثم جرى تحديد البيانات الشخصية بأنها تلك البيانات غير المنشورة، والتي لا يمكن الوصول إليها وغير المتاحة في السجلات العامة، وهذا المبدأ اعتمده المشرع الألماني في تعريفه للبيانات المالية معتبرا إياها أنها بيانات غير عامة، ومن ثم فهي بيانات شخصية[2].

وبالرغم من المعايير التعريفية للمعطيات المحددة لكونها شخصية والتي جاءت بها أغلب التشريعات في مجال حماية المعطيات ذات الطابع الشخصي، إلا أن صعوبات كثيرة قد تطرح أمام القضاء الذي يملك السلطة التقديرية في تحديد مدى توافر الطابع الشخصي لمعطيات معينة، مما يستلزم تقدير كل حالة على حدا بحسب ظروفها وملابساتها، مع الأخذ بالاعتبار ضرورة التوفيق بين حماية الحق في الخصوصية والتدفق الحر للمعلومات وكذلك التطور التكنولوجي الحديث.[3]

أولا: تعريف المعطيات ذات الطابع الشخصي

لقد أولت التشريعات عبر مختلف الدول إهتماما متعاظما لحماية المعطيات ذات الطابع الشخصي، نظرا لاعتماد أنماط الحياة المعاصرة باطراد على البنى التكنولوجية في مختلف أوجه الإدارة والإتصال، ما نتج عنه تعاظم في كمية البيانات التي تحوزها الدولة والمؤسسات والشركات الخاصة،وهو الأمر الذي استدعى

[1] منى الاشقر جبور، محمود جبور، مرجع سابق، ص76.

[2] مروة زين العابدين، مرجع سابق، ص82.

[3] غنام محمد غنام، الحماية الجنائية والإدارية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكومبيوتر، مجلة الأمن والقانون كلية الشرطة دبي العدد 02 جويلية 2003، ص94.

أن ينظر المشرع بوجه العناية إلى الكيفية التي يتم بها جمع وحفظ ومعالجة البيانات التي تحتوي على معلومات ذات طابع شخصي، لما قد ينتج عن إساءة استخدامها من انتهاك للحق في الخصوصية.

وبسبب الطابع الفني لمصطلح المعطيات ذات الطابع الشخصي أو البيانات الشخصية فقد تدخلت التشريعات في وضع تعريف لهذا المصطلح، حيث شكلت أساسا لعمل الفقه والقضاء ولجميع الأجهزة الإدارية التي تسهر على تطبيق القانون، ومن ثمة تحقيق ما يسمى بالأمن القانوني*.

فقد عملت مجموعة من التشريعات المقارنة على وضع تعريف للمعطيات ذات الطابع الشخصي، سار المشرع الجزائري على نهجها في تعريفه لهذه المعطيات في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخ

لقد عرفت الإتفاقية الأوروبية رقم 108 الصادرة عن مجلس أوروبا في 28 جانفي 1981 والمتعلقة بحماية الأشخاص في مواجهة المعالجة الآلية للمعطيات ذات الطابع الشخصي من خلال المادة 2/أ المعطيات الشخصية، على أنها "كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه".[1]

وبعبارة قريبة نصت المادة 02/أ من التوجيه أو الإرشاد الأوروبي رقم 46/95 بأن "المعطيات ذات الطابع الشخصي هي: "كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، ويعد قابلا للتعرف عليه الشخص الذي يمكن معرفته بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم تعريفه أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته، الطبيعية الفيزيولوجية، النفسية، الإقتصادية، الثقافية أو جتماعية" وهو نفس التعريف الذي حافظ عليه التنظيم الأوروبي الصادر عن البرلمان الأوروبي والمجلس الأوروبي بتاريخ 18 ديسمبر 2000 تحت رقم 45/2001 في المادة 02/أ منه[2]، وقد عرف النظام العام

* يعتبر التعريف عنصرا من العناصر المؤسسة للأمن القانوني من حيث تحديده للمفاهيم القانونية ومحتوى الإلتزامات والحقوق والأفعال الجرمية وغير ذلك مما يلجأ إليه في تطبيق القانون، ويستند الأمن القانوني إلى وضوح القوانين وحدود التطبيق لأية قاعدة قانونية، وفي هذا السياق يعتبر التعريف التشريعي مانعا إلى حد بعيد لتضارب الأحكام وضامنا لتطبيق التشريع بشكل عادل وسوي، فضلا عما يوفره من اطمئنان للمواطن من خلال وجود قاعدة قانونية واضحة تبنى على مفاهيم محددة يستطيع اللجوء إليها كإطار يضمن حمايته، كما أن هناك اختلافا حول ما يعتبر بيانات شخصية أو مجرد معلومات يتحفظ أصحابها على نشرها. لكن مقتضيات الأمن القانوني تفترض اعتماد قواعد واضحة لما يعتبر بيانات شخصية، بغية وضع النصوص القانونية المناسبة وتأمين الحد الأدنى من الحماية المطلوبة.

[1] تنص المادة 02: "تعريفات لغاية هذه الاتفاقية.

أ-"ذات طابع شخصي تعني كل معلومة تتعلق بشخص ذاتي معرف أو قابل للتعريف" (الشخص المعني)

[2] Règlement (CE) n°45/2001 du parlement européen et du conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes communautaires et à la libre circulation de ces données.

Article 02 :

Définition : « aux fins du présent règlement on entend par :

a/données à caractère personnel : toute information concernant une personne physique identifié ou identifiable (ci après dénommée personne concernée) est réputée identifiable une personne qui peut etre identifié directement ou indirectement, notamment par référence à un numéro d'identification ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »

الأوروبي لحماية المعطيات الشخصية « RGPD »[1] المعطيات ذات الطابع الشخصي بتعريف أكثر دقة وتناسبا مع التطورات الحاصلة في المجال المعلوماتي، باعتبارها أي معلومات تتعلق بشخص طبيعي معرف أو قابل للتعرف عليه، ويعتبر شخصا طبيعيا قابلا للتعرف عليه كل شخص طبيعي يمكن معرفته بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى عنصر معرف مثل الإسم، ورقم التعريف، بيانات الموقع، معرف الإتصال عبر الأنترنت، أو لواحد أو أكثر من العناصر المميزة لهويته الفيزيولوجية، الجينية، النفسية، الإقتصادية، الثقافية أو الاجتماعية.

وقد شكل كل من التعريف الوارد في الإتفاقية الأوروبية والإرشاد الأوروبي 46/95 مصدرا أساسيا لمختلف التشريعات، سيما الأوروبية منها في مجال حماية المعطيات ذات الطابع الشخصي، حيث عملت هذه التشريعات على ملاءمة نصوصها القانونية مع الإرشاد الأوروبي المذكور آنفا.*

فقد عرف المشرع الفرنسي المعطيات ذات الطابع الشخصي في المادة 2/2 من القانون 17/78 المتعلق بالمعلوماتية، الملفات والحريات[2] على أنها "كل معلومة متعلقة بشخص طبيعي معرف أو يمكن التعرف عليه بصفة مباشرة أو غير مباشرة بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر مميزة له، لتحديد ما إذا كان الشخص قابلا للتعرف عليه يلزم الأخذ بالاعتبار مجموع الوسائل التي من شأنها التمكين من تعريفه".

كما عرفها القانون البلجيكي لحماية المعطيات ذات الطابع الشخصي الصادر سنة 1992 والمعدل سنة 1998 بأنها "كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، ويعد قابلا للتعرف عليه كل شخص يمكن التعرف عليه بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية، الفيزيولوجية، النفسية، الاقتصادية أو الاجتماعية.

والمشرع التونسي عرفها في القانون رقم 63 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية حيث نصت المادة 04 على أنه "تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة أو غير

---

[1] Règlement (CE) n°2016/679 du parlement européen et du conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant le dirictives 95/46/CE (règlement général sur la protection des données).

* نأخذ بعض التعريفات للمعطيات الشخصية في بعض القوانين، مثل القانون

في قطر: عرف القانون القطري رقم 13 لسنة 2016 المؤرخ في 2016/11/03 في المادة الأولى منه البيانات الشخصية بأنها "بيانات عن الفرد الذي تكون هويته محددة أو يمكن تحديدها بصورة معقولة سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى".

في كندا: عرف قانون حماية البيانات الشخصية والمستندات الالكترونية البيانات الشخصية بأنها المعلومات الخاصة بشخص معرف ولكن لا تشمل الاسم، الوظيفة عنوان وهواتف العمل لموظف يعمل بإحدى الشركات.

[2] L'article 2/2 de la loi n 78/17 du 06 janvier 1978 relative a linformatique aux fichiers et aux libertes dispopse que : » Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »

مباشرة باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك"، وأردفت المادة 05 من نفس القانون أنه يعد قابلا للتعريف الشخص الطبيعي الذي يمكن التعرف عليه بصورة مباشرة أو غير مباشرة من خلال مجموعة من المعطيات أو الرموز المتعلقة خاصة بهويته أو بخصائصه الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية".

وكذلك عرف المشرع المغربي المعطيات الشخصية في القانون 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، حيث نصت المادة 1/1 من هذا القانون على أنه "يقصد بـ معطيات ذات طابع شخصي كل معلومات كيفما كان نوعها بغض النظر عن دعامتها، بما في ذلك الصوت والصورة والمتعلقة بشخص ذاتي معرف أو قابل للتعريف عليه والمسمى بعده "بالشخص المعني"، ويكون الشخص قابلا للتعرف عليه إذا كان بالإمكان التعرف عليه بصفة مباشرة أو غير مباشرة، ولاسيما بالرجوع إلى رقم تعريف أو عنصر أو عدة عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الإقتصادية أو الثقافية أو الإ جتماعية"

وفي الولايات المتحدة الأمريكية يطلق على البيانات الشخصية ببيانات التعريف الشخصي (PII)[1]، وقد عرفها قانون الخصوصية وأمن المعلومات على أنها "المعلومات التي يمكن استخدامها بمفردها أو مع غيرها من المعلومات للتعرف أو لتحديد شخص واحد أو لتحديد الفرد في سياق"[2]

أما عن المشرع الجزائري فإنه و في سياق عمله على ضمان توفير آليات حمائية للمعطيات الشخصية تكون موحدة مع التشريعات المقارنة، فقد اقتبس نفس التعريف الذي وضعه التوجيه الأوروبي 46/95، ذلك حينما نصت المادة 03 من القانون 07/18 المؤرخ في 10 يونيو 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، على أنه يقصد بالمعطيات ذات الطابع الشخصي "كل معلومة بغض النظر عن دعامتها، متعلقة بشخص معرف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الإ جتماعية"

وتطبيقا للتحديد السابق من المقصود بالبيانات الشخصية فإنه يعتبر إسم الشخص، صورته، جنسيته، فصيلة دمه، ديانته، عنوان سكنه، وأي صفة يعين بها كوظيفته، أو صفات شخصية كالبصمة المميزة له عن الآخرين، من البيانات الشخصية التي تحظى بالحماية القانونية، وذلك لاعتبارها جزءا من حقوق الشخصية المرتبطة ارتباطا جوهريا بأحد أهم الحقوق الدستورية اللصيقة بالشخصية الإنسانية ألا وهو الحق في الخصوصية، لذلك فقد أوضح الفقه بأن البيانات التي تحظى بالإهتمام هي المعلومات غير المبهمة عن الشخص وتحدده بشكل ينفي الجهالة بشخصيته[3].

[1] PII : Personel Identifiable Information.

[2] مروة زين العابدين، مرجع سابق، ص68.

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص75.

والملاحظ على مختلف هذه التعاريف التي وضعتها قوانين حماية المعطيات ذات الطابع الشخصي أنها تتسم بخاصيتين هما:

-أن المعطيات ذات الطابع الشخصي لا تتعلق إلا بالأشخاص الطبيعيين.

-أن تعرف المعطيات الشخص المتعلقة به أو تجعله قابلا للتعرف عليه.

فأما عن ارتباط المعطيات ذات الطابع الشخصي بالأشخاص الطبيعيين فقط دون الأشخاص المعنوية، فقد أكد الفقه ذلك واتجه الرأي الراجح فيه إلى أن نطاق المعطيات الشخصية يجب أن يقتصر على الأشخاص الطبيعية فقط، وذلك على اعتبار أن حماية المعطيات الشخصية هو بمثابة حماية للحق في الخصوصية والذي يعد من حقوق الشخصية الإنسانية، والذي يفي حقه في الإ حتفاظ بمعلوماته السرية وعدم اطلاع الغير عليها، ومن ثم كان اتصال هذا الحق بالإنسان يشكل أحد المظاهر الأساسية للشخصية الإنسانية، ولكن مقابل هذا الإتجاه هناك اتجاه ضيق في الفقه يمدد نطاق المعطيات الشخصية كأحد عناصر الحق في الخصوصية إلى الأشخاص المعنوية، وسار في فلك هذا الاتجاه بعض التشريعات التي مدت نطاق قانون حماية المعطيات الشخصية إلى الأشخاص الإ عتبارية، ومن بين هذه التشريعات القانون الفدرالي الأسترالي[1]. أما المستقر عليه في رأي غالب الفقه وغالب القوانين، أن المعطيات الشخصية لا تتعلق إلا بالشخص الطبيعي دون المعنوي، على اعتبار أن القوانين المتعلقة بحماية المعطيات الشخصية إنما شرعت لهدف حماية الحياة الخاصة للأفراد، وأن تمديد مفهوم المعطيات الشخصية ليشمل الشخص المعنوي سيخلق تعارضا في مفهوم سرية الأعمال،[2] وهو ما أكدته فعلا منظمة التعاون والتنمية الإقتصادية (OCDE) في توصيتها المتعلقة بالقواعد التوجيهية المنظمة لحماية الحياة الخاصة والتدفق العابر للحدود للمعطيات الشخصية، حينما اعتبرت أن هذه القواعد تتعلق بالحياة الخاصة للأفراد ولا يمكن أن تفسر في سياق سلامة مجموعة من الأفراد أو من الشركات أو سرية أنشطتها.[3]

إن هذه المسألة تكتسي نوعا من الأهمية، ذلك أنه بالإمكان أن نتواجد أمام مجموعة من الحالات التي يصعب فيها الفصل بين ما هو معطيات شخصية متعلقة بالفرد ومعلومات متعلقة بالشخص المعنوي، فقد تكون هناك معلومات معينة يجب العمل أولا على تصنيفها ما إن كانت تلحق بالشخص الطبيعي لوحده أم تلحق الشخص المعنوي أيضا، وذلك لتحديد نطاق تطبيق القانون، فهل يطبق القانون المتعلق بحماية المعطيات الشخصية في حالة ما إذا ارتبطت بيانات الأفراد بالشخص المعنوي، كارتباط معطيات صاحب الشركة بهذه الشركة، وهل تظل بيانات شخصية ومن ثمة متمتعة بالحماية القانونية للبيانات الشخصية، أم تلحق الشخص المعنوي وتخرج بذلك من دائرة تطبيق قانون حماية المعطيات الشخصية.

[1] محمد عبد المحسن المقاطع، مرجع نفسه، ص65.

[2] Pierre Kayser, la protection de la vie privée par le droit, protection du secret de la vie privée, Preface de Henri MAZEAUD 3 eme édition, Presses Universitaires D aix- marseille economica 1995 p 434

[3] Francois Rigaux, « la loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel, Rev.cr.dr.int.pr n°7 1980 p452

وأبرز مثال على ذلك أن ملفات المقاولات أو الشركات لا تحتوي على المعلومات المتعلقة بالأشخاص المعنوية فقط، بل تضم كذلك معطيات معرفة بالشركاء والمساهمين مثل المعطيات المتعلقة بذممهم المالية.

و لقد اعتبرت اللجنة الوطنية للمعلومات والحريات بفرنسا (CNIL) بأن القانون 17/78 المتعلق بالمعلوماتية والملفات والحريات يعد قابلا للتطبيق بخصوص ملف مقاولة مخصص لمعرفة الإمكان الصناعي والحرفي والتجاري لمجمع صناعي، وذلك فيما يتعلق بممارسة حق الولوج من قبل الأشخاص الطبيعيين الذين يمثلون قانونا المقاولة بمجرد ورود أسماء هؤلاء الأشخاص بالملف كمسيرين مساهمين أو شركاء، مع أن الأمر يتعلق من حيث المبدأ بمعلومات متعلقة بالمقاولة فقط[1]، وحسمت هذه اللجنة المسألة في قرار آخر لها عندما اعتبرت بأن إنشاء ملفات الأشخاص المعنوية عندما تحتوي على معطيات شخصية، يخضع لنفس القواعد التي تحكم إنشاء الملفات التي لا تتعلق إلا بالأشخاص الطبيعيين.[2]

وأما عن خاصية تمكين المعطيات من التعريف بالشخص الطبيعي فإن جميع التعريفات التي أوردتها التشريعات المقارنة وكذا المشرع الجزائري، قد ألزمت حتى تكتسب معطيات معينة الطابع الشخصي أن تعرف بالشخص المتعلقة به، أو تكون قادرة على التعريف به، وهو في اعتقادنا الأمر الذي دفع المشرع الفرنسي إلى استبدال عبارة البيانات الاسمية التي كان يستعملها قبل تعديل القانون17/78بعبارة البيانات ذات الطابع الشخصي استجابة للتوجيه الأوروبي لتعميم استخدام هذه التسمية، وقد جاء التعديل بموجب القانون 801/2004 المؤرخ في 06 أوت 2004 المعدل والمتمم للقانون 17/78،[3] حيث جاء في التقرير المقدم من لجنة المعلوماتية والحريات إلى البرلمان الفرنسي والمتعلق بمناقشة تعديل قانون الحريات والمعلوماتية،أن عبارة البيانات الإسمية يعيبها أنها تحوي لفظ "إسم"، فهي إلحاق الإسم بالبيانات للإشارة إلى ما يمكن أن يعرف الشخص أو يحدد هويته، أما عبارة ذات طابع شخصي فإنها تبدو أكثر تجريدا ووضوحا لتعني البيانات المتعلقة بالأفراد وليس حصريا المتعلقة بأسمائهم أو التي تحمل أسماءهم، ومن ثم فإن عبارة البيانات ذات الطابع الشخصي تكونأصوب مقارنة بعبارة البيانات الإسمية التي كان المشرع الفرنسي يأخذ بها، فالاقتصار على الإسم كمرجع للتعريف بالشخص له مساوئ تتجلى في كونه يحمل نظرة ضيقة تقود إلى تقدير خاطئ لا يأخذ في الحسبان تطور وسائل التعريف غير المباشرة الأخرى.[4]

كما أن التعريف الذي يعتمد على عبارة معطيات ذات طابع شخصي في اعتقادنا يكون أكثر دقة بالمقارنة مع اعتماد عبارة معطيات شخصية، فهذه العبارة الأخيرة قد تستثني بيانات يمكنها أن تساعد على تحديد هوية الشخص، ويرد في هذا السياق البيانات التي لا تعود إلى الشخص الطبيعي وإنما إلى وسائل قد يستعملها، فهي معطيات ليست شخصية بطبيعتها لكنها تكون كذلك بحكم ارتباطها بشخص معين فتكون

[1] André Lucas, Jeans Deveze et Jean Frayssinet, l'informatique et le secret des fichiers. Revue. Admi 1977 p79.

[2] Pierre Kayser, op, cit. p 435.

[3] Loi n 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[4] Ibrahim Coulibaly, la protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse doctorat université de grenoble Spécialité : DROIT PRIVE 2011 p10. Voir aussi André Lucas, Jeans Devese, et Jean Frayssinet. Op.cit, p77

ذات طابع شخصي à caractère personnel ، كرقم تسجيل السيارة، رقم الهاتف الثابت والنقال، لاسيما متى بقيت خارج إطار التنظيم الذي يستهدف حماية البيانات الشخصية، ويسمح هذا الاستبعاد بالتعدي على خصوصية الأشخاص دون رادع نظرا لعدم إمكانية تطبيق النص.[1]

وبالفعل فقد اعترضت اللجنة الخاصة بالمعلوماتية والحريات في فرنسا على قرارين متتاليين صادرين عن محكمة الاستئناف بباريس[2] اعتبرا أن العنوان الخاص برقم التعريف للعنوان الإلكتروني للجهاز « ip» ليس من البيانات الشخصية، كونه يسمح بتحديد هوية الجهاز (الحاسوب) وليس هوية الشخص الذي يستعمل الجهاز، وفي هذا حسب اللجنة خطر يفتح الباب للتعديات على الخصوصية من خلال جمع هذه البيانات من دون الحصول على ترخيص مسبق بذلك، كما هو مقرر لجمع البيانات الشخصية.

لذلك فإن المشرع الجزائري في القانون 07/18 اختار استعمال عبارة المعطيات ذات الطابع الشخصي، شأنه في ذلك شأن أغلب التشريعات ذات الصلة، ليصبح نطاق تطبيقه أكثر اتساعا، ليشمل أي معطيات من شأنها أن تعرف الشخص أو تجعل منه قابلا للتعرف عليه، طالما أن لها طابعا شخصيا، بل أكثر من ذلك فإنه لا يهم إن كانت هذه البيانات صحيحة أم غير صحيحة، فتحديد كون البيان ذو طابع شخصي يمكن من خلاله معرفة الشخص المرتبط به لا يرتبط بصحة البيان من عدمه، ولكن بكونه لصيقا بشخص معين[3]، فتوسيع مساحة أكبر للحماية يعني معدلا أعلى من الثقة، بالإضافة إلى استجابة هذا التعريف لحاجات العصر في مواكبة التطورات المتسارعة في مجال تقنيات المعلومات التي يمكن أن تفرز ما يمكن أن يعتبر كمعطيات ذات طابع شخصي، حيث لم يعد بالإمكان توقع قدرات تكنولوجيا معالجة المعطيات ولا نتائج الجمع بين التقنيات المختلفة على الحياة الشخصية، وعليه فحسنا فعل المشرع عندما أخذ بالتعريف الذي يوسع من مفهوم المعطيات الشخصية ليشمل أي معلومة من الممكن أن تحدد هوية أي شخص بطريقة مباشرة أو غير مباشرة، لأن التضييق في هذا المفهوم قد يسمح للعديد من الجهات بالتعدي على البيانات الشخصية خاصة مع تقدم تقنيات جمع البيانات ومعالجتها، فالبيانات الشخصية مخزنة و موزعة بقواعد بيانات مختلفة، قد لا تدل على هوية الشخص بحد ذاتها، لكن إذا تم ربطها

[1] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، دون تاريخ النشر ص.119

[2] CA Paris, 13e ch., sect. B, 27 avr. 2007, La cour d'appel de Paris avait quant à elle précisé, dans cet arrêt du 27 avril 2007, que « l'adresse IP ne permet pas d'identifier le ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur d'accès l'identité de l'utilisateur ».

CA Paris, 13e ch., sect. A, 15 mai 2007 « que cette série de chiffres en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure ou elle ne se rapporte qu'à une machine et non à l'individu qui utilise l'ordinateur pour se livrer à la contre facon. Voir Jean-Marie Hisquin. L'adresse IP : une donnée à caractère personnel au sens de la loi relative à l'informatique, aux fichiers et aux libertés. Article Publié le 20/01/2017sur le site https://www.actu-juridique.fr/informatique/

« La Cour de cassation considère, dans son arrêt n° 15-22595 du 3 novembre 2016, que les adresses IP (internet protocol) sont des données personnelles protégées au sens de la loi. Il convient à ce titre de faire une déclaration préalable pour le traitement de ces données auprès de la Cnil. Voir Jean-Marie Hisquin article sur le site : www.actu-juridique.fr

[3] مروة زين العابدين، مرجع سابق، ص74.

ببيانات أخرى عن طريق عمليات المعالجة قد تفصح عن هوية الشخص، كما أن هذا التعريف الواسع والمرن يسمح بتطبيق القانون على أية صورة حديثة للبيانات الشخصية يمكن ظهورها في المستقبل.[1]

وفي هذا السياق اتخذت المحكمة الأوروبية لحقوق الإنسان موقفا من اعتماد تعريف واسع للبيانات الشخصية التي يمكنها أن تعرض الحياة الخاصة للإنكشاف في عدد من قراراتها، وذلك بالرغم من أن مفهوم الحياة الخاصة لم يكن قد اتخذ بعده العالمي بعد، فقد اعتبرت في قرارها الصادر بتاريخ 16 فيفري 2000 أن الحياة المهنية تكون مشمولة بالمادة الثامنة من الإتفاقية الأوروبية لحقوق الإنسان التي تحمي الحياة الخاصة، معتمدة أيضا هذه المحكمة على الإتفاقية الأوروبية رقم 108 حول حماية الأشخاص من المعالجة الإلكترونية لبياناتهم الشخصية، مؤكدة بأنها تهدف إلى حماية أية معلومة تخص شخصا معرفا أو قابلا للتعريف.*

إن التوسع في تعريف مصطلح المعطيات الشخصية يتناسب مع الحاجة إلى توفير حماية فاعلة وتأمين معدل أعلى من الثقة والأمان في الفضاء المعلوماتي من جهة، ومواكبة التطورات المتسارعة في مجال تقنية المعلومات من جهة أجرى، حيث لم يعد ممكنا توقع المدى الذي تبلغه قدرات تكنولوجيا معالجة المعطيات الشخصية سواء على حرمة الحياة الخاصة أو على أمن الدول التي تجمع وتعالج وتتبادل هذه المعطيات الشخصية.[2]

والشيء الملاحظ على مجمل التعاريف في مختلف القوانين رغم ميلها إلى التعريف الواسع للمعطيات الشخصية لحاجة جوهرية تتعلق بتوسيع نطاق تطبيق القانون، إلا أنها اختلفت من حيث المصطلحات المستخدمة والمعتمدة في التعريف، فمنها من اعتمد مصطلح البيانات الشخصية ومنها من اعتمد مصطلح المعطيات ذات الطابع الشخصي، ومنها من اعتمد مصطلح المعلومات، فقد يبدو للوهلة الأولى أنها نفس المصطلح إلا أنها تحمل اختلافات دقيقة ومهمة لا بد من توضيحها، فما هو الفرق بين المعلومات والبيانات المعطيات؟

ثانيا: الفرق بين المعلومات والبيانات

إن هرم المعرفة يتكون من خمسة مراحل أساسية، هي مرحلة ما وراء البيانات ثم مرحلة البيانات ثم مرحلة المعلومات ثم مرحلة المعرفة ثم مرحلة الحكمة، وهي مراحل التقدم الإنساني لأي مجتمع إذ ينتقل من مرحلة التدهور والتخلف إلى التقدم والإبداع والإبتكار.[3]

---

[1] عثمان بكر عثمان، المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، منشورات كلية الحقوق، جامعة طنطا جمهورية مصر، ص09.

* أصدرت المحكمة الأوروبية لحقوق الإنسان هذا الحكم بعد اعتراض أحد المواطنين السويسريين على استعمال الأحرف الأولى من اسمه في ملف جمعته أجهزة الأمن لأن في ذلك خطر انكشاف هويته، وكانت البيانات المدونة تشير إلى واحدة من مكالماته الهاتفية المهنية مع إحدى زبوناته والتي كانت تعمل حينها لدى السفارة الروسية في زوريخ.

[2] منى الأشقر جبور، محمود جبور، مرجع سابق ص79.

[3] عادل عبد الصادق، البيانات الشخصية الصراع على نفط القرن الحادي والعشرين، مركز الأهرام للدراسات السياسية والاستراتيجية، عدد 287 المجلد السابع والعشرون، أفريل 2018، ص10.

لذلك فالتمييز والتفريق هنا ينصب على البيانات والمعلومات، على أساس أن كلا من مصطلح البيانات والمعطيات هما مصطلحان مترادفان ذات معنى واحد، فالمعطيات والبيانات لهما نفس الدلالة والمضمون فهما عبارة عن المدخلات input، فتعرف البيانات على أنها "المعطيات الخام أو المعطيات الأولية التي تتعلق بقطاع أو نشاط معين"[1]، وتعرف البيانات (المعطيات) أيضا بأنها "مجموعة من الكلمات أو الرموز أو الأرقام أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام وتخلو من المعنى الظاهر في أغلب الأحيان"، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات[2]، أي هي نتيجة تحليل وتلخيص البيانات وتصنيفها وتجميعها بطريقة معينة بواسطة النظام المعلوماتي، بحيث تثمر معنى محدد يمكن الاستفادة منه، مما يزيد من قيمتها بالنسبة للمستخدمين، وبالتالي تكون البيانات على هذا النحو هي مدخلات النظام المعلوماتي والمعلومات هي مخرجاتها.[3]

فالبيانات أو المعطيات ينظر إليها على أساس أنها سلسلة غير مترابطة من الحقائق الموضوعية التي يمكن الحصول عليها عن طريق الملاحظة أو عن طريق البحث، وفي حالتها الأولية صماء لا تعبر عن أي اتجاه، لا قيمة محددة لها إلا إذا ترابطت مع بعضها،سواء كانت مجموعة من الأحرف أو الكلمات أو الرموز أو الصور، أما المعلومات فهي تلك المعطيات أو البيانات التي تمت معالجتها، بحيث أصبحت ذات معنى وباتت مرتبطة بسياق معين[4]، لذلك اعتبرت المعلومات في العديد من التعريفات الفقهية أنها البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي هي البيانات التي أصبح لها قيمة بعد تحليلها أو تفسيرها أو تجميعها في شكل ذي معنى، والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل آخر.

وقد تبنت التوصية الصادرة عن منظمة التعاون الاقتصادي والتمنية في 1992/11/26 الخاصة بحماية أنظمة الحاسبات الآلية وشبكة المعلومات هذه التفرقة من خلال تعريفها للبيانات بأنها: "مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددا يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية، أما المعلومات فهي المعنى المستخلص من هذه البيانات[5]، لذلك فجانب كبير من الفقه يذهب إلى اعتبار أن البيانات هي مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة سواء كان ذلك التعبير بالكلمات أو الرموز، ولا تفيد هذه البيانات في شيء وهي على صورتها الأولية، لذلك يستدعي الأمر تحليلها وإجراء العمليات الحسابية والمنطقية عليها من خلال عملية معالجتها، للاستدلال

[1] يحي مصطفى حلمي، أساسيات نظم المعلومات، مؤسسة الأهرام للنشر والتوزيع، القاهرة 1998، ص72.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت لبنان 2005، ص97.

[3] محمد كمال محمود الدسوقي، مرجع سابق، ص37.

[4] عادل عبد الصادق، البيانات الشخصية، الصراع على نفط القرن الحادي والعشرين، مركز الأهرام للدراسات السياسية والاستراتيجية. كراسات استراتيجية، العدد 287، المجلد السابع والعشرون، أفريل 2018، ص12.

[5] نائلة عادل محمد فريد قورة، نفس المرجع، ص98. وأنظر كذلك هشام محمد فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، 1992، ص26.

منها على مجموعة من المعلومات، وبذلك تكون المعلومات هي النتيجة النهائية المترتبة على تشغيل البيانات وتحليلها واستقراء دلالتها واستنتاج ما يمكن استنتاجه منها.[1]

وتسمى العلاقة بين المعلومات والمعطيات أو البيانات بالدورة الإستراتيجية للمعلومات، إذ يتم تجميع ومعالجة البيانات فيتم الحصول على معلومات، ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة وهكذا.[2]

وعند الانتقال إلى المعالجة التشريعية لمصطلحي البيانات (المعطيات) والمعلومات نجد أن بعض التشريعات لا تقيم وزنا لهذه التفرقة واعتبرتهما مفهوما واحدا، ومنها المشرع الجزائري الذي عرف المعطيات المعلوماتية في المادة 02 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بأنها "أي عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية..." وكذلك تعريفه للمعطيات الشخصية في المادة 03 من القانون 07/18 أنها "كل معلومة بغض النظر عن دعامتها..."

وكذلك عرفت الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية[3] البيانات على أنها معلومات، حيث ورد في المادة الأولى بأنه يقصد بالبيانات "أية عملية عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل منظومة الكمبيوتر..."

ولعل هذا الترادف التشريعي بين المصطلحين جاء متوافقا مع الإتجاه الفقهي الذي ذهب إلى عدم أهمية التفريق بين البيانات (المعطيات) والمعلومات، ويعتبر كلا منهما مرادفا للثاني ولا يرى مسوغا أو فائدة ملموسة من التمييز بينهما طالما أن المعلومات هي المعنى المستخلص من البيانات أو المعطيات، ومن ثم فإن الحماية القانونية تشملهما معا، ومن ناحية أخرى قد لا تكون المعلومة مفهومة لدى متلقيها وهو ما يجعلها تخرج عن دائرة المعلومات طبقا لهذه التفرقة، ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر كبير من الخطورة ومن ثم فالذي يهم هو الحماية القانونية للمعلومات بغض النظر عن فهم محتواها[4]، وهي تشمل من الناحية الفعلية كلا من المعلومات والبيانات، فحسب هذا الرأي أنه طالما أن المعلومات هي المعنى الذي يمكن الإستفادة منه نتيجة تحليل وتلخيص البيانات أو المعطيات وتصنيفها وتجميعها بواسطة النظام المعلوماتي، وبالتالي فإن كلا منها انصهر واندمج مع الآخر وشكلا سويا كيانا واحدا وهو المعلومات الإلكترونية، وهذه الأخيرة هي في حقيقتها البيانات في شكلها الأولي والخام، لذلك نجد أن غالبية التشريعات لا تميز بين المعلومات والبيانات في مجال الحماية الجزائية، حيث أن هناك

[1] محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، القاهرة 2012، ص61.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان الأردن، الطبعة الثانية، 2010، ص102.

[3] الاتفاقية رقم 185، موقعة في بودابست بتاريخ 2001/11/23.

[4] نائلة عادل محمد فريد قورة، مرجع سابق، ص98.

تشريعات تبنت مصطلح المعلومات وعرفتها بأنها البيانات وهناك تشريعات تبنت مصطلح البيانات وعرفتها بأنها المعلومات.*

الفرع الثالث: أنواع المعطيات ذات الطابع الشخصي

إذا كان المقصود بالمعطيات ذات الطابع الشخصي كما سبق بيانه، أنها البيانات التي من شأنها تحديد هوية الشخص الطبيعي تحت أي شكل كان، سواء بصفة مباشرة أو غير مباشرة بعد اتصالها ببيانات أخرى في حيازة مستخدم هذه البيانات، فإن هذه البيانات أو المعطيات تتدرج في أهميتها ودرجة سريتها إلى أن تصل إلى بيانات شخصية يمكن أن تـ ، عامل على أنها حساسة، وعليه فقد تم تصنيف المعطيات الشخصية إلى معطيات شخصية عادية ومعطيات شخصية حساسة.

أولا: المعطيات الشخصية العادية

لا خلاف على أن تفاصيل حياة الشخص لابد أن تبقى خارج العلنية بجميع صورها سواء كانت طبية أو عاطفية أو مالية... وكلها تحتمي تحت ظل الخصوصية، لكن في عصر المعلوماتية لم يعد بالإمكان القول بأن للخصوصية سياج منيع، ذلك أن متطلبات الحياة المعاصرة تستلزم الكشف عن معطيات عديدة خاصة بالشخص كالوضع الصحي لطالب التأمين، أو الوضع المالي للمكلف بالضريبة وهكذا،[1] وهي معطيات اصطلح على تسميتها بمعلومات التعريف العام،وتحتوي على الإ سم، العنوان، بيانات البريد الالكتروني، رقم الهاتف الجنس، الحالة الإ جتماعية والحالة العائلية، تاريخ الميلاد، الشهادة التعليمية، السمات البدنية، سجلات الأنشطة المختلفة، الخبرات الفنية و الجهات التي ينتسب لها بالعضوية وغيرها من المعطيات التي ترتبط بالشخص.

وتعد بيانات الوقائع المدنية من أهم المعلومات التي تنتمي إلى هذا الصنف، وهي عبارة عن معلومات تتعلق بعناصر الحالة المدنية للفرد، وهي عموما: الميلاد، الزواج، الوفاة، الطلاق، الجنسية، الإقامة، كما تشمل رقم التعريف الوطني وعنوان المسكن، وهي وقائع غالبا ما تنظمها الدوائر الحكومية، وذلك للتعرف على المواطنين والتعامل معهم.[2]

---

* عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999 في المادة الثانية الفقرة العاشرة منه، بأنها تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكومبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.

-المشرع البحريني في القانون رقم 28 لسنة 2002 المتعلق بالمعاملات الإلكترونية عرف المعلومات في المادة الأولى منه بأنها "البيانات والنصوص والصور والأشكال والرموز وبرامج الحاسب والبرمجيات وقواعد البيانات والكلام وما شابه ذلك"

-المشرع السعودي في قنون مكافحة الجرائم المعلوماتية اعتمد مصطلح البيانات وعرفها بأنها المعلومات أو الأوامر، أو الرسائل أو الأ صوات، أو الصور التي تعد أو التي سبق إعدادها لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه ومعالجته ونقله وإنشاؤه بواسطة الحاسب الآلي كالأرقام والحروف والرموز وغيرها.

-قانون حماية البيانات البريطاني لسنة 1998 عرف البيانات بأنها المعلومات التي يجرى معالجتها بواسطة معدات التشغيل التلقائية استجابة لتوجيهات أعطيت لهذا الغرض.

[1] بارق منتظر عبد الوهاب لامي، مرجع سابق، ص64.

[2] علي أحمد عبد الزعبي، مرجع سابق، ص335

وتبقى العناصر التي تمكن من التعريف بالشخص بشكل مباشر أو غير مباشر ذات طبيعة متنوعة وكثيرة العدد، لذلك فقد حاول المشرع الجزائري على غرار التشريعات المقارنة وضع تعداد غير حصري لكل ما يمكن أن يدخل ضمن هذا النوع من المعطيات، حيث نصت المادة الثالثة من القانون 07/18 عند تعريف المعطيات ذات الطابع الشخصي "... لاسيما بالرجوع إلى رقم التعريف، أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية، أو النفسية أو الإقتصادية أو الثقافية أو جتماعية".

وكذلك فعل المشرع الفرنسي والبلجيكي والتونسي والمغربي وغيرهم، عندما تم تضمين النصوص القانونية تعدادا توضيحيا على سبيل المثال لا الحصر لمجموعة من المعطيات العادية، وهو ما يفهم من عبارة "لاسيما" أو «notamment»

وتجدر الإشارة إلى أن مفهوم المعطيات الشخصية العادية لا يتوقف فقط عند المعطيات المتعلقة بالحياة الخاصة بل أيضا المتعلقة منها بالحياة المهنية، مع الإشارة أيضا إلى أن طريقة عرض هذه المعطيات تعد كذلك من العناصر التعريفية للشخص، إذ يمكن أن تكون في شكل حروف أبجدية أو رقمية، مقروءة أم مشفرة أو في شكل صوتي أو في شكل صورة ثابتة أو متحركة، وهو ما نصت عليه الحيثية رقم 14 من التوجيه الأوروبي 46/95 بنصها "وحيث أنه يؤخذ بالاعتبار أهمية التطور الجاري في مجتمع الإعلام تقنيات التقاط، إرسال إدارة، تسجيل، حفظ، الإطلاع على المعطيات المنشأة عن طريق الأصوات أو الصور المتعلقة بالأشخاص الطبيعيين".[1]

لذلك نرى أنه كان على المشرع الجزائري عندما ذكر بعض المعطيات الشخصية التي تكون قادرة على التعريف بالشخص أو جعله قابلا للتعريف، أن ينص من بينها على الصوت والصورة انسجاما مع التصور الفقهي الذي يعتبر أن كلا من الصورة والصوت عبارة عن معطيات شخصية مرتبطة بصاحبها، بغض النظر عن دعامتها رقمية أو غير رقمية*، ومن ذلك نجد أن المشرع المغربي مثلا أدرج الصوت والصورة ضمن المعطيات الشخصية العادية في المادة الأولى من القانون 09/08 [2]

[1] « Considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données. »

* المشرع الفرنسي هو أيضا لم يذكر كلا من الصورة والصوت ضمن المعطيات الشخصية، وقد اعتبرت اللجنة الوطنية للمعلومات والحريات بفرنسا في نهاية الثمانينات أن الصوت والصورة لا يخضعان للقانون 17/78 المتعلق بالبيانات والملفات والحريات إلا إذا كانا رقميين، ثم لاحقا غيرت من رأيها معتبرة أن صورة الشخص الطبيعي سواء كانت ثابتة أم متحركة بيان شخصي يخضع للحماية القانونية، وكذلك الأمر بالنسبة لصوت الشخص، وقد استندت اللجنة في ذلك إلى أن التكنولوجيا الرقمية الحديثة قد سمحت بمعالجة الصوت والصورة ووضعهم على دعامة واحدة بجانب النص مما يؤدي إلى اعتبارهما بيانات شخصية. أنظر في هذا الإطار سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، بحث منشور بمجلة الحقوق جامعة الكويت، العدد الثالث، سبتمبر 2011 ص390

[2] تنص المادة 1/1 من القانون المغربي 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه المعطيات ذات الطابع الشخصي "يراد بما يلي من أجل تطبيق هذا القانون:

ونخلص للقول أن المعطيات الشخصية العادية تبقى من المعطيات المتعلقة بأدق تفاصيل الحياة الخاصة للشخص.

ثانيا: المعطيات الشخصية الحساسة

عرف المشرع الجزائري هذا النوع من المعطيات بنصه على أنها "معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية "*.

إن البيانات الحساسة هي كما نلاحظ من تعريفها فئة من البيانات الشخصية ذات نطاق أضيق من نطاق البيانات الشخصية العادية الأخرى، والملاحظ كذلك أن غالبية القوانين تحظر جمعها نظرا لارتباطها المباشر بحقوق إنسانية وحريات أساسية، وقد اعتبرتها الإتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص الطبيعيين اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي أنها أصناف خاصة من المعطيات، حيث نصت المادة 06 من هذه الإتفاقية أنه لا يمكن معالجة المعطيات ذات الطابع الشخصي التي تكشف الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو أي معتقدات أخرى مثل ما هو الحال بالنسبة للمعطيات ذات الطابع الشخصي المتعلقة بالصحة أو الحياة الجنسية... وهو ما ينطبق أيضا على المعطيات ذات الطابع الشخصي المتعلقة بالإدانات الجنائية".

وبحسب التعريف الذي أعطي لها، فهي معطيات شخصية ترتبط بحرية المعتقد، منع التمييز وحرية الرأي وكذا المعطيات الشخصية التي تبين العرق أو الأصل أو الانتماءات الدينية أو الفلسفية أو السياسية أو الحياة الصحية أو الجنسية أو المعطيات المتعلقة بالملاحقات الجنائية والإدانات، وتشمل أيضا العينات البيولوجية التي تحتوي على التركيبة الجينية المميزة للشخص[1]، وحساسية هذه المعطيات مستمدة من انطوائها على مخاطر عديدة قد تهدد حياة الشخص وأمنه، وهو ما نشهده بخاصة في البلاد التي تعاني من أزمات طائفية أو دينية[2]، ففي هذه المجتمعات ذات الطوائف والأديان المتعددة يفضل ألا يعرف انتماء الشخص الديني أو الطائفي، بالإضافة إلى أن انتماء الفرد السياسي وآرائه السياسية قد يؤدي الكشف عنها إلى إدخال صاحبها في صراعات عديدة وتعريضه لابتزازات كثيرة جراء الكشف عنها.

معطيات ذات طابع شخصي كل معلومة كيفما كان نوعها بغض النظر عن دعامتها بما في ذلك **الصوت والصورة** والمتعلقة بشخص ذاتي معرف وقابل للتعرف عليه"

* أنظر المادة 03 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وما ألاحظه على المشرع الجزائري هنا، أنه اعتبر المعطيات الجينية من المعطيات الحساسة في المادة 03 عند تعريفه لهذه الأخيرة، في حين أدرجها ضمن المعطيات العادية المنصوص عليها في المادة 02، وهذا على خلاف باقي التشريعات التي تصنف المعطيات الجينية فقط ضمن المعطيات الحساسة. أنظر مثلا المادة 03 من القانون المغربي 09/08 المعطيات الحساسة هي معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية والفلسفية أو الانتماء النقابي للشخص المعني، أو تكون متعلقة بصحته بما في ذلك المعطيات الجينية"

[1] أمين بن سالم الحارثي، ومحمد بن صالح الطويقري، تنظيم وإدارة المعلومات الشخصية، بحث مقدم إلى المؤتمر العلمي الأكاديمي الدولي التاسع تحت عنوان: "الإتجاهات المعاصرة في العلوم الإجتماعية، الإنسانية والطبيعية، تركيا 17-18 جويلية 2018، ص2017.

[2] نعيم مغبغب، مرجع سابق، ص165.

وإذا كان القانون يوفر الحماية للمعطيات الشخصية بشكل عام، إلا أن هاجس الخطورة يزيد كلما تعلق الأمر بالمعطيات الحساسة، ومرد ذلك التوجس، هو الخيفة من التمييز العنصري أو العرقي من خطر تصنيف الأشخاص بدافع إقصائهم أو تتبعهمو مراقبتهم، أو بالعكس من ذلك بهدف المفاضلة والمحاباة على الآخرين إلى غير ذلك من أوجه التمييز[1]،وبالتالي يعلو منسوب الخطر على الخصوصية مع الكشف على البيانات الشخصية الحساسة، وذلك نظرا لما يمكن أن يتركه هذا الإنكشاف من أثر سلبي على كيفية التعامل مع المعني بها، سواء من قبل السلطات المختصة أو من قبل الآخرين، ومن هنا تكون القاعدة فيما يتعلق بهذا النوع من المعطيات هي حظر معالجتها والسماح به هو الإستثناء، وذلك في حالات محددة حصرا كما سوف نرى ذلك لاحقا.

وهنا تجدر الإشارة إلى وجود صعوبة في إيجاد توافق عالمي على تحديد فئات من البيانات التي تعتبر حساسة، نظرا للاختلافات التقليدية بين الأنظمة القانونية، إذ ما يعد بيانا شخصيا ذو طبيعة حساسة في نظام قانوني قد لا يعد كذلك في نظام قانوني آخر، فمثلا المشرع الجزائري لا يعتبر المعطيات المتعلقة بالحياة الجنسية للشخص ضمن المعطيات الحساسة، على خلاف المشرع الفرنسي الذي يعتبرها كذلك،[2] كما أن القانون الأمريكي يوسع من دائرة هذا النوع من المعطيات، إذ يمكن أن يضاف على هذه الفئة عنوان الجهاز الإلكتروني، البيانات المالية، بطاقة الضمان وبيانات الأطفال.

ولذلك فقد تركت القواعد الأوروبية الجديدة للدول عملية تنظيم معالجة البيانات الحساسة[3]، لكن دون الخروج عن التزامها بأحكام التشريع الأوروبي الذي يعتبر أن البيانات المتعلقة بالأساس العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية والفلسفية، الإنتماء النقابي، البيانات الجينية، البيومترية والبيانات الصحية والجنسية هي بيانات شخصية حساسة[4]، وهذا يعني أن تلتزم الدول الأوروبية بإدراج هذه البيانات في قوانينها الداخلية ضمن البيانات الحساسة.

كما نشير أيضا في هذا الجانب أن المعطيات الشخصية العادية يمكن أن تنقلب إلى معطيات شخصية حساسة إذا أحاطت بها ظروف تضفي عليها نوعا من الخطورة، وتتمثل تلك الظروف في الكيفية أو

---

[1] العربي جنان، معالجة المعطيات ذات الطابع الشخصي، الحماية القانونية في التشريع المغربي والمقارن، المطبعة والوراقة الوطنية الداوديات، مراكش، الطبعة الأولى، 2010 ص10

[2] Art. 8. – I. – Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

[3] تنص الفقرة العاشرة من التوجيه الأوروبي 46/95:

Le présent règlement laisse aux etats membres une marge de manœuvre pour préciser ses règles y compris ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées « données sensibles »)

[4] Article 09 « de la directive 95/46/CE du parlement européen et du conseil du 24 octobbre1995 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dispose que « le traitement des données à caractère personnel qui relève l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique. Des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits »

التطبيقات المعلوماتية التي تتم حيازتها أو حفظها، أو الملابسات التي تثيرها أو الغايات المرسومة لها، حيث يسري عليها في مثل هذه الحالات حكم المعطيات الشخصية ذات الطابع الحساس[1]، فالمشرع القطري مثلا أتاح للوزير المختص إمكانية إضافة أنواع جديدة من البيانات ذات الطبيعة الحساسة –أو كما سماها القانون القطري البيانات ذات الطبيعة الخاصة- إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر جسيما بالفرد[2]، وهي الصلاحية التي أوكلتها بعض التشريعات للهيأة المكلفة بحماية المعطيات ذات الطابع الشخصي.

الفرع الرابع: أهمية المعطيات ذات الطابع الشخصي:

على الرغم من وجود أنماط مختلفة من البيانات مثل البيانات العسكرية أو الصناعية أو التجارية، إلا أن السياق الدولي يكشف أن هناك تصاعدا في إنتاج البيانات الشخصية، وأن هناك حالة تداخل كبير بين توظيف البيانات الشخصية في تحقيق أهداف تجارية أو صناعية أو أمنية، ومن ثم يصعب الفصل بين طرق توظيف تلك البيانات على النحو الذي يكشف عن الدور المهيمن للبيانات الشخصية سواء من حيث أهميتها الإ ستراتيجية، أو من خلال حجم الصراع حول الاستحواذ عليها.[3]

أولا: الأهمية الاقتصادية للمعطيات ذات الطابع الشخصي

لقد شهد العالم الحديث تطورا على مستوى التجارة الإلكترونية، الأمر الذي جعل من المعطيات ذات الطابع الشخصي عاملا اقتصاديا ومؤشرا مهما على اكتشاف الأسواق الجديدة والسيطرة عليها[4]، فأصبح للبيانات الشخصية دورا مهما في النهضة الإقتصادية، مثل ذلك الدور الذي لعبه النفط في القرنين الثامن عشر والتاسع عشر، فكلاهما كان محركا رئيسيا للتغيير الاقتصادي[5] ، حيث ساعد التقدم التكنولوجي واستخدام تقنية المعلومات على تعزيز القدرة في الحصول على البيانات الشخصية ومن ثم استخدامها لتلبية احتياجات العملاء من خلال رصد خياراتهم وآرائهم ومعرفة ميولاتهم واتجهاتهم.

و بالتالي ظهر الإقتصاد الرقمي الذي تصاعد دوره في نمو الإقتصاد العالمي، وأصبح للبيانات الشخصية قيمة أكبر من أي وقت مضى في خلق الوظائف ودعم عملية الإبداع والإ بتكار، وأصبحت بذلك البيانات الشخصية من ضمن ركائز القوة الإقتصادية للدولة، فكمية البيانات الشخصية الهائلة التي نخلفها خلال زيارتنا للمواقع الالكترونية عبر شبكة الأنترنت تعتبر أمرا مهما للشركات التجارية، حيث تقوم هذه الاخيرة بتجميعها ثم تحليلها بغية إنتاج أنماط من العلاقات يمكن استخدامها للحصول على ميزة تنافسية في التسعير والتسويق والتواصل مع المستهلكين ومعرفة أذواقهم، ومن هذا المنطلق تحولت البيانات الشخصية إلى مرتكز للاقتصاد الرقمي وإلى سلعة ذات قيمة اقتصادية، وإلى جزء من عناصر المؤسسات

[1] العربي جنان، مرجع سابق، ص44.

[2] أنظر المادة 12 من القانون القطري رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية مؤرخ في 2016/11/03.

[3] عادل عبد الصادق، مرجع سابق، ص13.

[4] عبد المجيد كوزي، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، فاس، السنة الجامعية 2014-2015، ص127

[5] عادل عبد الصادق، مرجع سابق، ص14.

التجارية، مما جعل البيانات الشخصية لمستخدم الأنترنت أن تتحول إلى مادة أولية في تحقيق الإنتاجية لأي شركة[1]، وبالفعل تتهافت الشركات الخاصة الناشطة على الأنترنت على جمع البيانات الشخصية ومعالجتها واستخدامها في عمليات الترويج لمنتوجاتها بعد أن يتم تحديد أطياف مستخدمي المعلوماتية من خلال فئاتهم العمرية وجنسهم ومكان تواجدهم بما يسمح باستهدافهم، فمثلا تلك التطبيقات المجانية التي نجدها على شبكات الأنترنت كمواقع التواصل الإجتماعي أو محركات البحث أو مواقع التجارة الإلكترونية... ليست فقط من أجل الإتصال أو الوصول إلى المعلومات، بل أيضا لجمع البيانات الشخصية ومعالجتها، مما يسمح باكتساب هذه الشركات القدرة على تعزيز وضعها التجاري والتنافسي في السوق العالمي، ويرى البعض أن البيانات الشخصية الخاصة بمرتادي المواقع الإلكترونية ومستخدمي وسائل التواصل الإ جتماعي ليست مملوكة لهؤلاء المستخدمين، بل إن لها قيمة تجارية واقتصادية تعود ملكيتها لمن جمعها وعالجها وحللها، وهي مقاربة تقترب أكثر من مفهوم البيانات الشخصية في الولايات المتحدة الأمريكية، في حين تنسجم تماما مع مبادئ حماية البيانات الشخصية في أوروبا.[2]

كما أن الدراسات المسحية في بيئة التجارة الإلكترونية أظهرت وجود اهتمام عريض ومتزايد لدى قطاعات الأعمال، وأصبحت تأخذ موضوع خصوصية البيانات الشخصية على محمل الجد وأحيانا كعامل خطير يهدد أعمالها، باعتبار أن عدم الثقة بالتجارة الإلكترونية بسبب خشية الأفراد على خصوصية بياناتهم الشخصية يمثل عائقا لرواج التجارة في البيئة الرقمية[3].

ثانيا: الأهمية الإ جتماعية والأمنية للمعطيات ذات الطابع الشخصي

إن توظيف التحول الرقمي في جمع ومعالجة المعطيات الشخصية كان له الأثر الإيجابي في تعظيم قدرة الدولة على تنظيم شؤون الأفراد على المستوى الاجتماعي والثقافي والأمني وغيرها، حيث تساعد عملية جمع البيانات الشخصية وتحليلها ومعالجتها في عملية صنع القرار ووضع السياسات العامة للدولة.

فمن الثابت أن البيانات الشخصية أصبحت تعد مرتكزا لبناء القرار الإداري والأمني الهادف إلى إدارة الشأن العام ورفاه الشعب، كما تعد مادة أساسية للعمل في مختلف أجهزة الدولة والقطاعات الأمنية، حيث تدار الأحوال الشخصية والأحوال المدنية والممتلكات العقارية والشؤون الاجتماعية والأمنية وغيرها، وهو الأمر الذي أدى إلى قيام العديد من الدول إلى إنشاء ما يعرف ببنوك المعلومات أو مراكز البيانات، والتي يمكن أن تكون مختصة بقطاعات بعينها، أو تكون شاملة مثل قاعدة البيانات لتنظيم السجلات الآلية للحالة المدنية أو قاعدة البيانات لتسيير البطاقات الرمادية التابعة لوزارة الداخلية، وأيضا مثل قاعدة البيانات لتسيير صحيفة السوابق القضائية التابعة لوزارة العدل...

[1] منى الأشقر جبور، هاجس السيبرانية، مرجع سابق، ص119.

[2] منى الأشقر جبور، نفس المرجع، ص120.

[3] يونس عرب، استراتيجيات وتقنيات الحماية من أنشطة الإعتداء على خصوصية المعلومات، بحث منشور على الموقع الإلكتروني http://www.al-tawfik.com/uploads/b2080a28be83271c4b2009e2.pdf تم زيارة الموقع يوم 2019/11/06 على الساعة 22.35.

وكل ذلك يصب في إطار التمكن من الإستحواذ على البيانات الشخصية، أو على الأقل تنظيم عملية استخدامها ومعالجتها، بغرض السيطرة على فوضى انتهاك الخصوصية أو تسريب البيانات الشخصية أو سوء استخدامها على نحو يضر بالأمن الشخصي للمواطن، أو عبر توظيف تلك البيانات الشخصية لمجموع المواطنين، بما قد يضر بالأمن القومي عبر استخدام تلك القاعدة في بث الشائعات أو في توجيه الرأي العام على نحو يضر بالمصلحة الوطنية.

وكنتيجة لأهمية المعطيات الشخصية فقد ظهرت برامج وتطبيقات لتحليل هذه المعطيات سواء عبر مواقع نترنت أو عبر الشبكات الاجتماعية، والتي أحدثت طفرة هائلة في إنتاج البيانات الشخصية وتحليلها، إلى جانب التوجه نحو المزيد من الرقمنة في كل قطاع من القطاعات الحكومية والذي يعتمد على تقديم البيانات الشخصية للاستفادة من الخدمات الأساسية مثل الصحة والنقل وغيرها، وهو ما أسهم في ظهور عصر البيانات الضخمة* the big data

المطلب الثالث: آثار الإعتراف بالخصوصية المعلوماتية

إن من أبسط المرتكزات الفكرية للعقل الإنساني هي الإقرار بأنه ليس هناك أي حق مطلق مهما كان نوعه، وبالتالي فإن حق الأفراد في الوصول إلى المعلومة ليس مطلقا وترد عليه بعض القيود، وهو الأمر ذاته بالنسبة لحق الدولة في الإطلاع على شؤون الأفراد لضرورات أمنية، فهل ثمة أثر مقيد للحق في الخصوصية المعلوماتية لهذين الحقين، أم أنها حقوق تتكامل في ظل معيار متوازن يجيد إدراك محتوى كل حق وأثره؟

الفرع الأول: أثر الحق في الخصوصية المعلوماتية على الحق في الوصول إلى المعلومات

إذا كان الحق في الوصول إلى المعلومات ينطوي على مكنة الفرد في الوصول إلى ما يريد من معلومات أو وثائق في القطاعين العام والخاص، وهو الحق الذي جرت الدساتير والقوانين إلى إقراره، فإنه في الوقت ذاته تم إقرار الحق في الخصوصية في مقابل ذلك، فهل يمكننا القول أن الحق في الخصوصية يعتبر بمثابة قيد على الحق في الوصول إلى المعلومات؟

أولا: المقصود بالحق في الوصول إلى المعلومات

ظهر مصطلح الحق في الوصول إلى المعلومات مع مصطلحات أخرى راجت في مطلع التسعينات من القرن الماضي وهي الشفافية (transparency) والإنفتاح أو الوضوح (openness)، والوصول إلى المعلومات يعد عنصرا من عناصر الشفافية وليس مفهوما مستقلا عنه، كما أن الإنفتاحية أو الوضوح هي

* يعتبر مصطلح البيانات الضخمة the big data من المصطلحات الحديثة التي ظهرت كاتجاه حديث في وصف التدفق الهائل للبيانات نتيجة الأنشطة التي يقوم بها الأشخاص بواسطة تقنيات الإتصال الحديثة كشبكات الأنترنت، فيتم تخزينها سحابيا في مختلف التطبيقات والبرامج المتاحة، وأن متخذي القرار يستفيدون كثيرا من معالجة وتحليل هذه البيانات في عمليات الاستشراف. للمزيد أكثر في هذا الموضوع أنظر: جمال بن مطر السالمي، البيانات الضخمة ودورها في دعم اتخاذ القرار والتخطيط الاستراتيجي، دراسة وصفية ورقة، مقدمة إلى المؤتمر السنوي الرابع والعشرون لجمعية المكتبات المتخصصة فرع الخليج، بعنوان البيانات الضخمة وآفاق استثمارها 6-8 مارس 2018، مسقط عمان، ص03.

حق الفرد في الوصول إلى المعلومات في كل وقت، لذلك فإن الحق في الوصول إلى المعلومة ما هو إلا أداة هامة لتعزيز الإنفتاح والشفافية.

وقد وردت عدة تعريفات لحق الأفراد في الوصول إلى المعلومات من أهمها أنه قدرة الأفراد في الحصول على المعلومات والبيانات من المؤسسات لحكومية والإ طلاع على السجلات ذات الصلة.[1]

كما عرف أيضا حق الأفراد في الوصول إلى المعلومات بأنه حق المواطن في السؤال عن أية معلومة وتلقي الإجابة عنها سواء من الحكومة أو البرلمان أو القضاء شريطة الإلتزام بحدود القانون.[2]

وقد تناولته بعض التعريفات الأخرى على أنه حق الفرد في أن توفر له الدولة شتى السبل الملائمة لتتدفق من خلالها المعلومات والآراء والأفكار، ليختار من بينها وفقا لإرادته الحرة، وعليها أن تحمي نفاذه المسير إلى تلك المعلومات بعيدا عن تدخلها أو تدخل الغير الذي من شأنه إعاقة أو الحد أو الإنتقاص من تمتعه بهذه الحرية.[3]

وفيي تعريف آخر اعتبر الحق في الوصول إلى المعلومات أنه حق أي فرد من العموم في طلب الوصول إلى الملفات التي تملكها أو تحوزها أي سلطة عامة وفي كل وقت، ولا يرفض الوصول إليها لا بالإستناد إلى أسس محددة ومقررة،[4] ويؤكد الفقه القانوني أن الحق في الوصول إلى المعلومات يعد ركنا محوريا في تأسيس دولة القانون واستباق الفساد من حيث كونه يمهد الطريق لإنتهاج عدة مسارات قانونية جديدة أساسها الإتاحة والإفصاح والشفافية بدلا من الحجب والمنع والتقييد، وينبثق هذا الحق من فلسفة عناصره الأساسية وهي الإتاحة المبدئية للمعلومات لفائدة الأفراد إلا ما استثني استثناءا محددا على متن القانون نفسه،لذلك فقد أصبح الوصول إلى المعلومات الرسمية والإ طلاع عليها حقا مضمونا بالمواثيق والمعاهدات الدولية، وكذا في دساتير وتشريعات العديد من الدول باعتباره من الحقوق الطبيعية للأفراد.[5]

ثانيا: الأساس القانوني للحق في الوصول إلى المعلومات

تحتوي مدونات ووثائق واتفاقيات حقوق الإنسان وكذا دساتير وقوانين الدول على إقرار الحق في الوصول إلى المعلومات، فقد حظي هذا الحق بأهمية بالغة في العصر المعلوماتي، لما لتقنية المعلومات من أثر عظيم في تمكين الأفراد من الوصول إلى المعلومات.

1) الحق في الوصول إلى المعلومات على مستوى المواثيق الدولية: يرجع الأساس القانوني للحق في الوصول إلى المعلومات إلى الإ عتراف المبكر للأمم المتحدة بهذا الحق من خلال القرار رقم 59 لسنة 1946 الصادر عن الجمعية العامة للأمم المتحدة والذي جاء في نصه "إن حرية الوصول إلى المعلومات حق

[1] أحمد درويش، حرية تداول المعلومات في مصر، مكتبة الإسكندرية للنشر، مصر 2009، ص72.

[2] أشرف فتحي الراعي، حق الحصول على المعلومات دراسة مقارنة، الطبعة الأولى، دار الثقافة للطباعة والنشر والتوزيع، عمان، 2010، ص36.

[3] قدري علي عبد المجيد، الإعلام وحقوق الإنسان قضايا فكرية ودراسة تحليلية وميدانية، دار الجامعة الجديدة الإسكندرية، مصر العربية 2010، ص225.

[4] بارق منتظر عبد الوهاب لامي، مرجع سابق، ص42.

[5] بارق منتظر عبد الوهاب لامي، نفس المرجع، ص43.

أساسي للإنسان، وحجر الزاوية لجميع الحريات التي تنادي بها الأمم المتحدة"، ثم جاء الإعلان العالمي لحقوق الإنسان[1] سنة 1948 لينص في المادة 19 منه "لكل شخص حق التمتع بحرية الرأي والتعبير ويشمل هذا الحق حريته في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقيها وإذاعتها بأي وسيلة كانت دون تقيد بالحدود الجغرافية"، وبالتالي فقد تضمنت هذه المادة الحق في تداول المعلومات في ثلاث نطاقات رئيسية: النطاق الأول هو الحق في التماس المعلومة، النطاق الثاني هو الحق في تلقي المعلومة والثالث هو الحق في نقل المعلومة بنشرها وإذاعتها.

كما صدرت قرارات دولية في الجمعية العامة للأمم المتحدة، و إعلانات دولية عن منظمة الأمم المتحدة للتربية والتعليم والثقافة (اليونيسكو) تؤكد حق الوصول الى المعلومة، ومنها قرار الجمعية العامة للأمم المتحدة 45/76/أبشان الإعلام في خدمة البشرية.[2] وكذلك أقرت المادة 19 من العهد الدولي للحقوق المدنية والسياسية[*] الحق في الوصول أو تداول المعلومات بطريقة مشابهة لما جاءت به المادة 19 من الإعلان العالمي لحقوق الإنسان من حيث نطاق ممارسة هذا الحق، ودون اعتبار للحدود الجغرافية أو لنوع الوسيلة المستخدمة في الوصول إلى المعلومة، بخلاف القيود على ممارسة هذا الحق التي جاءت بها المادة 19 من العهد الدولي وهي احترام حقوق الآخرين، سمعتهم، إحترام الأمن القومي والنظام العام و احترام الصحة والآداب العامة.[3]

وقد اكدت اللجنة المعنية بحقوق الإنسان التابعة للأمم المتحدة والتي تشرف على تطبيق العهد الدولي للحقوق المدنية والسياسيةحول كيفية تفسير حرية الر أيوالتعبير المنصوص عليها في المادة 19 من هذا العهد، أن الدول يجب عليها أن تبذل قصارى جهدها لضمان الوصول بسرعة وسهولة وفعالية للمعلومات التي تسيطر عليها الدولة في المجال العام، ويجب الكشف بشكل إستباقي عن المعلومة العامة، وربما يمتد هذا الحق الى الكيانات الخاصة التي تقدم خدمة عامة أو تدير مرفقا عاما.[4]

هذا عن الإعتراف بالحق في الوصول إلى المعلومات وإقراره على المستوى العالمي، أما على مستوى المواثيق الدولية الإقليمية فقد نصت المادة 10 من الإتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية[5] على أنه لكل شخص الحق في حرية التعبير، ويتضمن هذا الحق حرية الرأي وحرية تلقي وإرسال المعلومات والأفكار بدون عائق من السلطات العامة وبغض النظر عن الحدود، وقد كرست المحكمة الأوروبية

---

[1] علان العالمي لحقوق الإنسان، منشور بموجب قرار الجمعية العامة للأمم المتحدة 217 (ألف-د-3) بتاريخ 1948/12/10.

[2] يحي شقير، قانون ضمان حق الوصول الى المعلومات دراسة مقارنة مع المعايير الدولية، مركز القدس للدراسات السياسية، الطبعة الأولى، 2013، عمان الأردن، ص49.

[*] اعتمد هذا العهد وعرض للتوقيع والتصديق والإنضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 (ألف-د-21) المؤرخ في 1966/12/16 وكان تاريخ بدء النفاذ في 23 مارس 1976 حسب نص المادة 49 من هذا العهد.

[3] عماد مبارك وآخرون حرية تداول المعلومات، دراسة قانونية مقارنة، مؤسسة حرية الفكر والتعبير، الطبعة الأولى، القاهرة 2011، ص17متوفر على الرابط: https://www.transparency.org/files/content/activity/2011_AFTE_LegalStudyFreedomThought_AR.pdf أطلع عليه يوم 2020/06/26

[4] يحي شقير، مرجع نفسه، ص49.

[5] اتفاقية حماية حقوق الإنسان والحريات الأساسية موقعة بروما في 04 نوفمبر 1950 يمكن الاطلاع على حالة الاتفاقية وبروتوكولاتها وعلى كامل لائحة الإعلانات والتحفظات على الموقع int.coe.conventions.www

لحقوق الإنسان حرية تداول المعلومات في العديد من أحكامها، وعلى سبيل المثال الحكم الصادر في الدعوى المقامة من إحدى منظمات حقوق الإنسان ضد دولة هنجاريا الصادر في 14 أفريل 2009*، والذي قضت فيه أن قرار المحكمة الدستورية برفض طلب إحدى منظمات حقوق الإنسان الهنجارية في الحصول على نسخة من مشروع قانون المخدرات يعتبر عائقا أمام منظمات حقوق الإنسان فيما يتعلق بحقها في الحصول على المعلومات المنصوص عليه في المادة 10 من الميثاق الأوروبي لحقوق الإنسان وحرياته الأساسية، اللازم لتمكينها من القيام بدورها كمراقب لحالة حقوق الإنسان[1]، وقد جاء هذا نفتاح الأوروبي مترافقا مع خروج أوروبا من المجتمع المغلق إلى مجتمع مفتوح بفعل ما أحدثته إتفاقية أمستردام المنشأة للسوق الأوروبية المشتركة، حيث قررت هذه الإتفاقية صراحة حق مواطني الإتحاد في الوصول لكافة وثائق البرلمان الأوروبي ومجلس أوروبا والمفوضية الأوروبية[2].

كما قد بينت المادة التاسعة من الميثاق الإفريقي لحقوق الإنسان والشعوب* مضمون هذا الحق بنصها "أن من حق كل فرد أن يحصل على المعلومات وأن يعبر عن أفكاره وينشرها في إطار القوانين واللوائح، وقد تبنت اللجنة الإفريقية لحقوق الإنسان والشعوب إعلان مبادئ حرية التعبير في دورتها الثانية والثلاثين المنعقدة عام 2002 الذي أيد بوضوح الحق في الوصول إلى المعلومة، مقررة أن الجهات العامة لا تحتفظ بالمعلومات لنفسها بل كنائب عن الصالح العام، وكل فرد يتمتع بالحق في إتاحة المعلومات، وأنه يتم ضمان حق الوصول إلى المعلومات قانونا بناء على مجموعة من المبادئ.[3]

وقد أعطت الإتفاقية الأمريكية لحقوق الإنسان لعام 1969[4] اهتماما بحق الوصول إلى المعلومات معتبرة إياه من مشتملات الحق في حرية التعبير، حيث نصت المادة 13 من هذه الإتفاقية على أنه لكل إنسان الحق في حرية الفكر والتعبير ويشمل هذا الحق، الحرية في البحث وتلقي ونقل المعلومات والأفكار بكل

---

* تتلخص وقائع هذه القضيةفي قيام أحد أعضاء البرلمان بدولة هنجاريا بتقديم شكوى إلى المحكمة الدستورية تتعلق بقانون المخدرات المطروح أمامها قبل دخوله حيز التنفيذ، وقد علمت إحدى منظمات حقوق الإنسان بهذه الشكوى، فتقدمت بطلب إلى المحكمة الدستورية للحصول على نسخة من مشروع القانون السالف الذكر، فرفضت المحكمة الدستورية هذا الطلب مؤسسة رفضها على أساس أن الإفصاح عن أي معلومات يتطلب إذنا مسبقا من مقدم هذه المعلومات والوثائق.

[1] عماد مبارك وآخرون، مرجع سابق، ص22.

[2] بولين أيوب، مرجع سابق، ص75.

* تم إجازته من قبل مجلس الرؤساء الأفارقة بدورته العادية رقم 18 بنيروبي كينيا جوان 1981. والملاحظ أن الفقرة الأولى من المادة 09 من الميثاق الإفريقي لحقوق الإنسان والشعوب التي كفلت حق الأفراد في الوصول إلى المعلومة لم تحل تنظيم هذا الحق إلى القوانين الوطنية، كما لم تقيد النفاذ إليه بقيود محددة، وذلك عكس ما ورد في الفقرة الثانية من ذات المادة التي نظمت حرية التعبير، بما يتفق مع القوانين واللوائح التي تصدرها الدول الأطراف في الميثاق.

[3] تتمثل هذه المبادئ في:

-يحق للجميع الحصول على المعلومات التي تحتفظ بها الجهات العامة.

-يحق للجميع الحصول على المعلومات التي تحتفظ بها جهات خاصة إذا كان الأمر ضروريا لممارسة أي حق أو حمايته.

-سيكون مطلوبا من الجهات العامة حتى في حال عدم وجود أي طلب لذلك، نشر المعلومات الهامة بشكل فاعل والتي تعتبر ذات أهمية للمصلحة العامة.

-يتم تعديل القوانين المتعلقة بالخصوصية إذا اقتضت الضرورة ذلك للالتزام بمبادئ حرية المعلومات.

[4] تم إعداد نص الإتفاقية في إطار منظمة الدول الأمريكية بسان خوسيه في 1969/11/22.

أنواعها دونما اعتبار للحدود... وأن ممارسة هذا الحق يجب ألا يخضع لرقابة مسبقة ولكن يخضع إلى المساءلة القانونية لاحقا.

أما منظمة المادة 19* المتعلقة بحرية تداول المعلومات فقد عملت على بلورة عدد من المبادئ المتعلقة بحرية تداول المعلومات كمعايير أساسية يمكن الإسترشاد بها حال صياغة التشريعات المنظمة لحرية تداول المعلومات، من حيث حدود الإتاحة والإستثناءات ودور الحكومة في تعزيز الحق في الحصول على المعلومات.

ومن أهم المبادئ التي صاغتها هذه المنظمة، مبدأ الإفصاح المطلق عن المعلومات الذي يستند إلى قاعدة عامة مقتضاها أن لكل فرد الحق في الحصول على المعلومات التي تحوزها الجهات الحكومية، إلا إذا كانت هذه المعلومات واردة ضمن نطاق الإستثناءات المقيدة لهذا الحق.

2) إعتراف التشريعات الداخلية بالحق في الوصول إلى المعلومات: لقد اعتبر عام 2000 إيجابيا على الصعيد العالمي في ميدان حرية الوصول للمعلومات، إذ شهد هذا العام حملة من التطورات أبرزها سن العديد من دول العالم تشريعات منظمة لحق الأفراد في الوصول للمعلومات، حيث تعزز هذا الحق بالنص الدستوري عليه في العديد من الدول، فقد اعترف الدستور الجزائري بهذا الحق في المادة 51 منه عندما نصت على أن الحصول على المعلومات والوثائق والإحصائيات ونقلها مضمونان للمواطن، ولا يمكن أن تمس ممارسة هذا الحق بحياة الغير الخاصة، وبحقوقهم وبالمصالح المشروعة للمؤسسات وبمقتضيات الأمن الوطني، وبالرغم من هذا الإقرار الدستوري لهذا الحق فإنه لحد الساعة لم يصدر في الجزائر قانون خاص ينظم الحق في الحصول على المعلومات ويحدد كيفيات ممارسته.

ومن الدول العربية مثلا صدر في المغرب القانون رقم 03/13 المتعلق بالحق في الحصول على المعلومات[1] بعد أن كان قد تم تأصيله دستوريا في المادة 27 من الدستور المغربي، وفي تونس صدر القانون الأساسي عدد 22 لسنة 2016 مؤرخ في 24 مارس 2016 يتعلق بالحق في النفاذ إلى المعلومة، وقد عرفته المادة 03 من هذا القانون بأنه نشر المعلومة بمبادرة من الهيكل المعني والحق في الحصول عليها بطلب[2]، وفي مصر تنص المادة 68 من الدستور المصري لعام 2014 على أن المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب والإفصاح عنها من مصادرها المختلفة حق تكفله الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها وقواعد إيداعها وحفظها والتظلم من رفض إعطائها، وهناك مشروع قانون في مصر بشأن حرية المعلومات ينص على أنه للكافة الحق في الحصول على المعلومات والبيانات التي لدى الجهات العامة بالدولة، ويتعين على هذه الجهات

* منظمة المادة 19هي منظمة بريطانية لحقوق الإنسان تركز على الدفاع عن حرية التعبير وحرية المعلومات وتعزيزها في جميع أنحاء العالم. تأسست عام 1987 وتأخذ اسمها من المادة 19 من الإعلان العالمي لحقوق الإنسان.

[1] القانون 03/13 المتعلق بالحق في الحصول على المعلومات بالظهير الشريف رقم 1.18.15 الصادر في 22 فيفري 2018 جريدة رسمية عدد 6655 وقد نصت الأولى منه على أن هذا القانون يحدد مجال تطبيق الحق في الحصول على المعلومات الموجودة في حوزة الإدارات العمومية والمؤسسات المنتخبة والهيئات المكلفة بمهام المرفق العام وكذا شروط وكيفيات ممارسته.

[2] حددت المادة 02 من القانون التونسي الهياكل المعنية التي ينطبق عليها حق النفاذ إلى المعلومات لديها. أنظر المادة 02 من القانون عدد 22 لسنة 2016.

الكشف عن المعلومات والبيانات المحتفظ بها لديها وفقا للشروط والأحكام المنصوص عليها في هذا القانون[1].

وترتيبا على ما سبق فإنه يمكن القول بأن الحق في الوصول إلى المعلومات قد حظي بأهمية بالغة في العصر المعلوماتي لما لتقنية أنظمة المعلومات من أثر عظيم في تمكين الأفراد من الوصول للمعلومات وتعزيزها الحق.[2]

ثالثا: الحق في الخصوصية المعلوماتية قيد على الحق في الحصول على المعلومات

إذا كان جوهر الحق في الحصول على المعلومات أن يتم الكشف الكامل عن المعلومات حتى يتمكن الأشخاص من ممارسة حقوق أخرى كحرية التعبير والفكر والرأي باعتباره حجر الزاوية لهذه الحقوق، وإذا كان هذا الحق هو الغاية النهائية من استخدام تقنيات المعلوماتية، إلا أن ذلك لم يمنع من فرض بعض القيود التي تهدف إلى تحقيق التوازن بين حق المجتمع في المعرفة وحق الأفراد في احترام خصوصياتهم.

فالإدارات الحكومية لا تزال تحقق مزيدا من النجاح في التذرع بمقتضيات المصلحة والأمن القومي والنظام العام وكذا سرية الوثائق وغيرها من المبررات لحظر الوصول إلى المعلومات، وهو ما قد يؤدي إلى أن يصبح هذا الحق دون معنى إذا كثرت القيود عليه أو تاه المعيار الدقيق الذي تعمل في نطاقه الاستثناءات التي ترد عليه، لكن الحق في الخصوصية من خلال حماية المعطيات الشخصية يشكل أهم القيود والإستثناءات الحقيقية التي يجب مراعاتها عند ممارسة الحق في الحصول على المعلومات، فلا يمكن إنكار وجود مبررات حقيقية لحظر الوصول لطائفة معينة من المعلومات تتعلق بالحياة الخاصة للأفراد.

والمشرع الجزائري اعتبر الحق في الحياة الخاصة قيدا على ممارسة الحق في الحصول على المعلومة حيث نص صراحة في المادة 2/51 من الدستور الحالي أنه لا يمكن أن تمس ممارسة الحق في الحصول على المعلومات بحياة الغير الخاصة وبحقوقهم، بالإضافة إلى وجود بعض القوانين القطاعية والتي يمكن الإشارة إليها في هذا الإطار، فمثلا القانون رقم 09/88 المؤرخ في 1988/01/26 المتعلق بالأرشيف الوطني، الذي نصت المادة 10 منه أنه يتم فتح الأرشيف العمومي للاطلاع بحرية ومجانا بعد 25 سنة من إنتاجه، غير أنه ومن أجل حماية السيادة الوطنية والنظام العاموشرف العائلات فإن الإ طلاع على بعض الوثائق لا يتم إلا بعد انقضاء الأجل المحدد على النحو التالي:

-50 سنة ابتداء من اختتام القضايا المطروحة أمام القضاء وليست لها صلة بالحياة الخاصة للأفراد، وبالتالي إذا كانت هذه الوثائق تمس بالحياة الخاصة للأفراد والمعطيات الشخصية هي جزء منها، فإنه لا يجوز الإ طلاع عليها حتى بعد انقضاء ذلك الأجل.

[1] مؤسسة حرية الفكر والتعبير، حرية تداول المعلومات، دراسة مقارنة، الطبعة الأولى، 2011 القاهرة zoom، ص12.متوفر على الموقع:
. https://www.transparency.org/files/content/activity/2011_AFTE_LegalStudyFreedomThought_AR.pdf
[2] بولين أيوب، مرجع سابق، ص77.

وهو الإتجاه ذاته الذي سلكته معظم التشريعات المقارنة التي نظمت الحق في الحصول على المعلومات، حيث جعلت من الحق في الخصوصية المعلوماتية من خلال حماية المعطيات الشخصية قيدا على حق النفاذ والحصول على المعلومات، فالمشرع التونسي مثلا في القانون رقم 22 لسنة 2016 المتعلق بالحق في النفاذ إلى المعلومات السالفة الذكر، نصت المادة 24 منه أنه لا يمكن للهيكل المعني (الجهاز الإداري) أن يرفض طلب النفاذ إلى المعلومة ،إلا إذا كان يؤدي إلى إلحاق الضرر بحقوق الغير في حماية حياته الخاصة ومعطياته الشخصية، وكذلك المشرع المغربي فعل في القانون رقم 31/13 المتعلق بالحق في الوصول إلى المعلومات الذي نصت المادة 07 منه أنه تستثنى من الحق في الحصول على المعلومات كل المعلومات المتعلقة بالحياة الخاصة للأفراد أو التي تكتسي طابع معطيات شخصية، وكذا المعلومات التي من شأن الكشف عنها المس بالحريات والحقوق الأساسية المنصوص عليها في الدستور.

الفرع الثاني: أثر الحق في الخصوصية المعلوماتية على حق الدولة في الإ طلاع

إن استخدام الوسائل التقنية في ميدان جمع ومعالجة البيانات الشخصية من قبل الدولة قد عمق من حدة التناقضات التي برزت بين حق الأفراد في المحافظة على خصوصيتهم وموجبات الإ طلاع على شؤون الأفراد، بما فيها تلك التي تقع ضمن حدود ونطاق خصوصياتهم، وذلك بسبب تزايد تدخل الدولة في شؤون الأفراد[1] لدواعي الحفاظ على الأمن والنظام العام والآداب العامة.

أولا: المقصود بحق الدولة في الإ طلاع

تحتاج الدول عموما إلى جمع البيانات الشخصية حتى الحساسة منها، سواء على شبكات الأنترنت أو وسائل الإتصال أو عبر الأجهزة المختلفة، وذلك للقيام بمهامها كسلطة عامة، حيث تجمع تلك البيانات الشخصية بشكل متزايد في إطار تأديتها لدورها في إدارة أمور المواطنين وشؤونهم الحياتية ورغبة منها في حمايتهم، أو كمسؤولة عن الأمن والإستقرار الإ جتماعي.

وغالبا ما تستخدم السلطة البيانات الشخصية وتنقلها وتتبادلها تحت شعار الدفاع عن الأمن القومي أو نتيجة التزام الدولة في مكافحة بعض الأعمال والجرائم ذات الإ رتدادات السلبية كالإرهاب مثلا، سواء في أنشطتها الوطنية الداخلية أو في علاقاتها مع الدول الأخرى،[2] مثل ما قامت به الولايات المتحدة الأمريكية عندما أقرت صلاحيات واسعة للحكومة وأعطت للأجهزة الأمنية حرية أكبر في مجال التحقيق والإ طلاع على البيانات الشخصية للأفراد، واستبعدت المسؤولية عن الشركات الخاصة عند تسليمها للحكومة البيانات الشخصية العائدة لزبائنها، ترجيحا لكفة الأمن على كفة مصالح الأفراد الخاصة، من خلال القانون المعروف باسم « patriot-act » المتعلق بمكافحة الإرهاب، الذي دخل حيز التنفيذ في 26 أكتوبر 2001[3]، حيث يسمح هذا القانون لمكتب التحقيقات الفدرالي أن يطلب في إطار تحقيق مفتوح بسبب الإ شتباه حول نشاط إرهابي أو تجسس الحصول على مستندات من أي جهة أو شركة تخزن بيانات الخادم في هذا

[1] بولين أيوب، مرجع سابق، ص78.

[2] منى الأشقر جبور السيبرانية هاجس العصر، مرجع سابق، ص124

[3] بموجب هذا القانون تم تعديل قانون الخصوصية الإلكترونية، قانون مكافحة غسل الأموال وقانون السرية المصرفية بالإضافة إلى قانون الاستخبارات الأجنبية (fisa) الذي أقره الكونغرس في 25 أكتوبر 1978. (Foreign intelligence surveillance act)

البلد[1]، كما تفرض القوانين الأمريكية في إطار رصد التحركات المشبوهة للمسافرين الوافدين إليها من أي بلد، على شركات الطيران التي تقدم خدمة النقل الجوي من وإلى أراضيها أو عبر المرور بها، أن تزود وزارة الداخلية بالبيانات الشخصية للركاب، سواء تلك البيانات المتعلقة بشخص المسافر وسجله مثل إسم المسافر، تاريخ الرحلة، نقطة الإنطلاق، نقطة الوصول، رقم المقعد، عدد الحقائب، إسم وكالة السفر التي أجرت الحجز، أو تلك البيانات التي تؤخذ من جواز السفر والتي تجمع من خلال عملية التسجيل أمام السلطات المختصة بمراقبة الحدود قبل الوصول للتأكد من أن المسافر لا ينتمي إلى لائحة الأشخاص الذين يمثلون خطرا على سلامة الطيران، وهي مسألة تشكل عقبة أخرى أمام إمكانية الحفاظ على الحق في الخصوصية المعلوماتية للأفراد كونها تفقدهم القدرة على السيطرة والتحكم في بياناتهم الشخصية.[2]

ثانيا: حدود حق الدولة في الإ طلاع

لا يمكن حماية الأمن القومي بمعزل عن الحقوق الأساسية والحريات المدنية للمواطن، إذ لابد من مراعاة التوازن الذي يضمن عدم دفع هذه الأخيرة إلى مستوى متدن، ففي كل الأحوال يشكل جنوح الدولة عند سعيها لتأمين مستوى عال من الأمن مصدرا من مصادر الخطر على الخصوصية، نتيجة إمكانية ستخدام غير القانوني للبيانات الشخصية، لذلك فإنه من اللازم أن يتم رسم حدود واضحة لا يمكن للدولة أن تتجاوزها، منعا للاعتداء على حق الأفراد في خصوصيتهم المعلوماتية بذريعة حق الدولة في طلاع على بياناتهم الشخصية[3].

لذلك نجد أن البرلمان الأوروبي أعرب عن قلقه إزاء الأثر الذي يمكن أن تتركه الإجراءات التي تستهدف تحقيق الأمن على الحقوق والحريات خاصة على خصوصية الأفراد، فالتعاون الدولي في مجال مكافحة الإرهاب* مثلا من شأنه أن يؤدي إلى التخفيف من مستوى حماية الحقوق الأساسية للإنسان.

وفي نفس السياق أثار اقتراح قانون حول الأمن في الفضاء السيبراني في الولايات المتحدة الأمريكية احتجاجا كبيرا نظرا للصلاحيات التي يمنحها للحكومة في مواجهة خصوصية الأفراد على الأنترنت، حيث يمنح هذا الاقتراح لوزير التجارة حق الوصول إلى جميع البيانات الخاصة دون مراعاة لأي سياسة أو

[1] Olivier barrat, Informatique en nuage, Mettez de coté le patriot act. Penchez vous surFISAA Article, revue « Sécurité & Stratégie 2013. Page 64. disponible en ligne à l'adresse http://www.securite-strategie.fr/international-informatique-en.html-

[2] منى الأشقر، مرجع سابق، ص124.

[3] في هذا المعنى أنظر منى الأشقر جبور، محمود جبور، مرجع سابق، ص39.

من خلال قرار البرلمان الأوروبي المؤرخ في 14 جانفي 2009 بشأن الوضع الحقوقي في الإتحاد الأوروبي للفترة ما بين 2004 و2008 بعنوان حالة الحقوق الأساسية في الإتحاد الأوروبي (2004-2005).

* معاهدة "بروم" le traité de Prum المؤرخة في 27 ماي 2005 بألمانيا المتعلقة بمكافحة الإرهاب والجريمة العابرة للحدود والهجرة غير الشرعية، حيث يسمح هذا الاتفاق الدولي للدول الموقعة أن تتبادل المعلومات حول ملفات تعريف الحمض النووي، بصمات الأصابع، أو البيانات الخاصة بالمركبات وأصحابها. وقد تم نقل قرارات هذه المعاهدة إلى الإطار القانوني للاتحاد الأوروبي من خلال

DÉCISION 2008/615/JAI DU CONSEIL du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière Voir aussi le traité de Prum signé le 27 mai 2005 entre sept États membres de l'Union européenne qui renforce la coopération transfrontalière en matière de coopération policiè.

قانون يمنع هذا الوصول،[1] وهذا على الرغم من أن هدف قانون الخصوصية الصادر عام 1974 حسب ما تنص عليه المادة الأولى منه هو إعادة التوازن بين حق الدولة في الإطلاع على المعطيات الشخصية وتجميعها، وحق الفرد في حماية خصوصيته من التدخل غير المشروع للدولة، والذي يمكن أن ينتج عنه كشف هذه البيانات وإساءة استخدامها، لذلك كان للقضاء الأمريكي كلمته في هذا الصدد، في القضية المرفوعة من الإتحاد الأمريكي للحريات المدنية ضد عدد من الأجهزة الأمنية والإستخباراتية ووزير الدفاع على خلفية التنصت على المواطنين وجمع بياناتهم الشخصية، عندما صرحت المحكمة المدنية الجزئية للمنطقة الجنوبية بنيويورك في جوان 2013أن هذه الرقابة الشاملة تشكل تعديا صريحا على الحريات وأنه يخرج عن الصلاحيات المعطاة لهذه الهيئات في إطار مهمتها لحفظ الأمن القومي.[2]

ومما تقدم يتضح أن هناك حدودا فاصلة بين حق الأفراد في خصوصيتهم المعلوماتية من خلال قدرتهم في السيطرة على بياناتهم الشخصية،وبين حق الدولة في الإطلاع على هذه البيانات والتعامل معها إذا كان لازما في إطار قيامها بدورها في الحفاظ على الأمن القومي والنظام العام، ومن الضروري التأكيد على الأهمية القصوى لتوفير معيار منضبط يوازن بين الحق في الخصوصية وحق الدولة في الاطلاع، وهذا دور التشريع الذي ليس من الصعب عليه أن يضبط ويحدد نطاق وحدود كل من هذين الحقين.

المبحث الثالث: المخاطر التي تهدد الخصوصية المعلوماتية

لا يستطيع أحد إنكار الآثار الإيجابية العريضة التي خلفها استخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية، خصة في مجال تنظيم الدولة لشؤون الأفراد الإجتماعية والإقتصادية والعلمية وغيرها.

فالتطور التكنولوجي في مجال المعلوماتية أصبح يسهل عملية جمع أنواع جديدة من البيانات الشخصية، ويوفر أدوات تقنية لجمع وفهم أنواع مختلفة من المعلومات كان يستحيل أو من غير الممكن الوصول إليها في الماضي[3]، فقد صارت معظم معاملاتنا تتم بشكل الكتروني، الأمر الذي يمكن المؤسسات والدوائر والوكالات الحكومية وكذا الشركات الخاصة من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية، بل ويمكنها كذلك من مقارنة المعلومات المخزنة في ملفات إلكترونية بمعلومات في قاعدة بيانات أخرى، كما يسمح بنقلها عبر البلد في ثوان وبتكاليف منخفضة،[4] ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار، ظهر وبشكل متسارع أيضا الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية المعلوماتية، هذا الشعور نما وتطور بفعل الحالات الواقعية للإستخدام غير المشروع للبيانات الشخصية.[5]

[1] تم ترجمته من موقع: en.wikipidia.org/electronic-communication-privacy-act

[2] منى الأشقر جبور، محمود جبور، مرجع سابق، ص45.

[3] مروة زين العابدين، مرجع سابق، ص316.

[4] محمود إبراهيم غازي، مرجع سابق، ص276.

[5] منى تركي الموسوي، مرجع سابق، ص9.

فالتوسع الهائل لاستخدام التقنية في معالجة البيانات الشخصية أثار المخاوف من إمكانية انتهاك الحياة الخاصة، ومكمن إثارة هذه المخاوف، أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية، كالوضع الصحيوالأنشطة الإ جتماعية والمالية والآراء السياسية وغيرها يمكن جمعها وتخزينها لفترة غير محددة، ويمكن الرجوع إليها جميعا بمنتهى السرعة والسهولة، ومن ثم تضعف قدرة الفرد على التحكم في معطياته الشخصية والسيطرة عليها[1].

وبالرغم مما تقدم فإن مسألة كون التقنية المعلوماتية تشكل خطرا على الخصوصية المعلوماتية، إلا أنها تعد مسألة خلافية، أثارت جدلا واسعا في الفقه القانوني، حيث برز في هذا المجال اتجاهان فقهيان، الأول يرى أنه لا وجود لمثل هذه الخطورة، ومن ثم فلا حاجة لسن نصوص قانونية تحكم هذه المسألة، طالما أن عمليات التخزين والأرشفة الإلكترونية قد حلت فقط محل الوسائل اليدوية التقليدية، كالملفات الإلكترونية وقواعد البيانات، ومن ثم فإن القضاء قادر على تطويع النصوص العقابية التقليدية لمواجهة هذه المخاطر، كما أن النظام المعلوماتي ليس سوى آلة يمكن إحاطتها بعوامل الأمان لمنع تسرب البيانات المخزنة أو الاطلاع عليها أو استخدامها على نحو غير مشروع، فيما ذهب الإتجاه الفقهي الثاني إلى أن الأنظمة المعلوماتية و خاصة بنوك المعلومات تشكل خطرا على الحياة الخاصة للأفراد، الأمر الذي يستدعي وضع نصوص قانونية خاصة لمواجهة هذه الأخطار المستحدثة، كما أن هذه المخاطر تزداد كلما كان لكل مواطن رقم قومي تعريفي، لأن هذا الرقم يسهل الإ طلاع على كم هائل من المعلومات الخاصة بالأفراد والمخزنة إلكترونيا.[2]

لكن الرأي الأخير هو المرجح، والذي يقوم على نظرة تعكس وبحق حجم التخوف من الإ ستخدام غير المشروع للتقنية في كل ما من شأنه تهديد الحق في الخصوصية، سواء من خلال أنظمة المعالجة الآلية للمعطيات أو الإتساع بشكل سريع عبر معظم دول العالم في الإستخدام المتعاظم للأنترنت، وهو الأمر الذي نشأ عنه تحديات كبيرة وجديدة بشأن المعطيات الشخصية، وذلك من خلال تهيئة قدرات جديدة للحكومات والقطاعات الخاصة لتحليل المعلومات الشخصية.

فالقوة الحاسوبية الرائدة تعني أنه يمكن وبشكل فعال تخزين كميات هائلة من البيانات الشخصية ودمجها وتحليلها بمجرد جمعها، كما قد يسمح التطور التكنولوجي بالربط بين قواعد بيانات مع بعضها البعض، الأمر الذي يتيح المزيد من كميات البيانات التي يمكن معالجتها، ويهيئ فرصا كثيرة للاستخدام التجاري للبيانات الشخصية، ومن ثمة فإنه كلما زاد التطور التقني في مجال تكنولوجيا المعلومات زادت المخاطر التي تهدد خصوصية البيانات الشخصية.[3]

[1] يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي مقال متوفر عبر الموقع:
https://kenanaonline.com/users/ahmedkordy/posts/323471 اطلع عليهيوم الأربعاء2019/11/13 على الساعة 17:30

[2] عمار عباس الحسيني، جرائم الحاسوب والانترنيت، الجرائم المعلوماتية، منشورات زين الحقوقية، الطبعة الأولى، بيروت 2017، ص237.

[3] مروة زين العابدين، مرجع سابق، ص318.

المطلب الأول: مخاطر قواعد البيانات على الخصوصية المعلوماتية

لقد كان جمع البيانات الشخصية في وقت مضى يتم بإعلان إ ادي من الأفراد رغبة منهم في اكتساب وضع قانوني معين، فيتم تدوينها من قبل الموظف يدويا على الورق، وتكون مراجعتها أو الحصول عليها لا ينكشف إلا لأصحاب العلاقة وللأ جهزة المسؤولة في الدولة، وبطلب رسمي ولأهداف واضحة ومحددة، لكن التحول إلى الرقمنة حاليا نتيجة الثورة الهائلة والمتسارعة في مجال تكنولوجيا المعلومات، جعل هذه القيود تتخذ ركيزة جديدة ذات طبيعة مختلفة، ومن ثم أصبح السؤال المطروح كيف يمكن للحاسب الآلي أن يكون سببا للإعتداء على الخصوصية؟

إن الحاسبات وتقنياتها المختلفة وظهور النظام الآلي لمعالجة البيانات تمثل وسيلة جديدة ذات خطورة على البيانات الشخصية للفرد، وذلك لما تتميز به من سرعة في عملها، وسعة استيعابها غير المحدد للبيانات الشخصية، سواء في حالة تخزينها أو عند استخراجها من ذاكرة الكومبيوتر، و هو الأمر الذي يؤدي حتما إلى إمكانية الإطلاع على قدر لا يستهان به من هذه البيانات التي قد تكون متكاملة إلى حد بعيد ومتصلة بجوانب الحياة الخاصة للفرد[1]، وهذا راجع إلى الميزة التي يستأثر بها الكمبيوتر من حيث كمية البيانات الشخصية التي يحتويها.

وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تجميع وتحليل المعطيات واسترجاع المعلومات، اتجهت مختلف دول العالم إلى إنشاء قواعد بيانات لتنظيم مختلف الهيئات والمؤسسات والدوائر الحكومية، وبذلك اتسع على نحو كبير استخدام الكومبيوتر لجمع وتخزين وحفظ ومعالجة وتحليل البيانات ذات الطابع الشخصي لأغراض متعددة، وهذا ما أوجد ما يعرف حاليا ببنوك المعلومات أو قواعد البيانات[2]، والتي أدى ظهورها إلى تهديد أسرار الحياة الخاصة للأفراد، إذ أنها تضع تحت تصرف الدولة وأجهزتها المختلفة كقطاعات الصحة والقضاء والأمن وغيرها وكذا المشروعات العامة والخاصة، حجما كبيرا من المعطيات الشخصية عن الأفراد، تعجز الوسائل العادية والأساليب التقليدية اليدوية عن الوصول إليها[3]، وهو ما يستوجب وجود نظام قانوني لحماية المعطيات الشخصية من مخاطر قواعد البيانات.

الفرع الأول: مفهـوم قـواعد البيانات

إن جهاز الكمبيوتر وتقنياته المختلفة وما صاحبه من ظهور النظام الآلي لمعالجة البيانات، أصبح يمثل وسيلة جديدة أشد خطورة لتسجيل البيانات الشخصية للفرد، وذلك لما يتميز به هذا الجهاز من سرعة في عمله، وسعة غير محددة في استيعاب البيانات التي لا تنحصر فقط في حالة تخزين هذه البيانات، بل تتعداها عند استخراجها من ذاكرة الكومبيوتر، وهو الأمر الذي يمكن من الاطلاع على قدر لا يستهان به

[1] بولين أيوب، مرجع سابق، ص98.

[2] بولين أيوب مرجع نفسه، ص86.

[3] محمد رشيد حامد أبو حجيلة، الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار البنوك المعلومات، دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة الماجستير، كلية الدراسات الفقهية والقانونية، قسم الدراسات القانونية، جامعة آل البيت الاردن 2007، ص 17.

من هذه البيانات، والتي تكون متصلة إلى حد بعيد بجوانب الحياة الخاصة للفرد، واستغلالا لهذه الخصائص المذهلة للكومبيوتر تم إنشاء قواعد البيانات بغرض تنظيم الدولة لشؤونها.

أولا: تعريف قواعد البيانات

إن المقصود بقواعد البيانات هو قيام جهات معينة، بتجميع معطيات متصلة بموضوع معين لخدمة غرض معين، ويتم معالجتها آليا بواسطة أجهزة الكومبيوتر، لإخراجها في صورة معلومات تفيد مستخدمين في أغراض معينة[1]، ويتم ذلك وفقا لسجلات أو ملفات إلكترونية (fichier) رسمية، تديرها الإدارات الإلكترونية وتسجل فيها العديد من البيانات الشخصية.

والحاصل أنه قد كان لاختلاف شكل و الغرض من قواعد البيانات الأثر الواضح الذي انعكس على الفقه عندما تعرض لتعريف قواعد البيانات هذه، حيث نجد أن التعريفات الفقهية قد اتسمت بسمتين أساسيتين.[2]

السمة الأولى: الإتساع بحيث شملت بداية من الدلائل للبيانات إلى أن وصلت إلى الحقائق والرموز حتى ولو لم يكن بينهما رابطة.

السمة الثانية: لم تهتم سوى بتعريف قواعد البيانات المعالجة آليا فقط.

لذلك فقد عرف جانب من الفقه قواعد البيانات بأنها القواعد التي تؤسس أو تتضمن دلالة البيانات، كالحقائق والإحصاءات، والرموز والأنشطة الرقمية، كعمليات التحويل الرقمية دون أن يكون هناك رابطة بينها، سوى حين تحولها بالمعالجة الآلية إلى معلومات.[3]

وعرفت أيضا من جانب آخر من الفقه بأنها مجموعة مهيكلة من التسجيلات النصية أو غير النصية متاحة للقراءة آليا عبر خط مباشر مرتبط بخادم ملقم.[4]

أما من الناحية التشريعية فإن الإتحاد الأوروبي وسعيا منه نحو إرساء إتفاق بين الدول الأعضاء فيه، لوضع حل لمشكلة قواعد البيانات، فقد أصدر التوصية رقم (96/9/CE) المؤرخة في 1996/03/11 و التي بدأ سريانها في 1998/01/01،[5] متضمنة تعريفا لقواعد البيانات في المادة 12 منها، حيث نصت على أنها "مجموعة من الأعمال المنفصلة، بيانات ومواد أخرى يتم تنظيمها بأسلوب منظم ومنهجي يسمح بالولوج إليها بشكل فردي بواسطة الكترونية"[6].

---

[1] بولين أيوب، مرجع سابق، ص86.

[2] ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالانترنت والمعلوماتية، دراسة تطبيقية مقارنة، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر 2017، ص302.

[3] أحمد عمر حسبو، حماية الحريات في مواجهة نظم المعلومات، الطبعة الأولى، دار النهضة العربية، القاهرة 2000، ص41.

[4] ربيع محمود الصغير، مرجع نفسه، ص302.

[5] Au niveau du développement régional et national, la Communauté Européenne a adopté, en 1996, la Directive 96/9/EC du Parlement Européen ainsi que du Conseil, émise le 11 mars 1996 sur la protection des bases de données,

[6] أسامة أحمد بدر، الوسائط المتعددة بين واقع الدمج الإلكتروني للمصنفات وقانون حماية حق المؤلف، دار الجامعة الجديدة للنشر، الاسكندرية 2004، ص88.

وقد كان المشرع الفرنسي قد عرف قواعد البيانات إنطلاقا من قانون الملكية الفكرية رقم 361/94المؤرخ في 10 ماي 1994 في المادة 3/112[1]، حين اعتبر أنه يقصد بقواعد البيانات مجموعة مصنفات، معطيات أو عناصر أخرى مستقلة معدة في هيئة نظامية أو منهجية، يتم التوصل إليها انفراديا بوسائل إلكترونية أو بأية وسيلة أخرى" وكذلك عرفها في الملحق بالمرسوم رقم 95/240 المؤرخ في 1995/03/30 [2]المتعلق بتنفيذ القانون رقم 94/665 المؤرخ في 1994/08/04 المتعلق باستعمال اللغة الفرنسية على أن قواعد البيانات هي مجموعة المعطيات المنظمة بقصد استعمالها بواسطة برامج مرتبطة بتطبيقات مميزة وبشكل يسهل الحركة المستقلة لهذه المعطيات وتلك البرامج".

وقد أخذ المشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالة المعطيات الشخصية بنفس التعريف الذي جاء به المشرع الفرنسي في القانون 17/78 المتعلق بالمعلوماتية والملفات والحريات عندما عرف الملف الإلكتروني بأنه "كل مجموعة معطيات مهيكلة ومجمعة يمكن الولوج إليها وفق معايير محددة".

وترتيبا على ما سبق فإنه يمكن القول أن قواعد البيانات هي دعامة تحمل بيانات، تعتمد في تصفحها على قوة القيمة الإ سترادادية فيها، فليست فقط مجرد تجميع وفهرسة للبيانات، ولكن الهدف منها هو الوصول إلى هذه المعلومة بكل سهولة وهو ما يعرف بالقيمة الإ سترادادية لقاعدة البيانات.[3]

ثانيا: خصائص قواعـد البيانات

من السمات المميزة لقواعد البيانات بعد تزايد الإهتمام بها نتيجة ارتباطها بالحوسبة الإلكترونية أنها عبارة عن هيكلة أو نظام معالجة تخزيني مرتبط بنظام استردادي للمعلومة، ومن خلالها يتم معالجة البيانات وإمكانية استردادها في أي وقت كمعلومة تثري معرفة الإنسان.

بالإضافة إلى أن القدرة التخزينية للمعلومات داخل قاعدة البيانات أدى إلى سهولة عملية تخزين كميات كبيرة من البيانات على الوسائط الإلكترونية، حيث تحتوي هذه البنوك على معلومات طبية، مالية،

[1] Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française. Article 112-3 Modifié par Loi n°98-536 du 1 juillet 1998 - art. 1 JORF 2 juillet 1998 « On entend par base de données un recueil d'oeuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen. »

Le code de la propriété intellectuelle, créé par la loi n° 92-597 du 1er juillet 1992 relative au code de la propriété intellectuelle modifie par la, LOI no 94-361 du 10 mai 1994 portant mise en oeuvre de la directive (C.E.E.) no 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle.

[2] Décret n°95-240 du 3 mars 1995 pris pour l'application de la loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française.

[3] ربيع محمود الصغير، مرجع سابق، ص307.

أمنية، صحية، إدارية ... يتم تجميعها وتسجيلها على شرائط وأسطوانات، ثم يتم إدخالها إلى الحاسب الآلي وتخزينها بذاكرته.[1]

وقد تكون قواعد البيانات مقصورة على بيانات ومعلومات تتصل بقطاع معين[2]، كقطاع الصحة أو الضرائب وغيرها، أو قد تكون مهيأة للإستخدام على المستوى الوطني العام، أو تكون متعلقة بالقطاع الخاص كبنوك المعلومات للشركات المالية والبنكية وشركات التأمين وغيرها، وهو ما يجعل من قواعد البيانات لدى الإدار ات والقطاع الخاص تتعدد وتتكاثر وتتنوع.[3]

كما أن قواعد البيانات نظرا لاعتمادها على أنظمة المعالجة الآلية للمعطيات، فان لها القدرة على تخزين هذه المعطيات ومعالجتها أو نقلها عبر المسافات الطويلة، كما لها السرعة في آداء هذه العمليات وقدرتها على الربط والمقارنة بين الملفات المخزنة على خلاف الوسائل التقليدية، وهذا ما يثير قلقا متزايدا حول إمكانية إساءة استخدام البيانات الشخصية خلال هذه العمليات المعلوماتية، فيكون من شأن هذه الوسيلة انتهاك السرية التي يجب أن تحاط بها هذه المعلومات ومن ثم انتهاك حرمة الحق في الخصوصية، ويصبح الإنسان بالنتيجة مكشوفا أمام الكومبيوتر، فالمعلومات التي تم جمعها عنه لا تترك له أي زاوية يمكنه أن يختبئ وراءها، ومن ثم يصبح ذلك الحق في الإنزواء والسر والعزلة الذي كان في يوم ما مكسبا للإنسان دون معنى ولا مغزى[4].

ولفهم المخاطر الناتجة عن قواعد معالجة البيانات أثناء معالجة المعطيات ذات الطابع الشخصي، يستلزم الأمر منا أولا أن نعرج على تحديد مفهوم المعالجة الآلية للمعطيات الشخصية ثم إبراز المخاطر المرتبطة بها تجاه المعطيات الشخصية التي تتم معالجتها.

الفرع الثاني: مفهوم المعالجة الآلية للمعطيات ذات الطابع الشخصي

إن عملية المعالجة الآلية للمعطيات الشخصية تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير هذه المعطيات ومعالجتها، لذلك فقد ظهرت بالنتيجة فكرة نظام المعالجة الآلية وهي فكرة مركزية وجوهرية، ذلك أن نظام المعالجة الآلية للمعطيات هو شرط مفترض لمعالجة المعطيات ذات الطابع الشخصي وهو نظام معلوماتي يعتمد على المكونات والأجهزة البرمجية للحاسوب في معالجة المعطيات واسترجاع المعلومات.[5]

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان الاردن 2009، ص74.

[2] نعيم مغبغب، مرجع سابق، ص185.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص16.

[4] محمود عبد المحسن المقاطع، مرجع سابق، ص116.

[5] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي 2012-2013، كلية الحقوق جامعة باتنة، ص41.

أولا: تعريف نظام المعالجة الآلية للمعطيات

ليس هناك من الناحية الفقهية تعريف دقيق لنظام المعالجة الآلية، وذلك بسبب تعدد الإستعمال، ووجود أنظمة كبيرة تضم بداخلها أنظمة أصغر منها، وعليه فقد تم تعريفه على أنه مجموعة المكونات ذات علاقة متداخلة مع بعضها البعض تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما، وفي سبيل ذلك يقبل مدخلات ويقوم بالعمليات وينتج مخر جات[1].

و لقد عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بموجب الفقرة (ب) من المادة 02 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[2] بأنه "أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، كما عرفته الإتفاقية الدولية لإجرام تقنية المعلومات هي الأخرى في الفقرة الأولى من المادة الأولى من الفصل الأول بعنوان المصطلحات، على أنه "كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات"، وكذلك إتفاقية بودابست المتعلقة بالجريمة الإلكترونية[3] عرفته في المادة الأولى منها على أنه أي جهاز أو مجموعة من الأجهزة المتصلة أو المتعلقة ببعضها البعض، ويقوم واحد منها أو أكثر تبعا لبرنامج معين بمعالجة آلية للبيانات، كما ذهبت بعض الدول إلى وضع تعريف لنظام المعالجة الآلية للمعطيات، أو كما يسمى أيضا النظام المعلوماتي في قوانينها الداخلية حيث عرفه نظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية الصادر في 2007/03/26 بأنه مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية"،أيضا قانون سلطنة عمان رقم 2008/69 الخاص بالمعاملات الإلكترونية الصادر بتاريخ 2008/05/17 عرفه بالمادة الأولى من هذا القانون بأنه نظام إلكتروني للتعامل مع المعلومات والبيانات بإجراء معالجة تلقائية لها بغرض إنشاء أو إرسال أو تسليم أو تخزين أو عرض أو برمجة أو تحليل تلك المعلومات والبيانات، والقانون الإتحادي لدولة الإمارات رقم 2006/02 المتعلق بمكافحة جرائم تقنية المعلومات عرفه بأنه مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك.

كما حاول مجلس الشيوخ الفرنسي بمناسبة مناقشة قانون العقوبات الجديد إضافة نص يتعلق بتعريف نظام المعالجة الآلية للمعطيات كان قد اقترحه، والذي مؤداه أنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط التي يربط بينها مجموعة من العلامات التي يتم عن طريقها تحقيق نتيجة معينة، وهي معالجة البيانات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية.[4]

[1] طارق طه، مقدمة في تطور نظم المعلومات الإدارية والحاسبات الآلية، منشأة المعارف، الطبعة الثالثة الإسكندرية 2000، ص16.

[2] أنظر الجريدة الرسمية، عدد 47 لسنة 2009، الصادرة بتاريخ 06 أوت 2009.

[3] الإتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، موقعة في مدينة بودابست، بتاريخ 2001/11/23 رقم 185.

[4] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت لبنان، 1999، ص43.

وبالتالي فإن كل مجموع معلوماتي مهما كان حجمه وطريقة ربطه مع غيره وطريقة معالجته المرصودة، يشكل نظاما للمعالجة الآلية للمعطيات، وذلك من خلال مكوناته المادية كالحاسب الآلي، ودعامات البرامج والمعطيات ووحدات الإدخال والإخراج، وغير المادية كاللوغاريتمات التي تشكل البرامج والمعلومات المشفرة في شكل معطيات[1].

من خلال التعريفات التي صيغت لمصطلح نظام المعالجة الآلية للمعطيات، يمكن القول أنه مصطلح ينطبق على أي نظام مهما كان مسماه يتوافر له عدة عناصر مرتبطة ببعضها بعدد معين من الروابط لتحقيق المعالجة الآلية للمعطيات، من تجميعها وتخزينها ومعالجتها ونقلها وتبادلها... وذلك من خلال برنامج أو برامج معلوماتية[2].

ومن ثم فإنه يمكن تشبيه نظام المعالجة الآلية للمعطيات بنظام الإنتاج الذي يتعامل مع المادة الخام ليحولها الى المنتج النهائي، وكذلك نظام المعالجة يستخدم البيانات الخام كمدخلات ثم يحولها إلى معلومات كمخرجات يتم استخدامها بواسطة المستفيدين، ويعاد استخدامها مرة أخرى كمدخلات للحصول على معلومات جديدة، ولا يجب النظر الى النظام المعلوماتي أنه نهاية في حد ذاته، ولكنه بداية لعمليات كثيرة تساعد المنشأة على ممارسة أنشطتها المختلفة.[3]

ثانيا: المقصود بمعالجة المعطيات ذات الطابع الشخصي

إن المعالجة الآلية للمعطيات عموما وفق ما هو متعارف عليه في المجال التقني هي مجموعة من العمليات المترابطة والمتسلسلة، بدءا من جمع المعطيات وإدخالها إلى نظام المعالجة الآلية، ومعالجتها وفقا للبرامج التي تعمل بها نظم المعالجة الآلية وصولا إلى تحليلها وإخراجها بصورة معلومات، وقد عرفتها المذكرة التفسيرية للإتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية بأنها مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي[4].

كما عرفت الإتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي مصطلح المعالجة الآلية في المادة 02 على "أنها العمليات التي يتم القيام بها كليا أو جزئيا استنادا إلى طرق آلية، تسجيل المعطيات وتطبيق عمليات منطقية أو حسابية أو الاثنين معا على هذه المعطيات بتعديلها، محوها، إستخراجها أو نشرها.

أما عن المعالجة الآلية للمعطيات ذات الطابع الشخصي، فإنه بالرجوع إلى الإرشاد التوجيهي رقم 46/95 المؤرخ في 24 أكتوبر 1995 السالف ذكره، فقد عرف في المادة 02 الفقرة (ط) المعالجة الآلية للمعطيات ذات الطابع الشخصي بأنها كل عملية أو مجموعة من العمليات التي تنجز بواسطة طرق آلية أو بدونها،

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، 2007، ص27.

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، 2012، ص56.

[3] يحي مصطفى حلمي، مرجع سابق، ص170.

[4] رشيدة بوكر، مرجع سابق، ص53.

وتطبق على المعطيات ذات الطابع الشخصي، مثل التجميع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو الإذاعة أو أي شكل آخر من أشكال إتاحة المعلومات أو التقريب أو الربط البيني، وكذا الإغلاق أو الإتلاف، وقد حافظ التوجيه الأوروبي الجديد RGPD رقم 2016/679 المشار إليه سابقا، في الفقرة الثانية من المادة الرابعة على نفس التعريف، مع إضافة بعض العمليات المقدمة بما يتناسب مع التطورات التقنية في مجال المعالجة، حيث ورد تعريفها كما يلي: "هي كل عملية أو مجموعة من العمليات، تنجز بمساعدة طرق آلية وبدونها، وتطبق على المعطيات ذات الطابع الشخصي، مثل الجمع والتسجيل والتنظيم والهيكلة، أو الحفظ أو التعديل أو ستخراج أو التشاور أو الإستخدام أو الإتصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التسوية أو الترابط أو المحو أو التدمير"*، وهو نفس التعريف الذي تبناه المشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بشكل مطابق تماما، حيث نصت المادة 03 منه أنه "يقصد لأغراض هذا القانون بالمعالجة الآلية للمعطيات ذات الطابع الشخصي، كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو ستخراج أو الإطلاع أو الإ ستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف".

والملاحظ إذن من خلال هذه التعاريف التي صيغت في شأن معالجة المعطيات ذات الطابع الشخصي أنه لكي تكون هذه المعطيات داخل نطاق الحماية القانونية المقررة بالقانون 07/18 يستلزم الأمر أن تكون

---

* Article 4/2 de règlement (UE) 2016/679 : « traitement, toute opérations ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisées et appliquées à des données ou des ensemble de données à caractère personnel, tel que le collecte, l'enregistrement l'organisation, la structuration, la conservation, l'adoption ou le modification, l'extraction, la consultation, l'utilisation la communication par transmission, la diffusion ou toute autre forme de mise disposition, le rapprochement ou l'interconnexion la limitation, l'effacement ou la destruction »

وقد حظي مصطلح المعالجة الآلية للمعطيات ذات الطابع الشخصي بالتعريف في معظم التشريعات المتعلقة بحماية هذه المعطيات.

-المشرع الفرنسي عرفها بموجب المادة 03/02 من القانون 17/78 المؤرخ في 1978/01/06 المتعلق بالمعلوماتية والملفات الحريات:

Constitue un traitement de données à caractère personnel toute opérations ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment le collecte, l'enregistrement l'organisation, la structuration, la conservation, l'adoption ou le modification, l'extraction, la consultation, l'utilisation la communication par transmission, la diffusion ou toute autre forme de mise disposition, le rapprochement ou l'interconnexion la limitation, l'effacement ou la destruction »

-المشرع التونسي عرفها بموجب الفصل السادس من القانون الاساسي عدد 63 المؤرخ في 2004/07/27 المتعلق بحماية المعطيات الشخصية: "يقصد بمفهوم هذا القانون ب:

معالجة المعطيات الشخصية: العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي والتي تهدف خاصة إلى جمع معطيات شخصية أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو إتلافها أو الإطلاع عليها، وكذلك جميع العمليات المتعلقة باستغلال قواعد البيانات أو الفهارس أو السجلات أو البطاقات أو الربط البيني"

-المشرع المغربي عرفها بموجب المادة 2/1 من القانون 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي حيث نصت: يراد بما يلي لأجل تطبيق هذا القانون:

-معالجة المعطيات ذات الطابع الشخصي "معالجة" كل عملية أو مجموعة من العمليات تنجز بمساعدة طرق آلية أو بدونها وتطبق على معطيات ذات طابع شخصي مثل التجميع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الإستخراج أو الإطلاع أو الإستعمال أو الإيصال عن طريق الإرسال أو الإذاعة أو أي شكل آخر من أشكال إتاحة المعلومات أو التقريب أو الربط البيني وكذا الإغلاق أو المسح أو الإتلاف"

محلا للمعالجة، فهذه المعالجة هي السبب الرئيسي في استفادة المعطيات ذات الطابع الشخصي من الحماية القانونية[1]، لذلك فقد جعلت التشريعات المقارنة المعطيات ذات الطابع الشخصي محلا للحماية باعتبار أن هذه الأخيرة لا يلحقها أي خطر ما دامت لم تتم معالجتها، فالمادة الأولى من القانون 07/18 تنص على أن الهدف من هذا القانون هو تحديد قواعد حماية للأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي.

وتطبيقا لهذه الفكرة فقد قضي في فرنسا بأن مجرد إدخال البيانات في الكومبيوتر لا يحقق لها وصف البيانات المعالجة والمبرمجة آليا، إذا كان ذلك لا يعدو أن يكون كتابة لتلك البيانات وكان الغرض منها طبعها على ورق وليس الإ حتفاظ بها في الجهاز[2].

1) أشكال معالجة المعطيات الشخصية: تنطوي معالجة المعطيات ذات الطابع الشخصي على عملية أو مجموعة من العمليات دلت عليها تلك المصطلحات التي قام المشرع بتكديسها والتوسع في تعدادها، حيث يتضح جليا وبشكل واضح من خلال تعريف معالجة المعطيات ذات الطابع الشخصي السالف ذكره التراكم في تعداد عمليات المعالجة[3]، وقد سار المشرع في ذلك على نهج التوجهات الأوروبية وكذا التشريعات المقارنة في هذا الإطار، وهو الأمر الذي يعكس رغبة المشرع في توسيع مفهوم المعالجة ومنحها معنى واسعا، يجعل مدلولها يختلف عن مدلولها في نطاق لغة المعلوميات*، وكذا محاولة منه لسرد كل التقنيات الممكن استعمالها في هذه العملية، والتي تتجدد وتتطور بسرعة، وذلك مواكبة لتطور التقنية التي يعرفها العصر الحالي، ولعل الهدف من كل ذلك هو توسيع دائرة الحماية ضد أي فعل أو عملية قد تمس بالحق في الخصوصية أثناء معالجة المعطيات الشخصية، تجنبا للوقوع في حجة غياب النص القانوني.

كما نلاحظ من جملة التعاريف السابقة، أن التعداد الذي جاءت به عمليات المعالجة إنما هو على سبيل المثال وليس محصورا على هذه العمليات فقط، وهذا ما يظهر واضحا من استعمال المشرع الجزائري لعبارة "مثل" واستعمال المشرع الفرنسي لعبارة notamment واستعمال التوجيه الأوروبي لعبارة telles que، وهذا يعني أن معالجة المعطيات الشخصية يمكن أن تتم بأشكال أخرى غير تلك الواردة في التعريف التشريعي، قد تفرزها تكنولوجيا المعلومات المتطورة، لكن الفقه الفرنسي قابل هذه الرؤية التوسعية في تعريف معالجة المعطيات الشخصية باعتبارها توسعا تعسفيا.[4]

---

[1] حسن الحافظي، الحماية القانونية للمعطيات ذات الطابع الشخصي بين التشريع الوطني والاتفاقيات الدولية، مذكرة ماستر القانون الجنائي والتعاون الجنائي الدولي، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة مولاي إسماعيل، 2017 2018، ص45.

[2] غنام محمد غنام، مرجع سابق، ص104.

[3] André LUCAS, Jean DEVEZE et Jean FRAYSSINET, droit de l'informatique et de l'internet, presses universitaires de France, économies, paris 2001. Page 82.

* عمليات المعالجة التي ذكرها المشرع الجزائري هي: عملية الجمع، عملية التسجيل، عملية التنظيم، عملية الملائمة، عملية التغيير، عملية الاستخراج، عملية الاطلاع، عملية الاستعمال، عملية الإيصال عن طريق الإرسال أو النشر أو أي طريقة من طرق الإتاحة، عملية التخريب، عملية الربط البيني، عملية الإغلاق، عملية التشفير، عملية المسح، عملية الإتلاف.

[4] André LUCAS, Jean DEVEZE et Jean FRAYSSINET, op, cit p84.

وتجدر الإشارة إلى أن المشرع لم يعرف من بين تلك العمليات سوى عمليات الربط البيني، الإغلاق والإيصال، وهذا في اعتقادنا راجع لكون المعنى اللغوي للعمليات الأخرى لا يختلف عن معناها الفني، ومن ثمة فلا حاجة لتعريفها، عكس تلك العمليات المعرفة، فأما عن عملية الربط البيني فقد عرفها المشرع بأنها شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة لغاية محددة مع معطيات أخرى يمسكها مسؤول أو مسؤولون آخرون عن المعالجة، أو يمسكها نفس المسؤول لنفس الغرض أو لأغراض أخرى، أما عملية الإغلاق فهي جعل الدخول إلى المعطيات غير ممكن، وأما عملية الإيصال فهي كشف أو إعلام بمعطيات لشخص غير الشخص المعني.

إن معالجة المعطيات الشخصية قد تتحقق بعملية واحدة من العمليات المذكورة كتغيير هذه المعطيات أو استرجاعها مثلا، كما يمكن أن تتحقق من خلال عمليتين أو أكثر كتجميع المعطيات وتسجيلها ثم تنظيمها.

وتعتبر المعالجة متحققة حتى ولو احتفظت المعطيات التي خضعت لها بشكلها الأصلي، إذ ليس من اللازم أو الضروري أن يترتب عن المعالجة تحويل أو تغيير في شكل المعطيات التي خضعت لذلك[1]، وهذا واضح من خلال بعض أشكال المعالجة تم ذكرها من بين العمليات التي تتم بها المعالجة ولا يمكن أن ينتج عنها تغيير في ملامح المعطيات الخاضعة لها كالتجميع أو الحفظ.

2) طرق معالجة المعطيات ذات الطابع الشخصي: تحصل عملية معالجة المعطيات ذات الطابع الشخصي إما بطرق أو وسائل آلية أين تستعمل فيها آلية تقنية مثل جهاز الكومبيوتر،* وإما بطريقة يدوية تستعمل فيها وسائل تقليدية مثل السجلات والدفاتر وغيرها، لذلك نجد أن المشرع اعتبر أن معالجة المعطيات ذات الطابع الشخصي تنجز بالطرق والوسائل الآلية أو بدونها، ولم يعلق تحققها على نوعية الوسيلة المستعملة في المعالجة، سواء كانت آلية أم يدوية، وبالتالي فإن المعالجة المنصبة على المعطيات الشخصية تكون متحققة بإحدى العمليات المذكورة، ولو لم يتم استعمال أي طريقة آلية وتقنية، فالعبرة والغاية هو حماية المعطيات بغض النظر عن الوسيلة المستعملة في المعالجة، وهذا ما جعل الفقه يتحدث عن مبدأ الحياد التكنولوجي[2].

لذلك نجد أن بعض نصوص التجريم تتعلق بالمعطيات الشخصية المعالجة آليا، بينما تسري نصوص أخرى للتجريم على المساس بالمعطيات الشخصية، سواء منها ما تمت معالجته في الحاسب الآلي أو ما يتم معالجته يدويا، والبيانات المعالجة آليا هي تلك البيانات المبرمجة، أي التي تم إدخالها إلى نظام الكومبيوتر وتسجيلها داخل هذا الجهاز وحفظها في الذاكرة وإعدادها وتنسيقها وتوصيلها إلى الغير.

وهي الفكرة المؤكدة من خلال التوجيه الأوروبي رقم 46/95 المؤرخ في 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعيين في مواجهة معالجة المعطيات ذات الطابع الشخصي وحرية تدفق هذه المعطيات،

---

[1] أمنار إبراهيم، الحماية الجنائية للمعطيات ذات الطابع الشخصي على ضوء القانون المغربي والقانون المقارن، رسالة لنيل دبلوم الدراسات العليا المعمقة، جامعة الحسن الأول، ص31 منشورة في مجلة القانون والأعمال عبر الموقع الالكتروني www.droitetentreprise.org أطلع عليها يوم 2019/02/29 على الساعة 10.56.

* رغم أهمية جهاز الكمبيوتر أو الحاسوب في القيام بعمليات المعالجة الآلية للمعطيات ذات الطابع الشخصي إلا أنه ليس الوسيلة الوحيدة التي يمكنها القيام بذلك، فالتطور الهائل في مجال تكنولوجيا المعلومات سمح باستعمال وسائل تقنية كثيرة في مجال المعالجة الآلية للمعطيات.

[2] André LUCAS, Jean DEVEZE et Jean FRAYSSINET, op, cit page 83.

حيث تقرر الحيثية رقم 27 منه على أن حماية الأشخاص يجب أن تطبق بالإضافة إلى المعالجة الآلية للمعطيات على المعالجة اليدوية، وأن نطاق الحماية لا يجب أن يتوقف على التقنيات المستعملة.[1]

وقد جسدت اللجنة الوطنية للمعلومات والحريات الفرنسية (CNIL) في أحد تقاريرها هذه الفكرة، عندما أوردت أنه ليس هناك من شك في أن الدليل الورقي أو الإلكتروني للمشتركين في خدمة الهاتف أو تسجيل قدامى التلاميذ في مؤسسة تعليمية يشكل ملفا (fichier) شخصيا يدخل في نطاق حماية المعطيات الشخصية المقررة بالقانون 17/78 المؤرخ في 16 جانفي 1978.[2]

وتجدر الإشارة في هذا الصدد أن المشرع وإن كان قد حدد مجال ونطاق تطبيق القانون 07/18 بكل معالجة تنصب على المعطيات ذات الطابع الشخصي سواء بوسائل آلية أو غير آلية (يدوية)، إلا أن نصوصه جاءت في مجملها تضع إطارا قانونيا يحدد نظام معالجة المعطيات ذات الطابع الشخصي عندما يصار ذلك بواسطة التقنية الآلية، وذلك لحجم المخاطر التي تشكلها هذه الأخيرة على المعطيات الشخصية مقارنة بالمعالجة غير الآلية، بالإضافة إلى حجم التخوف من المعالجة الآلية الذي يكون على أشده مقارنة بالمعالجة التقليدية.

الفرع الثالث صور الإعتداء على المعطيات الشخصية خلال عملية المعالجة في قواعد البيانات

يمكن القول أن المقصود بمعالجة المعطيات (electronic data processing) يشير إلى استخدام الأساليب والعمليات الآلية لمعالجة هذه البيانات،[3] واستنادا لكل ما تقدم فإنه يمكن القول أيضا أن الوظائف الرئيسية التي تقوم بها النظم المعلوماتية على اختلاف أنواعها ومجالاتها تتمثل أساسا في عمليات الجمع والتخزين والتشغيل وإيصال المعلومات إلى المستخدم بعد معالجة المعطيات، ومن ثم فإن المخاطر التي تهدد المعطيات الشخصية، يمكن أن تظهر في كل وظيفة من هذه الوظائف، وهذا ما سوف نبينه تباعا.

أولا: المخاطر التي تهدد المعطيات الشخصية خلال عملية التجميع

لقد وفرت تقنيات المعلومات والأجهزة التي تستخدمها قدرة هائلة وإمكانات غير مسبوقة في مجال جمع البيانات الشخصية والتنقيب عنها بغية تحويلها إلى معلومات، وتعد عملية جمع البيانات الشخصية الخطوة الأولى في عمل النظام المعلوماتي، فمن خلالها يتم تغذية الحاسوب الآلي بهذه البيانات ومن ثم تمكنه من القيام بالوظائف اللاحقة الأخرى.[4]

ومن هذا المنطلق فإنه يقصد بعملية جمع المعطيات الشخصية تغذية الكومبيوتر بالبيانات المتعلقة بالحياة الشخصية للفرد، والتي تسمح بصورة مباشرة أو غير مباشرة بالتعرف عليه أو تجعله قابلا للتعرف عليه، كتلك المعطيات المتعلقة بهويته وحالته الصحية، المهنية، المالية، العائلية وغيرها.

---

[1] (27) considérant que la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel, que le champ de cette protection ne doit en effet dépendre des techniques utilisées…

[2] CNIL 2 eme rapport d'activité page 155 sur site : www.cnil.fr/médiathéque/rapport-annuels.

[3] مروة زين العابدين، مرجع سابق، ص399.

[4] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة 2001، ص71.

إن الكثير من الدوائر والوكالات الحكومية وكذا الشركات والمؤسسات الخاصة تعمل على تجميع كميات هائلة من البيانات الشخصية المختلفة والمفصلة عن الأفراد، كما هو الحاصل في قطاع الخدمات[1] مثلا، سواء تقوم بذلك بنفسها لتملكها لأجهزة الكومبيوتر، أو تلجأ إلى مؤسسات أخرى لتزودها بالمعطيات المطلوبة، لتقوم بإنشاء ملفات إلكترونية عنهم، إذ يمكن أن يجمع عن الشخص بهذا الملف الالكتروني العديد من المعطيات الخاصة به مثل تنقلاته، سفره، أوقات دراسته، اجتماعاته، نشاطه الحزبي، ديانته، وغيرها من المعلومات التي يؤدي جمعها عنه والحصول عليها بسرعة مذهلة أو جمعها بطريقة عشوائية غير منظمة إلى حرمان الفرد من الخصوصية، بعد أن ترسم عنه صورة واضحة لا مجال للشك أو الطعن فيها، من خلال هذه المعطيات المجمعة عنه، فهو بذلك حتما أمام خطر لا يمكنه تجاوزه أو تداركه، خاصة إذا كانت هذه البيانات تعط ـ ى مزورة أو مغلوطة وغير حقيقية أو غير دقيقة أو غير واقعية[2]، ومن ثم الحكم عليه بأحكام خفية من واقع الملفات الإلكترونية الشخصية المخزنة.

كما أن تجميع البيانات الشخصية في أجهزة الكومبيوتر يجعل من فرص الوصول إليها على وجه غير مأذون به أو بطرق التحايل أكثر من ذي قبل، وبالتالي يفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا، أو مراقبة الأفراد وتعرية خصوصياتهم، الأمر الذي يترك مسألة إدارة البيانات الشخصية في القطاعين العام والخاص في مواجهة تحديات أمام المشرع والقضاء وواضعي سياسات الحماية ومصنعي البرامج، من خلال الهواجس التي تثيرها مسائل الحفاظ على الحق في خصوصية المعطيات الشخصية وأمنها وأساليب جمعها ومصداقيتها[3]، لأن مسألة جمع المعطيات الشخصية سيزيد من فر ص المخاطر عليها إذا تم جمعها بطرق غير مشروعة، وذلك في الأحوال التي تكون فيها هذه المعطيات مما لا يجوز جمعها بحكم القانون، أو تم جمعها بدون موافقة صاحبها، ففي ظل عدم وجود قواعد قانونية تمنع تجميع المعطيات الشخصية بهذه الطريقة، فإن ذلك سيسهل من إمكانية فضح أسرار الحياة الخاصة[4].

لذلك نجد أن المشرع الجزائري في القانون 07/18 أوجب في المادة 09 منه أن تتم عملية تجميع المعطيات الشخصية بطريقة مشروعة ونزيهة، لما لهذه العملية من أهمية بالغة في سبيل معالجة المعطيات الشخصية، على اعتبار أن جمع البيانات الشخصية وتسجيلها هي نقطة البداية في إمكانية كشف أسرار الحياة الخاصة والإ عتداء عليها، وهي مسألة مؤكد عليها في الإتفاقية الأوروبية بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية السالف ذكرها، حينما أوصت بأنه يجب أن تكون البيانات الشخصية التي تمر بالمعالجة التلقائية قد تم الحصول عليها وتجميعها بصورة عادلة وقانونية، وكذلك الإرشاد الأوروبي رقم 95/46 المتعلق بحماية الأشخاص الطبيعيين في مواجهة معالجة المعطيات ذات الطابع الشخصي وحرية تدفق المعلومات، حينما أقر في مادته السادسة على وجوب أن تكون البيانات المعالجة قد جـ ـ معت لأغراض محددة وصريحة ومشروعة، بل هي هدف وموضوع المعلوماتية، إذ من خلالها يتم إدخال المعلومة في النظام الآلي للكمبيوتر بغرض معالجتها، فإذا تم إدخال بيانات وهمية أو إدخال بيانات

[1] Alain Marc Benssoussan, internet, aspects juridiques. Hermés. 2e édition 1998. page 164.

[2] بولين أيوب، مرجع سابق، ص113.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص32.

[4] بولين أيوب، مرجع نفسه، ص113.

بقصد التشويش على صحة البيانات القائمة، أدى ذلك إلى غياب النزاهة في عملية التجميع التي استوجبها القانون[1].

فإذا كان من الممكن تجميع المعطيات الشخصية بشتى الطرق، بصورة مباشرة أو غير مباشرة، ويسجل في الملف الإلكتروني للشخص جميع المعلومات المتعلقة به وبكل التفاصيل حتى نكون أمام صورة واضحة وجلية للفرد، فإن اصطناع معلومات وتسجيلها ونسبتها للشخص المعني بالملف الإلكتروني هو الأكثر سهولة في التنفيذ، لا سيما في المؤسسات المالية، حيث يكون المسؤول عن القسم المعلوماتي في هذه المؤسسة في أفضل وضع يؤهله لارتكاب هذا النمط غير النزيه من التلاعب[2]، كما تغيب المشروعية أيضا في عملية التجميع للمعطيات الشخصية، إذا ما تم تجميعها دون علم صاحبها، فأي تجميع للمعطيات الشخصية دون علم صاحبها يعتبر غير مشروع، لذلك فقد اعتبرت محكمة النقض الفرنسية أن تجميع عناوين البريد الإلكتروني للأشخاص دون علمهم يعتبر تجميعا غير مشروع للبيانات الشخصية، يستحق فاعله العقاب، حتى ولو لم يتم حفظ هذه العناوين[3].

كما نجد أن اللجنة الوطنية للمعلوماتية والحريات في فرنسا (CNIL) فرضت غرامة مالية على شركة جوجل (google)على إثر تفتيش قامت به عامي 2009 و2010 بسبب جمعها بيانات المحتوى (الهويات، كلمات المرور، تبادل رسائل البريد الالكتروني) عبر شبكات "الوي في" من أجل خدمتها الجديدة «google street view» دون علم أصحاب هذه البيانات، وقد تعهدت شركة جوجل بالتخلص من هذه البيانات التي تم تجميعها[4].

و إزاء تلك الخطورة التي يمكن أن تهدد المعطيات الشخصية في مرحلة تجميعها، فإنه ينبغي أن يكون تجميع هذه المعطيات فقط من أجل إنجاز الغاية التي جمعت لأجلها، فالمؤسسات الإدارية والحكومية تجمع البيانات الشخصية في إطار إدارة أمور مواطنيها وشؤونهم الحياتية، ورغبة منها في حماية هؤلاء، وكذلك المؤسسات الخاصة لأجل تقديم الخدمة المطلوبة دون أن تخرج هذه الغاية من جمع البيانات الشخصية عن إطارها المحدد، لأن ذلك سوف يجعل المعالجة تشكل مصدر خطر على الخصوصية المعلوماتية، نتيجة الإستخدام غير القانوني للبيانات الشخصية، بعد أن كانت وسيلة لحمايتهم وضمان أمنهم.[5]

والمشرع الجزائري تناول هذه الفكرة في المادة 09 من القانون 07/18 عندما نص في الفقرة "ب" أنه يجب أن تكون المعطيات ذات الطابع الشخصي مجمعة لغايات محددة وواضحة، لذلك فإنه يعد تهديدا للحياة

[1] هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، الطبعة الأولى، القاهرة، 1992، ص568.

[2] محمد سامي الشوا، الثورة المعلوماتية وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص74.

[3] Cour de cassation chambre criminel du 14mars 2006 N° de pourvoi : 05-83423 "alors que, d'autre part, en imposant, pour qu'une collecte de données nominative ne soit pas illicite, le consentement nécessaire de chaque personne concernée par les informations collectées, disponible sur www.legifrance.gouv.fr visite le 02/05/2020

[4] جبالي أيو هشيمة كامل، حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، المنعقد بكلية الحقوق، جامعة أسيوط الفترة من 12-13 أفريل 2016، ص4.

[5] منى الأشقر جبور، محمود جبور، مرجع سابق، ص124.

الخاصة للأفراد إذا ما تم استخدام المعطيات الشخصية التي جمعت في بنوك المعلومات عن الأشخاص في غير ما يلائم صاحبها، أو استخدامها في غير الغرض المخصص لها والذي جمعت من أجله، وتطبيقا لذلك فقد رفضت اللجنة الوطنية الفرنسية للمعلوماتية والحريات (CNIL) في مداولتها المنعقدة في 08 مارس 2007 طلب الشركة المسماة «experian westren europe» بشأن إنشاء معالجة للبيانات الشخصية خاصة بالحسابات البنكية، مما دفع الشركة للطعن أمام مجلس الدولة لإلغاء هذا القرار، حيث قضى هذا الأخير في حكمه الصادر في 30 ديسمبر 2009 بأن اللجنة الوطنية للمعلوماتية والحريات لم ترتكب خطأ في رفضها إنشاء هذه المعالجة للبيانات الشخصية ولم تخالف أحكام المادة 06 من القانون الصادر في 06 جانفي 1978، لكون هذه المعالجة تسمح باستغلال المعطيات الشخصية تجاريا فيما بعد، وهي بذلك تخالف الغرض من إنشائها، الذي نصت عليه المادة السادسة من القانون.[1]

ثانيا: المخاطر التي تهدد المعطيات الشخصية خلال عملية التخزين

إن عملية تخزين المعطيات الشخصية في ذاكرة الكومبيوتر يعني الإحتفاظ بها لمدة غير معلومة داخل ملفات إلكترونية (fichier)، ويقصد بالتخزين الرقمي حفظ المعلومات بطرق رقمية مستخدمة في ذاكرة الحاسوب مع إمكانية استرجاع المعلومات المخزنة بها بصورة عشوائية أو متتالية في أي وقت، كما يمكن مشاركتها، ويسهل تأمينها وعمل نسخ احتياطية لاستخدامها وقت الحاجة، والغرض من التخزين الرقمي للمعطيات هو جعل هذه المعطيات مخزنة في صورة تستطيع أجهزة الحاسوب بأنواعها المختلفة قراءتها والتعامل معها[2]، فسعة ذاكرات الحاسبات الآلية غير المحدود، وتزايد حجم تخزين الوسائط و الأوعية الإلكترونية للمعلومات مع صغر و تضاؤل حجمها الخارجي، كان مدعاة لإنشاء بنوك أو مراكز وطنية للمعلومات تخزن فيها الدولة ملفات تحتوي على أكبر قدر ممكن من المعلومات الشاملة والمفصلة عن ملايين من الأشخاص، والإحتفاظ بها الى الأبد، واستخراج بيانات كافية عن أي شخص من المسجلين بها، ومن ثم تعرية حياته الخاصة بكشف تفاصيل سابقة على زمن استخراجها بزمن طويل، قد لا يرغب في كشفها عنه، مما قد يسبب له أضرارا يصعب إصلاحها وتداركها،[3] ومن ثم فان قيام نظام المعالجة بتخزين المعطيات الشخصية يعتبر المدخل الرئيس لتعرف الغير عليها وإمكانية إفشائها، ومن ثم جعل الحياة الخاصة للفرد عالما شفافا تظهر فيه أدق الأسرار المتعلقة بالحياة الشخصية والعائلية والمعاملات المالية والآراء والمعتقدات السياسية، والوضعية الصحية والممارسات الدينية وكل ما يمكن أن يشكل معلومة شخصية عن الفرد، نظرا لإمكانية الوصول إلى المعطيات المخزنة إما بطريق الصدفة أو بطريق التحايل عن طريق الإتصال الإلكتروني بنظام المعلومات ذاته.[4]

---

[1] شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لحق الاطلاع على البيانات الشخصية دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، المنصورة، الطبعة الأولى 2015، ص50.

[2] ربيع محمد الصغير، مرجع سابق، ص65.

[3] محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية، جرائم الكومبيوتر والانترنت، منشاة المعارف الإسكندرية 2006، ص185.

[4] بولين أيوب، مرجع سابق، ص129.

فالمعطيات الشخصية للفرد تصبح في بنوك المعلومات بعد تجميعها وتخزينها متوافرة وسهلة المنال ومتاح أكثر من ذي قبل الإ طلاع عليها واستخدامها في أغراض الرقابة على الأفراد، بعد أن كانت فيما قبل تخزينها منعزلة ومتفرقة، ويصعب التوصل إليها أو يستحيل التوصل إليها،[1] وهو ما يجعل من الحق في السرية والحق في النسيان دون مغزىإذا كان لا يمكن لما يـ ء ختزن في ذاكرة الكومبيوتر أن ينمحي أو ينسى، فأجهزة الكومبيوتر تتمتع بقدرة فائقة على تخزين وحفظ قدر كبير من البيانات الشخصية لعدد كبير من الأفراد، الأمر الذي يجعل الحصول على هذه البيانات واسترجاعها أمرا يسيرا، بعد أن كان من الصعب الحصول على معلومات كاملة عن الشخص بالسهولة التي توفرها أجهزة الكومبيوتر، وهي مسألة فيها خطورة وتهديد لحق الأفراد في حماية خصوصياتهم من خطر العلانية، والفرق واضح بين مرحلة كانت فيها البيانات الشخصية للأفراد تدرج في ملفات ورقية محدودة العدد وموزعة في أماكن متعددة، وبين مرحلة ظهرت فيها الحاسبات الآلية و أصبحت تستخدم في إنشاء قواعد البيانات الشخصية، يجمع ويخزن فيها كميات ضخمة من هذه البيانات، مما أدى ذلك إلى القضاء على مسألة تفرق البيانات الشخصية وتشتتها، و هذا التشتت الذي كان في حد ذاته ضمانة للحق في الخصوصية[2].

ولعل من أكثر معالم الخطر الذي يتهدد المعطيات الشخصية المخزنة في بنوك المعلومات في شكل ملفات الكترونية، ما يمكن أن تحويه هذه الأخيرة من معطيات غير دقيقة أو غير كاملة ولم يجر تعديلها بما يكفل إكمالها أو تصويبها، ويستدل في هذا الشأن بما توصل إليه الدكتور "لوردن" وهو عالم في مجال الجريمة والكيـ لف من طرف مكتب تقييم التقنية (OTA) بإجراء دراسة عن قيمة بيانات التاريخ الإجرامي التي تحويها ملفات الشرطة الفيدرالية (FBI) وكذا ملفات شرطة نيويورك، فوجد أن نسبة عالية من البيانات المخزنة في هذه الملفات غير كاملة وغير دقيقة، وفي هذه النقطة بالذات أظهرت دراسات أن الكثير ممن فقدوا مناصب شغل أو لم يوظفوا من طرف أصحاب العمل كان بسبب سجلاتهم الإجرامية غير الدقيقة[3]، وفي فرنسا يمكن الاستدلال بالحادثة المتعلقة بأحد الأشخاص الذي فصل من عمله، وجوبهت كل طلباته في البحث عن عمل آخر بالرفض، مكتشفا بعدها أن كل المؤسسات التي راسلها رفضت تشغيله لأنها كانت مطلعة على بطاقات شخصية تخصه، كانت قد أعدتها شركتان تجاريتان يتمثل نشاطها في جمع المعطيات ذات الطابع الشخصي وتحتوي على معلومات سيئة بخصوصه[4].

وترتيبا على ذلك يظهر جليا أن خطورة عملية تخزين المعطيات الشخصية للفرد بأجهزة الكومبيوتر في إطار بنوك المعلومات لا تقتصر على ما يمكن أن تحتويه هذه الأخيرة من معطيات صحيحة، بل يظهر أيضا في حالة الخطأ أو التحوير في البيانات التي تسجل عن الشخص، مما قد يعطي صورة غير حقيقية عنه[5]، كما تتيح عملية تخزين البيانات الشخصية وتسهل لمن له مصلحة أن يقوم بتزويرها، من خلال وضع

[1] محد عبد الله أبو بكر سلامة، مرجع نفسه، ص185.

[2] حسام الدين كامل الأهواني، مرجع سابق، ص11.

[3] بولين أيوب، مرجع سابق، ص115، نقلا عن:

Vbrich sieber. The international emergence of criminal information law, cologne heymans. 1992 p85

[4] عبد المجيد كوزي، مرجع سابق، ص 64.

[5] حسام الدين كامل الأهواني، مرجع نفسه، ص12.

معلومات بديلة عن المعلومات الحقيقية المخزنة، وكثيرا ما تقع هذه الجريمة على البيانات الممثلة للمستحقات المالية والإيداعات والودائع المصرفية[1].

ثالثا: المخاطر التي تهدد المعطيات الشخصية خلال عملية المعالجة

يقصد بعملية معالجة المعطيات الشخصية هو إجراء مجموعة من العمليات بواسطة وحدة التشغيل المركزية (المعروفة بوحدة المعالجة المركزية) آليا بهدف استغلال المعطيات التي تم تغذية الكومبيوتر بها، وهي على الأخص عمليات الربط والتقريب ودمج معطيات مع أخرى وتحليلها للحصول في النهاية على معلومات ذات دلالة خاصة.

وتعتبر عملية معالجة البيانات مهمة دقيقة وصعبة، وهي تتم في بيئة تقنية متحولة وسريعة التطور، لذلك نجد أن النصوص القانونية التي تقر الحماية للبيانات الشخصية لا تتوقف المسألة عندها فقط في تحديد البيانات المعرفة للشخص، بل أيضا في تحديد عملية المعالجة، خاصة وأن المسألتان مرتبطتان ارتباطا عضويا، وغالبا ما يمكن التعرف على عملية المعالجة المرافقة للبيانات من خلال تحديد هذه الأخيرة والعكس صحيح، فالعودة إلى مسار المعالجة يمكن أن يكشف البيانات التي تم جمعها وحفظها.[2]

فالقدرة الفائقة التي تتمتع بها الحواسيب الآلية على تنظيم وترتيب وتحليل البيانات الشخصية يمكن من ترجمة حياة الفرد في ثواني محدودة[3] من خلال مزج البيانات المتعلقة بالشخص وتحليلها، بحيث تعطي في النهاية صورة كاملة عن الشخصية وجوانبها المختلفة للفرد المعني بالمعالجة، خاصة عند ربط الحاسبات بعضها ببعض، حيث يتسنى تبادل المعلومات فيما بين المراكز المعلوماتية المتباعدة مكانيا و المختلفة من حيث أغراض تخزين البيانات بها، و ربط هذه المعلومات ببعضها البعض و استكمالها وتحليلها ومعالجتها على نحو يتيح التوصل إلى معلومات جديدة عن الشخص[4].

ومكمن الخطورة على المعطيات الشخصية خلال هذه العملية التقنية، يتمثل في إمكانية إعطاء صورة كاملة عن شخصية الفرد محل المعالجة من خلال دمج وتحليل معطيات متعلقة به، فتجعل من خصوصيته في مختلف جوانبها كتابا مفتوحا، وهو ما يؤدي إلى انتهاك حريتها، وتزداد الخطورة واحتمال وقوع التهديد على الخصوصية في حالة قيام نظم المعلومات بمهمة التشغيل عندما يكون الهدف من معالجة المعطيات الشخصية الوصول إلى الحكم على الشخص أو تقييم شخصيته من خلال المعطيات التي سبق تجميعها وتخزينها، وذلك باللجوء إلى عملية دمج البيانات المتفرقة والموجودة سواء في قاعدة بيانات واحدة أو موجودة بقواعد بيانات مختلفة مترابطة في ما بينها شبكيا، وهنا نكون أمام احتمال عدم

[1] بولين أيوب، مرجع نفسه، ص130.

[2] منىالاشقر جبور، محمود جبور، مرجع سابق، ص 74.

[3] أسامة عبد الله قايد، مرجع سابق، ص57.

[4] محمد عبد الله ابوبكر سلامة، مرجع سابق، ص 186.

دقة النتائج والأحكام المتوصل إليها في تقييم شخصية الفرد سواء من حيث سلوكه أو صفاته أو سمعته، وهو الأمر الذي من شأنه المساس بشرفه واعتباره.[1]

وفي هذا السياق ذاته نصت المادة 11 من القانون 07/18 أنه لا يمكن أن تؤسس الأحكام القضائية التي تقتضي تقييما لسلوك الشخص على المعالجة الآلية للمعطيات ذات الطابع الشخصي، والمتضمنة تقييما لبعض جوانب شخصيته، وذلك راجع لاحتمالية أن يكون التحليل قد انصب على معطيات غير صحيحة وغير دقيقة، فالنتائج والأحكام التي يمكن الوصول إليها عن عملية دمج وتحليل بيانات غير صحيحة تكون حتما هي أيضا غير صحيحة،[2] و هذا ما أكدته ذات المادة في فقرتها الثانية أنه لا يمكن لأي قرار آخر من شأنه أن ينشئ آثارا قانونية تجاه الشخص كأن يرتب عليه التزاما قانونيا مثلا، أن يتخذ فقط بناءا على المعالجة التي يكون الغرض منها تحديد صفات الشخص المعني أو تقييم بعض جوانب شخصيته.

وأساس ذلك أن أي معالجة لبيانات شخصية من أجل استخلاص حكم أو تقييم لشخصية فرد ما، من واقع ما غذي به الحاسوب الآلي من معطيات ومحاولة الوصول إلى نتائج انطلاقا من البيانات المتفرقة دون دراسة شخصية ذلك الفرد محل التقويم، يهدد باستخلاص نتائج غير دقيقة سواء من حيث سلوكه أو صفاته أو سمعته، مما قد يؤدي إلى تلويث شخصيته.[3]

ومن هذا المنطق يجب أن يزول من الأذهان التسليم المطلق بالنتائج والمعلومات التي يقدمها الكومبيوتر، فكثيرا ما تحمل معها تقييما غير صحيح عن الشخص إذا ما استند إلى معطيات غير دقيقة وغير صحيحة، لذلك نجد أن المشرع أوجب أن تكون المعطيات التي يتم تجميعها صحيحة وكاملة وإذا اقتضى الأمر محينة.*

ولقد أكد الفقه الفرنسي على أنه من بين الأخطار الناشئة عن استخدام الحواسيب كبنوك معلومات ما يعرف بالأخطاء التقنية والبشرية، فأما الأخطاء التقنية هي التي قد تحدث من جهاز الحاسب الآلي ذاته، والتي يكون مرجعها إلى عيب فني في الجهاز، قد يترتب عليه دمج بيانات مختلفة قد لا ترتبط بنفس الشخص، أو اختلال في تصنيفها أو تنظيمها أو محوها، مما ينتج عنه نسبة معلومات معينة لأشخاص لا تتعلق بهم، وتعطي صورة غير حقيقية عن حالتهم سواء الإ جتماعية أو وضعهم من الناحية المالية أو السياسية أو المهنية أو الصحية، والخطأ البشري هو الذي يقع عادة من الأشخاص القائمين بعمليات ترتيب وتصنيف وتوزيع البيانات الشخصية، فقد يحدث خطأ في مرحلة ما قد يؤدي إلى دمج بيانات مختلفة لأشخاص مختلفين، ومن ثم الحصول على معلومات غير صحيحة عن كل منهم، سيما وأن

---

[1] نعيم عطية، حق الأفراد في حياتهم الخاصة، مجلة إدارة قضايا الحكومة، العدد الرابع، السنة 21، أكتوبر، ديسمبر 1977 ص87.

[2] بولين أيوب، مرجع سابق ص 133.

[3] حسام الدين كامل الأهواني، مرجع سابق، ص15.

* تنص المادة 9 من القانون 07/18 " يجب أن تكون المعطيات الشخصية صحيحة وكاملة ومحينة إذا اقتضى الأمر"

تنص المادة 3 من القانون المغربي 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي:" يجب أن تكون المعطيات ذات الطابع الشخصي".

د- صحيحة وعند الإقتضاء محينة ويجب اتخاذ كل التدابير المعقولة حتى يتم مسح أو تصحيح المعطيات الخاطئة أو غير المكتملة بالنظر إلى الغايات التي تم تجميعها أو معالجتها لاحقا من أجلها".

أصحاب هذه البيانات في أغلب الأحيان لا يكونون حاضرين في وقت إجراء هذه العمليات والتأكد من صحة هذه البيانات.[1]

رابعا: المخاطر التي تهدد الخصوصية المعلوماتية عند عملية إيصال المعلومات

تعتبر عملية إيصال المعلومات هي هدف أي نظام معلوماتي، إذ لا قيمة للمعلومات المتحصل عليها من عمليات جمع وتشغيل المعطيات إن لم تصل إلى علم المستخدم أيا كان هذا الأخير، سواء هيئة حكومية أو غير حكومية، حتى يتمكن من اتخاذ القرارات المناسبة وفي الوقت المناسب، بناءا على هذه المعلومات[2] .

وقد اعتبر الشرع الجزائري عملية الإيصال بأنها كل كشف أو إعلام بمعطيات لشخص غير الشخص المعني، وهو إما شخص طبيعي أو معنوي أو السلطة العمومية أو مصلحة أو أي كيان آخر يتلقى معطيات ذات طابع شخصه [3]

كما اعتبر المشرع أن الإيصال يكون عن طريق الإرسال أو النشر أو أي شكل من أشكال الإتاحة أو التقريب أو الربط البيني[4]، وتعدد الوسائل التي يمكن من خلالها نقل وإيصال المعلومات يترتب عليه سهولة إتاحتها وإيصالها في ثوان معدودة إلى أماكن مختلفة، مما يساعد على الإنتشار الرهيب لهذه المعلومات[5].

ومن هنا يتجلى بوضوح أن انتقال البيانات أو إيصالها أو تبادلها يشكل الحركة الأهم التي تتسم بها المعلومات في الفضاء المعلوماتي، حينما تنتقل إلى المستخدم عبر الشبكات أو التطبيقات les applications أو قواعد المعلومات (les bases de données) وغير ذلك من الأجهزة والبرامج التي تعالج فيها المعطيات لتتحول إلى معلومات، لتتم عملية نقلها أو توزيعها أو أية عملية أخرى من عمليات المعالجة، والتي تمكن في النهاية من الإطلاع عليها.

وتختلف درجة خطورة هذه العملية على الخصوصية المعلوماتية بحسب ما إذا كان نقلها أو إيصالها أو تبادلها يتم داخل الدولة الواحدة أو بين عدة دول.

1) مخاطر إيصال أو تبادل البيانات الشخصية داخل الدولة الواحدة: إن عملية تبادل المعلومات الشخصية الخاصة بالأفراد التابعين للدولة بين مختلف قواعد البيانات تحقق نوعا من التكامل والتناغم بين الخدمات التي تقدمها الجهات الحكومية، وكذا الإستفادة المثلى من المعطيات المتوفرة لدى مختلف قواعد البيانات للإدارات والمؤسسات العمومية، هذا بالإضافة إلى تعزيز الشفافية وإرساء قواعد الحكومة بشأن نشر وتبادل المعلومات وزيادة كفاءة الخدمات التي تقدمها الجهات الحكومية[6]، لكن الأمر ليس دائما

[1] أسامة عبد الله قايد، مرجع سابق، ص61.

[2] بولين أيوب، مرجع سابق ص133.

[3] عرف الشرع المرسل إليه في المادة 3 من القانون 07/18: " يقصد لأغراض هذا القانون".

" المرسل إليه ": الشخص الطبيعي أو المعنوي أو السلطة العمومية أو المصلحة أو أي كيان يتلقى معطيات ذات طابع شخصي".

[4] عرف المشرع الربط البيني في المادة 03 من القانون 07/18 على أنه أي شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة لغاية محددة مع معطيات أخرى يمسكها مسؤول أو مسؤولون عن المعالجة لنفس الغرض أو لأغراض مختلفة.

[5] حسام الدين الأهواني، مرجع سابق، ص11.

[6] منى جبور الأشقر، محمود جبور، مرجع سابق، ص36 بتصرف.

بهذا الوجه المشرق، حيث أن تبادل هذه المعطيات بين بنوك أو قواعد المعطيات المختلفة يؤدي إلى أن يشكل ذلك كشفا كاملا لخصوصية المعني بالمعالجة.

وقد زادت خطورة هذه العملية بعد ظهور شركات خاصة تعمل في مجال الأمن، تقوم بتجميع بيانات شخصية عن الأفراد لتضعها بعد ذلك تحت تصرف من يريد أن يعرفها مقابل دفع مبالغ مالية،[1] ومن ثم يكون نقل وإيصال البيانات الشخصية إلى جهات أخرى غير التي قبل المعني بالمعالجة مسبقا تقديم معطياته الشخصية لها مصدرا آخر يهدد الحياة الخاصة، سواء للفرد العادي أو للشخصيات العامة، وسواء كانت هذه المعلومات كاذبة أو صحيحة طالما أن صاحب هذه المعطيات سوف يعترض على من يقوم بتزويد الآخرين بمعلوماته الشخصية دون مبرر قانوني مقبول.

2) **مخاطر تبادل المعلومات بين دولتين أو أكثر**: يشكل انتقال أو إيصال المعطيات الشخصية خارج الحدود الوطنية البعد العالمي لعملية معالجة المعطيات الشخصية، ويعتبر هذا الإنتقال من الناحية القانونية إخراج لها من نطاق تطبيق القانون المحلي ومن دائرة اختصاص القضاء الوطني.

ولقد نصت اتفاقيات عديدة بين الدول على هذا البعد من خلال مصطلح نقل البيانات خارج الحدود أو الحركة الحرة للبيانات، أو التدفق الحر للبيانات، مثل الإتفاقيات المبرمة بين الولايات المتحدة الأمريكية والإتحاد الأوروبي، ومنها اتفاقية " بروم " بألمانيا الموقعة بتاريخ 27 ماي 2005، وهي اتفاق تعاون دولي يسمح للدول الموقعة بتبادل المعلومات حول ملفات تعريف الحمض النووي وبصمات الأصابع، أو البيانات الخاصة بالمركبات وأصحابها، بالإضافة إلى اتفاقية "درع الخصوصية" بين الإتحاد الأوروبي والولايات المتحدة الأمريكية، والمتعلقة بحماية تدفق البيانات عبر الأطلسي، وينظم نقل البيانات الشخصية من أوروبا إلى الشركات الأمريكية لأغراض تجارية، ويوفر وضوحا قانونيا للشركات التجارية التي تعتمد على نقل البيانات بين الجانبين.[2]

وبين دول الإتحاد الأوروبي فقد أعطيت هذه العملية اهتماما أساسيا في قوانين حماية المعطيات الشخصية الأوروبية، فالمادة الأولى من الإرشاد الأوروبي رقم 95/46 المتعلق بحماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حظرت على الدول الأعضاء في الإتحاد الأوروبي منع التدفق الحر للبيانات الشخصية أو الحد منه[3]، ونفس الشيء نجده في الفصل الخامس من الإرشاد الأوروبي الجديد لسنة 2018 المتعلق بحماية المعطيات ذات الطابع الشخصي الذي حمل عنوان " نقل البيانات إلى دولة ثالثة (أو) منظمات دولية، حيث تضمن هذا الفصل مواد ، ا أبرزت عددا من الشروط التي

[1] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكومبيوتر والأنترنات وجرائم الإحتيال المنظم باستعمال شبكة الأنترنات، دار الفكر والقانون، المنصورة مصر 2017، ص 103.

[2] مأخوذ من تقرير المفوضية الأوروبية في بروكسل بشأن المراجعة السنوية الثانية لأداء كل من الإتحاد الأوروبي والولايات المتحدة الأمريكية بشأن اتفاق درع المفوضية، منشور في جريدة الشرق الأوسط، العدد رقم 14633 بتاريخ 21 ديسمبر 2018، ص02.

[3] تنص المادة الأولى: من الإرشاد الأوروبي 95/46 على أنه " تضمن الدول الأعضاء وفقا لهذا التوجيه حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين ولا سيما حياتهم الخاصة فيما يتعلق بمعالجة المعطيات ذات الطابع الشخصي، ولا يجوز للأعضاء تقييد أو حظر حرية حركة البيانات الشخصية بين الأعضاء ... »

تحكم عملية نقل البيانات، أهمها أن هذه العملية لا تحتاج إلى إذن خاص عندما تتوافر الأطر القانونية المناسبة لحماية البيانات الشخصية في البلد المعني بتلقي هذه البيانات.[1]

وتطبيقا لذلك فإنه توجد أنظمة لتبادل المعلومات الشخصية التي تم إنشاؤها على مستوى الإتحاد الأوروبي مثل نظام المعلومات شنغن ((le système d'information Schengen (SIS)، نظام المعلومات الجمركية، أنظمة المعلومات Europolو.Eurojust

ويشكل تبادل المعلومات الشخصية أو نقلها على الصعيد الدولي مخاطر أكبر حدة من حالة تبادلها أو نقلها داخل نفس الدولة، فأهم هذه المخاطر هو الاستعمال غير المشروع للمعطيات الشخصية من خلال استعمالها في غير الأغراض التي جمعت لأجلها، أي في غير الهدف الأساسي الذي تم تبادلها من أجله، وهو حتما انحراف خطير سوف يعرض سرية المعطيات الشخصية للخطر، لأن الغرض الآخر الذي سوف تستغل فيه هذه المعطيات يكون دون علم الشخص المعني، بل قد تستعمل ضده[2]، وتزداد حدة المشكلة عندما يتم نقل المعلومات الشخصية إلى دولة لا تتوفر على مستوى كاف من الحماية للمعطيات الشخصية، مما يعني ضرورة الإهتمام في عملية التبادل للمعلومات الشخصية والأخذ بعين الإعتبار الوضع القانوني لمسألة حماية الخصوصية المعلوماتية في الدولة التي تنتقل إليها المعلومات الشخصية.[3]

وقد راعى المشرع الجزائري هذه المسألة في القانون 07/18 عندما ألزم الأشخاص الطبيعية أو المعنوية الخاصة أو العامة التي تقوم بمعالجة المعطيات الشخصية عدم نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية، إلا إذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية إزاء المعالجة التي تخضع لها هذه المعطيات.[4]

كما تثير عملية نقل وتبادل المعطيات الشخصية مشكلة إمكانية اعتراض والتقاط هذه المعلومات أثناء عملية التبادل، مما يعرض مبدأ السلامة المفترض للخطر.[5]

المطلب الثاني: مخاطر الأنترنت على الخصوصية المعلوماتية

إن الأنترنت *هي وسيلة اتصالات جديدة، تسمح لكل مستخدم نشر ما يشاء، والتدخل فيما يريد من مواضيع و أنشطة مختلفة، فالمستخدمون يمكنهم إنشاء اتصالات مع جهات عديدة بغض النظر عن

[1] Voir le règlement (CE) 2016/679 du parlement europeén et du conseil du 27 avril 2016. Relatif a la protection des personnes physiques a l'égard du traitement des données a caractères personnels et la libre circulation de ces données et abrogeant la directive 95/46/CE

Chapitre V : transferts de données à caractère personnel ver des pays tiers ou a des organisation internationales les articles 44 à 50.

[2] بولين أيوب، مرجع سابق، ص 137.

[3] بولين انطونيوس أيوب، تحديات شبكة الأنترنت على صعيد القانون الدولي الخاص، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت 2006، ص40. وما بعدها.

[4] انظر المادة 44 من القانون 07/18.

[5] بولين أيوب، تحديات شبكة الانترنت ...مرجع نفسه، ص 40.

* الأنترنت هي اختصار لـ international net work عرفت تقنية الأنترنت بالعديد من التسميات فقد سميت الشبكة العنكبوتية الالكترونية، أو الفضاء السيبراني الإلكتروني والأكيد أن مصطلح الأنترنت هو مختصر لتعبير international net work والتي تعني الشبكة البينية وهو إسم يدل

الحدود الجغرافية وعن المعيقات الإ جتماعية والسياسية، وهي واسطة غير متناهية في القدرة والحجم وأقل كلفة بالنسبة لإيصال الخدمات الحكومية والإ جتماعية والمعرفية في شتى مجالات النشاط الإنساني، فهي تعد من أهم إنجازات التقدم التقني في مجال الإتصالات وتقنية المعلومات، فمن الرسائل المحمولة يدويا، إلى المنقولة هاتفيا، إلى المعلومة المبثوثة عبر الأجهزة المسموعة والمرئية، ثم إلى شبكة الانترنت التي أحدثت ثورة عالمية لم يسبق لها مثيل في مفاهيم الإتصال الشخصي وتبادل المعلومات[1].

الفرع الأول: مفهوم الانترنت

تتمتع الأنترنت بالقدرة العلمية على إنشاء ومعالجة وتخزين ونقل وتوصيل المعلومات الرقمية، وبذلك تعد من أكثر الإ بتكارات أثرا في الحياة البشرية، فهي تتيح للأشخاص على اختلاف ألوانهم وأعمارهم وعقائدهم وأفكارهم، فرصة تبادل الأفكار والمعلومات دون التقيد بحدود الزمان والمكان، وبذلك تعتبر الانترنت من وسائل التقنية التي غيرت رؤية الإنسان بإيجاد نوع من الديمقراطية الإتصالية التي ليس لها محدد يتحكم فيه شخص معين.

فالأنترنت بهذا الوصف تعد شبكة دولية تربط آلاف الشبكات والملايين من أجهزة الكومبيوتر بعضها ببعض عبر العالم، لذلك يعتمد العديد من الأشخاص والمؤسسات على استخدامها لتبادل الرسائل والمعلومات،[2]ومن ثم فهي تقنية ترابطية تعاونية، لا يستطيع شخص أو منظمة حكومية أو غير حكومية أن تدعي ملكيتها أو سيطرتها عليها، وتساعد العديد من المنظمات والمؤسسات بمواردها الحاسوبية في صيانة أجزاء عديدة منها وتحديثها كلما تطلب الأمر ذلك،[*] كما أن رواد صناعة تكنولوجيا المعلومات يمارسون تأثيرهم على الأنترنت من خلال وضع معايير يجب أن تتوافق معها مختلف المعدات والبرمجيات المرتبطة بها.[3]

على بينية شبكة الأنترنت باعتبارها شبكة ما بين الشبكات ولذلك فمن الخطأ القول أن مقطع Inter هو مختصر ل Internationalوالتي تعني دولي، ومن ثم فانه يصبح التعبير عن الانترنت بالشبكة الدولية للمعلومات قول غير صحيح.

[1] حسين فاروق، الانترنت، الشبكة الدولية للمعلومات، دار الراتب الجامعية، بيروت، 1995.ص112.

[2] عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية (شبكة الانترنت، وشبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات)، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن2011، ص53.

[*] من بين المنظمات التي تلعب أدوارا مؤثرة في عملية تطوير الانترنت:

1/ منظمة هندسة الانترنت (IETF) وهو مجتمع دولي مفتوح يضم مصممي الشبكات عبر العالم، وهو يركز على تطوير الانترنت ويقترح حلولا للمشاكل التقنية المتعلقة به.

2/ مجموعة توجيه هندسة الانترنت (IESG) وهي المجموعة التي توجه نشاطات المجموعة الأولى، وتراجع لها المعايير التي تقترحها.

3/ جمعية الشبكة العنكبوتية (W3C) وهي هيئة تعمل على تطوير مقاييس الشبكة المفتوحة، ومن تلك المقاييس مثلا: مقاييس لغة النصوص الفائقة (HTML).

4/ مجلس معمارية الانترنت (IAB) وهو مجموعة استشارية فنية تضع المقاييس المعمارية الكلية للانترنت ولعمودها الفقري.

5/ مجتمع الانترنت (ISOC) وهو مجموعة محترفين تتكون من العديد من الهيئات المستثمرة في نشاط الانترنت وهم أشخاص ووكالات حكومية ومؤسسات ومنشآت ومنظمات غير ربحية يقومون بالتأثير على سياسات الانترنت.

6/ مركز معلومات شبكة الانترنت (InterNIC) وهو منظمة مسؤولة عن حجز أسماء المجالات.

7/ الاتحاد الدولي للاتصالات (ITU) والذي يشرف على منظمات الاتصالات العالمية.

[3] عادل عزام سقف الحيط، مرجع سابق ص 55.

أولا: تعريف الانترنت: لقد تعددت المحاولات الفقهية لتعريف الأنترنت ومن بين أهم هذه التعاريف أنها " عبارة عن آلية اتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للبيانات، ودواعم توصيل وروابط اتصال تعمل في بوتقة واحدة بفضل بروتوكول الأنترنت (TCP/IP)[1]

كما عرفها البعض أيضا بأنها "مجموعة ضخمة من شبكات الكومبيوتر، التي تربط ملايين من أجهزة الكومبيوتر، ويتصل بها الملايين من الأشخاص حول العالم وتحتوي على معلومات لا حصر لها في شتى المجالات".[2]

وعرفها أيضا مجلس الشبكات الفدرالي الأمريكي في القرار الذي أصدره في 1995/10/24 ،حين اعتبر نترنت أنها مصطلح يشير إلى النظام المعلوماتي الدولي والذي يرتبط منطقيا ببعضه بعنوان فضائي وحيد عالمي مؤسس على الانترنت ببروتوكول الأنترنت (Internet Protocol (IP ، أو امتداده اللاحق له، وأن هذا النظام المعلوماتي قادر على دعم الإتصالات باستخدام بروتوكول التحكم في الإرسال (TCP) ، Transmission control Protocol أو أي بروتوكول لأترنت متوافق يزود الإ ستعمال سواء بشكل عام أو خاص بالخدمات ذات المستوى العالي من طبقات الإتصالات والبنية التحتية ذات العلاقة بهذا الوصف".*

هذا وقد عرف التقرير التفسيريRapport explicatif للاتفاقية الأوروبية للجريمة الإلكترونية رقم 185 المنعقدة ببودابست في 23 نوفمبر 2001 في المادة الأولى منه الأنترنت بأنها شبكة عالمية تتكون من العديد من الشبكات المترابطة تستخدم جميعها نفس البروتوكولات.[3]

ولا بد من الإشارة في هذا الإطار أن شبكة الأنترنت ليست هي شبكة المعلومات الدولية والتي تعرف بالواب (WWW)*، وذلك أن الأنترنت هي أعم من شبكة الواب بل هذه الأخيرة هي أحد تطبيقاتها فقط أو إحدى الآليات التي تستعمل في الإتصال، كالبريد الالكتروني (Email) و الماسنجر (Messenger) ولكنها ليست نترنت، وإن اتسع نطاق استخدامها فإنها تضل أحد أقسام الأنترنت، هذه الأخيرة يقوم المستخدمون بواسطتها بالعديد من الأنشطة المدنية والتجارية مثل القيام بالإضافة إلى تصفح مواقع الواب، إرسال رسائل عن طريق البريد الالكتروني واستقبالها، الإنضمام إلى شبكة مجموعات الأخبار، الدردشة مع

---

[1] محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الأنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011.ص22. نقلا عن إيهاب السنباطي، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة 2007.ص78.

[2] مصطفى السيد، دليلك الشامل إلى شبكة الانترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة 1997.ص11.

* هذا التعريف متوفر على موقع: WWW.FNC.gov/internet

FNCهو اختصار ل : Fédéral net working Council(مجلس الشبكات الفيدرالي).

[3] تم اعتماد الاتفاقية وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتهما التاسعة بعد المئة في 08 نوفمبر 2001 وفتح باب التوقيع على الاتفاقية في بودابست في 23 نوفمبر بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.

* شبكة المعلومات الدولية هي حسب مخترعها " Tim Berners lée«مبادرة لنقل المعلومات عبر وسائل الكترونية على نطاق واسع بهدف اتاحة الفرصة للحصول على وثائق ومستندات عالمية في جميع أنحاء العالم". ويتمركز هذا النظام على بروتوكول (HTTP) أي بروتوكول نقل النصوص الترابطية. HYPERTEXT TRANSFER PROTOCOLوالذي يسمح بربط مواقع الواب الموصولة بالشبكة فيما بينها والتجول فيها، وهو لا يعمل إلا بواسطة برامج تصفح خاصة ويرمز لها WWW وتعني اختصار ل World wide web ويسبق هذا الاختصار عناوين الواقع على شبكة الويب ويشير إلى مجموعة من الخوادم (أنظمة الحاسوب الخادمة) المتصلة بالانترنت التي توفر صفحات من المعلومات.أنظر في هذا الإطار طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، منشورات صادر الحقوقية، الطبعة الأولى، بيروت 2001 ص48.

الأصدقاء الافتراضيين chatting ، تحميل الصور والأفلام والملفات والقواميس الإلكترونية وغيرها، ولكل مستخدم في العالم الإفتراضي أن ينشىء موقعا إلكترونيا خاصا به، على الشبكة العالمية يضمنه معلومات يمكن إعادة تخزينها وتهيئتها ليتمكن من استقبال أي مستخدم آخر في جميع أنحاء العالم.[1]

ثانيا: خصـائص الأنترنت:

من خلال ما صاغه الفقه من تعاريف للأنترنت فإنه يمكن القول أنها تتميز بما يلي:

1) شبكة الأنترنت وسيلة تواصلية: تقدم الفلسفة التقنية للأنترنت على أنه إذا ما وجد عدد من أجهزة الكومبيوتر يكون بينها اتصال، فإن ذلك يخلق نظاما اتصاليا، وباتصال هذه الأنظمة الاتصالية ببعضها البعض فإنها تكون شبكة، وباتصال عدد من هذه الشبكات وفق بروتوكول (TCP/IP) وهو المسؤول عن تنظيم الإتصال بين أجهزة الحاسوب عبـ نترنت، وهنا نصل إلى نقطة اللامركزية في الإتصال[2].أي إمكانية التواصل بين جميع هذه الأجهزة فيما بينها.

2)القيمة الإسترجاعية أو الإسترادادية للمعلومات: إن هذه الخاصية هي منطقية لكون شبكة الأنترنت تستلزم المعلومات، وبدون النظام المعلوماتي التبادلي، تصبح الأنترنت بدون موضوع، ومن ثم تظهر المعلومات التي يتم تبادلها عبر هذه الشبكة القيمة القصوى لها، إذ ليست للتقنية قيمة في حد ذاتها دون المعلومة التي تكون دائما في حاجة ملحة للإنسان لكي يدخلها إلى الشبكة وتكون هدفا للاتصال بين المستخدمين،[3] وتعتمد شبكة الأنترنت في إيصالها للمعلومة إلى المستخدم على آلية التخاطب الرقمي، وذلك بواسطة بروتوكول التحكم في النقل TCP وبروتوكول الأنترنت IP وكلاهما يسمى في التطبيق بروتوكول مراسل الانترنت TCP/IP، حيث يقوم بروتوكول التحكم في النقل TCP بتجزئة الرسالة (المعلومة) المراد إرسالها إلى رزم من المعلومات، بحيث تحمل هذه الرزم معلومات تعريفية حول المرسل والمرسل إليه، أما بروتوكول IP فهو المسؤول عن عنونة وترقيم وتوجيه الرسائل إلى عناوينها المقصودة، وأي شبكة لا تستخدم هذين البروتوكولين لن تتمكن من الإتصال بالأنترنت.[4]

3) **شبكة الأنترنت عابرة للحدود الدولية:** ليس لشبكة الأنترنت حدود دولية ولا تعترف بتلك الحدود القائمة بين الدول، وهذه الخاصية ليس فيها تعارض مع فكرة الدولة والسيادة، لأن الأنترنت ظاهرة علمية دولية، وقد أخذ القضاء الأمريكي بهذه الميزة في تحديده لنطاق الأنترنت عندما صرحت المحكمة العليا للولايات المتحدة الأمريكية في20 جوان 1997 أن نطاق الأنترنت هو مكان خارج الحدود الإقليمية، ليس له نطاق جغرافي محدود، ولكنه متوافر لكل شخص في كل مكان حول العالم.[5]

---

[1] عادل سقف الحيط، مرجع سابق، ص57، وكذلك علي حسن الطوالبة، الجرائم الالكترونية دراسة مقارنة، محكم وفق الأصول الاكاديمية، مطبوعات جامعة العلوم التطبيقية مملكة البحرين، الطبعة الثانية 2008 ص35 وما بعدها.

[2] ربيع محمود الصغير، مرجع سابق، ص 47.

[3] ربيع محمود الصغير، مرجع نفسه، ص48.

[4] محمد طارق عبد الرؤوف الحن، مرجع سابق، ص 24.

[5] ربيع محمود الصغير، مرجع نفسه، ص60، نقلا عن الموقع Http://www.loundy.com .

4) فقدان المركزية وآليات السيطرة تتصف الأنترنت باللامركزية وغياب السلطة التحكمية وأن دعوات إنشاء حكومة الأنترنت، أو معايير الإستخدام الموحد، أو سياسات التنظيم الذاتي للالتزامات، إلا وسائل افتراضية شأنها في ذلك شان البيئة التي نشأت فيها،[1] لكن طريقة العمل غير المركزية التي اعتمدت لإدارة شؤون الأنترنت بدأ التغيير يطاولها، وهكذا قررت المؤسسة العلمية الوطنية التي كانت تدير البنية التحتية الأساسية للأنترنت التعاقد مع مؤسسة خاصة هي NET work solution internet لإدارة أسماء النطاقات، وقد أدى ذلك الى إثارة تحفظات نشأ عنها ما سمي بحرب أسماء النطاقات، انتهت بإنشاء هيئة إدارة أرقام وأسماء الأنترنت (ICANN)[2]، غير أن هذه الأخيرة كانت محل جدل ونقاش نظرا لعلاقتها مع وزارة التجارة الأمريكية، حيث كانت تمارس عليها نوعا من الرقابة وهو ما دعا بدولة الصين عام 2009، خلال منتدى حوكمة الأنترنت المنعقد في مصر إلى المطالبة بإدخال هذا المنتدى في نظام الأمم المتحدة من أجل إعطاء الحكومات دورا أكبر في السيطرة على الأنترنت، لكن الولايات المتحدة والدول المتقدمة تقنيا رفضت هذا المقترح[3]، إلا أن ذلك لم يمنع من التوصل في حينه إلى إنشاء فريق عمل خاص بحوكمة الأنترنت في عام 2004 وقد تألف هذا الفريق من مجموعة من الخبراء المستقلين ينتمون إلى أكثر من ثلاثين بلدا، وذلك بقرار من الأمين العام للأمم المتحدة، أسندت له مهمة مراجعة ما يمكن أن يندرج تحت عنوان حكومة نترنت، وقد قدم هذا الفريق تقريره سنة 2005 في القمة العالمية لمجتمع المعلومات مشيرا فيه إلى عدة مبادئ*، تحكم هذه المسألة لا بد من مراعاتها وهي:

- عدم استحواذ حكومة واحدة على دور غالب على المستوى العالمي.

- مراعاة التعددية اللغوية وأصول الشفافية والديمقراطية.

- مشاركة الحكومات والمنظمات الدولية والقطاع الخاص وهيئات المجتمع المدني في إقرار القواعد التي تحكم الأنترنت.

وهي مبادئ تصب في اتجاه المحافظة على سمات البيئة التفاعلية للأنترنت وملتقى للعالم الافتراضي غير المحدود، فلعل طبيعة الأنترنت والاتجاه نحو تطور طريق المعلومات السريع، يعطي انطباعا أن الأنترنت ستبقى خارج أمنيات الحكومات في إيجاد تنظيم قانوني يحكمها أو يسيطر على شؤونها[4] .

[1] بولين أيوب، تحديات شبكة الانترنت على صعيد القانون الدولي الخاص، مرجع سابق، ص65.

[2] منى الأشقر جبور، هاجس السيبرانية، مرجع سابق، ص15.

[3] منى الأشقر جبور، السيبرانية، هاجس العصر، نفس المرجع، ص15.

* تعتبر هذه المبادئ بمثابة رد على الخطر الذي استشعرته بعض الحكومات نتيجة العلاقة التعاقدية الخاصة التي تربط حكومة الولايات المتحدة الأمريكية بالأيكان CANNاوكذا نتيجة طغيان اللغة الانجليزية، ولعل التعبير الأوضح عن هذا الإحساس بالخطر ما نقلته أجواء القمة العالمية لمجتمع المعلومات التي انعقدت في تونس في نوفمبر2003 من وجهات نظر حول ضرورة إخضاع تنظيم أسماء النطاقات والعناوين على الأنترنت إلى هيئات أخرى غير ICANNبحيث لا تكون الولايات المتحدة الأمريكية صاحبة النفوذ الوحيد في هذا المجال.أنظر منى الأشقر، جبور هاجس السيبرانية، مرجع سابق، ص15 ومابعدها

[4] بولين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، مرجع سابق، ص209.

الفرع الثاني: مظاهر تهديد الخصوصية المعلوماتية في بيئة الأنترنت

لقد أصبحت شبكة الأنترنت والتي سهلت الكثير من أمور الحياة، وساعدت على تجاوز العديد من العقبات التي كانت في الماضي من ضروب المستحيل، من أخطر آليات التكنولوجيا المعاصرة تهديدا لحياة الإنسان في أخص شؤونها وأكثرها التصاقا به، ألا وهو الحق في خصوصية بياناته الشخصية[1]، فقد تشكل البرامج المتطورة التي أوجدتها الأنترنت في غالب الأحيان تهديدا لخصوصية المستخدم، من خلال تسجيل بياناته الخاصة بمجرد دخول هذا الأخير لأي موقع يزوره عبر شبكة الأنترنت، وتتحول بذلك إلى وسيلة تمثل كشفا عن بيانات قد لا يرغب الشخص في الكشف عنها[2]، فالأفراد عندما يستخدمون مواقع الانترنت، فإنهم يتوقعون قدرا من الخفية في نشاطهم أكثر ما يتوقعونه في العالم المادي الواقعي، لكن نترنت عبر نظم الخوادم ونظم إدارة الشبكات تجمع قدرا كبيرا من البيانات عنهم عند كل وقفة للشخص في فضاء شبكة نترنت.[3]

وقد بدأ الوصول إلى الأنترنت في الإتساع بشكل سريع عبر معظم دول العالم، وهذا ما تشير إليه الإحصاءات الواردة من الإتحاد الدولي للاتصالات السلكية واللاسلكية (ITU)[4]، إلى أنه بين العام 2005 و2010 تضاعف عدد المستخدمين للانترنت من 0.4 % من سكان العالم سنة 1995 إلى أن وصلت 30.2% بحلول شهر مارس 2011، وهو ما يعادل أكثر من ملياري مستخدم للأنترنت[5]، هذا الارتفاع في نسبة استخدام الأنترنت كان نتيجة لتعدد استخدامات هذه الشبكة وتنوعها، ومن ثم فإنه وللوقوف أكثر على مخطرها وتهديداتها لخصوصية الأفراد يستلز م الأمر شارة إلى أهم استخدامات الأنترنت وخدماتها.

أولا: أهـم استخدامات شبكة الانترنت:

هناك عدد كبير لاستخدامات شبكة الأنترنت في مختلف مجالات الحياة البشرية، وتتطور بتطور تقنيات هذه الشبكة، خاصة مع ظهور الإتصالات الرقمية التفاعلية غير المكلفة،ومن أهم هذه الإ ستخدامات نذكر منها ما يلي:*

---

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الإ ستخدام غير المشروع لشبكة الانترنت -دراسة مقارنة- دار النهضة العربية، الطبعة الثانية، القاهرة،2009 ص189.

[2] حسين الغافري، محمد الألفي، جرائم الانترنت بين بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة 2008. ص64.

[3] مروة زين العابدين، مرجع سابق، ص 316.

[4] ITU/ International télécommunication union

[5] توبي مندل، Toby Mendel)أندرو بوديفات، Andrew Puddephattبن واجنر، Ben Wagnerديكسي هوتن DixieHawtinونتاليا توريس. Natalia Torres ،دراسة استقصائية عالمية حول خصوصية الأنترنت وحرية التعبير، سلسلة اليونسكو بشأن حرية الانترنت ص12. متوفر على الموقع: https://www.noor-book.com/ أطلع عليه يوم:2020/04/14

* هناك استخدامات أخرى للانترنت يمكن ذكره أهمها:

-خدمة تصميم المواقع الإكترونية حيث يستطيع المستخدم إنشاء موقع خاص سواء كان فردا أو شخصا معنويا لتحقيق غرض معين في تخصص معين علمي، ثقافي، وتجاري...

-التعلم عن بعد: مثل جامعات التكوين والتعليم عن بعد، (في الجزائر الديوان الوطني للتعلم عن بعد)

-الحصول على الخدمات الطبية عن بعد إذ يمكن من خلال هذه الخدمة أن يتصل المريض بالأطباء المختصين ووصف الأعراض المرضية لهم، ومن ثم تلقي التشخيص ونوع العلاج المناسب.

- خدمة البريد الالكتروني:[1]**(** electronic mail/ email): يعرف بأنه إرسال واستقبال للرسائل الإلكترونية عن طريق شبكة الأنترنت، وقد أصبحت هذه الخدمة بديلة عن البريد التقليدي، ويرمز لها بـ Email وهي عبارة عن خط مفتوح يستطيع من خلاله المستخدم إرسال واستقبال عدد كبير من الرسائل للعديد من الأشخاص في أي مكان من العالم وفي ثوان معدودة وبتكلفة زهيدة، كما يمكن البريد الإلكتروني مستخدمه من الوصول إلى الملفات والبيانات والمواقع على الأنترنت التي لا يمكنه الوصول إليها واستخدامها عن طريق البريد العادي.[2]

- شبكة المعلومات الدولية the world wide web وهو نظام برمجي يعمل على شبكة الأنترنت، يتكون من مجموعة كبيرة من النصوص الفعالة المكونة من كم هائل من المستندات المتصلة والمتشعبة، ويمكن من خلالها تصفح واقع المعلومات المتعددة الوسائط والمرتبطة فيما بينها، ويسبق الإ ختصار www عناوين المواقع على شبكة الويب ويشير إلى مجموعة من الخوادم (أنظمة الحاسوب الخادمة les serveures) المتصلة بالأنترنت التي توفر صفحات من المعلومات[3]، ويعد نظام فرعي من أنظمة الأنترنت إلا أنه مع ذلك يعد نظاما معلوماتيا عالميا مؤلفا من كم هائل من النصوص والصور والعينات الصوتية ولقطات الفيديو وغيرها.

وهو بذلك يشكل أعظم خدمة، وأكثرها شهرة على شبكة الأنترنت بحيث يستطيع المستخدم من خلال برنامج يسمى متصفح، أن يتصفح محتويات هذا النظام عن طريق تتبع الوصلات التشعبية، أو اختيار المواقع التي يرغب في زيارتها والقيام بنشاطات أكاديمية كالبحث العلمي، أو نشاطات اجتماعية كالتعارف والتخاطب والتراسل، أو القيام بنشاطات ترفيهية كالألعاب على مواقع التسلية، أو قراءة الصحف والمجلات أو القيام بأنشطة اقتصادية كالتسوق وشراء الأسهم وغيرها.[4]

- التخاطب عبر الأنترنت (Chatting يمكن للمستخدم من خلال هذه الخدمة، التحدث بطريقة الكتابة الإلكترونية مع مستخدم أو مستخدمين آخرين عبر رسائل يجري عرضها مباشرة أمام الطرف الآخر، موجود في أي مكان من العالم، وللطرف الآخر الرد مباشرة على هذه الرسالة، ويشغل هذا النظام حزمة كبيرة من حزم البيانات التي يتم تبادلها بين مستخدمي هذه الشبكة العالمية[5].

-التقاضي الإلكتروني: أو كما يصطلح عليه محاكم الكترونية .Les cybers tribunaux (المحاكمات عن بعد)

[1] أول رسالة الكترونية أرسلت في جويلية من عام 1982 عن طريق " توم لبسنون " أرسلها لنفسه ووصلت إليه على الفور. أنظر على حسن الطوالبة، مرجع سابق، ص33، نقلا عن غسان حزين، قصة اختراع البريد الالكتروني، مجلة العربي، العدد 530، الكويت، جانفي 2003 ص 164 وما بعدها.

[2] علي حسن الطوالية، مرجع نفسه، ص34.

[3] عوض منصور، محمد أبو النور، مقدمة في علم الحاسب الإلكتروني وبرمجة البيسك، دار الأمل للنشرو التوزيع، الطبعة الخامسة، 1996 ص113.

[4] عمار عباس الحسيني، مرجع سابق، ص 29.

[5] نهلا عبد القادر المومني، مرجع سابق، ص40.

- التجارة الإلكترونية: (E- commerce): تعد التجارة الالكترونية عبارة عن عملية تنفيذ وإدارة الأنشطة التجارية المتعلقة بالبضاعة والخدمات بواسطة تحويل المعطيات عبر شبكة الانترنت[1]، حيث أصبحت شبكة الأنترنت بمثابة سوق مفتوح لعمليات البيع والشراء، إذ يمكن للتاجر الإعلان عن بضاعته بالصوت والصورة مع إمكانية إجراء مقارنة مع السلع المتاحة في العالم ، وللمستخدم أن يختار أيا منها ومن ثم تصله البضاعة إلى غاية منزله، *وبهذه الوسيلة أي الأنترنت أصبحت تتم دون الحاجة إلى الإ جتماع أو اللقاء التقليدي للمتعاقدين، إذ يتم توجيه الإيجاب من أحد المتعاقدين عن طريق الأنترنت، ويتلقى القبول من الطرف الآخر بالوسيلة ذاتها، ويتم إبرام العقد الذي يوقع عليه بطريقة التوقيع الإلكتروني، ويمكن للمشتري أو المستورد أن يسدد قيمة البضاعة عن طريق الدفع الإلكتروني بواسطة شبكة نترنت، ويكفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به[2]. وقد عرف المشرع الجزائري التجارة الإلكترونية في القانون رقم 05/18 المتعلق بالتجارة الإلكترونية المؤرخ في 10 ماي 2018 بأنها ذلك النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الإتصالات الإلكترونية.

خدمة نقل الملفات :file transfer protocol ويرمز لها بـ (FTP) بروتوكول نقل الملفات، حيث تتبع هذه الخدمة نقل أي كمية من الملفات أو البرامج من جهاز الكومبيوتر إلى جهاز آخر عن طريق شبكة الإتصال الإلكتروني، ويمكن من خلال هذه التقنية مثلا للباحثين الحصول على أحدث الأبحاث العلمية من الجامعات ومراكز البحوث، وكذلك تستطيع شركات ومؤسسات أعمال وكذا إدارات تحويل ملفات العملاء والزبائن فيما بينها.

الحكومة الالكترونية: تعد الحكومة الإلكترونية نظاما حديثا تتبناه الحكومات في العديد من دول العالم يقوم على استخدام شبكة الأنترنت في ربط مؤسسات الدولة ببعضها، وربط مختلف خدماتها بالمؤسسات والجمهور لخلق علاقة شفافة بين المؤسسات الحكومية وبين الأفراد، مما يرفع من جودة الأداء الحكومي من خلال تيسير تقديم الخدمة للمستفيدين وإتاحة المعلومة،[3]فتطور تكنولوجيا المعلومات والإتصالات جعل المؤسسات الحكومية تستخدم هذه التكنولوجيا في معاملاتها الداخلية والخارجية، لتمكن المواطن من الحصول على المعلومة بأسرع وقت ممكن وبكفاءة وشفافية.

---

[1] يونس عرب، منازعات التجارة الإلكترونية، الإختصاص والقانون الواجب التطبيق وطرق التقاضي البديلة، ورقة عمل مقدمة إلى مؤتمر التجارة الإكترونية المنظم من طرف الإسكوا التابعة للأمم المتحدة خلال الفترة من 8 إلى 10 نوفمبر 2000 بيروت لبنان. ص،12. متوفر على الرابط:

http://maraji3-elondy.blogspot.com/2011/05/blog-post_5108.html

* في بداية دخول التجارة إلى العالم الإلكتروني، اتفقت شركتا " ماستر كارد " و" فيزا كارد " على تقنيات فنية مشتركة لحماية التسويق الذي يتم عبر الأنترنت باستعمال بطاقات الإئتمان (credit cards) والتي تعتمد عملية التشفير، أنظر في هذا الإطار جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة 2001، ص37.

[2] عبد الفتاح بيومي حجازي، الأحداث والانترنت: دراسة معمقة على أثر الانترنت في انحراف الأحداث، دار الفكر الجامعي، الطبعة الأولى، 2002، ص31.

[3] عمار عباس الحسيني، مرجع سابق، ص30.

والملاحظ بعد مسح الأدبيات العلمية حول مفهوم الحكومة الإلكترونية، فإنه لا يوجد تعريف مشترك واحد لها، ويشار إليها دائما بأنها تطبيق التقنيات على الأنترنت في القطاعات والأنشطة الحكومية وغير الحكومية[1].

وعلى العموم فقد قدمت تعريفات متعددة ومختلفة للحكومة الإلكترونية منها على سبيل المثال تعريف الأمم المتحدة عام 2002، بأنها "استخدام الأنترنت " والشبكة العالمية الواسعة لتقديم معلومات وخدمات الحكومة للمواطن، كما عرفتها منظمة التعاون والتنمية الاقتصادية في عام 2003 بأنها "استخدام تكنولوجيا المعلومات والإتصال، ولا سيما الأنترنت للوصول إلى حكومات أفضل"، وعرفها أيضا البنك الدولي عام 2005، بأنها عملية استخدام المؤسسات لتكنولوجيا المعلومات ومنها شبكة الأنترنت،[2] وقد عرفها خبراء المجال بأنها نظام افتراضي يمكن الأجهزة الحكومية من أداء التزاماتها لجميع المستفيدين باستخدام التقنيات الإلكترونية المتطورة بغض النظر عن المكان والزمان مع تحقيق الجودة والتميز والحرية وأمن المعلومات.[3]

وتوجه الحكومة الإلكترونية خدماتها إلى ثلاث جهات، وترتبط معها بشكل أساسي وهي:

- تقديم الخدمات الكترونيا إلى المواطنين: حيث تسعى الحكومة إلى تقديم جميع الخدمات العامة التي يحتاجها المواطنون، من خلال منفذ واحد يسهل الدخول إليه على موقع إلكتروني خاص بأي قطاع حكومي وطلب الخدمة، وهي ما يسمى بالبوابات الإلكترونية.[4]

- تبادل الخدمات والمعلومات بين القطاعات الحكومية إلكترونيا: وذلك وفقا لنوعية العلاقة أو الإرتباط ونوع النشاط، مما يستلزم ضرورة توحيد المعايير والتي تشمل توحيد نماذج الطلبات والبرمجيات ووسائل الإتصال.

- تقديم الخدمات وتبادل المعلومات بين القطاع العام والقطاع الخاص إلكترونيا.

ثانيا: مخاطر فضاء الانترنت على المعطيات ذات الطابع الشخصي

إذا كانت استخدامات الأنترنت التي سبق ذكرها تبين مدى مزايا الأنترنت وأهمية الخدمات التي تقدمها فإن ذلك لا يخلو من السلبيات والتهديدات التي تمس البيانات الشخصية لمستخدمي هذه التقنية التكنولوجية، فعلى الرغم مما قدمته الأنترنت من مزايا في حقل المعلومات والإتصال من عدة جوانب في غاية الأهمية الإيجابية لا يمكن إنكارها، إلا أن لها بعض الآثار السلبية على خصوصية الأشخاص

[1] إلياس شاهد، الحاج عرابة، عبد النعيم درفور، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، مقال منشور في المجلة الجزائرية للدراسات المحاسبية والمالية، عدد 2016/03، ص122.

[2] عمار عباس الحسيني، مرجع نفسه، ص30.

[3] نقلا عن بوقلقول الهادي، مشروع الحكومة الإلكترونية الجزائرية طموحات كبيرة وانجازات متواضعة، مداخلة مقدمة في إطار الملتقى الدولي الأول حول متطلبات إرساء الحكومة الإلكترونية في الجزائر، دراسة تجارب بعض الدول- المنظم من طرف مخبر تسيير الجماعات المحلية ودورها في تحقيق التنمية بالتعاون مع كلية العلوم الاقتصادية وعلوم التسيير، بجامعة سعد دحلب، البليدة يومي 13 و14 ماي 2013. ص42.

[4] مثال عن البوابات/ بوابة وزارة العدل www.mjustice.dz

المستخدمين لها، فشبكة الأنترنت لا تتوافر فيها الحرية الكاملة والأمان لما ينقل عبرها من بيانات شخصية، مما يسهل الحصول على هذه البيانات بطريقة غير مشروعة.

فغالبية مواقع الأنترنت التي يقوم المستخدمون بزيارتها تجمع بيانات حول المعاملات ومكان الدخول والتعريف الخاص بالجهاز، معرفة المواقع الأخرى التي قاموا بزيارتها، وهو ما يمثل أهمية كبرى للشركات التجارية لتحسين عملية تشغيلها عبر برامج تحليل هذه البيانات وتصنيفها وفق الإهتمام والعمر والمكان والجنس وغيره، كما تساعد هذه البيانات المجمعة في تحقيق ميزة تنافسية في التسعير والتسويق للحصول على زيادة في الأرباح[1]، كما أصبحت الحكومات من خلال الأنترنت تحوز على كميات هائلة من البيانات الشخصية للأفراد، يمكن لها أن تستخدمها في دراسة سلوكاتهم وتشكيل سياسات اقتصادية وسياسة أكثر مثالية، وقد يكون في هذا تهديد لخصوصية هؤلاء،ومن جهة أخرى فإن هناك أساليب تقنية تستخدم في التعدي على خصوصية البيانات الشخصية لمستخدمي شبكات الأنترنت تتمثل في البرامج الالكترونية.

1) المخاطر التي تهدد المعطيات ذات الطابع الشخصي الناجمة عن تداولها عبر شبكات الانترنت

إنه لمن المبادئ الأساسية أن رضا مستخدمي الأنترنت في تقديم معطياتهم الشخصية مقابل حصولهم على الخدمة لا يعني حرية تداول ونقل هذه المعطيات إلى الكافة[2]، فإذا كانت البيانات الشخصية المعلنة من قبل الأفراد تكون بمثابة تنازل ضمني عن تلك البيانات، فإن هذا لا يمنع من ضرورة وجود وسائل لحمايتها من المخاطر التي تهددها بإفشائها أو التلاعب بها أو استعمالها لغير الغرض الذي أعلن فيه عنها صاحبها لأجله، وبالتالي فإنه وبالرغم من أن وسائل الإتصال الحديثة وعلى رأسها شبكة الأنترنت ساعدت على سهولة وسرعة التبادل الإلكتروني للبيانات[3] (EDI)، فإن ذلك لا يعني ترك البيانات الشخصية المعطاة عرضة للقراصنة المتطفلين الهواة منهم والمخربين دون رقيب، وذلك لأهمية هذه البيانات بالنسبة للأشخاص المتعلقة بهم، وكذلك لوثوقهم في الجهة التي تطلب منهم معرفة بعض البيانات الشخصية للدخول إلى موقع أو مواقع معينة.

إن بروز الممارسات الخطيرة على شبكة الأنترنت تجاه المعطيات الشخصية، أصبح أحد أهم المسائل والتحديات التي لا بد من مواجهتها في مسيرة بناء الثقة في الفضاء السيبراني، حيث تتصاعد التهديدات وتبرز التعقيدات بشكل مستمر نتيجة التدفق الهائل للمعلومات على شبكة الأنترنت وما تخضع له من عمليات المعالجة، وعليه فلا بد من تحديد هذه المخاطر ونقاط الضعف والثغرات والتهديدات وتحليلها وفهمها بغية التمكن فيما بعد من وضع الإجراءات المناسبة والكفيلة بمكافحتها وتوفير حماية للخصوصية المعلوماتية تبعا لذلك، ومن أهم هذه المخاطر التي تهدد البيانات الشخصية في بيئة الأنترنت نذكر ما يلي:

[1] عادل عبد الصادق، مرجع سابق، ص17.

[2] عمر حسبو، مرجع سابق، ص155.

[3] Marie- Christine Piatti, les libertées individuelles a l'epreuve des nouvelles technologies de l'information, Presses universitaires de lyon- pul. 2001.page175

1-1) شبكة الأنترنت تسهل عملية جمع ومعالجة ونقل البيانات الشخصية: لقد التصقت النشاطات الإنسانية بكل أشكالها بأنظمة المعلومات وتكنولوجيا الإتصالات، فقد أتاحت الأنترنت نقل النشاطات جتماعية والتجارية والثقافية والسياسية من العالم المادي إلى العالم الإفتراضي والبيئة الإلكترونية،[1] وبسبب الأنترنت تغيرت البيئة التي تمر عبرها رحلة البيانات المتبادلة، وترك الأفراد خلفهم الوسائل التقليدية في الوصول إلى المعلومات، وأصبح اعتمادهم في ذلك على الأنترنت بشكل كبير باعتبارها مصدرا غنيا بالمعلومات[2].

والمستخدم في العالم الرقمي وعالم الشبكات الرقمية وهو يبحث عن هذه المعلومات المتاحة في هذه البيئة، حتما سوف يترك وراءه آثارا ودلالات كثيرة تتصل به في شكل سجلات رقمية، وذلك حول الموقع أو المواقع التي زارها، والوقت الذي قضاه على الشبكة، والمواضيع التي بحث عنها، والمواد التي قام بتنزيلها، والرسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها، كما تشمل كذلك معلومات تتعلق بعنوان بروتوكول الأنترنت لجهاز الكومبيوتر المرتبط بالشبكة، المتصفح المستخدم... وهي في الحقيقة نهر متدفق من البيانات الشخصية تتضمن تفاصيل دقيقة عن شخصية المستخدم وحياته وهواياته وميولاته، قد تكون كافية للتعريف بالشخص، يتم اصطيادها وجمعها في نقاط عديدة في الرحلة عبر الشبكات[3].

إن التصفح والتجول عبر شبكاتنتلأت يترك لدى المواقع الم ، زارة كمية هائلة من المعلومات، قد يكون جزء منها ضروري لإتاحة الربط بالمتصفح، فبمجرد الدخول إلى صفحة الموقع فإن معلومات معينة عن الزبون يطلبها الموقع، وهي ما يعرف بمعلومات رأس الصفحة، هذه المعلومات يزودها الكومبيوتر المستخدم للكومبيوتر الخادم الذي يستضيف مواقع الأنترنت، وتتضمن هذه المعلومات في الغالب ما يتعلق بالبيانات الشخصية للمستخدم، وما يهمنا منها ما يلي:

*عنوان بروتوكول الأنترنت adresse IP العائد للزبون المستخدم، وهذا الأخير يمكن من خلاله تحديد إسم النطاق وإسم الشركة أو الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها.

*مواقع الأنترنت وعناوين الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة عند كل زيارة، وتبعا لنوع المتصفح قد يطلب إدخال عنوان البريد الالكتروني للمستخدم وكلمة المرور، وتبعا لتشغيل المستخدم لأوامر خاصة حول إدارة التعامل مع الشبكة، قد تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وكذا بيان المعلومات التي أرسلت واستقبلت،وهناك أجزاء أخرى من المعلومات لا تكون ضرورية لعملية الربط،لكن كافة المواقع التفاعلية وتحديدا مواقع النشاط التجاري والتجارة الالكترونية[4] تطلب من المستخدم تعبئة نموذج يتضمن بيانات مختلفة كإسم المستخدم وعنوان إقامته أو عنوان

[1] بولين أيوب، مرجع سابق، ص193.

[2] عبد الحميد بسيوني، الحماية من أخطار الأنترنت، أخطار الأنترنت ومصادر التهديد، دار الكتب العلمية القاهرة، 2003. ص159.

[3] مروة زين العابدين، مرجع سابق، ص321.

[4] Pierre kayser, la protection de la vie privée, economica, presses universitaires d aix-Marseille,2eme édition 1990.p350.

محله، رقم الهاتف النقال، عنوان البريد الإلكتروني، معلومات حول الجنس،السن، الحالة الاجتماعية، الدخل الشهري، وأحيانا اهتمامات الشخص، أو قد يطلب المتصفح أيضا إدخال رقم بطاقة الإعتماد ونوعها وتاريخ انتهائها في مواقع البيع والشراء على الأنترنت.

وجمع هذه البيانات قد يشكل كشفا عن أنشطة الفرد، بل وفي مرحلة من المراحل تصبح هذه البيانات عند جمع شتاتها وتحليلها بواسطة برمجيات ذكية مخصصة لذلك مادة تكشف تفاصيل كثيرة عن خصوصية المستخدم، قد لا يرغب في كشفها، وفي الوقت نفسه تصبح هذه البيانات مادة غنية ومحلا للبيع من جهة أخرى لغايات تجارية[1].

وهذا ما أدى إلى ظهور ما يعرف بالحوسبة السحابية*، وهي تطور حديث نسبيا يمكن من تخزين كميات متزايدة من البيانات بما فيها البيانات الشخصية في سحابة على الأنترنت يتم نقلها بعد ذلك من مكان لآخر، ومن مزود إلى مزود آخر، أو من جهاز إلى آخر دون إشعار المستخدم، مما قد يشكل خطرا حقيقيا على مدى قدرة الفرد على التحكم في تلك البيانات[2]، فأي مستخدم للأنترنت لن يكون قادرا على تحديد المنطقة المحددة التي توجد فيها ببياناته الشخصية.

ومن أهم طرق جمع وتخزين البيانات الشخصية على شبكات الأنترنت فضلا عن نموذج الأعمال التجارية السالف ذكره والتي يتم من خلاله جمع البيانات الشخصية للزبون المستخدم في منصة معالجة مركزية عبر شبكة الأنترنت، يمكن أيضا أن يتم عبر محركات البحث* moteurs de recherche.

والتي تمثل الوسيلة الأهم من بين وسائل الوصول المباشر للمعلومات المطلوبة من قبل المستخدم عبر شبكات الانترنت، حيث قدمت هذه الأخيرة (محركات البحث) وظيفة حيوية على شبكات الأنترنت من خلال مساعدة المستخدمين على التنقل بين المصادر الهائلة المتاحة على الأنترنت، ورغم تباينها في وظائفها وأدوارها وفعاليتها، لكن ما يجمعها أنها أصبحت طريق المستخدمين لطلب المعلومات[3] .

---

[1] حسام شوقي، حماية وأمن المعلومات على الانترنت، دار الكتب العلمية، القاهرة، 2000. ص189.

* الحوسبة السحابية وهي باللغة الانجليزية cloud computing هي تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب، إلى ما يسمى السحابة، وهي جهاز خادم يتم الوصول إليه عن طريق الأنترنت، ومن خلاله تتحول برامج تكنولوجيا المعلومات من منتجات إلى خدمات، وقد عرفها المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة الأمريكية (NIST) بأنها نموذج تمكين شائع ملائم للوصول إلى الشبكة بناء على الطلب لمجموعة مشتركة من موارد الحوسبة والتي تمت تهيئتها مثل (الشبكات، الخوادم، وحدات التخزين، التطبيقات...) ويمكن توفيرها وإطلاقها بسرعة وبأقل جهد أو تفاعل مع مزود الخدمة". وعرفت أيضا بأنها تقنية تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة والتي يتم الوصول إليها عبر شبكة الانترنت. أنظر: حمدي حبيب الصالحي، الحوسبة السحابية، مدونة التقنية موجود على الرابط: http://www.tvtc.gov.sa/arabic/departements/faculty

[2] توبي مندل، وآخرون، مرجع سابق، ص30.

* محرك البحث هي عبارة عن بنك معلومات ضخم موصول بشبكة الأنترنت، يتضمن نظام فهرسة وتصنيف وتبويب لمواقع الواب والعناوين والمواضع، يساعد مستخدم الأنترنت في البحث عن المعلومات، وتدله على المواقع والموزعات المختلفة الموصول بها، وهي تتألف من ثلاث أجزاء، برنامج العنكبوت (spide program) برنامج الفهرس (indexer program) وبرنامج محرك البحث (search engine program) ومن أشهرها : google ، yahoo , Altavista .أنظر بدوية محمد البسيوني، نوال عبد العزيز راجح، مقال بعنوان: الأدوات البحثية على الأنترنت دراسة في أنماط الإفادة والاستخدام من جانب أعضاء هيئة التدريس ومعاونهم بجامعة الملك عبد العزيز، ص10 وما بعدها، متوفر على الرابط: http://www.libraries.kau.edu.sa.

[3] طوني عيسى، مرجع سابق، ص43.

ومكمن الخطورة والتهديد لمحركات البحث على خصوصية المعلومات يظهر عندما يضطر مستخدموها في الكشف عن بعض خصوصياتهم والإدلاء ببياناتهم الشخصية وتقديم عرض كامل عن حياتهم الخاصة مقابل الحصول على مزيد من مزايا تخصيص خدمات البحث، وهنا قد تكون قيمة الخدمة مرتفعة، لكن المستخدم يدفع مقابل هذه الخدمة المتطورة عن طريق التضحية ببعض بياناته الشخصية.[1]

بالاضافة إلى وسائل الدفع الإلكتروني التي تعد من أهم وسائل الدفع في بيئة الأنترنت، تتولى البنوك والمؤسسات المصرفية إصدارها إلى زبائنها الذين لديهم حسابات مصرفية، وقد عرفت على أنها بطاقات تحتوي على شريط ممغنط يتضمن بيانات عن العميل وحسابه لدى البنك، وتستخدم من أجل سحب المبالغ النقدية وفي دفع ثمن المشتريات[2]، وقد عرفها المشرع الجزائري في المادة الثالثة من قانون التجارة الإلكتروني بأنها كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به، تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية[3].

أما عن البيانات الشخصية التي تتضمنها بطاقات الدفع فهي إسم حاملها، رقم البطاقة السري، تاريخ إصدار البطاقة ومدة صلاحيتها، توقيع حاملها وإسم البنك الذي أصدر البطاقة، وبالتالي فإن عمليات الشراء وعمليات الإعلان وطلب الخدمات باستعمال هذه البطاقات في عالم الأنترنت، سوف يؤدي بكل بساطة أن تغيب فيها القدرة على التخفي خلافا للعالم المادي الواقعي، ومن ثم فإن نظام الدفع المالي على نترنت إذا كان دون حماية الخصوصية سوف ينقلنا من عالم الدفع النقدي المستتر إلى عالم مليء بوسائل الكشف والتعريف، تتزايد فيه قدرة تتبع الأشخاص ومشترياتهم، وهذا ما يؤثر سلبا على الثقة في التجارة الالكترونية[4]، لأجل ذلك يثور في هذا الصدد مسألة الإعتداء على البيانات السرية الخاصة ببطاقات الدفع الالكترونية[*].

وترتيبا على ما سبق فإنه يمكن القول أنه بالرغم من المنافع الكبيرة التي أفرزتها شبكات الأنترنت فإنها أوجدت أيضا خطرا حقيقيا يهدد البيانات الشخصية من خلال إمكانية جمعها وتخزينها والوصول إليها وجعلها متاحة على الخط وقابلة للإستخدام من قبل مختلف القطاعات دون علم أو رضا صاحبها.

2-1) المخاطر الناجمة عن كون الأنترنت يتيح عولمة المعلومات والإتصالات: من التحديات الأخرى التي تثيرها الأنترنت، ويبرز معها مخاطر إساءة استخدام البيانات الشخصية هو التدفق ونفاذ البيانات عبر

---

[1] توبي مندل، وآخرون، مرجع سابق، ص32.

[2] علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية (دراسة مقارنة)، المؤسسة الحديثة للكتاب، لبنان، الطبعة الأولى، 2011، ص15.

[3] عرفها المشرع الفرنسي في المادة الثانية من قانون أمن الشبكات ووسائل الدفع المؤرخ في 1991/12/03 بأنها أداة تصدر من أحد مؤسسات الإئتمان وتسمح لحاملها بسحب أو تحويل نقود من حسابه.

la loi n 91-1382 du 2 décembre 1991 relative a la sécurité des chéques et cartes de paiement,JORF n1 du 1janvier 1992 p 12.

[4] محمد أمين الشوابكة، مرجع سابق، 2009، ص194.

[*] من بين الإجراءات التقنية لمواجهة إساءة استخدام بطاقات الدفع الإلكتروني من خلال الأنترنت، النموذج التقني الموحد الذي أعلنت عنه شركتي فيزا (visa) وماستر كارد (master card) بتاريخ 1996/02/01 والمسمى نظام الصفقات الإلكترونية الآمنة (secure Elecronics transaction protocol).

الحدود دون اعتبار للجغرافيا والسيادة، فالأفراد يعطون معلوماتهم الشخصية لجهات داخلية وخارجية وربما إلى جهات ليس لها مكان معروف، وتزداد الخطورة عند نفاذ البيانات الشخصية إلى دول لا تتوافر فيها مستويات الحماية القانونية للبيانات الشخصية، وقد لا تخدم القوانين الوطنية كثيرا في هذه الحالة، كما أن تضمينها نصوصا قانونية بشأن السيطرة على نقل البيانات قد لا يكون فاعلا في ظل غياب التنسيق وضمان أن يكون نقل البيانات محكوما باتفاقات تكفل حمايتها، أو تضمن توفير حماية مماثلة في الدولة المنقول إليها هذه البيانات.

وتصبح المخاطر في هذا المجال أوسع عندما يتم إنشاء ملاجئ آمنة لا تقيد عمليات جمع ومعالجة البيانات الشخصية بأي قيد، وهي ملاجئ تهرب إليها مؤسسات الأعمال في بيئة الأنترنت للإفلات من القيود القانونية التي تهدف إلى حماية الخصوصية ومنع إساءة استخدام بيانات الأفراد الشخصية، إلى جانب غرضها في منع الأنشطة الإحتيالية والمساس بالمستهلك في بيئة الأنترنت[1].

3-1) المخاطر الناجمة عن عدم مركزية الأنترنت وفقدانها آليات السيطرة والتحكم: تتصف الأنترنت باللامركزية وغياب السلطة التحكمية، ومن ثم غياب قانون يحدد المسائل الخاصة بتنظيمها وباستعمالها، وبالنزاعات الناشئة عنها، ومن ثم يصبح موضوع تنظيم الأنترنت موضوعا شائكا إلى درجة كبيرة خاصة مع السياسة التي تنتهجها بعض الدول في مراقبة الأنترنت وفي منع وصول المواطنين إلى أنواع معينة من المعلومات.[2]

فإذا كان إقرار قانون وطني لحماية أحد حقوق الإنسان قد يكون فاعلا، فإن ذلك راجع لعنصر السيطرة والسيادة، وتوفر الجهة القادرة على الرقابة ومنع الإعتداء أو استمراره ومعاقبة المخالفين، لكن كيف يكون الوضع في ظل الأنترنت التي يملكها كل شخص وغير مملوكة لأحد، والتي لا تتوفر فيها سلطة توفر الحماية القانونية عند حدوث الإعتداء.[3]

فالطبيعة التقنية للأنترنت هي التي تحكم طبيعة العالم السيبراني، ذلك أن هذا الأخير يتصف بتقنية عالية متحركة وسريعة التحول، وأن هذه التقنية هي التي تتحكم أيضا في تقرير ما يمكن اعتماده من أساليب متابعة ومراقبة ضرورية في التنظيم القانوني للعالم السيبراني، لا سيما على مستوى تقرير قواعد المراقبة والملاحقة والتنفيذ.*

---

[1] مروة زين العابدين، مرجع سابق، ص323،

[2] منى الأشقر، السيرانيةهاجس العصر، مرجع سابق، ص14.

[3] Christiane féral – schuhl : cyber droit, le droit a l'épreuve de l'internet, dalloz dunod, 3eme édition. Janvier 2002.p.106.

* مع بدايات وضع الانترنت بين أيدي الجمهورالواسع، ترافق مع هذا الانفتاح اعتراضات على احتكار جهة واحدة لتوزيع أسماء النطاقات العليا (net.org.com) ظهرت عام 1998 الآيكان (ICANN) وهي التي أسست للسجلات الوطنية لأسماء النطاقات واعتمدت مبادئ حل النزاعات حول أسماء النطاقات التي أقرتها المنظمة الدولية لحماية الملكية الفكرية، فالآيكان هي الجهة المسؤولة عن ضمان حسن سير عملية انتقال المعلومات على الانترنت، وتحتفظ لهذه الغاية بقاعدة بيانات تضم جميع العناوين يتم تبويبها بشكل متواصل، وتشكل هذه القاعدة نقطة محورية في عمل الانترنت، حيث تقوم ب:

- تخصيص عناوين بروتوكول الانترنت.
- إدارة أسماء النطاقات العليا.

لكن البيانات الشخصية تنتقل عبر الأنترنت من دولة لأخرى، ومن منظمة لأ خرى ومن جهة عمل إلى أخرى ومن فرد إلى مؤسسة دون قيود وبكل اللغات، وفي رحلتها هذه تحط وتزور العديد من مناطق الإ ختصاص القضائي، وهو ما جعل مسألة حماية الأشخاص الطبيعيين في إطار معالجة البيانات ذات الطابع الشخصي أكثر تعقيدا في مثل خصائص هذه البيئة التقنية المتحركة، وأعيد بذلك طرح موضوع حماية الخصوصية المعلوماتية على بساط البحث مجددا من منظور عالمي وكوني.[1]

فالخطورة التي تعاني منها البيانات الشخصية في إطار هذا التحدي القائم على عالمية الأنترنت وانعدام سلطة مركزية، تكمن في معرفة مدى فعالية القوانين والتشريعات الداخلية التي تحمي البيانات الشخصية في مواجهة التدفق العالمي للبيانات في شبكة دولية لا تعرف حدودا جغرافية، وتزداد الخطورة أكثر عندما يستحيل التنسيق والتعاون بين الدول لتوفير حماية لهذه البيانات الشخصية، لأنها لا تنوي القيام بذلكأو كونها تنظر إلى المسألة برمتها نظرة مغايرة.*

لذلك نعتقد أنه أمام الأهمية الإستثنائية للبيانات الشخصية في العالم الإفتراضي الذي خلقته شبكات نترنت، يكون من الضروري إقرار قانون يشكل منهجا مستقلا لتنظيم التعاملات عبر العالم الإفتراضي، يوفر حماية للمعطيات الشخصية المتداولة عبره، وهو منهج يختلف عن منهج قواعد التنازع الذي قوامه التركيز المكاني للمعاملة محل النزاع، واعتبار المكان الذي ترتبط به من أكثر الروابط وثوقا واختيار قانون ذلك المكان ليحكم العلاقة أو الرابطة محل النزاع، وهذا المنهج يشير فقط إلى القانون الوطني، وليس إلى قانون عالمي يحكم جميع النزاعات المرتبطة بالبيانات الشخصية ويوفر لها الحماية انطلاقا من نفس المعايير.

2) المخاطر التي تهدد المعطيات الشخصية الناجمة عن البرمجيات التقنية: هناك أنماط متعددة للأساليب التقنية المستخدمة في الوصول إلى نظم المعلومات ومعرفة ما تحتويه من بيانات ذات طابع شخصي، هذه الأساليب المستخدمة على البيانات الشخصية تتطلب معرفة فنية يكون هدف المعتدي من خلالها التقاط أو تسجيل البيانات المعالجة الكترونيا وهي في مرحلة انتقالها عبر شبكات الإتصال

- إعطاء معرفات البروتوكول.

- إداة نظام مخدمات الجذر.

وتقوم الآيكان بعملها في كافة أنحاء العالم عبر مسجلي أسماء النطاقات الذين تعتمدهم بناء على التزامهم بدفتر الشروط يبين معايير آداء مهام التسجيل، وتعتمد أساليب تسمح بالتعرف على الأشخاص الطبيعيين والمعنويين الذين تنطبق عليهم هذه المعايير وتحدد القواعد والإجراءات التي تطبق على توفير خدمات المسجلين من خلال اتفاقية الاعتماد، وقراراتها تلزم الأشخاص والمؤسسات والحكومات، أنظر للمزيد منى الأشقر جبور هاجس السيبرانية، مرجع سابق، ص 21 وما بعدها.

[1] طوني عيسى، التنظيم القانوني لشبكة الانترنت، مرجع سابق، ص40.

* ويمكن أن نقدم الولايات المتحدة الأمريكية كنموذج ومثال على هذه المسألة، فهذه الأخيرة بالرغم من إقرارها بالمخاطر الأكيدة للانترنت في مجال الحياة الخاصة والبيانات الشخصية على وجه التحديد، إلا أنها لا تعتمد نظاما قانونيا خاصا في هذا الموضوع، والأكيد من منظور عالمي يظهر من الموقف الحازم الذي اتخذته الو.م.أ في هذا الشأن والذي جاء في الرسالة التي وجهتها وزيرة الخارجية غوندوليزا رايس إلى جاك سترو وزير الخارجية البريطاني ، بصفته كرئيس للاتحاد الأوروبي عبرت فيها عن استهجانها للموقف الأوروبي الذي يدعو إلى إيجاد هيئة جديدة تشرف على إدارة شؤون الانترنت، ورأت فيه تهديدا لسلامة الانترنت وإعاقة تطورها، والذي يتنافى مع منطق إخضاعها لإشراف بيروقراطي. أنظر منى الأشقر جبور، مرجع سابق، ص17.

الإلكترونية (الانترنت) ويطلق عليها صفة الإعتداءات المنطقية[1] " attaques logiques"ومن أهم هذه الوسائل نذكر ما يلي:

1-2) ملفات تعريف الإرتباط: (cookies) : إن من مخاوف الخصوصية المعلوماتية هو تسجيل المستخدم على الأنترنت، فقد يتم اعتبار تعريف هوية المستخدم كجزء من إجراءات الإشتراك في شبكة نترنت، وفي هذا السياق أي تحديد هوية المستخدم تساهم آليات تعريف هويته على الأنترنت في وضع قيود على الخصوصية وسرية الهوية على الأنترنت[2]، ومن جهة أخرى فإنه تبعا للهندسة التي تقوم عليها شبكة الأنترنت، تمر الرسالة عبر هذه الشبكة قبل وصولها إلى مقصدها عبر نقاط عديدةكعقد الإتصال (noeuds) والموجهات (routeures)، وموزعات موردي خدمة الإتصال والتي غالبا ما تكون موصولة بحاسبات آلية مزودة ببرامج مصممة خصيصا لتنفيذ نسخ منهجي وتلقائي للرسائل التي تمر عبر الحاسبات الآلية قبل وصولها إلى الجهة المرسلة إليها[3] .

ولعل من أشهر الآليات والوسائل التقنية التي تستعمل في شبكة الأنترنت، سواء في حالة تحديد هوية المستخدم أو في تتبع المعلومات الشخصية للمشتركين، نجد ملفات تعريف الإرتباط أو ما يعرف برسائل الكوكيز " cookies " التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع، وتتمكن من تسجيل بيانات خاصة تخص المستخدم، بحيث يتم تخزينها على جهاز حاسوب مستخدم الأنترنت عند زيارته لموقع من المواقع على الشبكة واستخدام متصفح الأنترنت، وبناء على ضبط طريقة إنشاء هذا الموقع وضبط أوضاع متصفح المستخدم يمكن تخزين عشرات ملفات تعريف الإرتباط cookies ومن خلالها يمكن تتبع كل مستخدم على الأنترنت، وجمع المعلومات باستمرار عنه مثل المواقع التي زارها ومقدار مكوثه فيها وما يفضله وغير ذلك.[4]

وقد تم تعريف نظام cookies بأنه عبارة عن برنامج ترسله مواقع الويب التي يزورها المستخدمون وقت اتصالهم بالشبكة في شكل ملفات نصية بامتداد (TXT)، يرسلها الخادم الخاص بالموقع الذي تتم زيارته عبر الانترنت إلى القرص الصلب للكومبيوتر الخاص بالمستخدم ويحتفظ بنسخة منها لديه، وتستقر في الحاسبات الآلية الشخصية لهؤلاء المستخدمين بعد قطع الإتصال، وتقبع بداخلها إلى حين قيامهم بزيارة المواقع ذاتها مجددا، بحيث تعود هذه الملفات أو الرسائل النصية أدراجها نحو المواقع ذاتها التي أتت منها محملة ببيانات ومعلومات مختلفة عنهم ومنها البيانات الشخصية.[5]

وتكمن خطورة هذا البرنامج على خصوصية المستخدمين في ملاحقتهم و اقتفاء أثرهم وجمع بياناتهم الشخصية وتحليلها لغايات الإعلان ولغايات الدراسات التسويقية من الشركات التجارية في إطار أنشطتها الدعائية، وذلك قد يمثل كشفا عن بيانات شخصية قد لا يرغب الشخص في الكشف عنها، ويكون ذلك

[1] محمد أمين الشوابكة، مرجع سابق، ص140.
[2] توبي مندل وآخرون، مرجع سابق، ص40.
[3] طوني ميشال عيسى، مرجع سابق، ص392.
[4] مروة زين العابدين، مرجع سابق، ص335.
[5] بولين أيوب، مرجع سابق، ص197.

دون علم صاحبها ودون أن تتيح له خيارات قبول هذا الإستخدام أو رفضه، كما أن المعلومات التي تقوم بجمعها هذه البرامج قد تكون كافية لإعطاء صورة جانبية عن المستخدم، سياسية، دينية، إجتماعية أو ثقافية، وقد ينطوي هذا النوع من الدراسات السلوكية على تهديد جدي وخطير لحياة الأفراد الشخصية.[1]

ومن ثم يمكن القول أن خطورة وجود مثل هذه الملفات التقنية أو البرمجيات على جهاز الكومبيوتر الخاص بالمستخدم بالإضافة إلى معرفة البيانات الشخصية التي تخصه، فإنه يستطيع الموقع أيضا أن يتعرف وبسهولة على خطوات واتجاهات المستخدم عبر الأنترنت، عن طريق معرفة المواقع التي يدخلها، وبالتالي يمكن معرفة سلوك المستخدم عبر الشبكة، ومن ثم يكون من اليسير على المواقع الدعائية توجيه الإعلانات التي تناسبه بالتحديد.*

ومن مكامن الخطورة أيضا في هذا الإطار، هو إمكانية أن تكون هذه الملفات عرضة للسرقة من جهاز المستخدم واستخدام المعلومات التي يحتويها ملف الكوكيز في التصفح بدلا من المستخدم ذاته، وهذا طبعا سوف يسهل اختراق الصفحات الشخصية التي تخص المستخدم والبريد الإلكتروني الخاص به، والأخطر من كل هذا عندما يتم اختراق الموقع والاستيلاء على ملف الكوكيز الخاص بصاحب الموقع، فإن ذلك يعني تهديدا لخصوصية جميع المستخدمين عبر الأنترنت لهذا الموقع.[2]

2-2) برامج الدعاية (Ad ware) والبرمجيات المؤذية (M al ware) وبرامج التجسس (Spy ware): تندرج هذه البرامج ضمن فئة البرمجيات المعتدية على الخصوصية والمتجاهلة لموافقة المستخدم، وهي برمجيات يصعب على المستخدم إدراكها، لأنها عادة ما تظهر على شكل برامج مكافحة للفيروسات " antivirus " أو أداة بحث أو تقنية مفيدة يرغب المستخدم في تحصيلها، كما أنها غالبا ما تتجمع مع البرامج التي تبدو مجانية.

من خلال هذه البرامج تنشأ تهديدات أخرى على خصوصية المستخدمين على شبكة الأنترنت، حيث تقوم هذه البرامج بجمع البيانات الشخصية واستخدامها لأغراض إجرامية مثل سرقة أموال الأشخاص واختراق حساباتهم على الأنترنت* وإساءة استخدام بياناتهم الشخصية بأي طريقة أخرى، ومع الظهور

---

[1] مأخوذ من موقع: http//www.ietf.org أطلع عليه يوم 2019/11/29.

* ومن أشهر القضايا في هذا السياق قضية: FTC V.GOOGLE.INC والتي تدو حول واقعة وضع شركة google ملفات كوكيز في المتصفح "سفاري " SAFARI " الخاص بشركة " APPELE" بحيث تمكنت شركة GOOGLE من خلال ملفات الكوكيز من تتبع نشاط المستخدمين لمحرك بحثها والذين يتصلون به من خلال المتصفح سفاري،عبر استغلال ثغرة داخل هدا المتصفح، ووضعت ملفات الكوكيز داخله دون علم المستخدمين أو موافقتهم مستهدفة من وراء ذلك إرسال إعلانات إليهم من أجل تحقيق الربح، وقد تم تقديم الشكوى ضد شركة جوجل من طرف غرفة التجارة الفدرالية FTC أمام محكمة الولايات المتحدة للمنطقة الشمالية في ولاية كاليفورنيا، أنظر هيثم السيد أحمد، المسؤولية المدنية في إطار المعاملات عبر شبكة الانترنت، رسالة دكتوراه كلية الحقوق جامعة المنوفية، مصر، ص367.

[2] هيثم السيد أحمد، مرجع نفسه، ص327.

* حدث في شهر أفريل من سنة 2011 أن تم اختراق شبكة PlayStation net work التابعة لشركة (Sony) والمرتبطة بوحدة التحكم sony playstation ونتج عن ذلك اختراق للبيانات الشخصية الخاصة بـ 77 مليون مستخدم للشبكة بما في ذلك اسم المستخدم وعنوانه والبلد وعنوان بريده الالكتروني وتاريخ الميلاد، ورقم بطاقة الائتمان وكذلك إسم الدخول وكلمة السر وإجابات الأمن المستخدمة في كلمة السر بالشبكة، وقد استغرق الأمر أكثر من أسبوع لشركة سوني حتى تخبر المستخدمين للشبكة أن بياناتهم الشخصية في خطر، أنظر مجلة the Guardian / على الرابط: http://www.guardian.co.uk

السريع لعدد من الأجهزة المتصلة بالأنترنت والتي يطلق عليها إسم " أنترنت الأشياء " internet of things وجد المستخدمون أن من الصعب السيطرة على معطياتهم الشخصية، لأن هذه الأجهزة المتصلة بشبكة نترنت توفر في العادة إعدادات الخصوصية، كما تستخدم في كثير من الأحيان برامج تجسس من جانب الملاحقين الذين يرغبون في التعدي على الحياة الشخصية لضحاياهم، قد تتضمن تفاصيل المكان الفعلي للشخص واتصالاته ومعلومات شخصية أخرى وكلمات المرور[1]، بل ولا يقتصر التجسس على ما ذكرناه فقط، بل قد يمتد إلى نظم المعلومات الشخصية، والتي تكون عرضة للوصول إلى المعلومات المخزنة فيها بواسطة زرع فيروس في الكومبيوتر بقصد التطفل على الحياة الخاصة للفرد، من خلال الوصول إلى معلوماته الشخصية واستخدام هذه المعلومات بصورة غير مشروعة، مثل التسلل إلى نظم قواعد البيانات الطبية للحصول على معلومات عن صحة مريض معين، وهي معلومات شخصية ذات طابع سري[2]. ومن ثم فإن هذه الأساليب التقنية* تفرض تحديات خطيرة تهدد خصوصية المستخدم وقدرته على التحكم في بياناته الشخصية في بيئة الانترنت.

المطلب الثالث: مخاطر وسائل التواصل الاجتماعي على الخصوصية المعلوماتية

بالمقارنة مع العالم المادي جاءت وسائل التواصل الاجتماعي بمفاهيم جديدة للتواصل لم تكن معروفة قبل تطور الإتصالات وتكنولوجيا المعلومات وانتشارها بين الناس، حيث أصبحت هذه المواقع جزء أساسيا في حياة معظم الناس، وفرضت نفسها في جميع مجالات حياتهم من حيث تكوين العلاقات

[1] مقال منشور على موقع مركز معلومات الخصوصية Electronic privacy information centre http://www.epic.org/privacy: أطلع عليه اليوم 2019/11/29.

[2] بولين أيوب، مرجع سابق، ص167نقلا عن: ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس الكومبيوتر ووسائل حمايتها، دار النهضة العربية.1989 .ص54.

* هناك برامج أخرى تمثل تهديدا على خصوصية البيانات الشخصية نذكر:

- برامج مراقبة الحزم (IPD) تعتبر هذه البرامج من التقنيات المستخدمة كأداة تحكم عامة في أجزاء كثيرة من الأنترنت، وتتميز بقدرتها على الإختراق داخل الحزم التي تنتقل عبر شبكة الأنترنت، ثم تقوم بفحص محتواها وتتفاعل مع هذا المحتوى، وقد ارتبطت هذه التكنولوجيا بأكبر التعديات على الخصوصية على شبكة الأنترنت، فمن الاستخدامات الشائعة لها هو تصنيف المستخدمين بملفات تعريف على شبكة الإتصالات، لذلك فقد استعملت برامج (IPD) في سياق الإحتجاجات الشعبية في إيران، ومنطقة الشرق الأوسط وكذا شمال إفريقيا في سنوات 2001.2010.2011 حيث كانت تستخدمها الحكومات في تتبع ومراقبة مواطنيها.
- برامج تحديد المواقع الجغرافية (GPS): توفر هذه الخدمة الموقع الجغرافي لعناوين بروتوكول الأنترنت (IP) الخاص بالمستخدمين، وتسمح لمزودي خدمات الأنترنت بوضع تقدير دقيق نسبيا حول الموقع الذي يتواجد فيه المستخدم، ومع ارتفاع نسبة استخدام الانرنت زادت قدرة هذه البرامج على تحديد الموقع الجغرافي لمستخدمي الأنترنت. وتثير أنظمة المواقع الجغرافية على ما هو واضح بعض الإشكاليات المتعلقة بموافقة المستخدم وتحكمه في بياناته الشخصية الخاصة بموقعه الجغرافي، حيث لا يستطيع المستخدم إحكام السيطرة الكاملة والفعلية على البيانات الخاصة به، وأشكال معالجتها، كما تتميز أنظمة تحديد المواقع العالمية (GPS) بدقتها العالية التي تفوق تحديد الموقع الجغرافي باستخدام أبراج الاتصالات النقالة، وتوفر صورة أكثر دقة لتحركات الفرد، ويمكن عندئذ استخدام بيانات الموقع الجغرافي التي تم جمعها بهذه الطريقة في إنشاء ملفات تعريف لحركة الأفراد.

جتماعية أو تأسيس مجموعات مشتركة من حيث الميول أو التوجه، وشغلت مساحة إجتماعية وهمية تضمن لهم حرية إبداء آرائهم.[1]

ولقد تعاظم استخدام الأفراد لوسائل التواصل الإجتماعي بحيث أصبحت جزءا من حياتهم اليومية وإحدى الطرق الأساسية لتبادل الرسائل والمعلومات والصور والأخبار والأحداث، فقد وصل عدد المستخدمين لمواقع التواصل الاجتماعي في عام 2010 أي بعد 04 سنوات فقط من انطلاق أول شبكة اجتماعية في العالم وهي FACEBOOK[2] نحو 500 مليون مستخدم[3]، ونتيجة لذلك أصبح لهذه الوسائل تأثير كبير على الحياة اليومية للبشر.

وتستوعب وسائل التواصل الإجتماعي 22% من الوقت الذي يقضيه المستخدمون على الأنترنت، وفي دراسة مجراة من قبل المشغل البريطاني O2 في العام 2012 تبين أن مستخدمي الهواتف الذكية يقضون قرابة 25 دقيقة في اليوم بالتصفح على شبكة الأنترنت، منها 17 دقيقة يقضونها على مواقع التواصل الاجتماعي.[4] ونتيجة لذلك أصبح لهذه الوسائل تأثير كبير على الأشخاص، ويظهر هذا التأثير ليس فقط من خلال عدد المستخدمين الكبير والمتزايد، بل أيضا من خلال الدور الذي تؤديه في حياتهم، لا سيما من جهة تقديمهم معلومات خاصة عن أنفسهم، وهو ما ينعكس سلبا على واحد من أهم الحقوق المتعلقة بالحرية الشخصية التي يمكن أن تتعرض لها وسائل الإتصال الإجتماعي وهو الحق في الخصوصية وحماية البيانات الشخصية.[5]

ونتيجة لذلك فإن وسائل الإتصال الإجتماعي تطرح تحديات في مواجهة تأثيرها على الخصوصية، فهي إن كانت قد أتاحت للمستخدم مجالا واسعا للتعبير عن رأيه والوصول إلى أوسع شريحة من الناس دون أي كلفة، إلا أنها بالمقابل تعرضه لمخاطر انتهاك خصوصيته.

فشبكة الفايسبوك مثلا إذا كانت قد حققت نجاحا كبيرا في أن تصبح موقعا لا غنى عنه بالنسبة للعديد من مستخدميه، إلا أنها تنتج آثارا سلبية كبيرة على خصوصية المستخدمين، ومن ثم يمكن القول أن هذه الشبكات أصبحت تعد في الآونة الأخيرة وسيلة جذابة لتفاعل وتجاذب الإتصالات، وأصبحت سمة مميزة

[1] محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، مقال منشور في أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، طرابلس لبنان 2019/07/20 منشور في مجلة سلسلة كتاب أعمال المؤتمرات، دورية دولية محكمة تصدر فصليا عن مركز جيل البحث العلمي العام السابع - العدد 26 - يوليو 2019، ص87.

[2] تعتبر شبكة FACEBOOKهي أول شبكة اجتماعية في العالم، انطلقت يوم الجمعة 18 ماي 2006 على يد مارك زوكيربيرج. موقع www.ar.wikupedia.org

[3] Monica Tremblay, réseaux sur internet et sécurité de la vie privée, analyse des impactes de la mondialisation sur la sécurité, Rapport 9.E.N.A.P.l université de l'administration publique, laboratoire d'etude sur les politiques et la mondialisation, Septembre 2010.p.1. disponible sur le site http://www.leppm.enap.ca/leppm/docs/Rapportspdf

[4] وسيم شفيق الحجار، النظام القانوني لوسائل الإتصال الإجتماعي- دراسة قانونية مقارنة حول الخصوصية والحرية الشخصية والمسؤولية والاختصاص، المركز العربي للبحوث القانونية والقضائية لجامعة الدول العربية – بيروت. الطبعة الأولى 2017.ص09.

[5] عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، كلية الحقوق، جامعة طنطا، منشور على الموقع www.law.tanta.edu.eg

لحياة المستخدمين في العصر الرقمي، ولكن في المقابل لذلك أصبحت أيضا تثير مخاوف على خصوصية المستخدمين لها.[1]

الفرع الأول: مفهوم مواقع التواصل الاجتماعي:

لقد غيرت ثورة الويب مجرى الأنشطة الإجتماعية وقلبت نمط الحياة العلائقية ونقلتها من المجتمعات الحقيقية إلى المجتمعات الشبكية، والتي أصبحت تقدم تسهيلات جمة في مجال الإتصال ونشر وتشارك الأفكار والصور والفيديوهات والتعليق على الأحداث اليومية.

أولا: تعريف شبكات التواصل الاجتماعي:

عرفت شبكات التواصل الإجتماعي على أنها عبارة عن منصات اتصال عبر شبكة الأنترنت تسمح للمستخدمين أصحاب المصالح المشتركة بالإنضمام إليها من خلال إنشاء حساب على مواقعها مجانا من أجل تبادل الحوار والمناقشة[2]، كما دأبت أدبيات الفقه في هذا المجال على تعريف وسائل التواصل جتماعي على أنها أية خدمة إلكترونية، أو موقع إلكتروني على الخط أو على شبكة معلوماتية أو على نترنت تتيح إنشاء علاقات اجتماعية أو تجمعات بين أشخاص يتشاركون اهتمامات معينة ويتبادلون معلومات مختلفة ومتنوعة، وهي تسمح للأشخاص تشارك أفكار أو نشاطات أو أحداث أو تعليقات أو نصوص أو فيديو أو غيرها من الأشياء ذات الاهتمام المشترك.[3]

وقد عرفت اللجنة الإقتصادية والإجتماعية الأوروبية وسائل التواصل الاجتماعي بأنها خدمات على الخط تهدف إلى إنشاء مجموعات من الأشخاص و الربط بينها، حيث يتشارك هؤلاء الأشخاص نشاطات واهتمامات مشتركة، أو يرغبون في معرفة الأشياء المفضلة أو نشاطات الأشخاص الآخرين، وتضع هذه الخدمات تحت تصرف هؤلاء مجموعة من الوظائف تسمح بالتفاعل بينهم[4]، وقد عرف المشرع الفرنسي التواصل الإجتماعي عبر الأنترنت من خلال القانون رقم 575/04 المؤرخ في 21 جوان 2004[5]، حيث نصت المادة الرابعة منه على أنه بروتوكول اتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل إلى الجمهور دون قيد، أي محتوى تبادلي من قبل مقدمي الخدمات التقنية.

ومن ثم فإن تعريفات وسائل التواصل الاجتماعي على اختلافها ترتكز على ثلاثة عناصر:

---

[1] تومي فضيلة، إيديولوجية الشبكات الإجتماعية وخصوصية المستخدم بين الإنتهاك والإختراق، مقال منشور في مجلة العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة (الجزائر) العدد 30. سبتمبر 2017. ص 02 نقلا عن:

Alessandro acquisti and Ralph gross, imagined communities, awareness information sharing and privacy on the facebook, pre-proceedings version, privacy enhancing technologies work shop " PET" H john Heinz III school of public policy and management. Carnegie melon university, pitts byrgh.2006.

[2] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات التواصل الاجتماعي دراسة مقارنة، ص 1933، مقال منشور على الموقع: http://www.mKsq.journals.eKb.eg

[3] وسيم شفيق الحجار، مرجع سابق. ص17.

[4]. Avis du Comité économique et social européen sur « L'impact des réseaux de socialisation et leur interaction dans le domaine du citoyen/consommateur » (avis d'initiative) (2010/C 128/12) Journal officiel de l'Union européenne C 128/69.

[5]. Loi n2004/575 du 21 juin 2004, pour la confiance dans léconomie numérique JORGE n 143 du 22 juin page 11168 texte n 02.

- إنشاء سيرة ذاتية من قبل المستخدم.
- وجود أدوات تسمح بإنشاء لائحة بالمعارف والتفاعل معهم.
- تمكين المستخدم من وضع المحتوى الخاص به على الشبكة.[1]

كما تعتبر وسائل التواصل الاجتماعي أنها تقوم على مبدأ تعاقدي، ذلك أن المستخدم حتى يفتح حساب عليها أو يسجل فيها، عليه الإذعان للشروط العامة لاستعمال هذه الوسيلة، ويمكن تقسيم مواقع التواصل الاجتماعي من حيث الإ ستخدام إلى ثلاث أنواع:[2]

الأول: وهو يتكون من ملفات شخصية للمستخدمين وخدمات عامة مثل المراسلات الشخصية، ومشاركة الصور والملفات الصوتية والمرئية والروابط والنصوص والمعلومات، بناء على تصنيفات محددة مرتبطة بالدراسة أو العمل أو النطاق الجغرافي، وذلك مثل موقع: .MY SPACE, FACEBOOK

الثاني: وهو نوع مرتبط بالعمل، بحيث يربط أصدقاء العمل وأصحاب الأعمال والشركات ويتضمن ملفات شخصية للمستخدمين تشتمل على سيرتهم الذاتية وما قاموا به في سنوات دراستهم وعملهم ومن قاموا بالعمل معهم، مثل موقع linked in وهو من أهم أنواع مواقع الشبكات جتماعية.

الثالث: وهو نوع المميزات الإضافية، ويشمل التدوين المصغر، مثل موقع .twitter

ثانيا خصائص شبكات التواصل الاجتماعي:

لقد انتشر استعمال وسائل التواصل الاجتماعي[3]، بشكل مخيف بين الناس وأصبح حاجة يومية لا يمكن ستغناء عنها، تترجم طبيعة الإنسان كمخلوق اجتماعي غير قادر على العيش لوحده وبحاجة للتواصل الدائم مع أقرانه، ومن ثم فلم يعد الأفراد قادرين على الإ ستغناء عن هذه الوسائل التي أصبحت تلبي إحدى الحاجات الأساسية للإنسان، بل امتد ذلك إلى قطاع المؤسسات والأعمال والأشخاص المعنويين، فأصبحت الشركات التجارية ترى أن وجودها على مواقع التواصل الاجتماعي أمر مهم لأغراض الدعاية والترويج واستقطاب الزبائن والتواصل معهم، واستقراء ميولهم حول البضائع والخدمات التي يرغبون في الحصول عليها، ولعل هذا ما جعل عدد المستخدمين على وسائل التواصل الاجتماعي يتزايد بشكل مطرد ومستمر، خصوصا مع وجود عدة أسباب تحفز على استعمالها، كمجانية الخدمات المقدمة وسهولة استعمالها والتواصل مع الغير في كل حين ومكان.[4]

---

[1] Ludovic Pailler, Les réseaux sociaux sur Internet et le droit au respect de la vie privée Bruxelles, Larcier, coll. Droit des technologies, 2012, page07.

[2] مها شبانة أحمد، تأثير توظيف الإعلام الجديد على الجوانب الإدارية في المؤسسات الصحفية، رسالة ماجستير، جامعة المنوفية كلية الآداب، 2016. ص55.

[3] تتعدد وسائل التواصل الاجتماعي ومن أهمها:" my space ,linked In, whats app, twitter, facebook, instgram,imoo,skype
وتتكون الشبكات الاجتماعية عموما من عدة تطبيقات ومواقع أهمها:
-مواقع التواصل الإلكترونية: المدونات الإلكترونية (blogs)، الويكيز wikis، البودكاستس podcasts، المنتديات الإلكترونية.

[4] وسيم شفيق الحجار، مرجع سابق، ص 19.

ومن ثم فإنه مما لا شك فيه، أن تعاظم دور وسائل التواصل الاجتماعي وازدياد عدد المشتركين في شبكة نترنت يعود إلى ما تملكه هذه المواقع من خصائص تميزها عن باقي المواقع الإلكترونية، مما شجع متصفحي الأنترنت على الإقبال المتزايد عليها، ومن جملة هذه الخصائص[1] نذكر منها ما يلي:

- **التفاعلية** ذلك أن المستخدم في مواقع التواصل الإ جتماعي كما أنه مستقبل وقارئ، فهو كاتب ومرسل ومشارك، ومن ثم فهي تلغي السلبية التقنية في وسائل الإعلام القديمة كالتلفاز والصحف، وتعطي حيزا للمشاركة الفعالة بين المستخدمين.

العالمية: يستطيع المستخدم التواصل مع أي شخص آخر في أي مكان من العالم بكل سهولة وفي أي زمن، فهي تلغي الحدود الجغرافية والمكانية.

المجانية في ظل مجانية التسجيل والإشتراك والإ ستقلال يستطيع أي شخص أن يمتلك حيزا على شبكات التواصل الإ جتماعي، فهي ليست حكرا على أصحاب المال أو جماعة دون أخرى.

الحرية: أدت هذه المواقع إلى رفع سقف حرية التعبير والحصول على المعلومات، ذلك أن أي شخص مرتبط بهذه الشبكات له الحرية المطلقة في أن يكون ناشرا وأن يوصل رسالته إلى جميع أنحاء العالم وله أن يناقش أي موضوع مع عدد غير محدود من المستخدمين الآخر ين.

سهولة الإ ستخدام: لا يحتاج رواد هذه المواقع في التعامل معها إلى خبرة معلوماتية ولا إلى خبرة للتفاعل مع محتواها، بل يكفي فقط على المستخدم القيام بعملية التسجيل في موقع التواصل الإ جتماعي باختيار إسم ورقم سري والموافقة على شروط العضوية، ويكون له بعد ذلك حيز خاص به يسمح له بمباشرة أعماله الرقمية بكل حرية.

إعلام متعدد الوسائط تتضمن شبكات التواصل الإ جتماعي محتوى اتصالي يضم مزيجا من النصوص والصور، ومقاطع الفيديو وملفات صوتية.

الفرع الثاني: مخاطر وسائل التواصل الاجتماعي على الخصوصية المعلوماتية

إنه وعلى الرغم من الدور الذي تلعبه شبكات التواصل الإ جتماعي في حياة الأفراد بالنظر إلى كونها أصبحت سمة مميزة في العصر الرقمي، حيث يمكن من خلالها أن يتفاعل المستخدمون في حياتهم اليومية، إلا أنها تثير بعض المخاوف حول أمن وخصوصية البيانات التي يدلي بها المستخدمون عبر هذه الشبكات التي أثرت بما تحمله من بيانات شخصية على الحياة الخاصة للأفراد.

أولا: تداول البيانات الشخصية على مواقع التواصل الاجتماعي وأثره على الخصوصية المعلوماتية:

لقد أصبحت في الوقت الحاضر مواقع التواصل الإ جتماعي تعرض مستخدميها إلى الكثير من المخاطر، لما يتطلبه من ضرورة إدلائهم ببعض البيانات الشخصية، حيث يجب على الشخص الذي يرغب في التسجيل

[1] مجدي محمد عبد الجواد عبد الفتاح الداغر، استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشاعات المتحققة منها، دراسة تطبيقية على القائم بالاتصال بالمؤسسات الإعلامية بالسعودية، مجلة كلية الآداب جامعة الزقازيق العدد 64، مارس 2013. ص542.

على موقع معين من مواقع التواصل الإ جتماعي كالفايسبوك مثلا أن يدلي ببعض البيانات الشخصية مثل سم الشخصي و إسم العائلة وعنوان البريد الإلكتروني وكلمة المرور والجنس وتاريخ الميلاد.. كل هذه المعطيات تعد متعلقة بشخص طبيعي معرف ومحدد ومن ثم فهي معطيات ذات طابع شخصي.

وباعتبار أن وسائل التواصل الإ جتماعي على اختلاف أنواعها مصممة من طرف شركات تجارية، فإنه لا يمكنها أن تقدم خدماتها بشكل مجاني دون أن تحقق منفعة منها، لذلك فإن المقابل هو استفادتها من البيانات الشخصية للمستخدمين والمحتوى المحمل من قبلهم وتحليل توجهاتهم وبيعها إلى شركات تجارية قصد استغلالها في الإعلانات لترويج منتجاتها وسلعها فنموذج أعمال مواقع الشبكات الإ جتماعية يقوم على الإعلانات، وتعتمد في ذلك على المحتوى الذي تقدمه، وبما أن معظم المحتوى المقدم من مستخدمي الشبكات الإ جتماعية هو عبارة عن معطياتهم الشخصية، فإنه لا يبدو غريبا أن يعتبر تبادل هذه المعطيات هو بمثابة المقابل للحصول على الخدمة المجانية التي توفرها هذه الشبكات.[1]

ومن ثمة فليس هناك علاقة مالية مباشرة بين هذه الشبكات ومستخدميها، ولكن في الجهة الأخرى توجد علاقات تعاقدية مالية بين الشبكات الإ جتماعية وأصحاب الإعلانات الذين يتولون تمويل الشبكات، وبالتالي يكون لهذه الشبكات حافز تجاري طبيعي في الإ ستمرار بتحسين عملية تحديد أهدافهم وإعلاناتهم من خلال الإ ستعانة بالبيانات الشخصية لمستخدميها.[2]

ومن المتفق عليه أنه عند قيام المستخدم باستخدام شبكة من شبكات مواقع التواصل الإ جتماعي، فإن هذا الأخير يقوم بالإدلاء بهذه البيانات الشخصية طواعية من أجل الإتصال بهذه الشبكات والحصول على خدماتها، أو قد يقوم بالإدلاء بهذه البيانات دون إدراك أو وعي من جانبه.[3]

1) تنازل المستخدم عن بياناته الشخصية بإرادته عبر مواقع التواصل الاجتماعي: في هذه الحالة يتدخل المستخدم بإرادته لتقديم بعض البيانات الشخصية الخاصة به لمواقع التواصل الاجتماعي، وذلك مثل سم وعنوان البريد الإلكتروني، الجنس، تاريخ الميلاد.. وكذلك بعض البيانات الشخصية المتعلقة بالوظيفة، حيث تشترطها هذه الأخيرة عليه من أجل التمكن من الإتصال بهذه الشبكات والإ ستفادة من خدماتها، كما تلزم كل مستخدم أن يقوم باستكمال ملفه الشخصي من خلال الإدلاء ببعض البيانات الشخصية الأكثر خصوصية، مثل المعتقدات الدينية والسياسية، وإذا كان دائما ما يقال بأن مستخدمي مواقع الشبكات الإ جتماعية يوافقون صراحة على تقديم بياناتهم الشخصية وعلى استخدامها من طرف هذه المواقع في إطار شروط الخدمة وسياسة الخصوصية، إلا أن الموافقة الموضوعية ذات المغزى تفترض أن المستخدمين كانوا على علم بسياسة الخصوصية، وقادرين على فهم اللغة القانونية المعقدة المستخدمة في هذه السياسات، بالإضافة إلى استعدادهم لبذل الوقت في قراءة هذه السياسات، وقادرين

[1] طارق جمعة السيد راشد، مدى حجية رسائل التواصل الاجتماعي النصية smsفي الإثبات دراسة تحليلية مقارنة، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، العدد الثاني 2016.ص45.

[2] توبي مندل وآخرون، مرجع سابق، ص34.

[3] محمد أحمد المعداوي، مرجع سابق، ص43.

على قبول أجزاء معينة من سياسة الخصوصية دون الأجزاء الأخرى وحتى وإن تمكن المستخدم من فعل ذلك فإنه يمكن تغيير سياسة الخصوصية في أي وقت من قبل مزودي الشبكات الاجتماعية.[1]

2) إدلاء المستخدم لبياناته الشخصية عن غير قصد منه: في هذه الحالة تتحصل مواقع التواصل جتماعي على البيانات الشخصية من خلال القيام بتجميعها عن طريق استخدام ملفات الإرتباط "cookies لاستعمالها فيما بعد في الإعلانات المستهدفة(التسويق المباشر)، وفي هذا الشأن تستخدم شبكة الفايسبوك ملفات تعريف الإرتباط على نطاق واسع، حيث تستخدمها في تسجيل مختلف الوظائف بما في ذلك التفاعل مع الإعلانات،كما يمكن لمواقع التواصل الإجتماعي وخاصة موقع facebook أن يقوم بتجميع البيانات الشخصية الخاصة لغير الأعضاء عن طريق استخدام الزر " j'ame ".

في كلا الحالتين فإن مواقع التواصل الإجتماعي هدفها هو السعي إلى جمع كميات هائلة من البيانات الشخصية الخاصة بمستخدميها، وذلك من أجل القيام بأغراض دعائية أو إعلانية بعد تحليل هذه البيانات والتعرف من خلالها على توجهات المستخدمين، أي ما يرغبون وما لا يرغبون فيه، أو العمل على إعادة بيع هذه البيانات الشخصية إلى شركات تجارية، فباعتبار أن وسائل التواصل الاجتماعي على اختلاف أنواعها مصممة من طرف شركات تجارية، فإنه لا يمكنها أن تقدم خدماتها بشكل مجاني دون أن تحقق منفعة، لذلك فإن المقابل هو استفادتها من البيانات الشخصية للمستخدمين والمحتوى المحمل من قبلهم وتحليل توجهاتهم وبيعها إلى شركات تجارية قصد استغلالها في الإعلانات لترويج منتجاتهم وسلعهم.

والحاصل أنه من الصعب جدا من الناحية العملية أن يعترض مستخدمو مواقع التواصل الإجتماعي على جمع بياناتهم الشخصية، طالما أنهم وافقوا على الكشف عنها والإدلاء بها من أجل السماح لهم بالدخول المجاني لمواقع التواصل الإجتماعي، حتى ولو كان المستخدم قد قام بالإدلاء بهذه البيانات دون وعي أو إدراك من جانبه.

ثانيا: أهم المخاطرالتي تشكلها مواقع التواصل الإجتماعي على الخصوصية المعلوماتية:

يبدو أن انتهاك الخصوصية المعلوماتية أصبح أمرا سهلا على شبكات مواقع التواصل الاجتماعي، وذلك بالنظر إلى سهولة اختراق هذه الشبكات، إذ يمكن للكثيرين الوصول إلى البيانات الشخصية لمستخدمي الشبكات الاجتماعية[2]، حيث باتت هذه المواقع الإلكترونية التي يعتقد البعض أنها عالم مثالي يقوم فيه المستخدمون بالتفاعل مع غيرهم من خلال تبادل الصور ونشر تفاصيل حياتهم اليومية، عرضة للاختراق من طرف الغير، ومن جهة أخرى قد تتعرض البيانات الشخصية للمستخدم للإعتداء من طرف مزودي الخدمة لمواقع التواصل الإجتماعي، كما تكون المخاطر على البيانات الشخصية للمستخدم ناجمة عن سلوكاته هو نفسه في التعامل مع هذه المواقع،ومن ثم فإن مجتمع شبكات التواصل الإجتماعي يحتوي على مصادر متعددة تهدد البيانات الشخصية نذكر منها:

[1] خصوصية الشبكات للتواصل الاجتماعي، مركز معلومات الخصوصية الإلكترونية، على الرابط: http://epic.org/privacy/ social net/ أطلع عليه يوم: 2019/12/04على الساعة 20:50.

[2] بارق منتظر عبد الوهاب لامي، مرجع سابق، ص25.

1) المخاطر التي تهدد البيانات الشخصية الناتجة عن اختراق مواقع التواصل الاجتماعي: فشبكات التواصل الإ جتماعية لا تتوافر فيها الحرية الكاملة والأمان لما ينقل عبرها من بيانات شخصية مما يسهل الحصول من خلالها على هذه البيانات بطريقة غير مشروعة عن طريق اختراقها، ويشكل الإ ختراق اعتداء على خصوصية المكان الإفتراضي من طرف أحد الأشخاص غير المأذون لهم بالإطلاع، ويشمل هذا الأسلوب في قيام قراصنة[1] نترنت باستخدام تقنيات وبرامج تتيح لهم الإطلاع على البيانات الخاصة بالمستخدمين، ومن ثم استخدام هذه البيانات في ممارسة أنشطة جنائية[2]، وتمكن دائما هؤلاء المخترقين من التقاط البيانات الشخصية بصورة غير مشروعة من خلال استخدام أساليب تقنية عديدة، كقرصنة كلمات المرور التي تدون في قوائم ملفات كلمات المرور أو الولوج عبر ملفات التجسس التي يزرعها في جهاز الحاسوب الشخصي للمستخدم، فقد يترتب على هذا الإ ختراق حصول المخترق لمعطيات شخصية عن المستخدم قد لا يرغب هذا الأخير في إفشائها للغير، كما يمكن أن يستعملها في عملية التشهير عبر الشبكات من خلال نقل وقائع وبيانات فيها معنى الإساءة أو الإهانة للشخص مما يترتب عليها الحط من كرامته وسمعته، وقد تستعمل هذه البيانات في القيام بفعل الإبتزاز وهو محاولة الحصول على مكاسب مادية عن طريق الإكراه المعنوي للشخص صاحب هذه البيانات وذلك بتهديده بكشف أسراره ومعلوماته الخاصة، وقد أصبحت هذه الصورة من صور الإ عتداء على البيانات الشخصية هي الأكثر انتشارا، حيث بات من المعروف لدى أغلبية مستخدمي شبكات التواصل الإ جتماعي أنه من الممكن سرقة البيانات الشخصية وابتزاز أصحابها أو التشهير بهم[3]، وهذا من دون شك اعتداء صارخ على خصوصية الأفراد.

2) المخاطر التي تهدد البيانات الشخصية من طرف المسؤول عن إدارة مواقع التواصل الاجتماعي: من أخطر صور الإ عتداء على البيانات الشخصية من طرف المزود بخدمة مواقع التواصل الاجتماعي، هو استخدامها لأغراض تجارية، فعلى الرغم من وجود أنماط مختلفة من البيانات إلا أن السياق الدولي يكشف أن هناك تصاعدا في إنتاج البيانات الشخصية[4]، وأن هناك حالة تداخل كبير في توظيف البيانات الشخصية في تحقيق أهداف تجارية، ومن ثم يظهر بصورة واضحة حجم الصراع حول الإ ستحواذ عليها خاصة من خلال ارتباطها بشبكات التواصل الاجتماعي، والتي أصبح لها دور كبير في تصنيف وتخزين ومعالجة البيانات الشخصية، نظرا لارتباط هذه الشبكات وملازمتها للنشاط الإ جتماعي للأفراد، الأمر الذي صاحبه تصاعد في دور شبكات التواصل الإجتماعي في الإ ستحواذ على البيانات الشخصية للمستخدمين[5]، والتي يقوم عليها صناعة الإعلانات التجارية.[6] ويكون الهدف من وراء ذاك عموما هو بيع مواقع التواصل

---

[1] اختلفت الأعمال والاعتداءات التي يقوم بها القراصنة وبذلك تعدد تسمياتهم، فمنهم الهاكرز " hackers " ومنهم الكراكرز " crackers».

[2] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية، الطبعة الأولى 199، ص36.

[3] عثمان بكر عثمان، المسؤولية عن الإعتداء على بيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، جامعة طنطا كلية الحقوق، ص21. مقال منشور على موقع. www.law.tanta.edu.eg

[4] عادل عبد الصادق، مشروع قانون التنظيم عمل كاميرات المراقبة بين الإعتبارات الأمنية والخصوصية، مجلة قضايا برلمانية، مركز الأهرام للدراسات السياسية والإستراتيجية، العدد 64. سبتمبر2017، ص13.

[5] تستحوذ شركتي فيسبوك facebook، وجوجل googleعلى 80% من إعلانات الأنترنت في الولايات المتحدة الأمريكية.

[6] عادل عبد الصادق، مرجع نفسه، ص14.

جتماعي للبيانات الشخصية الخاصة بمستخدميها إلى الشركات التجارية، وهذه خيرة تعتمد على هذه البيانات الشخصية بعد تحليلها إلى إنتاج أنماط من العلاقات يتم استخدامها فيما بعد للحصول على ميزة تنافسية في التسعير والتسويق لزيادة إراداتها، ومن ثم فالبيانات الشخصية التي يتم تجميعها تساعد الشركات التجارية من معرفة أنماط الإ ستهلاك والتنبؤ للسلوكيات، وإجراء أبحاث عن التسويق ومعرفة أذواق المستهلكين، وكنتيجة لذلك نشأت وظائف تحليل البيانات الشخصية ونشأت معها سوق برامج وتطبيقات تحليل هذه البيانات عبر مواقع الأنترنت ومواقع الشبكات الإ جتماعية خصوصا.

لذلك فليس من المبالغ فيه عندما نقول أن شبكات التواصل الإ جتماعي أحدثت تطورا كبيرا فيما يتعلق بالقدرة على جمع البيانات الشخصية والقدرة كذلك على تحليلها، ثم توظيفها لأغراض وأهداف تجارية، وهذا راجع لعدة عوامل أهمها حجم المستخدمين الضخم عالميا لهذه الشبكات، وكذلك ارتباطها في غالب هؤلاء المستخدمين بفئتي الشباب والنساء وهم أكثر فاعلية في حركة البيع والشراء[1]، وهنا تبرز فرص تهديد الخصوصية المعلوماتية للأشخاص، حيث يقوم المشغل أو مزود خدمة موقع التواصل الإ جتماعي ببيع البيانات الشخصية الخاصة بالمستخدمين الذين يترددون على موقعه إلى شركات الإعلان، ثم تقوم هذه الأ خيرة بإعداد قواعد بيانات تصنف من خلالها احتياجات المستخدمين ورغباتهم وأذواقهم.

وتزداد الخطورة إذا علمنا أن البيانات الشخصية سواء التي يدلي بها المستخدم طواعية على مواقع التواصل الإ جتماعي أو التي يتم التنقيب عنها من طرف أصحاب هذه المواقع، تفهرس وتستثمر دون تمكين صاحب هذه البيانات من ممارسة حقوقه عليها، بل دون علمه أصلا، وهذا راجع إلى مجانية الخدمات المبتكرة التي تقدمها مواقع التواصل الإجتماعي ويكون الاستغلال التجاري للبيانات الشخصية هو المقابل في ذلك.[2]

لكن من المتفق عليه أن استخدام البيانات الشخصية الخاصة بمستخدمي مواقع التواصل الاجتماعي لأغراض تجارية يعد عملا غير مشروع، ويشكل تهديدا و اعتداء على الخصوصية المعلوماتية، وهذا ما أكدته محكمة النقض الفرنسية في حكمها الصادر بتاريخ 22 أكتوبر 2013 من خلال اعتبارها أن الإعلانات التي تستغل البيانات الشخصية تشكل عقبة أمام الحق في احترام الحياة الخاصة[3]،كما نجد أن اللجنة الوطنية للمعلومات والحريات CNIL في فرنسا طلبت من موقع facebook إعلامها عن ملفات مستخدميه وطالبت بضرورة أن يكون المستخدم على دراية بنشر معلوماته الشخصية وعن حياته الخاصة وآرائه السياسية والدينية.[4]

3) المخاطر التي تهدد البيانات الشخصية الناتجة عن سوء استخدام الشخص لمواقع التواصل الاجتماعي:في مقابل المنافع التي تؤمنها وسائل التواصل الإ جتماعي فإنه تنشأ عنها مخاطر يتعرض لها المستخدمون قد يكونون هم ذاتهم سببا فيها، وهذا بالنظر إلى طبيعتها المفتوحة وطابعها الدولي العابر

[1] عادل عبد الصادق، مرجع سابق، ص18.

[2] عثمان بكر عثمان، مرجع سابق، ص18.

[3] Cour de casss.1er chambre civile 22 oct 2013, bull.civ. I. n197.

[4] جبالي أبو هشيمة، حماية البيانات الشخصية في البيئة الرقمية، بحيث مقدم إلى مؤتمر العصر الرقمي واشكالياته القانونية، منعقد بكلية الحقوق، جامعة أسيوط في الفترة من 12-13 أفريل .2016. ص30.

للحدود، وما يترتب عنه من إمكانية التعامل مع أشخاص مجهولين، أو يخفون هويتهم الحقيقية[1]، لذلك فمن السلوكات التي تشكل خطرا على خصوصية الأفراد في بيئة مواقع التواصل الإ جتماعي هو الثقة الزائدة للمستخدمين وعدم فهمهم لطبيعة وسائل التواصل الاجتماعي وخصائصها، ولما هو مقبول نشره على صفحات هذه المواقع وما هو غير مقبول، ولما يشكل إفراطا في المشاركة مع باقي المستخدمين، بالإضافة إلى عدم إدراك الكثير من مستخدمي مواقع التواصل لإمكانية استخدام ما ينشرونه من معلومات ضدهم ، والأكثر من هذا للنتائج الخطيرة التي قد تترتب عن سلوكاتهم، فالكثير من المستخدمين مثلا يجرى محادثات عبر هذه الشبكات مع أشخاص لا يعرفونهم، ولكن يطمئنون إليهم لدرجة أنهم يظنون أنفسهم يجرون محادثات حميمية مع أعضاء عائلتهم وأصدقائهم المقربين دون إدراك لخطورة هذا التصرف[2]، كما تعتبر من السلوكات التي تشكل خطرا على البيانات الشخصية هو استعمال جهاز كومبيوتر واحد من قبل جميع أفراد العائلة الواحدة بحيث يكون لأفرادها الوصول إلى كلمة السر و المحتوى وهو ما يتيح فرصة إصدار البيانات الشخصية بصورة واسعة النطاق.

وترتيبا على ماسبق فإنه ينبغي أن يعي المستخدم على وسائل التواصل الإجتماعي أنه في هذه البيئة لا يفكر الآخرون إلا بمصالحهم، وأن الكثير من المعلومات والبيانات الشخصية التي ينشرها يمكن استخدامها ضده وأنه لا يمكنه التحكم بكيفية استعمال الغير لهذه البيانات التي نشرها، وأن عليه قبل مشاركة أي معلومة عنه مع الآخرين partagerيجب عليه التفكير في الآثار السلبية المحتملة لتلك المعلومات إذا أصبحت علنية.[3]

[1] شفيق النجار، مرجع سابق، ص28.

[2] Lothar Deitrmann, Social Media Privacy: A Dozen Myths and Facts Stanford Technology Law Review volume 7. 2012. p14.

متوفر على الرابط: http://stlr.stanford.edu/ أطلع عليه يوم: 2019/11/05 على الساعة 16:15.

[3] شفيق النجار، مرجع سابق، ص 30.

ملخص الفصل الأول:

عرفنا في هذا الفصل أن حق الإنسان في الخصوصية يعتبر جوهر الحقوق والحريات الشخصية، وأن الإعتراف بهذا الحق ما هو إلا مجرد الكشف عنه وليس إنشاء له، ذلك أنه قديم قدم الإنسان وأنه من الحقوق اللصيقة به، ولأن مفهومه يتبدل ويتطور باستمرار تبعا لاختلاف المفاهيم الاجتماعية والاقتصادية والثقافية والسياسية والدينية زمانا ومكانا، أصبح هذا الحق يعد من أكثر الحقوق المثيرة للجدل بين فقهاء القانون منذ زمن بعيد، لذلك كان من الصعب على الفقه القانوني وكذا القضاء على حد سواء الوصول إلى رسم الحدود المنطقية للحق في الخصوصية على الرغم من وجود النصوص القانونية التي تحمي مظاهره، وكثرة الأحكام القضائية المتعلقة بحالات الإعتداء عليه.

لكن بالرغم من ذلك، فليس هناك شك في أن خصوصية الإنسان تحتاج إلى الإعتراف القانوني الذي تظهر أهميته في توفير الحماية الضرورية لهذا الحق إزاء كل تدخل غير مشروع من شأنه الإعتداء عليه والمساس به، خاصة بعد زيادة المخاطر التي تتهدد هذا الحق نتيجة التقدم العلمي والتكنولوجي الحديث، الذي كان سببا في ضرورة الإسراع بالاعتراف بهذا الحق.

ويعتبر المشرع الجزائري واحدا من بين التشريعات التي توجهت نحو الإعتراف بالحق في الخصوصية بمفهومه الشامل واعتباره حقا مستقلا، ويعد الدستور في مقدمة النصوص القانونية التي اعترفت بالحق في الحياة الخاصة في التشريع الجزائري، أين عنى المشرع الدستوري من خلالها بضرورة احترام الحياة الخاصة للأفراد، حيث كان للمشرع الدستوري في دستور 1996 أن اهتم بالحق في الحياة الخاصة، عندما أورد نصين الأول من خلال المادة 39 الواردة تحت عنوان الحقوق والحريات، والتي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون"، والنص الثاني يتمثل في المادة 63 الواردة تحت عنوان الواجبات والتي تنص على أنه "يمارس كل واحد جميع حرياته في إطار إحترام الحقوق المعترف بها للغير لاسيما إحترام الحق في الشرف وسر الحياة الخاصة..."

ثم جاء التعديل الدستوري المؤرخ في 06 مارس 2016 الذي اعترف من خلاله المشرع الجزائري في المادة 46 منه بالخصوصية المعلوماتية، أين نص صراحة على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ولم يكن هذا الحق محلا لاهتمام القوانين الوطنية فحسب، بل امتد إلى اهتمام المنظمات الدولية والإقليمية الخاصة بحماية حقوق الإنسان حيث تعددت المواثيق والاتفاقيات والمؤتمرات الدولية التي أقرت وأكدت حق الإنسان في حياته الخاصة.

ثم تبين لنا ضرورة القاء الضوء على مسألة لا تقل أهمية عن مسألة تحديد مفهوم هذا الحق، وهي تحديد الطبيعة القانونية للحق في الخصوصية، أين انشغل بال الفقه والقضاء منذ زمن بعيد بمسألة تحديد الطبيعة القانونية للحق في الخصوصية باعتبارها تؤثر تأثيرا مباشرا في تحديد الأشخاص الذين يتمتعون به، وظهر لنا أن الإتجاه الغالب يعتبر أن الحق في الخصوصية من الحقوق الملازمة للشخصية.

ثم يثور بعد ذلك التساؤل حول المجال الذي يمكن أن يمتد إليه هذا الحق، سواء تحديد نطاق التمتع به من حيث الأشخاص، أو تحديد نطاقه من حيث المضمون، فأما نطاقه من حيث الأشخاص فإن الشخص الطبيعي يعد الحجر الأساسي في الحماية التي تقررها القوانين للحق في الخصوصية وهو المخاطب بنصوصها، كونه من الحقوق اللصيقة بالشخصية وهي الحقوق التي لا تثبت إلا للإنسان، ومن ثمة عدم إمكانية تمديد قواعد حماية الخصوصية للأشخاص المعنوية، إضافة إلى النقاش والجدل الذي ثار حول مدى انتقال الحق في الخصوصية إلى الورثة، أين يذهب اتجاه إلى تأسيس موقفه بعدم انتقال الحق في الخصوصية إلى ورثة صاحب هذا الحق المتوفي طالما أن الحق في الخصوصية يعتبر من الحقوق اللصيقة بالشخصية التي تزول وتنقضي بزوال الشخصية نفسها ولا يقبل الإنتقال إلى الورثة، أما أنصار الإتجاه الثاني اعتبروا أن الحق في الخصوصية من بين الحقوق القابلة للإنتقال إلى الورثة بعد وفاة صاحبها وذلك انطلاقا من فكرة الإرث المعنوي، أما عن نطاق الحق في الخصوصية من حيث المضمون فهي تلك القيم التي يحميها هذا الحق ضد التدخل الخارجي من الغير، و ركزنا على العناصر المهمة التي لها مساس مباشر بخصوصية الإنسان، أهمها عناصر الخصوصية المتعلقة بالكيان المادي للإنسان، و العناصر المكونة للكيان المعنوي للإنسان، ليتبين بعدها أن ارتباط الخصوصية بالتطور التكنولوجي المعاصر أدى إلى ميلاد مفهوم جديد للخصوصية تمثل في الخصوصية المعلوماتية، نتيجة الخوف والخشية من مخاطر التقنية وأثرها على النظام القانوني ومسائله في سياق حماية الأفراد من مخاطر التقنية التي تهدد حياتهم الخاصة. والذي كان محل موجة تشريعية انطلقت منذ السبعينات من القرن الماضي، وهي التشريعات التي عر ،فت بتشريعات حماية الخصوصية المعلوماتية،والمشر ع الجزائري كان قد لحق حديثا بركب هذه التشريعات، واعترف بالخصوصية المعلوماتية من خلال التعديل الدستوري المؤرخ في 06 مارس 2016 بنص المادة 46 من الدستور، وكذلك بالقانون رقم 07/18 بتاريخ 10 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث يهدف هذا القانون إلى وضع إطار قانوني يحدد نظام معالجة المعطيات ذات الطابع الشخصي والتصدي للآثار المترتبة عن التطور السريع لتكنولوجيات الإعلام والإتصال على الحياة الخاصة.

ثم قادنا الأمر إلى طرح أهم التعريفات التي ساقها الفقه للخصوصية المعلوماتية انطلاقا من كونها قدرة الأفراد في السيطرة على معطياتهم الشخصية وحرصهم أن تضل في سرية، وطبيعة البيانات المكونة للخصوصية المعلوماتية هي نوع من المعلومات يطلق عليها المعلومات الخاصة، كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الإسم، العنوان، رقم الهاتف وغيرها من المعلومات التي تأخذ شكل بيانات تلزم الإلتصاق بكل شخص طبيعي معرف أو قابل للتعريف، وقد تم تصنيف هذه المعطيات الشخصية إلى معطيات شخصية عادية ومعطيات حساسة، ثم ناقشنا الأهمية الاقتصادية والاجتماعية والأمنية التي أصبحت تحظى بها المعطيات الشخصية في عصر تقنية المعلومات وتكنولوجيات الإتصال، وأثر الحق في الخصوصية المعلوماتية على الحق في الوصول إلى المعلومات وعلى حق الدولة في الإطلاع.

وانتهيت بالمخاطر التي تهدد الخصوصية المعلوماتية وهي إما مخاطر مرتبطة بقواعد البيانات وتقنياتها المختلفة وظهور النظام الآلي لمعالجة البيانات، أو مخاطر ناتجة عن استعمال شبكة الأنترنت، أو مخاطر ترتبها وسائل التواصل الاجتماعي.

الفصل الثاني

القواعد القانونية لحماية الخصوصية المعلوماتية

الفصل الثاني: القواعد القانونية لحماية الخصوصية المعلوماتية:

إن المخاطر الناجمة عن التقنية المعلوماتية وشبكات الإتصال الإلكترونية تجاه المعطيات ذات الطابع الشخصي تثير الأهمية الإستثنائية لهذه المعطيات، ولقد كانت هذه المخاطر من العوامل الرئيسية والدوافع الأساسية نحو وجوب سن تشريعات في هذا الحقل بغية توفير الحماية القانونية لهذه المعطيات، ذلك أن القوانين التقليدية المتعلقة بحماية شرف الإنسان وحياته الخاصة عموما، لا تغطي حماية هذا الجانب من الحقوق الشخصية وبعيدة عن توفير حماية للمعطيات الشخصية من مخاطر التجميع والتخزين والمعالجة والوصول إليها في بيئة الإتصالات التقنية الجديدة.[1]

فإذا كانت الحياة الخاصة للأفراد تحظى بحماية دستورية وقانونية في مختلف تشريعات الدول، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا، فإن الحياة الخاصة بصورتها المستحدثة المرتبطة بقواعد البيانات وشبكات الأنترنت والطريق السريع للمعلومات باتت مهددة بالعديد من الإنتهاكات والإعتداءات، حتى أصبحت النصوص القانونية عاجزة أمام هذه الإعتداءات على خصوصيات الأفراد وأسرارهم[2]، لذلك بدت الحاجة ملحة لسد كل فراغ تشريعي في مجال حماية ما يتم تداوله ومعالجته من بيانات شخصية.

وعلى هذا الأساس فقد كان التزايد المستمر في استخدام التكنولوجيا في مجال معالجة المعطيات ذات الطابع الشخصي والتي تمثل الجزء المعنوي من الحياة الخاصة، وكذا تغول شبكات الإتصال العالمية سببا في فرض الإنتقال من حماية الحياة الخاصة بشكل عام إلى الإهتمام بحماية المعطيات الشخصية، ولهذا السبب تضافرت الجهود الدولية والإقليمية لوضع الإطار القانوني لحماية الخصوصية المعلوماتية.[3]

وانطلاقا من هذا الواقع، فقد تبنت غالبية الدول قوانين حماية المعطيات الشخصية وذلك بهدف الإنسجام والتوافق مع الأنظمة القانونية المقدمة في هذا الإطار، وأصبح يوجد في مختلف التشريعات الوطنية قواعد تحمي الخصوصية المعلوماتية، وتتضمن مجموعة من المؤيدات لحماية الأشخاص الطبيعيين المعنيين بمعالجة المعطيات ذات الطابع الشخصي، وذلك من خلال إقرار ضوابط تحكم عملية معالجة البيانات الشخصية من حيث وجوب تحديد الغرض الذي من أجله يتم جمع هذه البيانات وتخزينها ومعالجتها واستخدامها والمدة المحددة لحفظها بالنظر إلى غرض الإستخدام، وكذا عدم الكشف عن البيانات و إفشائها لغير المصرح لهم بذلك.

وكذلك من خلال منح الأشخاص المعنيين بالمعالجة بعض الحقوق وإلزام المسؤولين عنها ببعض الإلتزامات، بالإضافة إلى تكريس مبدأ الإشراف والرقابة غير المباشر للدولة على مباشرة الأنظمة المعلوماتية

---

[1] بولين أيوب، مرجع سابق، ص 292.

[2] محمد أمين الشوابكة، مرجع سابق ص59.

[3] رزق سلمودي، ليندا ربايعة، هديل الرزي، الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، مجلة الجامعة العربية الامريكية للبحوث، فلسطين، مجلد 3، العدد 2، 2017 ص17. متوفر على الموقع:https://www.aaup.edu/

لنشاطاتها في معالجة المعطيات الشخصية من خلال وجود جهة خاصة للرقابة والإشراف، وصولا إلى تكريس الحماية الجزائية من خلال نصوص عقابية.

المبحث الأول: الضوابط القانونية الموضوعية لمعالجة المعطيات ذات الطابع الشخصي:

إن قيام الدولة والأجهزة التابعة لها أو قطاع الأعمال الخاص بإنشاء قواعد البيانات ليس من الأمور المطلقة دون ضوابط، فقد وضعت التشريعات المقارنة مجموعة من هذه الضوابط والضمانات التي تهدف إلى رقابة فاعلة على إنشاء نظم المعلومات وكيفية استخدامها، وذلك حماية للحريات الشخصية ومنها الخصوصية المعلوماتية[1].

لذلك فإنه مما لا شك فيه أن ترتكز قوانين حماية المعطيات الشخصية أثناء معالجتها بشكل أساسي على فلسفة احترام مبادئ حقوق الإنسان* لضمان حماية الحق في الخصوصية وإقرار آليات تضمن تحقيق أهدافه ضمن هذه الفلسفة.

وعليه كان لا بد من الإلتفات إلى ضمان سلامة عملية معالجة المعطيات الشخصية عبر إقرار عدد من المبادئ يتوجب احترامها من قبل المسؤول عن معالجة المعطيات الشخصية، وذلك في مختلف مراحل هذه المعالجة، كمشروعية المعالجة، شفافيتها، نزاهتها، وضرورتها، وحظر معالجة البيانات الشخصية بطريقة تمس بحقوق أصحابها أو بحرياتهم الخاصة والعامة أو تسيء إليهم وتشهر بهم، أو أن تتم المعالجة دون علمهم أو رضا منهم، ومن ثم فإن المعطيات الشخصية لا يجب أن تكون محلا لأية معالجة إلا باحترام مجموعة من المبادئ (المطلب ول)، ومراعاة الحصول على الرضا المسبق للمعني بالمعالجة (المطلب الثاني).

المطلب الأول: مبادئ معالجة البيانات ذات الطابع الشخصي

لقد أقرت معظم القوانين الخاصة بحماية البيانات الشخصية ومنها القانون الجزائري 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي، عددا من المبادئ التي يتوجب احترامها عند كل معالجة لهذه المعطيات كي لا ينتج عن ذلك أي إساءة إلى أصحابها.

لذلك فإنه يجب أن تقوم معالجة المعطيات الشخصية على مبدأ المشروعية في كل مرحلة من مراحل عمليات المعالجة الآلية لهذه المعطيات، وكذا على مبدأ الشفافية من خلال توفير الإعلام الكافي عن عملية المعالجة.[1]

---

[1] عمرو أحمد حسبوا، مرجع سابق، ص91.

* الإرشادات والتوجيهات الأوروبية التي صدرت في سياق حماية المعطيات ذات الطابع الشخصي كالإرشاد الأوروبي 46/95/CE واللائحة الاروبية UE/2018/1725 جاءت كلها مبنية على فلسفة المادة 08 من الإتفاقية الأوروبية لحقوق الإنسان (ECHR) وتعتبر هذه الاتفاقيات التابعة لمجلس أوروبا بالغة الأهمية في هذا المجال، إذ تحتوي على أحكام صريحة لحماية البيانات الشخصية حيث تنص في مادتها الثامنة أنه:

- للجميع الحق في حماية بياناتهم الشخصية التي تعنيهم.
- يجب معالجة هذه البيانات بشكل عادل لأهداف محددة وعلى أساس موافقة الشخص وعلى أساس مشروع آخر ينص عليه القانون، وللجميع الحق في الوصول إلى البيانات التي تم جمعها عنهم والحق في أن يتم تصحيحها.

يخضع الإلتزام بهذه القواعد إلى رقابة من هيئة مستقلة.

الفرع الأول: مبدأ مشروعية المعالجة الآلية للمعطيات الشخصية:

تقتضي حماية المعطيات ذات الطابع الشخصي أن يكون مبدأ المشروعية هو الأساس الذي تقوم عليه عملية معالجتها، أي أن تكون كل مرحلة من مراحل المعالجة الآلية لهذه المعطيات قائمة على أساس مشروع، بدءا من جمع وتسجيل البيانات، انتهاء بإيصال المعلومات المعالجة إلى الغير.[2]

أولا: مشروعية معالجة المعطيات الشخصية:

لقد نص المشرع الجزائري[3] في المادة الثالثة البند"أ" من القانون 07/18 على أنه "يجب أن تكون المعطيات الشخصية معالجة بطريقة مشروعة ونزيهة"، وتقتضي مشروعية المعالجة أن تكون العمليات التي تتم آليا بهدف استغلال المعطيات الشخصية عن طريق الربط والتقريب ودمج معطيات شخصية مع معطيات أخرى وتحليلها للحصول على معلومات ذات دلالة خاصة، قائمة على عدم الإعتماد على بيانات شخصية غير صحيحة أو غير دقيقة، وهذا ما أكده المشرع في المادة 03 الفقرة "د" من نفس القانون، حينما أوجب أن تكون المعطيات الشخصية المعالجة صحيحة وكاملة ومحينة إذا اقتضى الأمر، خاصة إذا كان الهدف من ذلك هو الحصول على حكم أو تقييم لشخصية الإنسان، كون النتائج التي يمكن الوصول إليها من عملية دمج وتحليل بيانات غير صحيحة ستكون غير صحيحة أيضا، وهذا من شأنه إلحاق الضرر بالشخص المعني بالمعالجة.[4]

ومن ثمة فإن مصطلح المشروعية يفيد أن كل معالجة للمعطيات الشخصية يجب أن تتم وفق احترام المقتضيات القانونية اللازمة، والتي تستلزم أن تكون بحسن نية وبعلم من الشخص المعني، وتستند إلى مبررات كافية ومشروعة، أو أن تكون لازمة لحماية مصالح مشروعة للمعني بالمعالجة أو للمسؤول عنها، وفي كل الأحوال فإن المعالجة تكون مشروعة إذا كانت هناك مصلحة مشروعة تبررها بشرط أن لا تنصب إلا على الحد الأدنى من المعطيات الشخصية[5] .

---

[1] منى الأشقر جبور، ومحمود جبور، مرجع سابق، ص122.

[2] بولين أيوب، مرجع سابق، ص459.

[3] يقرر التوجيه الأوروبي 46/95 ضرورة التعامل مع البيانات الشخصية بالشروط التي نص عليها في المادة 06 ومنها أن تكون المعالجة مشروعة ونزيهة.

تنص المادة 06 من القانون الفرنسي 17/78: على المعالجة النزيهة والمشروعة.

Les données sont collecteés et traiteés de manières loyale et licite ».

تنص المادة 03 من القانون المغربي 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي "يجب أن تكون المعطيات ذات الطابع الشخصي معالجة بطريقة نزيهة ومشروعة".

تنص المادة 10 من القانون التونسي 2004/63 المتعلق بحماية المعطيات الشخصية: "يجب أن تتم معالجة المعطيات الشخصية بكامل الأمانة".

[4] بولين أيوب، مرجع نفسه، ص469.

[5] أمنار إبراهيم، مرجع سابق، ص75.

كما تقتضي المشروعية أيضا في معالجة المعطيات الشخصية، عدم استخلاص حكم أو تقييم لشخصية الإنسان من خلال البيانات التي سبق جمعها وتخزينها فقط، دون البحث في الظروف والأحوال الأخرى التي تخص كل حالة على حدى.[1]

أما عن مصطلح أن تكون المعالجة نزيهة فإنه ينطوي على تقدير معنوي وأخلاقي أكثر منه قانوني، يكون للقضاء دور أساسي في تقديره، وقد قضت محكمة الدرجة الثانية بباريس في قرارها الصادر بتاريخ 1985/12/16 بأن الطريقة التي تم بمقتضاها جمع المعلومات حول ملائمة الشخص بغير علمه، تعتبر طريقة غير نزيهة[2].

ومبدأ مشروعية معالجة البيانات الشخصية ينبغي أن يكون ضابطا لجميع مراحل هذه العملية، وذلك كما يلي:

1) مشروعية جمع وتسجيل البيانات الشخصية: باعتبار أن البيانات الشخصية مرتبطة بشخص صاحبها مثل اسمه، وحالته الاجتماعية، موطنه، حالته الصحية، صحيفة سوابقه القضائية، رقم حسابه المصرفي، عنوان بريده الالكتروني، عنوانه الالكتروني، بالإضافة إلى بياناته الحساسة كمعتقداته الدينية والسياسية والفلسفية وانتمائه النقابي وغيرها من البيانات التي تسمح بصورة مباشرة أو غير مباشرة بتعريف الشخص أو جعله قابلا للتعريف، فإن الأساس الذي يقوم عليه جمع وتسجيل هذه البيانات حتى يكون مشروعا، يقتضي أن يتم بناء على موافقة الشخص المعني بالمعالجة والذي تتعلق به هذه البيانات، أو أن يتم بناء على نص قانوني صريح في الحالات الاستثنائية التي لا يتطلب الأمر فيها الحصول على موافقة هذا الأخير.[3]

فإذا كانت البيانات التي تمكنت الجهة المسؤولة عن المعالجة والقائمة على قاعدة بيانات في قطاع ما، من الوصول إلى بيانات شخصية ثم تغذية النظم المعلوماتية بأجهزة الكومبيوتر التابعة لها دون موافقة وعلم الأشخاص أصحاب هذه البيانات كانت عملية التجميع غير مشروعة.

لذلك فقد نصت المادة 06 من التوجيه روبي رقم 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية وحرية انتقال وتداول هذه المعطيات في هذا الإطار" أن البيانات ذات الطابع الشخصي يجب أن تجمع بطريقة مشروعة ".

2) **مشروعية تخزين ونقل المعلومات إلى الغير (إيصال المعلومات):** تقتضي مشروعية تخزين البيات الشخصية أن يكون تخزين هذه البيانات متناسبا مع الهدف من إنشاء قاعدة البيانات وأن يكون التخزين محدد المدة.

[1] Eric meillan, les menaces à la sécurité des systèmes d'information la réponse des institution francaise. Revue internationale de police criminelle.mai-juin 1991.page30.

[2] André lucas. Jeans deveze et jeans frayesinet op.cit. page126.

[3] Jacques robert, Jean duffar. Droit de Lhomme et libertés fondamentale, domat droit public, monchrestien, textenso edition.8 eme edition 2009.page50.

فأما عن مسألة التناسب بين عملية تخزين البيانات الشخصية والهدف من إقامة قاعدة النظام المعلوماتي، فإن المقصود بها أن تكون البيانات الشخصية التي تم تغذية جهاز الكومبيوتر بها لازمة وضرورية للوصول إلى الهدف المقصود من إنشاء النظام المعلوماتي.[1]

وأما عن مسألة تخزين البيانات لمدة محددة، فإن مشروعية التخزين للبيانات الشخصية يقتضي أن يكون مؤقتا وليس أبديا، la durée limitée de conservation،وهذا يعني أنه لا يمكن الإ حتفاظ بالمعطيات الشخصية لفترة غير محددة، بل فقط لفترة زمنية لا تتجاوز المدة الضرورية واللازمة لإنجاز الغايات التي تم لأجلها جمع البيانات الشخصية ومعالجتها.

ومن الغالب أن تتأثر مدة حفظ البيانات مباشرة بالهدف المرجو من عملية المعالجة، لذلك يفترض على المسؤول عن المعالجة وهو القائم على تنظيم عمل النظام المعلوماتي أن يحدد هذه المهلة على ضوء طبيعة البيانات والهدف من معالجتها، بحيث يتم محوها أو إتلافها أو تشفيرها بعد تحقيق هذا الهدف وعدم تركها محفوظة على وجه نهائي ودائم بالملفات الآلية.

وعلى هذا الأساس نصت المادة التاسعة الفقرة " ه " من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي أنه "يجب أن تكون المعطيات ذات الطابع الشخصي محفوظة بشكل يسمح بالتعرف على الأشخاص المعينين بالمعالجة خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي تم من أجلها جمعها ومعالجتها"، وهو الأمر الذي نجده في القوانين المقارنة المتعلقة بحماية المعطيات الشخصية[2].

وهو المبدأ الذي أكدته المادة 06 الفقرة الأخيرة من التوجيه الأوروبي 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية انتقال المعطيات[3]، وتعتبر مسألة تخزين المعطيات الشخصية لمدة محددة ذات أهمية كبيرة في إطار حماية الحق في الخصوصية، وذلك لارتباطها بحق آخر وهو الحق في النسيان " le droit a l'oubli "[4]، وقد عرفت اللجنة الوطنية للمعلوماتية والحريات بفرنسا (CNIL) الحق في النسيان الرقمي بأنه الحق الذي يخول صاحبه مكنة السيطرة من حيث الزمان

[1] Antoine latreille, La protection juridique des bases de données éléctronique, petites affiches n 51 du 28 avril 1995 page 14. disponible sur le site : http://www.labase.lextenso.fr/revue.

[1]Larticle 06 de la loi Fransaise n 78/17du 06janvier 1987 relative a l informayique aux fichiers et aux libertes modifiant par la loi n 2004/801 du 06 aout 2004 relative a la protection des personnes physiques a l'egard des taitements de donnees a caractere personnele dispose que : Les données a caractère personnelles sont conservées sous une forme permettant l'indentification des personnes concernées pendant une durée qui n' excède pas la durée nécessaire aux finalités pour les quelles elles sont collecteés et traiteés.

نصت الفقرة 3 " ه" من القانون 09/08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي للملكة المغربية المؤرخ في 18 فيفري 2009 على أنه "يجب أن تكون المعطيات ذات الطابع الشخصي محفوظة وفق شكل يمكن من التعرف على الأشخاص المعنيين طوال مدة لا تتجاوز المدة الضرورية لإنجاز الغايات التي تم جمعها ومعالجتها لاحقا من أجلها".

[3] Article 6 : Les états membre prévoient que les données à caractère personnel doivent etre : conservées sous une forme permettant l'indentification des personnes concernées pendant une durée nexédent pas celle nécessaire a la réalisation des finalités les quelles, elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

[4] Roymond lindon. Dictionnaire juridique. Les droits de la personnalité, dalloz. Paris, 2003.page271.

على بياناته الشخصية، بغية الحصول على حذفها أو محوها عندما يرغب في ذلك"، في حين عرفه جانب من الفقه على أنه حق يخول للشخص الطبيعي مكنة محو معلومات تخصه أو طلب التوقف عن نشرها بعد مرور فترة زمنية معينة[1] .

وينحصر مجال تطبيق الحق في النسيان الرقمي فيما يسمى بالآثار الإلكترونية أو الذكريات الرقمية، والمقصود بها كل البيانات المتعلقة بنشاط الشخص خلال استخدامه لنظام معلوماتي أو وسيلة إتصال إلكترونية كشبكات نترنيت ومواقع التواصل الإ جتماعي.

وانطلاقا من هذا فقد أوصت اللجنة الوطنية الفرنسية للمعلوماتية والحريات (CNIL) أن يتم مسح المعطيات المتعلقة بمستعملي شبكة الأنترنت، حيث تكون لهم صفة مستقرئين خلال مدة قصوى لا تتجاوز سنة واحدة بعد تجميعها، كما اقترحت هذه اللجنة أيضا أنه عندما يتعلق الأمر ببيانات خاصة بأشخاص تجمعهم علاقة تعاقدية مع المسؤول عن المعالجة، يجب ألا يتجاوز مدة الإ حتفاظ بهذه البيانات مدة وجود أو تنفيذ هذا العقد[2].

ويرى الفقه في هذا السياق أن المدة القصوى للاحتفاظ بالبيانات المخزنة في قواعد البيانات تختلف من قاعدة بيانات إلى أخرى، فمدة الإ حتفاظ بالبيانات الشخصية التي تجمع عن الموظفين تختلف عن تلك التي تجمع في المجال الطبي لمتابعة المرضى مثلا.

وتجدر الإشارة إلى أن المشرع قد أعطى للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي صلاحية ذن بحفظ المعطيات الشخصية رغم انتهاء المدة والأجل المحدد لحفظها، وذلك بناءا على طلب المسؤول عن المعالجة إذا تعلق الأمر بغايات تاريخية أو علمية أو إحصائية، وأن تكون هناك مصلحة مشروعة، حيث تنص المادة التاسعة من القانون 07/18 في فقرتها الأخيرة أنه "يمكن للسلطة الوطنية في حالة وجود مصلحة مشروعة بناءا على طلب من المسؤول عن المعالجة أن تأذن بحفظ المعطيات ذات الطابع الشخصي لغايات تاريخية أو إحصائية أو علمية بعد المدة المشار إليها في الفقرة هـ من نفس المادة"

والملاحظ هنا أن المشرع الجزائري لم يحدد المدة التي يمكن أن تأذن بها السلطة الوطنية للاحتفاظ بالمعطيات الشخصية، مما يعني ترك هذه المسألة للسلطة التقديرية لهذه اللجنة لتحديد هذه المدة، كما أن المشرع قد حصر إمكانية منح الإذن في الغايات التاريخية والعلمية والإحصائية فقط، ومن ثم لا يجوز للسلطة الوطنية أن تأذن بحفظ المعطيات لغايات أخرى غير هذه الغايات.

والحكمة من تحديد مدة الاحتفاظ بالمعطيات الشخصية محل المعالجة هي توفير إحدى الضمانات الوقائية لحماية الحق في الخصوصية، ذلك أن الإ حتفاظ ولمدة طويلة ببيانات قابلة للتغيير والتطور يؤدي

[1] Jean-Christophe Duton et Virginie Bechtle, droit a l'oubli numirique.une vide juridique Mars 2010 disponible sur le site : https://www.village-justice.com/articles/droit-oubli-numerique-juridique,7614.html visité le 07 / 12/ 2019.

[2] Thibault verbiest, et Etienne wery, le droit de l'internet et de la société de l'informatique, droit européen, belge et francais, lacier, bruxelles, Belgique 2001 page 445

استرجاعها بعد مدة طويلة من الزمن إلى الإضرار بصاحبها، واسترجاعها قد يعطي صورة غير حقيقية عن الشخص مما قد يلحقه ضرر جراء ذلك.

أما مشروعية نقل وإيصال المعلومات إلى الغير بعد عملية معالجة البيانات الشخصية باعتبارها الوظيفة الأساسية لنظم المعلومات، فإنها تقتضي أن يقتصر هذا النقل إلا على الجهات والأشخاص المتوقع اطلاعهم على هذه البيانات طبقا للغرض من نظام المعلومات، وعدم إيصالها إلى من ليس لهم الحق أو الصفة في الإطلاع عليها، وهذا فيه حماية لخصوصية الأفراد في مواجهة توسع قواعد نظم المعلومات في نشر المعلومات الشخصية على أوسع مدى تحقيقا للربح المادي.[1]

ثانيا: مشروعية الهدف المعلن من معالجة المعطيات الشخصية

لقد تضمنت جميع النصوص القانونية التي صيغت في إطار حماية المعطيات الشخصية مبدأ الهدف المعلن والمحدد والمشروع، وضرورة الإلتزام بهذا الهدف والغاية طوال مدة المعالجة، ومن ثمة يقتضي الأمر أن يكون تجميع المعطيات ذات الطابع الشخصي قد تم لغايات محددة ومعلنة ومشروعة، وأن تكون كل معالجة لاحقة متناسبة مع هذه الغايات، وترتيبا على ذلك يستلزم هذا المبدأ توفر أمرين هما:

1) **الغاية المشروعة:** يجب أن تكون الغاية من تجميع المعطيات الشخصية والأغراض من معالجتها مشروعة من خلال كونها واضحة ومحددة ومحترمة طوال فترة استمرار العملية واستخدام البيانات والاحتفاظ بها، ولا يجوز استخدام البيانات الشخصية المحفوظة لأهداف أخرى غير تلك التي تم الإعلان عنها، ومن خلال تحديد الهدف يمكن معرفة البيانات الضرورية لعملية المعالجة ونوعيتها.[2]

ومن ثمة فإن أي استعمال للمعطيات الشخصية يجب أن يحدد بدقة وحصريا على أساس غاية محددة بشكل واضح ومسبق، حيث يلزم في كل تجميع لهذه المعطيات أن يكون ضروريا من أجل الوصول إلى الأهداف المعلن عنها مسبقا من قبل الجهة التي تجمع هذه المعطيات، والتي يمكن أن تكون إدارة عمومية أو إدارة أعمال، فلا يجوز على سبيل المثال استخدام البيانات التي جمعت لغاية إدارة شؤون المواطنين في قطاع معين لأغراض وغايات أخرى كتوجيه إعلانات دعائية لهم تخص حملات انتخابية، أو استعمالها في جمع توقيعات انتخابية لفائدة مترشحين معينين، وقد اعتبرت في هذا السياق محكمة الإستئناف بباريس في قرارها الصادر عن الغرفة الإجتماعية بتاريخ 31 ماي 1995 بأنه لا يمكن استعمال ملفات الأجراء وعناوينهم الإلكترونية لغاية الدعاية السياسية، وأن البيانات الشخصية المسجلة في برنامج الحاسوب « logiciel » من أجل حجز تذاكر النقل، لا يمكن استعمالها من طرف صاحب قاعدة البيانات لمراقبة نشاط العمال.[3]

[1] محمد عبد المحسن المقاطع، مرجع سابق، ص254.

[2] منى الأشقر جبور، محمود جبور، مرجع سابق، ص122.

[3] La CNIL, guide pour les employeurs et les salaries, edition 2008 page 12 disponible sur le site : http://www.cnil.fr .visité le 07/12/2019

وفي سياق مرتبط فإذا كان المسؤول عن معالجة المعطيات الشخصية ملزم باحترام الغايات التي تم على أساسها تجميع هذه المعطيات وعدم الخروج عن الأهداف التي على أساسها تم جمع المعطيات في البداية، فإن هذا الإلتزام يبقى نفسه عندما يتم إحالة هذه المعطيات إلى هيئة أو إلى شخص آخر، حيث يلزم أن يكون استعمال المعطيات الشخصية في هذه الحالة من أجل تحقيق نفس الغرض والأهداف.

والمشرع الجزائري على غرار باقي التشريعات التي نظمت عملية معالجة المعطيات الشخصية أوجب في المادة 09 من القانون 07/18 أن تكون المعطيات الشخصية مجمعة لغايات محددة وواضحة ومشروعة، وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات.

2) **ملائمة البيانات**: وهو ما يعبر عنه في كثير من الكتابات بمبدأ التناسبية principe de proportionnalité، ويستلزم هذا المبدأ أن تكون المعطيات ذات الطابع الشخصي مناسبة وملائمة وغير مفرطة بالنظر إلى الغاية التي تم على أساسها تجميع هذه المعطيات، بحيث لا تجمع إلا البيانات الشخصية التي تخدم الوصول إلى هذا الهدف بصورة حصرية.[1]

فالأمر هنا يتعلق بالحرص على عدم جمع البيانات بطريقة مبالغ فيها ولا حاجة للمسؤول عن المعالجة بها في خدمة الهدف وغايات المعالجة، حيث يلزم الأمر أن تبنى كل معالجة على معطيات شخصية تجمعها علاقة مباشرة بالغايات التي حددت ابتداء للمعالجة، ومن الأمثلة التي يمكن أن نسوقها في هذا الإطار أنه في عملية معالجة ملفات زبائن لوكالات نقل المسافرين، أن نتخيل سببا يستدعي طلب رقم بطاقة الضمان جتماعي من الزبون أو معلومات عن محيطه العائلي أو المهني.

وقد تطرق المشرع الجزائري بوضوح إلى هذه المسألة عندما نصت المادة 09 الفقرة "ج" على أنه يجب أن تكون المعطيات الشخصية ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها، وقد جاء هذا النص متطابقا بشكل تام مع ما جاء به التوجيه الأوروبي رقم 46/95 المشار إليه سابقا حيث نصت المادة 6 الفقرة "ب":

Les états membres prévoitent que les données à caractère personnel doivent etre : collectées pour des finalités déterminées, explicites et ligitimes et ne pas etre traiteés ultérieurement de manière incompatible avec ces finalités.

وهو نفس النص تقريبا الذي أخذ به المشرع الفرنسي في المادة 06 من القانون 17/78 المعدل بالقانون 2004/801 السالف ذكرهما.

وقد أشارت كل من المحكمة الأوروبية لحقوق الإنسان ومحكمة العدل الأوروبية إلى هذا المفهوم في العديد من قراراتها، حينما اعتبرت التدخل في الحياة الخاصة ممكنا ومقبولا عندما يتوفر مبدأ الملائمة الذي يمكن قياسه على مدى توازنه مع شرعية هذا التدخل ومبرراته المشروعة كالمصلحة العامة.[2]

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص123.

[2] قرار المحكمة الأوروبية لحقوق الإنسان المؤرخ في 02 أوت 1984 رقم 8691/79 متوفر على الموقع:

لكن ما يمكن الإشارة إليه أن الطابع الملائم والمناسب وغير المفرط، يبقى طابعا شخصي أكثر منه موضوعي، لذا فقد يثير صعوبة في التطبيق من حيث تقدير مدى التناسب والملاءمة فضلا عن صعوبة في الإثبات.[1]

ومن جهة أخرى فإن شرط ملائمة المعطيات الشخصية المطلوبة لعملية معالجتها في ملف معين يقتضي أيضا أن تكون هذه الأخيرة صحيحة ومحينة، وإذا اقتضى الأمر أن يتم اتخاذ كل التدابير اللازمة والمعقولة من أجل تصحيح المعطيات الخاطئة أو غير المكتملة بالنظر إلى الغايات التي تم من أجلها تجميع أو معالجة هذه المعطيات، لذلك فقد نصت المادة 09 الفقرة "د" من القانون 07/18 أنه "يجب أن تكون المعطيات الشخصية صحيحة وكاملة ومحينة إذا اقتضى الأمر"*، وبالتالي فإن المسؤول عن المعالجة يلتزم بعدم تجميع بيانات خاطئة عن الشخص أو غير محينة، لأن ذلك فيه إساءة إلى الشخص المعني بالمعالجة وإضرار بحقوقه وحرياته، ولا تفيد صحة المعلومات أن تكون مطابقة للحقيقة فقط، وإنما أن تكون صحيحة بالنظر إلى الغايات من تجميع هذه المعطيات في البداية ومعالجتها فيما بعد، ومن أخطر المضار التي يمكن أن تصيب المعني بالمعالجة جراء معالجة معطيات ناقصة وغير صحيحة مخزنة آليا عنه، هو فقدانه لحقوق أخرى كثيرة، فعلى سبيل المثال عندما يتم تداول معلومات ناقصة وغير صحيحة عن فرد من الأفراد كان قد تقدم بها لمؤسسة الضمان الإجتماعي للحصول على مساعدات معينة من هذه المؤسسة، ثم يتفاجأ برفض طلبه، رغم إصرار واعتقاد ذلك الشخص بأحقيته لهذه المساعدة، في حين أن مؤسسة الضمان الإجتماعي استندت في هذا الرفض إلى ما هو متوفر لديها من معلومات شخصية تحصلت عليها من هيئات حكومية أخرى أسست عليها قرارها، على الرغم من أن تلك المعلومات غير صحيحة وغير دقيقة كانت نتيجة معالجة بيانات شخصية خاطئة،[2] وهنا يقودنا الحديث إلى ضمان حق الشخص المعني بالمعالجة في طلب تصحيح بياناته الشخصية في حال كانت معالجة بياناته الشخصية مخالفة لأحكام مبدأ المشروعية بسبب نقصها أو عدم صحتها، وهو ما سوف نعرضه لاحقا.

---

http://www.doctrine.fr/d/CEDH l'affaire malone contre royaume uni .visite le 07/12/2019 a 23:45

[1] André LUCAS jeans DEVEZE et jean FRAYSSINET. Op.cit page 1271

* تنص الاتفاقية الأوروبية لحماية الأشخاص الطبيعيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي رقم 108 المؤرخة في 28 جانفي 1981 في المادة 5 منها بعنوان نوعية المعطيات أن المعطيات الشخصية الخاضعة للمعالجة هي معطيات صحيحة وعند الاقتضاء محينة"

-تنص المادة 4 من الفقرة "د" من اللائحة الأوروبية رقم 2018/1725 المؤرخة في 23 أكتوبر 2018 المتعلقة بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي والتي عوضت الإرشاد الأوروبي 46/95 السالف الذكر.

Les données à caractère personnel doivent etre : « exates et si nécessaire tenues à jour »

-تنص المادة 06 الفقرة الرابعة من القانون الفرنسي 17/78 المتعلق بالمعلوماتية والملفات والحريات المعدلة بالقانون 41/2016 المؤرخ في 26 جانفي 2016: « Un traitement ne peut porter que sur des données à caractère personnel qui satisfant aux conditions suivantes: elles sont exates. Complètes et si nécessaire, mise à jour »

[2] محمد عبد المحسن المقاطع، مرجع سابق، ص104.

الفرع الثاني: مبدأ الموافقة المسبقة للمعني بالمعالجة:

ترتكز القوانين المعمول بها في مجال حماية الخصوصية المعلوماتية بشكل كبير وأساسي على مدى موافقة صاحب المعطيات الشخصية لمعالجة هذه المعطيات، إذ يمكن لهذا الأمر أن يعطي انطباعا بنوع من السيطرة للشخص المعني على معطياته الشخصية، فماذا يقصد بهذا المبدأ وهل ترد عليه استثناءات؟

أولا: المقصود برضا المعني بالمعالجة:

تقضي المادة 07 من القانون 07/18 أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني صاحب هذه المعطيات، وعلى هذا الأساس فإنه من حيث المبدأ لا يمكن معالجة المعطيات الشخصية المتصلة بالشخص إلا إذا أعرب المعني بالمعالجة عن موافقته المسبقة.*

ويعتبر الرضا أحد الإستثناءات الخارجة عن القواعد الأصولية التي تحكم التشريعات الجنائية باعتبار أن قواعدها من النظام العام ولا تكاد تترك لإرادة الأشخاص سبيلا، خاصة إذا تعلق الأمر بالحقوق الشخصية اللصيقة بالإنسان، فالصورة التي يغلب فيها وصف الرضا تنحصر في إباحة المساس بالحق في الخصوصية ومن ثم عدم مساءلة من يقوم بالإعتداء عليه.[1]

والملاحظ أن أغلب الفقه لم يهتم بوضع تعريف للرضا، حيث نزل الغالب الأعم منه على مسلك المشرع في عدم تناول الرضا بالتعريف، وإنما اقتصر التصدي لهذا المبدأ على النطاق الذي يبين مدى اعتباره سببا للإباحة من عدمه، لذلك فإن المعالجة الفقهية لمبدأ الرضا أقيمت في منهج استنباطي[2]، لكن لا يمكن اعتبار أن فكرة الرضا تفتقر إلى سندها من التشريع، وإنما هو منظم قانونا على نحو لا يثير الخلاف في طبيعته ونطاقه.

وعلى هذا الأساس سوف نحاول أن نتناول أهم المحاولات الفقهية في شأن تعريف الرضا، حيث يعرفه بعضهم أنه "الإذن المعطى بواسطة شخص يدور في نطاق القانون الخاص، إلى شخص آخر على ما هو

---

* وقد نص على هذا المبدأ كل من المشرع: المغربي في المادة 04 من القانون 08/09 المتعلق بحماية الأشخاص الذاتيين في مجال معالجة المعطيات ذات الطابع الشخصي "لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا إذا كان الشخص المعني قد عبر بما لا يترك مجالا للشك عن رضاه عن العملية أو مجموع العمليات المزمع إنجازها..."

المشرع التونسي في المادة 27 من القانون 2004/63 المتعلق بحماية المعطيات الشخصية:" فيما عدا الصور المنصوص عليها بهذا القانون أو القوانين الجاري بها العمل، لا يمكن معالجة المعطيات الشخصية إلا بالموافقة الصريحة للمعني بالأمر..."

المشرع الفرنسي في المادة 32 من القانون 801/2004 المعدل للقانون 17/78:

« Sauf consentement exprés de la personne consernée, les données à caractère personnel recueillies par les prestataires de services de certification éléctronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures éléctroniques doivent l'être directement aux prés de la personne concernée ... »

[1] خالد بن محمد عبد الله الشهري، رضا المجني عليه وأثره على المسؤولية الجنائية –دراسة مقارنة بين الشريعة والقانون مع التطبيق بين أحكام القضاء الشرعي والوضعي، مذكرة لنيل شهادة ماجيستار، قسم العدالة الجنائية، معهد الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السنة الجامعية 2000-2001، ص 60.

[2] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، مرجع سابق، ص 203.

محل للحماية من لدن القانون الوضعي، أو ما يصيب بالضرر ما تعلق بصاحب الرضا[1]، وعرفه بعضهم الآخر بأنه "إذن صادر بإرادة حرة حقيقية، عن شخص من أشخاص القانون الخاص أو العام، حال تعامله ضمن إطار القانون الخاص إلى شخص آخر للقيام بفعل مخالف للقانون من شأنه تعريض المجني عليه للضرر أو الإيذاء شريطة عدم المساس بالمصلحة العامة".[2]

كما أثير تعريف الرضا من زاوية أخرى باعتباره تعبير عن إرادة القبول سواء عن رغبة لوقوع فعل المساس بالحق أم كان القبول عن غير رغبة، وقد يصدر هذا التعبير في صورة صريحة تعارف الناس عليها، وقد يصدر بصورة ضمنية تستخلص من الظروف والملابسات التي تحيط بالواقعة محل الرضا.[3]

وذهب جانب آخر من الفقه إلى تعريف الرضا على أنه الإذن أو التصريح لشخص أو أكثر لارتكاب عمل محظور قانونا قد يؤدي إلى الإضرار بمصلحة أو تعريضها للخطر بشرط أن تكون تلك المصلحة متعلقة بمصدر الإذن أو التصريح[4]، والإتجاه السائد في الفقه العربي يذهب إلى تعريف الرضا بأنه تعبير عن الإرادة واتجاهها نحو قبول الإعتداء على مصلحة يحميها القانون، ويشترط في هذه الإرادة علمها التام بما يصدر في شأنه الرضا.[5]

ونتيجة لهذه التعاريف يمكن القول أن الرضا هو إرادة إيجابية في تفكير الإنسان يترتب عليه أن يسمح بارتكاب الفعل محل التفكير فيه والعلم والإدراك التامان بآثاره، ويستخلص مما تقدم من تعاريف أن الرضا يقوم على مجموعة من العناصر تتمثل في:

- **الإرادة**: وتمثل الحالة النفسية التي تسبق في الوجود الجانب الإرادي، وتدور الإرادة معه وجودا وعدما ويعكس اتجاه الإرادة القوة النفسية المتحركة تجاه واقعة معينة تهدف إلى نتيجة بذاتها، من خلال العلم بالعناصر المحيطة بالواقعة وحرية الاختيار[6].

- **المعني بإصدار الرضا**: وهو الشخص محل الحماية القانونية التي يهدف إليها المشرع ممن يقع عليه الفعل أو يتناوله الترك المؤثم قانونا.

قبول الفعل المتراضى عليه ويكون ذلك بتحديد نطاق الفعل المتراضى عليه الذي ينال بالإعتداء حقا قابلا للتصرف فيه قانونا، وكذا تحديد وسيلته وفق ما نص عليه القانون، بحيث لا ينصب الرضا على فعل فيه مساس بالمصلحة العامة أو مخالف للآداب والنظام العام[7]، ولا يكون إلا بالطرق والأساليب التي

---

[1] أحمد عبد الزعبي، مرجع سابق، ص 408 نقلا عن كمال عبد الرزاق خريسات، رضا المجني عليه ودوره في المسؤولية الجنائية، دار آفاق للنشر والتوزيع، الطبعة الأولى، 1995، ص 41.

[2] ضاري خليل محمود، أثر رضا المجني عليه في المسؤولية الجزائية، دار القادسية للطباعة، الطبعة الأولى، 1982، ص 21.

[3] أحمد عبد الزعبي مرجع سابق، ص 409 نقلا عن حامد راشد، أحكام تفتيش المسكن في التشريعات الإجرائية العربية، دراسة مقارنة، دار النهضة العربية، الطبعة الأولى، دون سنة النشر، ص 437.

[4] أحمد فتحي سرور، أصول قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 199، ص 439.

[5] محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية للنشر والتوزيع، طبعة الأولى ،1988، القاهرة، ص 535.

[6] أحمد عبد الزعبي، مرجع سابق، ص 411 نقلا عن كمال عبد الرزاق خريسات مرجع سابق، ص 43.

[7] ضاري خليل محمود، مرجع سابق، ص 21.

حددها القانون مسبقا، كما يكون بتحديد وسيلة التعبير عن الرضا وذلك من خلال كل وسيلة من شأنها أن تؤدي إلى القطع بحصول الرضا صراحة أو ضمنا.[1]

و المبدأ العام أنه لا يتطلب إفراغ الرضا في شكل معين لإثبات وجوده، فالرضا قد يكون شفاهة أو كتابة وقد يكون صراحة أو ضمنيا أو مفترضا،[2] غير أن السكوت لا يعد رضاء في كل الأحوال، ذلك أن السكوت لا يكون وسيلة تعبير إلا إذا أحاطت به ظروف واضحة وإرادة حقيقية مدركة ومميزة وخالية من أي ضغط أو خوف أو تهديد أو أي عيب قد يصيب الرضا حسب الظروف والأحوال[3]، إلا أن بعض التشريعات وتفاديا للمنازعات التي قد تثور حول وجود الرضا من عدمه، تقتضي أن يكون مكتوبا، على أساس أن الرضا الشفوي لا يصلح من حيث المبدأ أن يكون سببا لإباحة المساس بالحق في الخصوصية، والذي يعد من أهم الخصائص الذاتية للإنسان، لذلك وجب التأكد من صدور الرضا حقيقة وهو الأمر الذي يقتضي ضرورة أن يصدر الرضا مكتوبا.[4]

لكن في مقابل ذلك كان اتجاه تشريعات أخرى[5]لا تشترط أن يكون الرضا كتابة في بعض الحالات، كما في حالة الرضا بنشر الذكريات الخاصة بالفرد، طالما كان وجود الرضا ثابتا ومؤكدا ولا يتسرب إليه أي غموض أو لبس، وفي كل الأحوال تذهب التشريعات في هذا السياق إلى ضرورة أن يكون الرضا سابقا على القيام بالفعل المتراضى عليه والذي من شأنه المساس بأحد مظاهر الحق في الخصوصية، واستثناء صلاحية الرضا اللاحق بشرط أن يتوافر الرضا اللاحق قبل تمام الفعل.[6]

وتذهب هذه التشريعات إلى اعتبار أنه طالما أن الحق في الخصوصية مقرر لمصلحة الشخص نفسه، فإنه بالتالي يجوز له التنازل عن حمايته، بخصوص وقائع محددة وبصفة مؤقتة، وهذا التنازل يمكن أن يأخذ شكل الرضا اللاحق، ومن ثم ينتفي المساس بهذا الحق في هذه الحالة.[7]

ومما يؤثر في صحة الرضا مجموعة من الشروط إذا توافرت اعتبر هذا الرضا صحيحا من الناحية القانونية وهي:

- صدوره عن إرادة صحيحة حيث يشترط في الإرادة المعبرة عن الرضا أن تكون سليمة مما يعيبها لكي يعتد القانون بالرضا الصادر عنها، وعيوب الإرادة هي الغلط، التدليس، الإكراه، الغبن، والإستغلال، فوجود أي منها ينفي الرضا ويجرده من أي قيمة قانونية.

- صدور الرضا من ذي أهلية، ذلك أن الرضا يعبر عن إرادة ذات قيمة قانونية، ولذلك وجب أن يصدر من شخص مميز يتمتع بكامل الأهلية، مدركا لما يصدر عنه من أقوال وأفعال، وقد ذهب بعض الفقه إلى

[1] أحمد عبد الزعبي، مرجع نفسه، ص 413.
[2] حسام الدين الأهواني، مرجع سابق، ص 204.
[3] ممدوح خليل بحر، مرجع سابق، ص 399.
[4] أحمد عبد الزعبي، مرجع نفسه، ص 415.
[5] مثل التشريع الفرنسي، أنظر حسام الدين الأهواني، مرجع سابق، ص 205.
[6] حسام الدين الاهواني، مرجع سابق، ص 210.
[7] أحمد عبد الزعبي، مرجع سابق، ص 414.

القول أن تحديد سن التمييز لا يكون بالرجوع إلى أحكام القانونين المدني والجزائي، بل يتعلق التحديد بموضوع مختلف، فإذا لم يحدد المشرع في القانون المنظم للحق في الخصوصية المعلوماتية سنا معينة يعتد بها للرضا، فإن على قاضي الموضوع أن يبحث عن مدى فهم الشخص لطبيعة الفعل وإدراكه لآثاره وتقديره لخطورته دون أن يكون مقيدا بسن محددة.[1]

- أن يكون الرضا صادرا ممن يملكه قانونا، ومن ثمة فلا عبرة بالرضا الصادر عن غير الشخص صاحب الحق أو المصلحة المحمية قانونا، وهو ما يعبر عنه بشرط الصفة.

- أن يكون الرضا خاصا ومحددا، بحيث يجب أن يقتصر الرضا على الموضوع والوقائع محل الرضا ولا يتعداها إلى غيرها، فإذا كان رضا الشخص منصبا على التقاط صورة له، لا يعني قبوله استخدام تلك الصورة في الدعاية السياسية أو التجارية أو لأغراض أخرى.[2]

ثانيا: أثر الرضا المسبق على صحة معالجة المعطيات الشخصية

الأمر المستقر عليه في الفقه والقضاء المقارن هو أن لكل فرد الحق في تحديد ما يمكن نشره من أسرار حياته الخاصة، وهوالأمر الذي أخذت به التشريعات صراحة باعتبارها أن رضا الشخص وموافقته على ما يقع على حياته الخاصة من كشف يعد سببا لإباحة هذا الكشف،[3] وتأسيسا على هذا المفهوم أصبح رضا الشخص وموافقته المسبقة على معالجة معطياته الشخصية أحد أهم وأبرز الضمانات لتحقيق معالجة صحيحة ومشروعة، ويذكر الفقه في تحليله للموافقة المستنيرة من طرف الشخص المعني بالمعالجة خمسة عناصر وهي:[4]

- الإفصاح عن المعطيات محل المعالجة للشخص من قبل المسؤول عن المعالجة.

- الفهم الواضح للشخص المعني للبيانات التي يتم تجميعها.

- الأهلية: وهي قدرة الشخص المعني بالمعالجة على اتخاذ القرار.

- الطوعية: وهي القدرة على اتخاذ قرار الموافقة على المعالجة دون إكراه.

- وأخيرا الموافقة وهي القبول والإذن للمسؤول عن المعالجة للقيام بتجميع المعطيات الشخصية ومعالجتها.

1) توقف المعالجة الصحيحة للمعطيات الشخصية على شرط الموافقة المسبقة (الرضا المسبق):

إن رضا الشخص المعني بالمعالجة يشمل كل تعبير عن الإرادة الحرة والمميزة وعن علم، يقبل بموجبه هذا الشخص معالجة معطياته الشخصية، فلا يجوز للمسؤول عن المعالجة جمع البيانات الشخصية أو

[1] محمود نجيب حسني، مرجع سابق، ص 273.

[2] مصطفى عبد الجواد حجازي، مرجع سابق، ص 168.

[3] ممدوح خليل بحر، مرجع سابق، ص 397.

[4] محمد لطفي عبد الفتاح، القانون الجنائي واستخدامات التكنولوجيا الحيوية، دراسة مقارنة، دار الفكروالقانون، الطبعة الأولى، المنصورة، 2012، ص 479.

معالجتها أو استعمالها لأي غرض دون الموافقة الصريحة للشخص صاحب هذه البيانات، حيث يلزمه الحصول على الموافقة المسبقة للشخص المعني قبل كل معالجة يقوم بها تخص المعطيات ذات الطابع الشخصي المتعلقة بهذا الأخير، ومن ثم تعتبر معالجة غير مشروعة كل معالجة لبيانات شخصية تتم في غياب هذا الرضا المسبق.

1-1) الأحكام العامة للرضا المسبق في معالجة المعطيات الشخصية: لقد اعتبر المشرع الجزائري هذه الموافقة ضمن المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي، حيث قضت المادة 07 من القانون 07/18 أنه لا يمكن لأي مسؤول عن المعالجة أن يقوم بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني بهذه المعالجة، وهو نفس الحكم الذي كرسه التوجيه الأوروبي رقم 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة البيانات ذات الطابع الشخصي وحرية تداول وانتقال هذه البيانات في المادة السابعة منه[1] ، وكذلك المشرع الفرنسي في المادة السابعة من القانون رقم 801/2004 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والمعدل للقانون 17/78 المتعلق بالمعلوماتية والملفات والحريات.[2]

و يفرض مبدأ الرضا المسبق أو الموافقة المسبقة على المسؤول عن المعالجة ضرورة تنظيم عملية تجميع المعطيات بعد الإتصال بالشخص المعني بالمعالجة والحصول منه على رضا صريح، بمعنى أن الموافقة الضمنية لا يعتد بها*، واشتراط الرضا الصريح هو الأصل العام في مجال معالجة المعطيات الشخصية، لذلك فهناك تشريعات مثل المشرع التونسي اشترطت أن تكون هذه الموافقة مكتوبة[3] إضافة إلى كونها صريحة، وهذا ما لم ينص عليه المشرع الجزائري الذي لم يحدد طريقة وشكل الموافقة وترك المجال بذلك مفتوحا لأي طريقة يعبر من خلالها المعني بالمعالجة بما لا يترك مجالا للشك عن موافقته لمعالجة معطياته الشخصية، ويكون على المسؤول عن المعالجة عبئ إثبات ذلك.

ويفترض مبدأ الموافقة المسبقة أن يكون له رابطة مطابقة للحق في الإعلام الذي يقوم به المسؤول عن المعالجة، ذلك أنه بعد إعلام الشخص المعني بالمعالجة بأن معطياته سوف تكون محل معالجة، فإنه يتعين حصول المسؤول عن المعالجة على الموافقة الصريحة من الشخص المعني قبل البدء في عمليات

[1] L'article 07 de la directive95/46 dispose que : « les états membres prévoient que le traitement de données à caractère personnel ne peut être éffectué que si :

A/ la personne concernée a indubitablement donnée son consentement.

[2] L'article 07 de la loi 78/17 : » un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée... »

*أجاز القانون الفرنسي المتعلق بالمعلوماتية والملفات والحريات في المادتين 32،33 منه للكنائس والتنظيمات والجامعات ذات الطابع الديني أو السياسي أو النقابي بتسجيل المعطيات الشخصية المتعلقة بأعضائها ومعالجتها آليا، (دون حاجة إلى موافقتهم الصريحة) وهذا راجع إلى الموافقة الضمنية لأعضاء هذه الجماعات والتنظيمات، ففي قبول الإنضمام إلى هذه الجمعيات والتنظيمات موافقة ضمنية على قيد البيانات التي يتوجب توافرها للأعضاء في السجلات الخاصة بها والتي منها نظم المعلومات.

[3] المادة 27 من القانون التونسي 2004/63 المتعلق بحماية المعطيات الشخصية تنص على أنه لا يمكن معالجة المعطيات الشخصية إلا بالموافقة الصريحة والكتابية للمعني بالأمر.

المعالجة،[1] وانطلاقا من هذا الأساس فإن الإخلال بمبدأ الرضا المسبق على معالجة المعطيات الشخصية يترك أثرين على صحة المعالجة:

الأثر الأول يتعلق بعدم الموافقة وهنا يعد جمع وتسجيل البيانات الشخصية دون موافقة صاحبها عملا غير مشروع تقوم بموجبه المسؤولية القانونية في مواجهة المسؤول عن المعالجة، فعدم موافقة الشخص على تسجيل ما يخصه من بيانات شخصية باعتبارها من أسرار حياته الخاصة التي لا يجوز للغير الإطلاع عليها، ينفي عن عملية الجمع والتسجيل للبيانات صفة المشروعية.

الأثر الثاني ويتعلق بكون الموافقة غير صحيحة، ذلك أن الموافقة والرضا الذي يصدر عن الشخص المعني يجب أن يصدر منه بتبصر وتنبه، ويقع تبصير الشخص المعني على عاتق المسؤول عن المعالجة من خلال توضيح الحقوق والضمانات، وذلك انطلاقا من الأسئلة التي يقدمها المسؤول عن المعالجة، فإذا كانت الأسئلة التي تتضمنها الإستمارة التي يفترض على الشخص المعني بالمعالجة الإجابة عليها من أجل الحصول على موافقته لا تتناسب مع ما يتوجب أن يدلي به هذا الأخير من بيانات شخصية لهذا الغرض، بل تتعدى بكثير ما تستوجبه هذه الخدمة المقدمة من بيانات شخصية ، واضطر الشخص إلى إعطاء البيانات الخاصة به، فهذا يجعل من موافقة الشخص غير صحيحة، كون عدم التناسب ينطوي على غش يعيب الإرادة[2]، ويدخل في إطار الحصول على بيانات شخصية بطريق الغش والتدليس[3]، كما هو الشأن في الحالة التي تصدر فيها موافقة الشخص المعني بناء على ما عرضته الجهة القائمة على نظام المعلومات من وعود كانت الدافع إلى أن يقوم الشخص المعني بتقديم بيانات شخصية خاصة به، ما كان ليقدمها لولا هذه الوعود، ثم يتبين عدم صحتها، ففي هذه الحالة تكون موافقة الشخص غير صحيحة لما أصابها من تأثير الخداع الناتج عن الوعود الكاذبة.[4]

ويترتب على عدم تبصير الشخص انتفاء رضاه، ومن ثم صيرورة جمع معطياته ومعالجتها وتحليلها غير مشروع، وربما يكون ذلك من بين الأسباب التي أعطى فيها المشرع للشخص المعني بالمعالجة إمكانية أن يتراجع في أي وقت عن موافقته التي سبق له إبداؤها.[5]

ويبقى من الجدير الإشارة إلى مسألة كيفية تحصيل الرضا المسبق للشخص المعني للقيام بكل عملية معالجة عندما تتعدد غايات وأسباب المعالجة؟

[1] André Lucas, Jeans devez et Jean Frayssinet, OP, CIT, P130.

[2] بولين أيوب، مرجع سابق، ص 461.

[3] George Kellens, Nouvelles fraudes, permanence et evolutions de droit pénal au regard du renouveau de la fraude, Revue internationale de criminologie et de police technique et scientifique, orange officiel de l association internationale des criminologues de la langue francaise 1991 n°2 page 243.

[4] بولين أيوب، مرجع نفسه، ص 462.

[5] انظر المادة 3/07 من القانون 07/18.

لقد اعتبر الفقه الفرنسي بأن الرضا في هذه الحالة يكون انتقائيا، بمعنى أن تكون هناك موافقة على الأقل بالنسبة للمعالجات التي لها علاقة بالغاية المقبولة، حتى لو كان هناك رفض وعدم موافقة الشخص للمعالجات الأخرى، تكريسا لمبدأ أن كل معالجة تستلزم الموافقة المسبقة الخاصة بها.[1]

وزيادة في حماية الرضا المسبق فقد تم توسيع نطاقه ليشمل أشخاصا آخرين غير المسؤول عن المعالجة ينبغي حصولهم على الموفقة المسبقة حتى يمكنهم الإ طلاع على المعطيات للشخص المعني، وذلك بمناسبة إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليهم، إذ لا يمكن لهؤلاء الإطلاع على المعطيات الشخصية إلا بعد موافقة الشخص المعني*، وفي نفس السياق نجد أن قانون حماية خصوصية المستهلك في الولايات المتحدة الأمريكية لسنة 1997 يحظر على الشركات تقديم خدمات البرامج التفاعلية والمتمثلة أساسا في مزودي خدمات الأنترنت أن تكشف لطرف ثالث أي معلومات تعريفية شخصية قدمها المشترك دون الموافقة المكتوبة للمشترك، كما يسمح لهذا الأخير إبطال مثل هذه الموافقة في أي وقت ويطالب شركة تقديم الخدمة التوقف عن كشف مثل هذه المعلومات.[2]

وزيادة في حماية الرضا المسبق أيضا،فإنه لا يمكن الإ طلاع على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة من طرف أي شخص آخر طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر غير المسؤول عن المعالجة إلا بعد الموافقة المسبقة للشخص المعني.[3]

2-1) الأحكام الخاصة بالرضا المسبق في معالجة المعطيات الشخصية: إذا تعلق الأمر بمعالجة معطيات ذات طابع شخصي تخص الطفل فإن المشرع الجزائري اعتبر أنه لا يمكن للمسؤول عن المعالجة القيام بأي معالجة تخص المعطيات الشخصية المتعلقة بهذا الأخير إلا بعد الحصول على موافقة ممثلة الشرعي أو بعد ترخيص من القاضي المختص.[4]

والطفل هو كل شخص تكون سنه أقل من 18 سنة، وهي السن المحددة بنص المادة 02 من القانون رقم 12/15 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل، ومن ثم فالمعالجة التي يكون موضوعها معطيات لشخص تكون سنه أقل من 18 سنة فإنه يستلزم على المسؤول عن المعالجة قبل البدء في هذه المعالجة أن يحصل على موافقة الولي الشرعي لهذا الأخير.

والولي الشرعي كما عرفته المادة الثانية من القانون 12/15 المتعلق بحماية الطفل هو وليه[5]، وصيه[1]، المقدم[2]، أو حاضنه[3]. وعند الإقتضاء يجب الحصول على ترخيص من القاضي المختص، وهذه الحالة

---

[1] André Lucas, Jeans Deveze et Jean Fraysinet, OP, CIT, P131.

* حدد المشرع المقصود بالغير في المادة 14/03من القانون 07/18 وهو كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن، والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.

[2] مروة زين العابدين، مرجع سابق، ص 238.

[3] أنظر المادة 4/7 والمادة 03/14 من القانون 07/18.

[4] تنص المادة 08 من القانون 07/18: "لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بالطفل إلا بعد الحصول على موافقة ممثله الشرعي أو عند الاقتضاء بترخيص من القاضي المختص..."

[5] الولي حسب نص المادة 87 من قانون الأسرة يكون الأب وليا على أولاده القصر وبعد وفاته تحل محله الأم.

تكون عند انعدام الممثل الشرعي للطفل أو عند عدم موافقة هذا الأخير على معالجة المعطيات الشخصية لمن تحت ولايته، إذ يجوز للمسؤول عن المعالجة التقدم أمام القاضي المختص وهو رئيس المحكمة المختصة إقليميا، وهي محكمة إقامة الطفل المعني بالمعالجة، بطلب من أجل الترخيص بمعالجة معطيات ذات طابع شخصي تخص الطفل المعني، ويجوز للقاضي الترخيص والأمر بالمعالجة حتى دون موافقة الولي الشرعي للطفل إذا اقتضت المصلحة الفضلى للطفل هذه المعالجة، ويبقى للمحكمة سلطة تقدير هذه المصلحة.

لكن ما يلاحظ أن المشرع لم يتطرق إلى حالة المجنون، باعتبار أن الجنون حالة من حالات فقدان الأهلية وتحتاج إلى أحكام خاصة في التعبير عن الإرادة كحالة الطفل[4]، لذلك يمكن القول أنه في حالة ما إذا استلزم الأمر معالجة معطيات ذات طابع شخصي متعلقة بشخص مجنون فإن المسؤول عن المعالجة يتقيد بنفس الأحكام الواردة في المادة 08 من القانون 07/18 التي تخص الطفل.

2) ستثناءات الواردة على مبدأ الموافقة المسبقة: بالرغم من إلزامية حصول المسؤول عن المعالجة الموافقة المسبقة للشخص المعني، فإن هذا المبدأ ترد عليه استثناءات، وهي حالات اعتبر فيها المشرع أن الرضا المسبق للشخص المعني ليس مطلوبا للقيام بالمعالجة، وترتبط المعالجة في هذه الحالات أساسا بتحقيق مصالح مشروعة للشخص المعني أو المسؤول عن المعالجة، وكذا مصالح مرتبطة بالصالح العام، حيث تنص المادة 7 الفقرة الخامسة من القانون 07/18 أن موافقة الشخص المعني لا تكون واجبة إذا كانت المعالجة ضرورية:

أ- لاحترام التزام قانوني يخضع له الشخص المعني بالمعالجة أو المسؤول عن المعالجة، وينصرف معنى الإلتزام القانوني إلى كل إجراء يأخذ مصدره من القانون، سواء بنص تشريعي أو تنظيمي كما هو الشأن بالنسبة للمعالجات التي تقوم بها إدارة الجمارك المتعلقة بالبيانات الشخصية للمستوردين أثناء عمليات الجمركة، أو معالجة البيانات الشخصية المتعلقة بالخاضعين للضريبة من طرف إدارة الضرائب أثناء عمليات المراقبة الضريبية، فهي التزامات قانونية لا يحتاج فيها المسؤول عن المعالجة لموافقة الشخص المعني، غير أن ما يلاحظ في هذا الإطار أن كلا من التوجيه الأوروبي 95/46 والقانون الفرنسي لم يشيرا إلا إلى الإلتزام القانوني الذي يكون على عاتق المسؤول عن المعالجة دون الشخص المعني.[5]

---

[1] الوصي حسب نص المادة 92 من قانون الأسرة في حالة غياب الأب ولم تكن له أم تتولى أموره أو ثبت عدم أهليتها لذلك، يجوز تعيين وصي للقاصر وإذا تعدد الأوصياء يختار القاضي الأصلح منهم.

[2] المقدم: حسب المادة 99 من قانون الأسرة هو من تعينه المحكمة في حالة عدم وجود ولي أو وصي على من كان فاقد الأهلية أو ناقصها بناء على طلب أحد أقاربه أو من له مصلحة.

[3] الحاضن: حسب نص المادة 64 من قانون الأسرة فإنه بعد فك الرابطة الزوجية بين الأبوين تكون الأم هي الأولى بحضانة الأولاد ثم الأب ثم الجدة لأم، ثم الجد لأب، ثم الخالة، ثم العمة ثم الأقربون درجة.

[4] تنص المادة 42 من القانون المدني أنه لا يكون أهلا لمباشرة حقوقه المدنية من كان فاقدا للتمييز لصغر السن أو عتة أو جنون" ويخضع فاقدو الأهلية أو ناقصوها حسب نص المادة 44 من القانون المدني بحسب الأحوال لأحكام الولاية، الوصاية أو القوامة ضمن الشروط المقررة قانونا.

[5] Voir l'article 07/C de la directive 46/95 et l'article 7 de la loi française 78/17.

ب- لحماية حياة الشخص المعني صاحب المعطيات ذات الطابع الشخصي، حيث اعتبر المشرع أن معالجة المعطيات ذات الطابع الشخصي إذا استلزمتها ضرورات لأجل حماية الشخص المعني فإن المسؤول عن المعالجة لا يكون ملزما بتحصيل موافقة هذا الأخير للقيام بهذه المعالجة، كما هو الشأن مثلا بالنسبة للمعالجة التي تقوم بها إدارة المستشفى لتكوين ملف طبي لشخص في حالة حرجة أو غيرها من الحالات التي يكون فيها الشخص في وضع تكون فيه حياته معرضة للخطر، لذلك فإن نص الحيثية رقم 31 من الإرشاد الأوروبي 95/46 كانت أكثر دقة عندما عبرت عن ذلك بحماية مصلحة أساسية لحياة الشخص المعني.[1]

والملاحظ أن المشرع الجزائري يبدو أنه أخذ بحرفية النص الفرنسي الوارد في المادة 2/7 من القانون 17/78 الذي اعتمد نفس العبارة وهي "المحافظة على حياة الشخص المعني".[2]

ج- للحفاظ على المصالح الحيوية للشخص المعني، وإن كانت عبارة المصالح الحيوية واسعة وغير دقيقة وتشكل مصدر لبس وغموض في تحديد ما هي المصالح الحيوية للشخص وماذا يندرج ضمنها، وفي كل حوال إذا كان التماس القبول المسبق والحر والواعي من الشخص المعني غير لازم، فإنه ينبغي أن يتعلق الأمر فعلا بمصلحة تصنف أنها حيوية بالنسبة للشخص المعني، وهو أمر نسبي يختلف من شخص لآخر.

وما يمكن ملاحظته في هذا الإطار أن المشرع الجزائري تميز عن كل من التوجيه الأوروبي والمشرع الفرنسي في أنه استلزم في الشخص المعني المراد المحافظة على مصالحه الحيوية أن يكون من الناحية البدنية أو القانونية غير قادر للتعبير عن رضاه.*

د- لتنفيذ عقد يكون الشخص المعني طرفا فيه، أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه، ويتعلق الأمر في هذه الحالة بالتعبير عن الرضا الضمني، فقد يكون الشخص المعني طرفا في عقد مهما كان نوعه وشكله، فإنه يمكن الإطلاع على معطياته الشخصية في إطار تنفيذ هذا العقد، كما هو الحال في عقود الشراء التي تتم عبر الأنترنت، فمن الواضح أن معطيات الشخص ضرورية للتسليم والأداء دون حاجة المسؤول عن المعالجة أن يتحصل على رضا صريح منه، أما بالنسبة لتنفيذ إجراءات سابقة للعقد تتخذ من أجل تنفيذ العقد، فهي تجد تطبيقها بشكل خاص في عدد من المعاملات التي تتم عبر شبكة نترنت، ويدخل في هذا الإطار بعض الإجراءات التي تتم في مجال التجارة الإلكترونية، كالتسجيلات، أو الاشتراكات، أو طلبات الوثائق للتوطين البنكي.[3]

---

[1] « Considérant qu'un traitement de données à caractère personnel doit être également considéré comme licite l lorsqu' il est effectué en vue de protéger un intérêt essentiel à la vie de la personne concernée ».

[2] Le sauvegarde de la vie de la personne concernée.

* وهو مسلك لا نوافقه، فهل إذا كان الشخص المراد حماية مصالحه الحيوية قادر على التعبير عن إرادته سواء من الناحية القانونية بأن كان راشدا يتمتع بكامل أهليته وغير مكره أو قادرا من الناحية البدنية والجسمانية، فهل يسقط هذا الاستثناء، وتصبح موافقة الشخص واجبة لمعالجة معطياته الشخصية في إطار الحفاظ على مصالحه الحيوية.

[3] Christiane Féral-Schul, Cyberdroit, le droit à l'épreuve de l'internet, Dalloz, Dunod 7ème édition 2018-2019, page 100.

والمشرع الفرنسي عبر عن هذا الاستثناء في المادة07-3 من القانون 17/78 المعدل بالقانون 801/2004 بـ:

و- تنفيذ مهمة تدخل ضمن الصالح العام أو ضمن ممارسة مهام السلطة العمومية، فإذا تعلق الأمر بمعالجة معطيات شخصية تكون ضرورية لتنفيذ إحدى المهام التي تدخل ضمن الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها ويقوم بها المسؤول عن المعالجة بتفويض من السلطة العمومية، لا يكون رضا الشخص المعني بالمعالجة لازما، ويمكن للمسؤول عن المعالجة القيام بأي معالجة في هذا الإطار دون حاجة لموافقة الشخص المعني.

ويندرج ضمن هذا السياق المعالجات التي تكون ضرورية لتسيير المصالح العامة، والمهام التي يقوم بها أشخاص القانون العام مثل معالجات مصالح الجمارك وإدارات الضرائب ومصالح وزارة العدل والقنصليات والمحافظات العقارية وغيرها، بالإضافة إلى بعض المؤسسات والهيئات التابعة للقانون الخاص والتي توكل إليها مهام وصلاحيات السلطة العامة وبتفويض منها.

هـ- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو من قبل المرسل إليه، ويلاحظ أن هذا المقتضى جاء غامضا من جانبين، الأول أن المشرع لم يحدد لمن ترجع المصلحة التي يتم إنجازها، هل تتعلق بالشخص المعني بالمعالجة أم تتعلق بالمسؤول عنها، وهذا اللبس جاء نتيجة لصياغة النص القانوني وفق ترجمة غير سليمة لما ورد في نص المادة 7/F من التوجيه الأوروبي[1]، إلا أنه يفهم من نص المادة أن هذه المصلحة تخص المسؤول عن المعالجة أو المرسل إليه، طالما أن المشرع اشترط في صلب نفس الفقرة ضرورة احترام ومراعاة مصلحة الشخص المعني بالمعالجة وحرياته وحقوقه الأساسية، وإذا كان المشرع الجزائري قد اشترك مع القانون الفرنسي في التنصيص على المصلحة المشروعة للمسؤول عن المعالجة والمرسل إليه، فإن التوجيه الأوروبي أضاف كذلك المصلحة المشروعة للغير.*

أما الجانب الثاني فإن المشرع لم يضع معايير معينة يمكن من خلالها تحديد المصلحة المشروعة لهؤلاء والتي يجب في كل الأحوال ألا تتعارض مع حقوق وحريات الشخص المعني، مع ترجيح هذه خيرة في كل الظروف، وبالرجوع إلى نص الحيثية رقم 30 من التوجيه الأوروبي نجد تعدادا لمجموعة من الأمثلة التي تدخل في هذا الإطار مثل: الإستكشاف التجاري، الإستكشاف الذي تقوم به الجمعيات، التسيير الجاري للمقاولات.[2]

L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demende de celle-ci.

[1] L'article 7/F de la directive : « il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par les tiers auxquels les données sont communiquées. »

فالترجمة التي كان على المشرع الأخذ بها هي المصلحة المشروعة المتابعة أو التي يتابعها المسؤول عن المعالجة.

* يقصد بالغير في مفهوم القانون 07/18 هو كل شخص طبيعي أو معنوي عام أو خاص أو أي كيان آخر غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.

[2] Voir la directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995, Relative à la protection des personne physiques à l'égard du traitement des données à caractère personnel et à libre circulation de ces données, journal officiel des communautés européennes N°L 281/31.

الفرع الثالث: مبدأ الشفافية في معالجة المعطيات الشخصية

وهو ما يعرف أيضا في كتابات أخرى بمبدأ السيطرة على المعلومات الشخصية، حيث ألزمت جميع النصوص القانونية المتعلقة بحماية الأشخاص الطبيعيين في إطار معالجة المعطيات الشخصية وجوب أن تتم هذه المعالجة في إطار الشفافية والنزاهة واحترام كرامة الإنسان والممارسات المقبولة قانونا.

لذلك كان من المبادئ الأساسية لحماية الحق في الخصوصية في مواجهة نظم المعلومات الشخصية، وضع القواعد القانونية التي تكفل للفرد موقعا متقدما في مواجهة المخاطر التي تهدد بياناته الشخصية التي تجمع عنه، حتى يتمكن من السيطرة عليها.

ولقد أقرت التشريعات وساندها في ذلك الفقه والقضاء مجموعة من الوسائل حتى يتمكن الشخص المعني بالمعالجة من متابعة وملاحقة والسيطرة على معلوماته التي تمسه وتتعلق به بشكل مباشر[1]،فالعديد من الأشخاص يجهلونحجم ما يـ ٍ جمع عنهم من بيانات شخصية وما يعالج منها، والأهداف الكامنة وراء هذه المعالجة، كما لا يدرك البعض منهم أن لديه إمكانية استعادة زمام السيطرة على حدود ما يـ ٍ كشف عن حياته الخاصة والأمور التي تتعلق بشخصيته، من خلال الحقوق التي تمنحه إياها قوانين حماية البيانات الشخصية، لذلك فإن هذه الوسائل هي بمثابة حقوق للمعني بالمعالجة تمنحه قدر ٍا من الإطمئنان على صحة ما يتم معالجته من بيانات شخصية تتعلق به وعدم إفشاء ما يخصه من معلومات لا يرغب في الاطلاع عليها من قبل الغير، وذلك بمنحه الحق في الإطلاع على ما يتم تسجيله من بيانات ونتائج المعالجة لهذه البيانات للتأكد من صحتها وتصحيح ما يشوبها من أخطاء، وهذا لضمان شفافية المعالجة، وإذا كان مصطلح الشفافية لا يحوز على تعريف موحد يمكن اعتماده، إلا أن تحديده ممكن من خلال ما يشار إليه عادة من حق الإستعلام، والحق في الوصول إلى البيانات، وبشكل عام تتعلق الشفافية بإمكانية الفرد من الوصول إلى بياناته الشخصية المحفوظة ضمن دائرة خاصة والإطلاع على دقة وصحة هذه البيانات، وبما يمكن له من القيام به من اعتراض على تجميع بياناته أو المطالبة بتصحيحها في حال كانت بياناته المخزنة غير صحيحة أو غير دقيقة.[2]

ومن ثم نستطيع القول أن وجود مثل هذه القواعد القانونية، يعد من الضمانات الوقائية الأساسية في حماية الخصوصية والضوابط الهامة لعملية المعالجة للمعطيات الشخصية، كونها تضمن تجنب الإعتداء على البيانات الشخصية قبل وقوعه.

وتحقيقا لمبدأ الشفافية، يتمتع الأشخاص عند معالجة بياناتهم الشخصية بمجموعة من الحقوق والضمانات التي توفر لهم الحماية اللازمة، والتي أقرتها جميع القوانين التي توفر الحماية للمعطيات الشخصية دون استثناء لأصحاب هذه المعطيات الشخصية، وتتوزع بين الحق في معرفة أغراض المعالجة بطريقة لا لبس فيها، من خلال الإطلاع على عمليات المعالجة وحق الإعتراض عليها وطلب وقفها وتصحيحها وتعديلها، وهي الحقوق التي تناولها المشرع الجزائري في المواد من 32 إلى 37 من القانون

[1] عبد المحسن المقاطع، مرجع سابق، ص106.

[2] بولين أيوب، مرجع سابق، ص470.

07/18 تحت عنوان حقوق الشخص المعني بالمعالجة، وهي عبارة عن سلسلة من الحقوق المتكاملة فيما بينها، وتعبر عن شكل جديد من حقوق الإنسان المعاصرة.[1]

وهكذا يعتبر مبدأ الشفافية الأساس الذي يؤمن الثقة في ممارسة صاحب البيانات الشخصية للحقوق التي يقرها له القانون.

المطلب الثاني: حقوق الشخص المعني بالمعالجة:

يهدف إقرار مجموعة من الحقوق لأصحاب البيانات، إلى إعطاء هؤلاء الأشخاص كمعنيين بالمعالجة، إمكانية السيطرة على بياناتهم، لذا يتعين على المسؤول عن المعالجة تمكينهم من ممارسة هذه الحقوق والمتمثلة فيما يلي:

الفرع الاول: الحقوق المتعلقة بالإعلام والولوج

من المبادئ الأساسية لحماية الحق في الخصوصية وضع القواعد القانونية التي تكفل للفرد قدرا من طمئنان على صحة ما يتم معالجته من بيانات شخصية خاصة به، وذلك بمعالجتها وفقا لمبدأ الشفافية الذي يتحقق من خلال إعلام الفرد قبل تجميع معطياته، وتمكينه من الإ طلاع عليها بعد معالجتها، وعليه يرتبط هذا الحق بمقتضى إلزام المسؤول عن معالجة البيانات الشخصية بإعلام صاحبها عن رغبته في جمعها ومعالجتها وعن الأهداف والإ ستخدامات المحتملة والجهات التي ستنقل إليها.

أولا: الحـق في الإعـلام (الإخبار) droit d'information

لابد من الإ عتراف للشخص المعني بالمعالجة بحقه في الإعلام من قبل الحائز على معطياته الشخصية أو من قبل مستخدمها، حتى لا يكون ضحية لانتهاك حقه في الخصوصية دون أن يعلم بذلك، فالفرد ربما لا يكتشف مطلقا بأنه مادة لملف مخزن آليا، لذلك لابد وأن يتم إعلامه بأنه سوف يتم جمع بياناته الشخصية[2].

ولقد عالج المشرع الجزائري هذا الحق في نص المادة 32 من القانون 07/18 وحدد مقتضياته، والتي تختلف بين ما إذا كان تجميع المعطيات الشخصية سيتم لدى الشخص المعني أو لدى الغير، فضلا عن استثناء بعض الحالات من الحق في الإعلام[*].

1) الحق في الإعلام عند تجميع المعطيات لدى الشخص المعني: في هذه الحالة وانطلاقا من الفقرة الأولى من المادة 32 السالفة الذكر فإنه يجب على المسؤول عن المعالجة أو من يمثله أن يعلم مسبقا

---

[1] André LUCAS, Jeans DEVEZE et Jean FRAYSSINET, op, cit page 99.

[2] عبد المحسن المقاطع، مرجع سابق، ص110.

[*] تقضي المادة 39 من القانون الفرنسي الصادر في 06 جانفي 1978 المعدل بمقتضى القانون 2004/801 المتعلق بالمعلوماتية والملفات والحريات، بأن "من حق كل شخص طبيعي أبرز هويته أن يتوجه إلى المسؤول عن المعالجة للاستعلام منه عن البيانات ذات الطابع الشخصي، ويتأكد منه أن هذه البيانات الشخصية الخاصة به تخضع للمعالجة أم لا، وكذلك طلب معلومات حول أغراض المعالجة، ومجموعة البيانات الشخصية محل المعالجة والمستفيدين منها، وعند الإقتضاء طلب معلومات عن العمليات التي تجرى على البيانات ذات الطبيعة الشخصية والتي يتم نقلها لدولة أخرى غير عضو في الإتحاد الأوروبي.

وبصفة صريحة ودون لبس كل شخص يتم الإتصال به قصد تجميع معطياته ذات الطابع الشخصي، بمعنى أنه قبل البدء في عملية التجميع يتعين على المسؤول عن المعالجة إخبار الشخص المعني بمجموعة من العناصر تتمثل في:

*هوية المسؤول الذي يتولى عملية المعالجة وعند الإقتضاء هوية من يمثله.

*أغراض المعالجة التي لأجلها يتم طلب البيانات الشخصية.

*كل معلومة إضافية مفيدة، لاسيما الجهةالتي سترسل إليها هذه المعطيات، ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي، إذ يتعين على كل مسؤول عن المعالجة إخبار كل شخص معني بها فيما إذا كانت بياناته الشخصية سيتم معالجتها على مستواه فقط أم قد تكون محل إرسال الى جهات أخرى ينبغي تحديدها، وفيما إذا كانت هذه البيانات ستنقل إلى خارج التراب الوطني.

ومن ثمة يبدو واضحا ضرورة إلزام المسؤول عن المعالجة اتخاذ التدابير الضرورية لتوفير المعلومات اللازمة لأصحاب البيانات الشخصية بطريقة دقيقة وواضحة ومفهومة وسهلة الإستيعاب، كما عبر عن ذلك المشرع من خلال استعماله لعبارة صريحة و"دون لبس"، ويكون هذا متوفرا عند استخدام تعابير سهلة وواضحة لا تثير الشك ولا تحتمل التأويل أو يصعب على المعني بالمعالجة فهم القصد منها.[1]

ويقع الإلتزام بإعلام الشخص المعني بالمعالجة على عاتق المسؤول عن المعالجة أو من يمثله، ولا يسقط هذا الإلزام إلا إذا ثبت أن الشخص المعني بالمعالجة على علم مسبق بهذه العناصر اللازم إخباره بها*، كما ويفترض بالمسؤول عن المعالجة الإجابة على أي سؤال يمكن أن يطرحه صاحب البيانات حول عملية المعالجة وأهدافها والجهات التي يمكن أن تنقل إليها، وذلك ضمن مدة زمنية معقولة يمكن أن تطول أو تقصر حسب طبيعة وحجم نشاط الجهة المسؤولة.[2]

وكما هو الشأن بالنسبة للعناصر التي وردت في الإرشاد الأوروبي 46/95 في نص المادة 108 منه، فإن المشرع الجزائري قد وضع حدا أدنى من العناصر التي يلزم إعلام المعني بالمعالجة بها، بالإضافة إلى أنه جعل ضمن العناصر الإضافية مجموعة من المعلومات يفترض أن تكون ضمن المعلومات التي يلزم أن يزود بها المعني بالمعالجة بشكل أساسي وإجباري بالنظر إلى طبيعتها، وهو ما كان المشرع الفرنسي موفقا فيه

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص136.

* تنص المادة 32 من القانون 07/18 "ما لم يكن على علم مسبق بها يجب على المسؤول عن المعالجة أو من يمثله إعلام مسبقا وبصفة صريحة كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابعالشخصي بالعناصر التالية:

-هوية المسؤول الذي يتولى عملية المعالجة وعند الإقتضاء هوية من يمثله.

-أغراض المعالجة التي لأجلها يتم طلب البيانات الشخصية.

-كل معلومة إضافية مفيدة، لاسيما المرسل إليه هذه المعطيات، ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

[2] المشرع الجزائري لم يتحدث عن المدة التي يتعين على المسؤول عن المعالجة إعلام المعني فيها قبل البدء بالمعالجة على خلاف المشرع التونسي الذي اشترط أن يتم الإعلام في أجل لا يقل عن شهر من التاريخ المحدد لمعالجة المعطيات.

حسب اعتقادنا، إذ أن المعلومات التي اعتبرها المشرع الجزائري إضافية جعلتها المادة 32 من القانون الفرنسي 17/78 إجبارية[1]

وهي الطريقة التي اعتمدها المشرع التونسي أيضا، حيث فصلت المادة 31 من القانون 2004/63 المتعلق بحماية المعطيات في تعداد العناصر التي يلزم المسؤول عن المعالجة إعلام الأشخاص الذين ستجمع عنهم المعطيات الشخصية، وذلك بصورة إجبارية وأساسية ولم يعتبر أيا منها معلومات إضافية.*

والملاحظ أن المشرع الجزائري لم يحدد الوسيلة التي يتم بها هذا الإخبار أو الإعلام للشخص المعني بالمعالجة، ولا المدة التي يتعين إعلامه فيها قبل البدء في المعالجة، على خلاف تشريعات أخرى كالمشرع التونسي مثلا، الذي اشترط أن يتم الإعلام بواسطة رسالة مضمونة الوصول أو بأي وسيلة تترك أثرا كتابيا في أجل لا يقل عن شهر قبل التاريخ المحدد لمعالجة المعطيات الشخصية.

ومن جهة أخرى إذا كان تجميع البيانات في شبكات مفتوحة، أي شبكات الإتصال الإلكتروني (الأنترنت)، فإنه يتعين إعلام الشخص المعني بجمع البيانات الشخصية بأن هذه البيانات المتعلقة به يمكن أن تكون محل تداول في هذهالشبكات دون ضمانات السلامة، وأنها قد تتعرض للقراءة والإستعمال غير المرخص به من طرف الغير.[2]

2) الحق في الإعلام عند تجميع المعطيات ذات الطابع الشخصي لدى الغير: إذا كان المبدأ هو أن المعطيات ذات الطابع الشخصي يتم تجميعها لدى الشخص المعني، إلا أنه في بعض الحالات يمكن أن يتم تجميع معطيات شخصية تخص هذا الأخير لدى شخص آخر، أي لا يتم تحصيلها من المعني مباشرة وإنما من مصدر آخر، كأن يتخلى المعالج الأصلي عن الملفات الإلكترونية المتضمنة لمعطيات شخصية لمستخدمين لديه لمعالج آخر، سواء بمقابل أو دون مقابل[3]، أو أن يتم تحصيل البيانات الشخصية عن

---

[1] Voire l'article 32, la loi n° 78/17 du 6 janvier 1978

* نصت المادة 31 من القانون التونسي 2004/63 المتعلق بحماية المعطيات الشخصية "يجب إعلام الأشخاص الذين ستجمع عنهم المعطيات الشخصية مسبقا وبأي وسيلة تترك أثرا كتابيا بما يلي:

-نوع المعطيات الشخصية المراد معالجتها

-أهداف معالجة المعطيات الشخصية

-الطابع الإلزامي أو الاختياري لأجوبتهم

-نتائج عدم الجواب

-إسم الشخص الطبيعي أو المعنوي المستفيد من المعطيات أو الذي له حق النفاذ إليها ومقره

-إسم المسؤول عن المعالجة ولقبه أو تسميته الاجتماعية وممثله عند الإقتضاء ومقره

-حقهم في النفاذ

-حقهم في الرجوع عن الموافقة على المعالجة في كل وقت

-حقهم في الاعتراض على معالجة معطياتهم الشخصية

-مدة حفظ المعطيات

-وصف موجز للاحتياطات المتخذة لضمان أمان المعطيات الشخصية

-البلد الذي يعتزم المسؤول عن المعالجة نقل المعطيات الشخصية إليها عند الإقتضاء

[2] أنظر المادة 3/32 من القانون 07/18.

[3] العربي جنان، مرجع سابق، ص70.

طريق شبكة الأنترنت، وفي هذه الحالة أيضا يبقى للشخص صاحب البيانات الحق في إعلامه من قبل المسؤول عن المعالجة أو من يمثله بنفس العناصر والمعلومات المشار إليها في الحالة الأولى.

ولكن الإ ختلاف يكمن في التوقيت أو المرحلة التي يجب أن يتم فيها الإعلام، فإذا كان الحق في الإعلام في الحالة الأولى مستوجبا قبل البدء في أي عملية معالجة، فإنه في هذه الحالة يلزم على المسؤول عن المعالجة أن يزود المعني بالمعالجة بتلك المعلومات قبل تسجيل المعطيات أو قبل إرسالها إلى الغير، في حين أضافت تشريعات أخرى إلزامية الإعلام عند الإيصال الأول للبيانات على أبعد تقدير إذا كان المسؤول عن المعالجة يعتزم إيصالها إلى الغير.[1]

ويتعلق الأمر في هذه الحالة بتجميع ٍ غير مباشر للمعطيات، ويكون الإلتزام بالإعلام فيه التزاما غير مرن، مكلف ومعقد من حيث القيام به، وهو من جانب آخر ذو أهمية من الناحية الإقتصادية بالنسبة لمن يحوز ملفات تحتوي على معطيات الغير[2]

كما يصبح هذا الإلتزام أساسيا عند القيام بعمليات التسويق المباشر والتجارة الإلكترونية، والملاحظ أن المشرع الجزائري لم يحدد الوسيلة التي يتم من خلالها تقديم هذه المعلومات إلى المعني بالمعالجة وتزويده بها، فما يفهم نص المادة 32 من القانون 07/18 من خلال عبارة "بصفة صريحة ودون لبس" أن يتم هذا الإعلام أو الإخبار إلى المعني بأي وسيلة تحقق هذه الغاية، وهذا على خلاف المشرع التونسي أو المغربي حين اشترط الأول أن يتم الإعلام بواسطة رسالة مضمونة الوصول، أو بأي وسيلة أخرى تترك أثرا كتابيا، ونص الثاني في المادة 34 من المرسوم رقم 165.09.2 الصادر في 21 ماي 2009 لتطبيق القانون رقم 09/08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي على الإعلام بواسطة رسالة إلكترونية أو دعامة ورقية أو العرض على شكل نموذج إلكتروني، أو الاعلان على دعامة مناسبة أو خلال مقابلة شخصية. في حين أشار المشرع الفرنسي أنه يمكن لصاحب الشأن التقدم بطلب إلى المسؤول عن المعالجة للبيانات الشخصية يطلب فيه الحصول على صورة من البيانات ذات الطبيعة الشخصية التي تم تسجيلها عنه، على أن يقوم بدفع رسوم لا تتجاوز التكلفة الحقيقية للصورة.

3) ستثناءات الواردة على الحق في الإعلام: نصت المادة 33 من القانون 07/18 على مجموعة من الحالات على سبيل الحصر استـ ٍ بعدت من نطاق الحق في الإعلام، ولا يكون فيها للشخص المعني بالمعالجة الحق في إعلامه بتلك المعلومات من قبل المسؤول عن المعالجة قبل البدء في معالجة بياناته الشخصية ويتعلق الأمر بـ:

-الحالة التي يتعذر فيها إعلام الشخص المعني بالمعالجة لأي سبب كان، خاصة إذا تعلق الأمر بمعالجة المعطيات الشخصية لأغراض إحصائية أو تاريخية أو علمية،[3] ويأتي استبعاد تطبيق حق الإعلام في هذه الحالة بسبب صعوبته، وأحيانا استحالته من الناحية العملية، ويتوجب على المسؤول عن المعالجة عند

[1] أنظر المادة 05 من القانون المغربي 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والمادة 32 من القانون الفرنسي 17/78 المتعلق بالمعلوماتية والملفات والحريات.

[2] André LUCAS, Jeans DEVEZE et Jean FRAYSSINET, op, cit, page 13.

[3] انظر المادة 33 البند أ من القانون 07/18.

تعذر إعلام الشخص المعني أن يشعر السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بهذه ستحالة، مع تقديم أسباب ومبررات ذلك، وإذا كان المشرع الجزائري قد استبعد الحق في الإعلام في هذه الحالة سواء تم تجميع المعطيات لدى الشخص المعني أو لدى الغير، فإن التوجيه الأوروبي 46/95 في المادة 11 وكذلك القانون الفرنسي 17/78 في المادة 32 استبعدا هذا الحق عندما يتم تجميع المعطيات لدى الغير فقط.[1]

-الحالة التي تتم فيها المعالجة تطبيقا لنص قانوني، وهي الحالة التي توجد فيها نصوص تشريعية تنص صراحة على تسجيل المعطيات الشخصية وإيصالها.

-الحالة التي تتم فيها معالجة المعطيات الشخصية لأغراض صحفية أو فنية أو أدبية.

وما يمكن ملاحظته على هذه الإستثناءات أن المشرع لم يتطرق إلى الحالة التي يكون فيها تجميع ومعالجة المعطيات الشخصية ضرورية للدفاع الوطني والأمن الداخلي أو الخارجي للدولة، وذلك خلافا لما نصت عليه تشريعات أخرى[2]، و ربما يعود ذلك إلى كون أن هذا النوع من المعطيات مستثناة أصلا من نطاق تطبيق القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ومن ثم يكون من غير المفيد أن تذكر كاستثناء على حق الإعلام، وهي غير معنية بالحماية القانونية التي جاء بها هذا القانون[3]،بل نجد أن الإرشاد الأوروبي قد وسع من حالات الإستثناء على حق الإعلام، بأن أدرج حالات أخرى لا يتوجب إعلام الشخص فيها إذا كانت المعطيات الشخصية التي سوف تعالج ضرورية للمصلحة الإقتصادية أو المالية للدولة، سيما في الميادين النقدية والضريبية، أو في حالة ضرورتها لحماية الشخص المعني أو لحماية حقوق وحريات الآخرين.[4]

ونعتقد أنالمشرع قد تجنب هذا التوسع في الإستثناءات على حق الشخص المعني في الإعلام لعدم إثقاله باستثناءات تضيق من نطاقه، ومن ثم تضعف الحماية للمعطيات الشخصية والتي جاء هذا القانون أصلا لتكريسها.

[1] Yves mayaud, code penal 14 eme edition, dallaz, 2009, page 699

[2] أنظر المادة 32/v من القانون الفرنسي 17/78 المؤرخ في 06 جانفي 1978 المتعلق بالمعلوماتية والملفات والحريات:

« Les dispositions ne s'appliquent pas aux données recueilles, et utilisées lors d'un traitement mis en œuvre pour le compte de l'état et intérissant la sureté de l'état, la défense, la sécurité publique ou ayant pour l'objet l'exécution de condamnations pénales ou de mesures de sureté »

[3] تنص المادة 06 من القانون 07/18 "تستثنى من مجال تطبيق هذا القانون المعطيات ذات الطابع الشخصي 1/.....

2/المحصل عليها والمعالجة لمصلحة الدفاع والأمن الوطنيين".

[4] أنظر المادة 13 من التوجيه الأوروبي 46/95 المؤرخ في 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية تداول البيانات.

ثانيا: الحق في الولوج droit d'acces:

يعد حق المعني بالمعالجة في الولوج أو النفاذ إلى قاعدة البيانات والوصول إلى بياناته المخزنة آليا والإطلاع عليها من أكثر الضمانات فعالية لحفظ حقه في الخصوصية، ومن أكثرها تمكينا له من ممارسة حقه في السيطرة على بياناته الشخصية.[1]

وبالتالي فمن الضمانات الوقائية لحماية الحق في الخصوصية المعلوماتية في مواجهة نظم المعلومات، إقرار التشريعات لحق الشخص صاحب البيانات بالولوج إليها من أجل الإطلاع على ما يخصه من بيانات ومعلومات.[2]

لذلك فنظرا لأهمية هذا الحق فقد أقرته جميع القوانين المتعلقة بحماية المعطيات الشخصية[3]، بل إن بعض الدول قد اعتبرت هذا الحق من الحقوق الدستورية وضمنته في دساتيرها، مثل دولة البرتغال التي تنص المادة 35 الفقرة الأولى من دستورها على حق المواطن في الإطلاع على المعلومات التي تتعلق به وما تتضمنه نظم المعلومات من بيانات خاصة به.[4]

وهو الحق الذي نص عليه المشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في المادة 34 منه، متأثرا في ذلك بالصيغة التي جاءت في نص المادة 12 من الإرشاد الأوروبي 46/95 التي أكدت هي الأخرى على هذا الحق.

وتقتضي ممارسة الحق في الولوج إحترام مجموعة من الأحكام واتباع بعض الإجراءات.

1) أحكـام الحق في الولوج: يقصد بالحق في الولوج وصول المعني إلى بياناته الشخصية بغية الإطلاع عليها، ومعرفة كل ما يتعلق به من بيانات شخصية تخصه تم تسجيلها على الكومبيوتر ومصادرها وطرق معالجتها، وكذا مضمون البيانات المتعلقة به بعد معالجتها.

فهذا الحق الممنوح للشخص كضمانة وقائية لحماية حقه في الخصوصية، لا يقتصر على توفير سبل معرفته بمضمون البيانات والمعلومات التي تم تخزينها في الكومبيوتر، بل يشمل أيضا حقه في معرفة مصدرها وطرق معالجتها آليا والأسس التي قام عليها نظام المعالجة[5].

ومن ثمة فإن مقتضيات هذا الحق لا تقتصر فقط على تأكد الشخص المعني بأن معطياته الشخصية تعالج أم لا، بل يعني أيضا تمتع الشخص المعني بالمعالجة في مواجهة المسؤول عنها بالحق في العلم بمجموعة من المعلومات تنصب على غايات المعالجة، وفئات المعطيات المتعلقة بها، وفئات المرسل إليهم الذين أوصلت إليهم المعطيات ذات الطابع الشخصي، بالإضافة إلى تمتع الشخص المعني بالحق في إحاطته

[1] عبد المحسن المقاطع، مرجع سابق، ص111.
[2] نعيم مغبغب، مرجع سابق، ص203.
[3] أسامة عبد الله قايد، مرجع سابق، 1994، ص51.
[4] مدحت عبد الحليم رمضان، مرجع سابق، ص80.
[5] بولين أيوب، مرجع سابق، ص472.

وإفادته بالمعطيات الشخصية الخاصة به التي تخضع للمعالجة، وبكل معلومة متاحة متعلقة بمصدر المعلومات.

وقد تم النص على هذا الحق في المادة 12 من التوجيه الأوروبي 95/46 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية وحرية تداولها المؤرخ في 24 أكتوبر 1995، وفي المادة 07 من القانون المغربي رقم 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، وكذلك في المادة 32 من القانون الفرنسي 801/2004 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل للقانون 17/78 المتعلق بالمعلوماتية والملفات والحريات.

ولعل ما يبرر منح المعني بالمعالجة الحق في الولوج من أجل الإطلاع على بياناته الشخصية محل المعالجة والتي يتم تخزينها آليا، هو ما تتمتع به نظم المعلومات من إمكانيات فائقة في تجميع وتخزين البيانات من مختلف المصادر من غير موافقة الشخص المعني ودون علمه، وكذا ما تتمتع به من إمكانية نقل هذه البيانات والمعلومات إلى مختلف أرجاء العالم.[1]

وهذه الخصائص من شأنها أن تخلق عدم التوازن بين نظم المعلومات وبين الأفراد، ومن ثم كان سببا كافيا لإقرار حق الفرد في الولوج إلى هذه النظم والتأكد من بياناته محل المعالجة من حيث مصدرها وأغراض معالجتها وكل معلومة متاحة تفيد صحتها وسلامة هذه البيانات، ذلك أن معرفة الشخص لمصدر البيانات التي تم تجميعها عنه وتسجيلها وتخزينها في الكومبيوتر، تعد ضرورة تستلزمها حماية الحياة الخاصة للأفراد، خاصة في نظم المعلومات التابعة للقطاع الخاص، وأن معرفة الشخص أيضا للطرق التي ستتم بها المعالجة الآلية للبيانات المتعلقة به ونتائج هذه المعالجة يحمل أهمية خاصة، سيما إذا تعلق الأمر بالمعالجة التي يترتب عنها استخلاص حكم أو تقييم للشخص يحتج به الغير في مواجهته.[2]

لهذه الأسباب يستفيد كل شخص معني في إطار ممارسته لحق الولوج من معرفة المنطق الذي يحكم كل معالجة آلية للمعطيات ذات الطابع الشخصي الخاصة به، وهو حق له علاقة بالتطور الذي تعرفه الأنظمة الآلية لاتخاذ القرارات في مجموعة من الميادين، في مجال رسم ملامح شخصية الفرد، تقييمه، تقدير مستوى المخاطر التي يمثلها، معالجة نتائج اختبار التشغيل، أو من أجل تسيير المستخدمين وغيرها، ومن ثم فهذا الحق يعطي في النهاية للشخص إمكانية مراقبة الأسس المعلوماتية والمنطقية لطريقة اتخاذ القرار في مواجهته،[3] وقد تصدى القضاء لمثل هذا الموقف عندما أقرت المحكمة الإتحادية العليا في أمريكا في قضية greene v. mc elory على أن للفرد الحق في أن يعرف عن المعلومات السرية الخاصة به إذا كانت ستؤدي إلى التأثير عليه عن طريق رسم صورة خاطئة عنه.[4]

[1] هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية الطبعة الأولى 1992، القاهرة، ص145

[2] بولين أيوب، مرجع نفسه، ص473 نقلا عن: Robert badinter, le droit au respect de la vie privée, j,c,p 1968 n2136

[3] Yves Mayaud, code pénal, 14 eme édition, dallaz, 2009, page 699

[4] محمد عبد المحسن المقاطع، مرجع سابق، ص112.

ولقد عالج المشرع الجزائري حق المعني بالمعالجة في الولوج في المادة 34 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]، وما يلاحظ على هذا النص القانوني أن المشرع كان جد مقتضب من حيث تنظيمه لهذا الحق، وهو ما يظهر من خلال عدم التنصيص على مجموعة من المقتضيات المرتبطة بهذا الحق.

كما ولا بد من الإشارة إلى أن الحق في الوصول إلى البيانات الشخصية ينحصر فقط في حق الشخص المعني في الولوج إلى بياناته الشخصية المتعلقة به وحده، ولا يشمل الإطلاع على بيانات أشخاص آخرين.[2]

وكذلك إذا كانت قواعد البيانات المطلوب الولوج إليها لا تحتوي على بيانات شخصية، فإن الوصول إليها في هذه الحالة يخضع لنظام قانوني آخر غير القانون المنظم لحماية المعطيات الشخصية، بل إلى نظام قانون حرية الوصول إلى المعلومات الذي يتعلق بإقرار حق المواطن في المعرفة والوصول إلى المعلومة والمشاركة في الحياة العامة.

2) إجراءات ممارسة الحق في الولوج: لم يحدد المشرع الجزائري الإجراءات التي من خلالها يتبين للمعني بالمعالجة كيفية ممارسة حقه في الولوج، لكن ومن خلال تشريعات أخرى[3] يمكن الإستعانة بها في هذا الإطار، يمكن تقديم توضيح لهذه المسألة.

فالمستقر عليه أن حق الولوج يمارس من قبل الشخص المعني للإطلاع على البيانات المختزنة في نظام المعلومات سواء من قبل الشخص المعني أو من قبل شخص آخر نيابة عنه.

ففي الحالة الأولى وهو الولوج المباشر يكون إذا قام الشخص المتعلقة به البيانات الشخصية بالإطلاع عليها بنفسه أمام الجهة التي تقوم بتجميع معطياته الشخصية، أو أمام الجهة التي تحوز هذه المعطيات حسب الأحوال، ويقتضي الإطلاع المباشر أن يمارسه الشخص نفسه ولا يجوز التوكيل فيه لأنه من الحقوق الفردية التي لا يجوز ممارستها عن طريق الغير، إلا إذا كان الشخص المتعلقة به المعطيات الشخصية ناقص أو عديم الأهلية، فإن الممثل القانوني هو الذي يمارس هذا الحق نيابة عنه[4]، كما يمكنه الاستعانة بمستشار يرافقه عند الإطلاع.

أما في الحالة الثانية وهي المتعلقة بالولوج غير المباشر، فإنه يحصل إذا تم الإطلاع على المعطيات ذات الطابع الشخصي من قبل شخص آخر غير الشخص المعني المتعلقة به هذه المعطيات، ومن ثم يكون علم

---

[1] تنص المادة 34 المذكورة أعلاه "يحق للشخص المعني أن يحصل من المسؤول عن المعالجة على:
-التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم.
-إفادته وفق شكل مفهوم بالمعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات"

[2] لقد كان رأي لجنة lindopالإنجليزية هو عدم ضرورة إيجاد حق عام للفرد في الاطلاع أو الوصول إلى البيانات المخزنة عنه، كالنظام الذي تأخذ به كل من أمريكا وألمانيا، وذلك لكون وصول الشخص الخاضع لنظام المعلومات المبرمجة آليا عنه، هو أحد أسباب تحقيق الهدف وليس الهدف ذاته، أنظر عبد المحسن المقاطع، مرجع نفسه، ص112

[3] المرسوم رقم 2.09.165 المؤرخ في 21 ماي 2009 لتطبيق القانون 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للمملكة المغربية عدد 5744 مؤرخة في 18 يونيو 2009.

[4] حسام الدين الأهواني، الحق في احترام الحياة الخاصة، مرجع سابق، ص50.

هذا الأخير ومعرفته ببياناته المعالجة عن طريق الشخص الذي اطلع عليها[1]، ويكون الإطلاع غير المباشر في الأحوال التي يحظر فيها القانون على الشخص المتعلقة به البيانات الإطلاع عليها شخصيا وإعطاء هذا الحق لغيره نيابة عنه.

وقد اعتبر المشرع الفرنسي الولوج غير المباشر على المعالجات المتعلقة بأمن الدولة والدفاع والأمن العمومي،والمعالجات التي تقوم بها مصالح الإستعلامات العامة والمعالجات المجراة على المعطيات الصحية قيدا على ممارسة الحق في الولوج[2]، حيث أنه في هذه الحالة حسب ما تضمنته المادة 41من القانون 17/78 يقدم طلب الولوج إلى اللجنة الوطنية للمعلوماتية والحريات CNIL والتي تحيله بدورها إلى أحد أعضائها المنتمين لمجلس الدولة أو محكمة النقض أو مجلس المحاسبة لدراسته والتحقق منه وإجراء التعديلات الضرورية، على أن يخطر مقدم الطلب بذلك، وإذا ثبت للجنة بالإتفاق مع المسؤول عن معالجة البيانات الشخصية أن البيانات التي تتضمنها المعالجة لا تضر بسلامة الدولة والدفاع والأمن العام، يمكن السماح لصاحب الشأن المعني بالمعالجة بالإطلاع عليها، كما يمكن للجنة القومية للمعلوماتية والحريات CNIL أن تنص في القرار المتعلق بإنشاء قاعدة البيانات الخاصة بسلامة الدولة والدفاع والأمن العام أن يكون الإطلاع على البيانات المعالجة بواسطة الوكيل المباشر للملفات الالكترونية.[3]

وفي حالة رفض اللجنة الوطنية للمعلوماتية والحريات إخطار صاحب الطلب المقدم إليها من أجل إطلاعه على بعض البيانات التي وردت عليها المعالجة على أساس أنهاتتضمن أسرار ا خاصة بالدفاع والأمن العام، فإنه يمكن له الطعن أمام القضاء الإداري ضد هذا القرار.

ولعل من أهم صور الولوج غير المباشر أيضا هو إعطاء الطبيب المعالج الحق في الولوج والإطلاع على البيانات الصحية للمريض التي تتعلق بحالته الصحية، ويقوم الطبيب بعدها بإطلاع المريض على هذه المعلومات وفقا للقواعد العامة التي تحكم العلاقة بين الطبيب والمريض ووفقا لأخلاقيات مهنة الطب.[4]

وفي كلتا الحالتين سواء الولوج المباشر أو غير المباشر فإنه يمكن التمييز بين طريقين لممارسة هذا الحق:

-الطريقة الأولى ويكون الولوج عن طريق الإطلاع في عين المكان، حيث يقدم طلب الولوج من طرف المعني بالمعالجة، أو من طرف من يمثله أو من قبل الولي بالنسبة للقاصر إلى المسؤول عن المعالجة، ويتضمن هذا الطلب كل العناصر الوطيدة الصلة بالموضوع، كطبيعة البيانات وظروفها أو مصدر الإطلاع على معالجة هذه المعطيات، وكذا تحديد السلطة أو المصلحة المعنية، وإذا كان الطلب يفتقر إلى الدقة، بسبب تخلف أحد العناصر اللازمة لتمكين المسؤول عن المعالجة من ممارسة العمليات المرتبطة بالحق في

[1] بولين أيوب، مرجع سابق، ص475.

[2] Voir pierre Kayser, la protection de la vie privée par le droit, protection du secret de la vie privée, economica, 3 eme édition, 1995, page 434

[3]Voir jean fraysinet, condition du droit d'accés et communication aux données figurant dant les fichiers des services des renseignement généraux. A.J.D.A 1994, page 145

[4] نعيم مغبغب، مرجع سابق، ص232. وكذلك شريف يوسف خاطر، مرجع سابق، ص96.

الولوج، فإنه يمكن لهذا الأخير أن يطلب من الشخص المعني بالطلب أن يزوده بالعناصر الضرورية المختلفة، قبل انتهاء الأجل الذي تحدده السلطة الوطنية بناء على طلب المسؤول عن المعالجة بقصد الإجابة على طلبات الولوج المشروعة.

ويكون إطلاع المعني في هذه الحالة من خلال إظهار المسؤول عن المعالجة له شاشة الكومبيوتر الذي تمت فيه معالجة البيانات الخاصة به، إذ يتم استدعاء الشخص المعني بالمعالجة من طرف المسؤول عنها للإطلاع على ملفه أو بطاقته كما تسمى في تشريعات أخرى (المشرع التونسي) وقراءة ما يوجد على شاشة الحاسوب الآلي.

-الطريقة الثانية ويكون الولوج فيها عن طريق الإطلاع بموجب طلب كتابي، حيث يقدم الطلب كتابيا وموقعا عليه من طرف الشخص المعني إما ورقيا أو إلكترونيا من أجل الحصول على نسخة من المسؤول عن المعالجة بالبيانات التي تمت معالجتها، وقد أعطى المشرع الفرنسي للمعني بالمعالجة الحق في الحصول على نسخة من المعطيات المسجلة،[1] وهو حق لم ينص عليه المشرع الجزائري.

وفي الحالة التي يكون فيها ملف الشخص المعني الذي يحتوي معطياته الشخصية خاضعا لإدارة مشتركة لعدة مسؤولين عن المعالجة، فإنه يمكن مباشرة حق الولوج إلى المعطيات لدى أي منهم، إلا إذا كانت مسؤولية إدارة الملفات يتحملها مسؤول واحد فقط.

وإذا ما تم توجيه الطلب بالولوج إلى شخص غير مخول له بتبليغ البيانات المطلوبة، فإن هذا الأخير يلزم عليه إحالة الطلب في أقرب وقت على الجهة المختصة.

وقد أشار المشرع الجزائري في المادة 34 الفقرة الأخيرة من القانون 07/18 أنه بإمكان المسؤول عن المعالجة أن يعترض على الإ ستجابة لطلبات الولوج التي يبدو من خلال عددها وطابعها المتكرر أنها طلبات تعسفية، وله في هذه الحالة أن يمتنع من تمكين المعني بالمعالجة من الولوج، شريطة أن يلتزم بتبرير وإثبات فعلا وجود الطابع التعسفي لهذه الطلبات، وهو نفس الحكم الذي كان المشرع الفرنسي قد كرسه بنص المادة 39 من القانون 17/78 المتعلق بالمعلوماتية والملفات والحريات لسنة 1978، عندما قضت هذه المادة أن المسؤول عن المعالجة يمكنه أن يعترض على بعض الطلبات التي يظهر فيها التعسف في استعمال هذا الحق، سواء من خلال عددها أو طبيعتها التكرارية أو المنتظمة، وفي حالة النزاع فإن عبء إثبات عدم معقولية الطلبات وتكرارها تقع على المسؤول عن المعالجة[2]

وإن كان المشرع الجزائري لم نجده وضع أي استثناء على ممارسة هذا الحق، فإن الإرشاد الأوروبي 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية وحرية تداولها، وكذلك القانون الفرنسي، وضعا مجموعة من الإستثناءات على ممارسة الحق في الولوج ولم يـ ، ترك على إطلاقه، و هي نفس

[1] L'aticle 39/1 Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction

[2] Jean frayssinet, conditions du droit d'accès et de communication aux données figurant dans les fichiers des services des renseignement généraux, A.J.D.A (Actalite Juridique Droit Administratif) revue, dalloz, 1994, p 145.

ستثناءات على الحق في الإعلام[1]، فالقانون الفرنسي 17/78 استثنى تطبيق أحكام المادة 39 من هذا القانون والمتعلقة بالحق في الولوج على البيانات الشخصية التي يتم حفظها بشكل واضح ومحدد يستبعد كل خطر على الحياة الخاصة للأشخاص المعينة وخلال مدة لا تتجاوز بالضرورة أهداف البحوث الإحصائية أو العلمية أو التاريخية.[2]

كما يجدر بنا الحال أن نشير إلى أن المشرع الجزائري لم يشر إلى مسألة تمكين المسؤول عن المعالجة الشخص المعني من الولوج بمقابل أو دون مقابل، على خلاف ما نصت عليه تشريعات أخرى مثل المشرع الفرنسي الذي جعل ممارسة هذا الحق مقابل مصاريف جزافية[3]، والإرشاد الأوروبي نص على أن يكون ذلك نظير مصاريف غير مكلفة[4]، أما المشرع المغربي[5] فنص على أن يتمتع الشخص المعني بهذا الحق دون أي مقابل.

كما لم يحدد المشرع الجزائري أيضا المدة التي يتعين فيها على المسؤول عن المعالجة الإستجابة لطلب المعني في الولوج*، على خلاف التشريعات المقارنة التي تتحدث عن ضرورة استجابة المسؤول عن المعالجة لهذا الطلب فورا[6]، لكن في المقابل أعطى للمسؤول عن المعالجة الحق في أن يطلب من السلطة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة.[7]

وتجدر الإشارة أيضا إلى أنه إذا كان المشرع الجزائري لم يعط ممارسة حق الولوج للإطلاع على البيانات الشخصية محل المعالجة لورثة صاحب هذه البيانات واكتفى بمنح هؤلاء حق التصحيح فقط، كما سوف نرى لاحقا، فإن تشريعات أخرى منحت حق الولوج إلى ورثة الشخص المعني على غرار المشرع الفرنسي في

---

[1] Yves Mayaud, op, cit page 697

[2] L'article39/2 dispose que Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique.

[3] Yves mayaud, op, cit page 696, voir aussi l'article 39 de la loi francaise 2004/801 « une copie des données à caractère personnel est délivrée à l'intéressé à sa demande, le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut éxcéder le cout de la reproduction ».

[4] Voir l'article 12 de la directive 46/95 : « les états membres garantissent à toute personnes consernée le droit d'obtenir du responsable du traitement » à sans contrainte, à des intervalles raisonables et sans délais ou frais excessifs....

[5] المادة 07 من القانون المغربي 09/08 تنص فيما يتعلق بحق الولوج أنه يحق للشخص المعني بعد الإدلاء بما يثبت هويته أن يحصل من المسؤول على المعالجة في فترات معقولة وعلى الفور ودون عوض.

* في القضاء الفرنسي توجد قضية تتلخص وقائعها في قيام أحد الأشخاص من شركة centrapel الاطلاع على ملفه الشخصي، لكنها رفضت الإطلاع بحجة أنها سلمت صورة من الملف لمحامي الطالب من قبل أثناء تسوية نزاع بينهما بشأن الفصل من الخدمة، لكن بعد لجوء هذا الأخير إلى اللجنة الوطنية CNIL قررت توقيع غرامة على الشركة ب 5000 يورو، فقامت الشركة بالطعن ضد قرار اللجنة أمام مجلس الدولة، هذا الأخير الذي رفض الطعن، مقررا أن من حق كل شخص الإطلاع في أي وقت وبدون مبرر على ملفه الشخصي وبياناته الشخصية، إعمالا لأحكام المادة 39 من القانون 17/78 التي تعطي الحق في الإطلاع على ملفه الشخصي في أي وقت وبدون مبرر، ومخالفة هذا الالتزام يعرض المخالف للعقوبة من جانب اللجنة الوطنية للمعلومات والحريات CNIL أنظر: Voir, l'affaire société centrapel Conciel d' Etat 10eme 9 eme sous section reunies20/10/2010 n°327916 https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000022952197 .

[6] أنظر المادة 07 من القانون المغربي لحماية المعطيات الشخصية، المادة 32 من القانون الفرنسي، المادة 12 من الإرشاد الأوروبي46/95.

[7] أنظر الفقرة الأخيرة من المادة 34 من القانون 07/18.

المادة 40 من القانون 801/2004[1] ، وكذلك المشرع التونسي حيث تقضي المادة 32 من القانون 2004/63 المتعلق بحماية المعطيات الشخصية أنه "يقصد بحق النفاذ على معنى هذا القانون حق المعني بالأمر أو ورثته أو وليه في الإطلاع على جميع المعطيات الشخصية الخاصة به..."

والقضاء الفرنسي كان له موقف حاسم من هذه المسألة في قضية عرضت على مجلس الدولة تتعلق بقيام ورثة بتقديم طلب لجهة إدارية للإطلاع على ملف بيانات مورثتهم المتمثلة في قائمة بالحسابات البنكية، حتى يتم تصفية التركة وسداد الضرائب والديون، لكن إدارة البنك رفضت الإستجابة لهذا الطلب، فتم رفع دعوى أمام المحكمة الإدارية ب MELAN والتي قضت بإلغاء قرار الجهة الإدارية برفض حق الورثة في الإطلاع على حسابات مورثتهم، وعلى إثر الطعن ضد هذا الحكم أمام مجلس الدولة من طرف الإدارة، إلا أن هذا الأخير رفض الطعن لمخالفة الجهة الإدارية أحكام المواد 02 و 39 من القانون 17/78 مؤيدا بذلك حكم المحكمة الإدارية بموجب حكمه الصادر في 39 جوان 2011.[2]

الفرع الثاني الحقوق المتعلقة بالتصحيح والإعتراض

من الضمانات الوقائية الأساسية لحماية المعطيات الشخصية أثناء معالجتها في نظم المعلومات الشخصية، ضرورة ضمان حق كل شخص في تمكينه من حق تصحيح بياناته الشخصية، بسبب نقصها أو عدم صحتها أو الإعتراض على معالجتها في حال كانت هذه المعالجة مخالفة للأحكام القانونية.

أولا: الحق في التصحيح droit de rectification

المبدأ الذي يقوم عليه هذا الحق هو قدرة كل شخص علم بأن هناك بيانات شخصية تخصه مخزنة لدى جهاز من الأجهزة الحكومية أو مؤسسة خاصة، وقام بالإطلاع على هذه البيانات، أو حصل على نسخة منها، أن يطلب من الحائز لتلك البيانات الشخصية المتعلقة به والقائم عليها، أن يقوم بتصحيح الخاطئة أو الناقصة منها، ويعدل ما يشوبها من مغالطات لتتوافق مع الحقيقة، لكيلا يؤثر ذلك على مركزه لدى جمهور المتعاملين مع تلك الهيأة، بما قد يؤثر على سمعته ويسبب له خسائر لا سبيل له في تجنبها.[3]

وإذا كان الحق في التصحيح تمليه القواعد القانونية العامة، فإن التشريعات الخاصة بالمعلوماتية عملت على تنظيم هذا الحق، ومنها المشرع الجزائري الذي أعطى في المادة 35 من القانون 07/18 للشخص المعني بمعالجة بياناته الشخصية، الحق في تصحيح بياناته الشخصية أو استكمالها أو محوها أو تنقيحها، متى كانت هذه البيانات غير صحيحة أو غير كاملة أو غير مناسبة لتغيرها أو قدمها، أو متى كانت معالجتها أصلا

[1] Article 40/6 dispose que : « Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leurconnaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'untraitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération ledécès et procède aux mises à jour qui doivent en être la conséquence ».

[2] شريف يوسف خاطر، مرجع سابق، ص 90

Voir aussi CNIL 22e rapport d'activité 2001 La Documentation française - Paris, edition 2002, p35

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص113.

ممنوعة، كحال البيانات الشخصية الحساسة، ومن واجب المسؤول عن المعالجة متى كان الطلب مشروعا أن يبادر إلى تنفيذ العملية المطلوبة.[1]

وبهذه الصورة يعد حق التصحيح حقا أساسيا خوله المشرع للأشخاص المعنيين لغرض الرقابة على معالجة المعطيات الشخصية المتعلقة بهم، ومكملا للحق في الإعلام والحق في الولوج، ذلك أنه بعد إتاحة الفرصة للشخص المعني بالحق في الإعلام بكون معطياته ستكون محل معالجة من قبل جهة معينة، فيمكنه بعد ذلك الإطلاع عليها، من خلال حق الولوج، وعند اكتشافه لأي نقص أو خطئ في هذه المعطيات، كان له حينها الحق في طلب تصحيحها، فما هي إذن أحكام هذا الحق وإجراءات وطرق ممارسته.

1) أحكام الحق في التصحيح: يشكل الحق في التصحيح ضمانة أساسية لحماية الحق في الخصوصية المعلوماتية للأفراد، حيث يتيح لهؤلاء سلطة حقيقية لمراقبة مختلف المعالجات التي يمكن أن تكون معطياتهم الشخصية محلا لها، ومن ثم فهو يشكل بالمقابل التزاما على عاتق المسؤول عن المعالجة الذي يلزمه تصحيح أو إكمال المعطيات المعالجة، وبالتالي يكون للشخص المعني من خلال هذا الحق، الإمكانية في تصويب الأخطاء في المعطيات الشخصية المعالجة والمخزنة في نظام المعلومات الخاصة به، والتي من شأنها أن تولد لدى الغير فكرة مختلفة عن حقيقة الشخص، وله من جهة أخرى طلب محو البيانات التي تم تخزينها بطرق غير مشروعة.[2]

وهي الفكرة ذاتها التي قامت عليها صياغة نص المادة 35 من القانون 07/18 التي أعطت الحق للشخص المعني بالمعالجة أن يحصل من المسؤول عن المعالجة على:

-تصحيح أو تحيين أو مسح أو إغلاق المعطيات الشخصية التي تكون غير مكتملة أو غير صحيحة، أو تكون معالجتها ممنوعة قانونا.

وترتيبا على هذا الأساس يكون التصويب من خلال التحيين والتصحيح للمعطيات في الحالة التي يتبين فيها للشخص بعد اطلاعه على بياناته الشخصية والتي تم تجميعها وتخزينها بطريقة مشروعة، بأنها غير دقيقة أو أنها قديمة أو خاطئة، فيكون له الحق في هذه الحالة أن يطلب من الجهة القائمة على نظام المعلومات إجراء التصحيح والتحيين والتعديل المناسب الذي يتطابق مع حقيقة شخصيته، ويكون لزاما على هذه الجهة إجراء التصحيحات التي طلبها الشخص المعني، وإلا قامت مسؤوليتها القانونية على أي ضرر قد يلحقه جراء استمرارها في معالجة معطيات شخصية غير صحيحة عنه.

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص149.

[2] بولين أيوب، مرجع سابق، ص477. نقلا عن:

Ulrich seiber, the international handbook on computer crime, (computer related economic crime on the infringements of privacy) john wiley and sons, ltd 1986 p121.

وأما مطالبة الشخص بمحو البيانات أو مسحها أو جعل الوصول إليها غير ممكن، فيتعلق بالبيانات الشخصية التي تم تجميعها وتخزينها عنه بطريقة غير مشروعة، مثل تسجيل البيانات المحظورة، أو التي تم الحصول عليها بالغش والتدليس وكذلك البيانات القديمة[1].

وقد كانت الهيئة الوطنية الفرنسية للمعلوماتية والحريات (CNIL) قد وضعت لائحة بعدد من المعايير التي يجب العودة إليها لتقدير الإستجابة لطلب المحو،[2]ومن أهم هذه المعايير:

-يصبح الإلتزام بموجب طلب الحذف أكثر صرامة، متى كان الشخص المعني قاصرا، إنطلاقا من مبدأ تفضيل مصلحة الطفل على أية مصلحة أخرى.

في حال كانت البيانات المطلوب محوها مغلوطة، يفترض الإستجابة فورا لطلب المحو، على أن يقوم طالب المحو بتقديم الإثبات على ذلك إلى الهيأة الوطنية المسؤولة عن متابعة مسائل حماية البيانات الشخصية، أما في حال البيانات المفرطة أو المعتبرة غير ذات صلة، فلا بد من التمييز بين كونها خاصة بالحياة المهنية أو بالحياة الخاصة، إذ لا يتوجب الإلتزام بحذف الأولى، كون الحق في المحو يهدف إلى حماية الحياة الخاصة وليس إلى إخفاء ممارسات خاطئة من حق الجمهور الإطلاع عليها.

-لا يمكن محو المعلومات التي تشكل تشهيرا أو إهانة إلا بناء على حكم قضائي، أو بناء على قرار من الهيئة الوطنية للمعلوماتية والحريات cnil.

لابد من الإستجابة إلى طلب المحو في كل مرة تكشف البيانات المقصودة، العرق والمعتقد والآراء السياسية والميولات الجنسية، أو غير ذلك من البيانات الحساسة.

- ستجابة لطلب المحو إذا تعلق الأمر بقدم المعلومة، والمدة الزمنية التي توضع فيها في متناول الجمهور، لاسيما متى تعلقت بقرار إدانة صادر عن محكمة للدرجة الأولى تم إلغاؤه.

والملاحظ في نص المادة 35 من القانون 07/18 المنظمة لحق التصحيح، أن المشرع أسس سبب المطالبة بالتصحيح على كون أن المعطيات الشخصية تمت معالجتها بطريقة غير مطابقة للقانون، وذكر المشرع حالتين فقط تكون فيهما المعالجة كذلك، وهما إما بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات محل المعالجة، في حين تكون المعالجة غير مطابقة للقانون في حالات أخرى كثيرة، وليس فقط بسبب هاتين الحالتين، لذلك نجد أن المادة 40 من القانون الفرنسي رقم 17/78 المتعلق بالمعلوماتية والملفات والحريات جاءت بحالات أخرى وهي الطابع الملتبس أو غير الواضح أو المتقادم للمعطيات.[3]

ومن مقتضيات الحق في التصحيح أن يعطى الفرد هذا الحق في وقت مبكر، قبل أن يضار من المعلومات الخاطئة، كما يكون المسؤول عن المعالجة ملزما تجاه الشخص المعني بالقيام بالتصحيحات اللازمة التي

[1] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة، دار النهضة العربية، الطبعة الأولى، القاهرة، 2000، ص65

[2] La CNIL, droit au déreferencement les critères communs utilisés pour l'examen des plaintes, disponible sur le site : https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf visite le 30/01/2020.

[3] Yves Mayaud, op, cit, p 699.

تفرض نفسها في أقرب الآجال من إخطاره بالتصحيح من قبل الشخص المعني، لأجل ذلك فإننا نجد المشرع الجزائري ألزم المسؤول عن المعالجة أن يقوم بالتصحيح في أجل 10 أيام من إخطاره.[1]

وهنا يجب أن نميز بين حالتين في موقف المسؤول عن المعالجة تجاه طلب التصحيح.

الموقف الأول: وهو قبول المسؤول عن المعالجة طلب التصحيح، وموافقته على القيام إما بتحيين أو مسح أو تصحيح أو إغلاق المعطيات الشخصية حسب المطلوب منه، وفي هذه الحالة يكون المسؤول عن المعالجة حسب نص المادة 5/35 ملزما بتبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تدبير متخذ، إما التحيين أو التصحيح أو المسح أو الإغلاق ما لم يكن ذلك مستحيلا.

وما يلاحظ كذلك هنا أن المشرع لم يلزم المسؤول عن المعالجة بإخبار الشخص المعني صاحب المعطيات محل طلب التصحيح بالتدابير المتخذة في شأنها بعد استجابته للطلب، واكتفى فقط بإلزامه بإخبار الغير بهذا التصحيح، لكننا نرى أنه كان حريا بالمشرع الجزائري من باب أولى إلزام المسؤول عن المعالجة إخبار صاحب المعطيات بأية تدابير تدخل في إطار حق التصحيح، وهي حسب اعتقادنا مسألة جوهرية تتعلق بالممارسة الفعلية لهذا الحق، إذ كيف يصل الى علم المعني بالمعالجة أن المسؤول عن المعالجة قد استجاب لطلبه بالتصحيح، و إذا كان كذلك هل تم التصحيح حسب رغبته التي عبر عنها في الطلب أم لا.

لذلك فان المشرع الفرنسي ألزم المسؤول عن المعالجة إخبار الشخص المعني كتابة بما طرأ على بياناته من تصحيح مع إرفاق نسخة من التعديلات التي تم إجراؤها.[2]

بالإضافة إلى أن المشرع أسقط هذا الإخطار إذا كان ذلك مستحيلا دون أن يضع أي ضابط لتحديد متى يكون الإخطار ممكنا أو مستحيلا، ومن ثم يكون ذلك من تقدير القضاء في حالة وجود نزاع في المسألة.

أما الموقف الثاني: وهو رفض المسؤول عن المعالجة الإ ستجابة لطلب التصحيح المقدم له من طرف المعني، أو عدم الرد عليه بعد أجل 10 أيام من تقديمه للطلب، في هذه الحالة أعطى المشرع بنص المادة 4/35 للشخص المعني أن يودع طلب التصحيح لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وهذه الأخيرة بدورها تكلف أحد الأعضاء التابعين لها للقيام بإجراء تحقيقات،* تقرر السلطة بموجبها العمل على إجراء التصحيحات اللازمة وذلك في أقرب الآجال، مع ضرورة اطلاع المعني بالنتائج المتوصل إليها عن طريق إخباره بمآل طلبه.

[1] انظر المادة 35 البند ألف من المادة 40 من القانون 07/18

[2] L'article 40/2 de la loi 78/17 dispose que : « Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent ».

* ذهبت التشريعات الخاصة بالمعلوماتية إلى الخروج عن القواعد العامة في الإثبات والتي يكون حسبها على الشخص المعني عبء إثبات عدم صحة البيانات، لكن حسب هذه التشريعات أصبح عبء الإثبات على عاتق الجهة القائمة على نظم المعلومات، باستثناء الحالة التي يكون الشخص نفسه هو الذي قدم المعلومات، وذلك بهدف حماية الشخص من خلال جعل حق التصحيح أكثر فعالية، أنظر حسام الدين الأهواني، مرجع سابق، ص56.

وما يلاحظ في هذا السياق أن المشرع الجزائري لم يتطرق إلى الحالة التي قد ترفض فيها السلطة الوطنية القيام بإجراء التصحيح بناءا على نتائج التحقيقات المتوصل إليها، موافقة في ذلك رفض المسؤول عن المعالجة، وإن كنا نرى أنه لا يبقى للشخص المعني في هذه الحالة سوى اللجوء إلى القضاء المختص إعمالا للقواعد العامة.

ويبقى أن نشير إلى أن الحق في التصحيح باعتباره من الحقوق غير المالية الملازمة للشخصية، فإن ممارسته تتم من قبل الشخص نفسه، إلا إذا كان الشخص المعني ناقص أو عديم الأهلية فإن الولي أو الوصي هو الذي يقوم بممارسة هذا الحق نيابة عنه، وفي حالة وفاة الشخص يكون لورثته الحق في ممارسة هذا الحق، بهدف تصحيح كل ما من شأنه الإساءة إلى مورثهم، وهو ما أشار إليه المشرع الجزائري في الفقرة الأخيرة من المادة 35 في القانون 07/18 عندما نصت على "أنه يمكن استعمال الحق في التصحيح من قبل ورثة الشخص المعني،" كما يمكن أيضا أن يمارس حق التصحيح من غير الشخص المعني عندما لا يكون له الحق في الإطلاع بصفة مباشرة، ويكون لمن مارس حق الإطلاع على البيانات الحق في طلب تصحيحها وتحيينها، كما هو الحال بالنسبة للمريض، ففي هذه الحالة يكون للطبيب الذي اختاره المريض للإطلاع على البيانات الصحية له الحق في طلب تعديلها وتصويبها ومحوها.[1]

2) مبررات منح الشخص المعني الحق في التصحيح: إن من أهم مبررات إعطاء الشخص المعني الحق في التصحيح لبياناته الشخصية المعالجة:

- توفير قدر من الطمأنينة للشخص بصحة بياناته، ذلك أن اطمئنانه على ما تم تخزينه في نظم المعلومات من بيانات، وأنه يتفق وحقيقة ماهو في الواقع لا يتحقق فقط بالولوج، بل بما يكون له من حق في تصحيح الأخطاء.
- القدرة الفائقة للكومبيوتر في تجميع وتسجيل وتخزين واسترجاع قدر كبير من البيانات في وقت قصير، يسهل من إمكانية الوصول إلى البيانات الشخصية بطريقة غير مشروعة، وهو ما يجعل من نظم المعلومات تعتمد في جمعها وتخزينها للبيانات على وثائق غير موثوق بها أو على تحريات غير دقيقة، وهذا الأمر يستبعد معه وجود أخطاء من شأنها أن تعطي الغير فكرة مخالفة عن حقيقة الشخص،[2] ومن ثم فمن أجل تفادي ما قد يلحقه من أضرار البيانات الخاطئة، أعطي الشخص المعني الحق في طلب التصحيح كضمان وقائي لحماية خصوصيته.
- المخاطر الناتجة عن الأخطاء التقنية التي تحدث في جهاز الكومبيوتر قد يترتب عنها دمج بيانات مختلفة ببعضها أو اختلال في تصنيف وترتيب هذه البيانات، مما ينتج عنه نسبة بيانات معينة لشخص لا تتعلق به أصلا، من شأنها إعطاء فكرةغير حقيقية عن حالته الإجتماعية أو وضعه المالي أو انتمائه

[1] بولين أيوب، مرجع سابق، ص481.

[2] بولين أيوب، مرجع نفسه، ص 479.نقلا من:

Frédérique – Jérôme pansier, La criminalité sur internet, Édition puf. 2000.page 187.

السياسي، ومن ثم فمن أجل تفادي مثل هذه الأضرار قبل حصولها، يكون مبررا إعطاء الشخص المعني الحق في طلب التصحيح.[1]

ثانيا: الحق في الإعتـراض: droit doppsition

يعد الحق في اعتراض الشخص المعني على معالجة بياناته الشخصية أحد الحقوق الأساسية الممنوحة له لحماية خصوصيته، فهو بمثابة سلطة في مواجهة استعمال معطياته الشخصية من قبل المسؤول عن المعالجة أو من قبل الغير.[2]

ويعتبر هذا الحق أو الضمانة من أهم وأقدم ما أعطي للفرد في مواجهة تدخل الدولة في حياته الخاصة، وعملا به يكون للفرد أن يحتفظ لنفسه بجميع المعلومات التي تتعلق به، بل ويحدد ما يسمح للغير بالإطلاع عليه من هذه المعلومات، كما يحق له أن يرفض إعطاء بيانات عنه مرغما، وهذا هو الأصل ويجوز ذلك على سبيل الإستثناء.[3]

وعلى هذا الأساس يعود للفرد الحرية في رسم الأطر التي يريد أن يسمح للغير بالإطلاع على بياناته الخاصة، ولا يجوز إلزام الشخص بإعطاء بياناته الشخصية للغير أو للدولة إلا في الحالات الإستثنائية التي يلزمه بها القانون.[4]

ولقد عالج الشرع الجزائري الحق في الإعتراض بنص المادة 36 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث يحق حسبها للشخص المعني بالمعالجة أن يعترض على معالجة معطياته الشخصية لأسباب مشروعة، كما يحق له أن يرفض استعمال هذه المعطيات لأغراض دعائية لا سيما التجارية منها.

ومن ذلك يفهم من نص المادة 36 أنالمشرع قد ميز بين نوعين من الإعتراض، الأول يجب أن يكون مبررا بأسباب مشروعة، أما الثاني فلا يكون فيه الشخص المعين مجبرا على تقديم أي تبرير أو سبب.

1) حق الاعتراض المشروط: إنطلاقا من مقتضى الفقرة الأولى من المادة 36 من القانون 07/18 التي تنص على أنه يحق للشخص المعني أن يعترض ولأسباب مشروعة على معالجة معطياته الشخصية، فإنه يلزم أن يتضمن طلب الإعتراض الذي يقدمه الشخص المعني للجهة القائمة على معالجة معطياته الشخصية تبيانا للأسباب التي يستند إليها في اعتراضه على معالجة معطياته الشخصية، والتي يجب أن تكون أسبابا مشروعة بالإضافة إلى شرط آخر أضافته المادة 14 من التوجيه الأوروبي 46/95 وهو أن تكون الأسباب مرجحة بالإضافة إلى كونها مشروعة.[5]

[1] أسامة عبد الله قايد، مرجع سابق، ص160.

[2] André lucas. Jean deveze, Jean frayssinet, Op. Cit, Page 112.

[3] محمد عبد المحسن المقاطع، مرجع سابق، ص107.

[4] نعيم مغبغب، مرجع سابق، ص 204.

[5] Article14 : « droit d'opposition de la personne concernée : Les états membres reconnaissent à la personne concernée le droit : Au moins dans les cas visés à l'article 7 point " e et f " de s'opposer à tout moment pour des raisons prépondérantes et légitimes.

ولا شك أن هذين الشرطين سيطرحان مجموعة من الإشكالات تتعلق خاصة بكيفية تقدير مشروعية الأسباب، ومن هي الجهة أو الجهات المؤهلة للترجيح بين مصالح الشخص المعني ومصالح المسؤول عن المعالجة، وكذا حول العناصر التي يستند إليها هذا الأخير لرفض أو قبول الإستجابة للإعتراض، بالإضافة إلى الطابع المهم والذاتي للشرط المتعلق بكون الأسباب مرجحة[1]، وهو ما جعل أغلب التشريعات المنظمة للمعلوماتية لا تأخذ بهذا السبب ومنها المشرع الجزائري.

بالإضافة إلى شرط المشروعية لأسباب الإعتراض، أضافت الفقرة الأخيرة من المادة 36 شرطين آخرين وهما ألا تكون المعالجة تستجيب لإلتزام قانوني، و أن لا يكون الشخص المعني قد تنازل صراحة عن الحق في عتراض في المحرر الذي يأذن ويرخص بالمعالجة، وبالتالي فإذا كانت المعالجة تجري بناء على التزام قانوني على عاتق المسؤول عن المعالجة أو الشخص المعني، كما هو الحال بالنسبة للمعالجات التي تجريها مصالح الجمارك أو مصالح الضرائب مثلا، فإن الشخص المعني لا يتمتع بحق الإعتراض، وكذلك الأمر نفسه في حالة ما إذا كان الشخص المعني قد تنازل عن ممارسة هذا الحق في المحرر الذي يأذن بالمعالجة، حيث يتعين على المسؤول عن المعالجة أن يسأل المعني بالمعالجة عما إن كان يرغب في ممارسة حق الإعتراض أم لا، وذلك من خلال الوثيقة المستعملة كدعامة لجمع المعطيات، مع وجوب تمكين الشخص المعني من التعبير عن اختياره قبل المصادقة النهائية على الأجوبة.*

2) حق الاعتراض غير المشروط: إذا كان المشرع الجزائري قد اشترط ممارسة المعني بالمعالجة حق عتراض أن يكون ذلك مبنيا على أسباب مشروعة، وأن لا تكون المعالجة تستجيب لالتزام قانوني، وألا يكون الشخص المعني قد استبعد صراحة ممارسته لهذا الحق، فإنه لم يضع أي شرط بالنسبة لاعتراض الشخص المعني على استعمال بياناته الشخصية لأغراض دعائية، لا سيما التجارية منها، إذ له الحق في أن يقدم اعتراضه إلى المسؤول عن المعالجة الحالي أو إلى أي مسؤول عن معالجة لاحقة[2]، دون أن يكون ملزما في ذلك بتقديم أي سبب أو مبرر لهذا الإعتراض،حيث تخضع ممار سة هذا الحق للسلطة التقديرية الواسعة للشخص المعني.

وفي سياق متصل يتم الإعتراض عن المعالجة اللاحقة من خلال الإتصال بالمسؤول عن المعالجة أو إرسال بريد إلكتروني أو غير ذلك من وسائل الإتصال، وعلى الأنترنت يمكن للمستخدم بكل بساطة ممارسة حق عتراض بأن ينتقي ويختار الرفض في خانة الإختيار بين الرفض والموافقة، والتي ترد على نموذج جمع المعلومات.[3]

[1] أمنار ابراهيم، مرجع سابق، ص70.

* المشرع الجزائري لم يعالج هذه المسألة، لكن يمكن الإستناد إلى القانون المقارن، أنظر في هذا الإطار المادة 43 من المرسوم التطبيقي رقم 165.09.2 المؤرخ في 21 ماي 2009 لتطبيق القانون رقم 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المنشور في الجريدة الرسمية للمملكة المغربية 5744 مؤرخة في 18 يونيو 2009.

[2] أنظر الفقرة 02 من المادة36، من القانون 07/18.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص 148.

وما يمكن ملاحظته بعد هذا التحليل أن المشرع الجزائري لم يحدد أثر ممارسة الشخص المعني للحق في اعتراض، وهذا على خلاف المشرع التونسي الذي أكد في المادة 42 من القانون 204/63 المتعلق بحماية المعطيات الشخصية أن الإعتراض يوقف المعالجة فورا.

بالإضافة إلى ذلك لم يحدد المشرع الجزائري وقت إبداء الشخص المعني لاعتراضه، وهذا خلافا للمشرع المغربي الذي حدد بنص المادتين 43 و 44 من المرسوم 165.09.2 المتعلق بتطبيق القانون 09/08 المتعلق بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات الشخصية، أين فرق بين حالتين: الحالة التي يتم فيها جمع المعطيات الشخصية كتابة، فإن المعني بالمعالجة صاحب هذه المعطيات ينبغي عليه أن يعبر عن اعتراضه قبل التصديق النهائي على أجوبته عن الأسئلة التي يتلقاها من المسؤول عن المعالجة حول رغبته في إبداء الإعتراض من عدمه، والحالة الثانية وهي التي يكون جمع المعطيات الشخصية فيها بطريقة أخرى غير الكتابة، فإن المعني بالمعالجة يبدي اعتراضه في أي وقت، و قبل الإنتهاء من عملية الجمع لهذه المعطيات، ورغم ذلك فقد أشار المشرع الجزائري إلى وقت إبداء الشخص المعني بالمعالجة اعتراضه على استعمال بياناته الشخصية عندما يتعلق الأمر بالإستكشاف المباشر، ويكون ذلك وقت جمع هذه المعطيات، وكذا كلما وجه إليه بريد إلكتروني لأجل الإستكشاف أو التنقيب الإلكتروني، و الذي يعد الإعتراض عليه أحد الحقوق غير مباشرة التي يتمتع بها الشخص المعني بالمعالجة[1].

ثالثا: حق منع ستكشاف المباشر: Interdiction de la prospection directe

يعتبر منع الإستكشاف المباشر من بين الحقوق التي يتمتع بها المعني بالمعالجة، إضافة إلى حقه في الإعلام والولوج والتصحيح والإعتراض،وهو حق منع الاستكشاف أو كما تسميه تشريعات أخرى الاستقراء المباشر أو التنقيب المباشر لمعطياته ذات الطابع الشخصي، فماذا يقصد بهذا الحق وماهي أحكامه؟

1)تعريف الإستكشاف المباشر: هو عملية إشهارية دعائية محظة، تلجؤ إليها الشركات التجارية، مستغلة قواعد بيانات متوفرة في الغالب لدى متعاملي الإتصالات، تتعلق بزبائنهم وتشمل عناوينهم، أرقام هواتفهم المحمولة، أرقام الفاكس، العنوان الالكتروني "iP " ... وذلك بغرض توجيه إليهم رسائل ذات مضامين تجارية دعائية، إلى فئات مختلفة من الأشخاص من خلال معايير إجتماعية وإقتصادية مدروسة، لعرض عليهم السلعة أو الخدمة الملائمة لكل فئة عبر وسائل الإتصال[2].

ولقد عرف المشرع الجزائري الإستكشاف المباشر في المادة 03 من القانون 07/18، بأنه إرسال أي رسالة مهما كانت دعامتها وطبيعتها موجهة للترويج المباشر وغير المباشر لسلع وخدمات، أو لسمعة شخص يبيع سلعا أو يقدم خدمات، وبذلك يجد الشخص نفسه مضطرا لاستقبال رسائل إشهارية غير مرغوب فيها، لا سيما إذا روجت لخدمات مشبوهة تشوش عليه باستمرار، مثل الإشهارات المتعلقة بالملاهي الليلية أو

[1] ، أنظر المادة 3/37 من القانون 07/18.

[2] يعتبر الإستكشاف المباشر عصب حرب التنمية التجارية، ذلك أن الشركة التجارية التي لها القدرة على استكشاف عملاء جدد هي القادرة على التطور أنظر في ذلك:

René moulinier, prospection commerciale. Stratégie et tactiques pour acquérir de nouveaux clients, revue et augmentée EYROLLES édition d'organisation, 3eme édition, SEBTEMBER 2009.page 11.

الدعاية لمنتجات من خلال صور فاضحة وغيرها من الأمور التي قد ينتج عنها مشاكل عائلية، أو تترك أثرا سلبيا وسيئا على نفسية المرسل إليه.[1]

لأجل ذلك فإنه مما لا شك فيه أن توسيع المشرع الحق في الإعتراض على المعالجة التي يكون غرضها ستكشاف مباشرة للمعطيات الشخصية لأشخاص طبيعيين دون ضرورة إحترام موافقتهم ورضاهم بذلك هو من باب الوقاية للحق في الخصوصية المعلوماتية، من خلال حماية المعطيات الشخصية من هذا النوع من المعالجة، وهو في نفس الوقت يشكل واجبا يفرض على المسؤولين عن المعالجة الإمتناع عن استعمال بيانات شخص طبيعي مهما كان شكلها، لم يعبر عن رضاه بشأن استقبال استكشافات مباشرة.

2)أحكام الحق في منع الإستكشاف المباشر: يعد الإستكشاف المباشر من بين أهم المشكلات التي تتعلق بحماية البيانات الشخصية في المعاملات الإلكترونية ومنها التجارة الإلكترونية، لذلك فقد حثت التوجيهات الأوروبية الصادرة في هذا المجال الدول الأعضاء في الإتحاد الأوروبي إلى إعطاء المستهلك الحق عتراض وبدون مقابل على معالجة بياناته الشخصية إذا استخدمت لأغراض التسويق المباشر، كما في أغراض الدعاية لخدمة أو سلعة تقدم عبر الأنترنت.

لذلك اتجهت أغلب التشريعات المقارنة إلى تقرير عدم جواز إجراء إتصالات لأغراض الإستكشاف المباشر دون رضا المشترك بخدمة الأنترنت والبريد الإلكتروني.

والمشرع الجزائري على غرار هذه التشريعات، اعتبر أن التنقيب أو ستكشاف عن المعطيات الشخصية لشخص طبيعي بصورة مباشرة دون الحصول على موافقته المسبقة عملية غير مشروعة، وقد جاءت المادة 37 من القانون 07/18 واضحة في هذا الشأن،عندما أكدت صراحة على منع الإستكشاف المباشر الذي يكون بواسطة آلية اتصال أو جهاز الإستنساخ البعدي أو البريد الإلكتروني أو بواسطة أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، ويستعمل بيانات شخصية لم يعبر صاحبها عن رضاه المسبق على استقبال مثل هذه الإستكشافات، ولقد نص المشرع الفرنسي عن عملية الإستكشاف المباشر في قانون البريد والإتصالات، واعتبره عملية تستعمل من أجل إنشاء روابط بين الشركة وعملائها، فيتم إخبارهم على الفور بالعروض التجارية المختلفة التي تقدمها علاماتهم التجارية، وجاءت المادة 05/34 من هذا القانون لتقيد هذه الممارسة وتخضعها لقواعد صارمة، حيث يحضر حسبها ستكشاف المباشر عن طريق أنظمة الإتصال والإتصال الآلي أو البريد الإلكتروني باستخدام تفاصيل الإتصال الخاصة بشخص طبيعي أو مشترك لم يعرب عن موافقته من قبل عن تلقي الإستكشاف المباشر بهذه الطريقة.

إلا أن المشرع الجزائري في المادة 2/37 من القانون 07/18 واستثناءا على هذا المنع، أجاز إمكانية القيام بالاستكشاف المباشر عن طريق البريد الإلكتروني إذا ما توافرت الشروط التالية.

- أن تطلب البيانات مباشرة من المرسل إليه.

[1] العربي جنان، مرجع سابق، ص74.

- أن يكون الإستكشاف بمناسبة عمليات بيع أو تقديم خدمات.
- أن يكون الإستكشاف المباشر يخص منتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي أو المعنوي.
- إذا تبين للمرسل إليه بشكل صريح لا يشوبه لبس إمكانية إعتراض الشخص بإرسال الرفض على استعمال بياناته وقت جمع هذه البيانات، كلما وجه إليه بريد إلكتروني لأجل الإستكشاف.[1]

ومن أجل توفير حماية أكبر في هذا الشأن للأشخاص المعنيين، فإنه يلزم في كافة الأحوال التي يتم فيها إرسال رسائل بواسطة آليات الإتصال الهاتفي وجهاز الإستنساخ البعدي والبريد الإلكتروني من أجل ستكشاف المباشر، أن تتم الإشارة إلى بيانات صحيحة ومتعلقة فعلا بالمرسل لهذه الإعلانات الدعائية، بغية تمكين المرسل إليه من إرسال طلب توقيف هذه الإيصالات، لذلك فإنه يمنع إخفاء هوية الشخص الذي أرسلت لفائدته الرسائل وعدم ذكر المواضيع التي لا علاقة لها بالخدمات المقترحة، وهذا لمنع خداع متلقي عملية الإستكشاف.[2]

المبحث الثاني: الضوابط القانونية الإجرائية لحماية المعطيات ذات الطابع الشخصي

إن قيام الدولة والأجهزة التابعة لها أو قطاع الأعمال الخاص بإنشاء نظم المعلومات الآلية أو ما يسمى أيضا بقواعد البيانات، ليس من الأمور المطلقة دون ضوابط فقد وضعت التشريعات المقارنة مجموعة من الضوابط والضمانات التي تهدف الى رقابة فعالة على إنشاء قواعد البيانات وكيفية استخدامها[3].

وبشكل عام تفرض هذه التشريعات ضرورة إتمام إجراءات مسبقة قبل البدء في أية عملية لمعالجة البيانات الشخصية، تتنوع هذه الإجراءات بين التصريح أو الإعلام البسيط أو ضرورة الحصول على ترخيص مسبق.

وتعد هذه الإجراءات من أساسيات الشفافية في التعامل مع المعطيات ذات الطابع الشخصي كونها تفتح أمام السلطة المختصة بحماية المعطيات الشخصية ليس فقط إمكانية ممارسة مهمتها في ضمان حماية حقوق الأشخاص أصحاب البيانات الشخصية، بل يتيح لها أيضا إجراء الرقابة اللازمة على مدى تقيد المسؤولين عن المعالجة بالأحكام القانونية المقررة والتوصيات والإجراءات، ويعتبر عدم إتمام هذه الإجراءات سببا لإقرار عدم مشروعية أي معالجة للمعطيات الشخصية. (المطلب الأول)

ومن جانب آخر فإن هذه النظم المعلوماتية تتبع وسائل أمان عديدة من أجل الحفاظ على البيانات الشخصية محل المعالجة، وتتسم بالسرية والقدرة على حماية هذه البيانات التي يشملها النظام

[1] انظر المادة 2/37 من القانون 07/18.

[2] انظر الفقرة الأخيرة من المادة 37 من القانون 07/18.

[3] عمر أحمد حسبوا، مرجع سابق، ص 91.

المعلوماتي والتي يحكمها عدة عوامل أهمها سرية البيانات والحرية في تداولها و إتاحتها وكذا سلامة البيانات ذاتها[1]، ويعتبر توفير هذه الوسائل من أهم التزامات القائمين على هذه النظم المعلوماتية. (المطلب الثاني)

وبالنظر الى وجود مشاكل تتعلق بحماية البيانات الشخصية في المعاملات الإلكترونية ومنها على الخصوص التجارة الإلكترونية، فقد عملت تشريعات على إعطاء مزودي خدمة الأنترنت دورا في إطار توفير نوع من الحماية للمعطيات الشخصية. (المطلب الثالث)

المطلب الأول: إحترام الإجراءات المسبقة على معالجة المعطيات ذات الطابع الشخصي:

على غرار الإتفاقية الأوروبية لحماية الأشخاص الطبيعيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي وكذا الإرشادات الأوروبية والتشريعات المقارنة في هذا المجال، فإن المشرع الجزائري وضع جملةمن الإ جراءات المسبقة التي تقع على عاتق المسؤول عن المعالجة، من شأنها توفير حماية للأشخاص المعنيين بمعالجة معطياتهم الشخصية من جهة، وتميكن المسؤولين عن المعالجة من إيجاد إطار قانوني واضح وصريح لتطوير معالجة المعطيات الشخصية على أساس احترام الشرعية القانونية ومقتضيات الثقة التي يجب أن تكون متبادلة مع الأشخاص المعنيين، ومن جهة أخرى إعطاء الجهة المختصة لحماية المعطيات الشخصية ممارسة دورها الإشرافي والرقابي بشكل يكفل التطبيق الدقيق لقانون حماية المعطيات.

وبناء على ذلك فان كل شخص طبيعي أو معنوي ينتمي للقطاع العام أو الخاص يقوم بمعالجة معطيات ذات طابع شخصي يعتبر معنيا باحترام هذه الإجراءات القانونية بغض النظر عن غاية أو خطورة المعالجة، وبالتالي فإن المشرع يفرض قبل الإنطلاق أو البدء في إنشاء ملفات معلوماتية تحتوي على معطيات شخصية أو تنفيذ معالجة آليه لمعطيات شخصية، التصريح لدى السلطة الوطنية لحماية المعطيات الشخصية ما لم يكن الأمر يستوجب أو يندرج تحت نظام الترخيص المسبق.

الفرع الأول: التصريح المسبق لدى السلطة الوطنية لحماية المعطيات الشخصية

تخضع معالجة المعطيات الشخصية بشكل عام إلى تصريح من قبل المسؤول عن المعالجة لدى السلطة الوطنية لحماية المعطيات الشخصية، وهو بمثابة إخطار لهذه السلطة بتنفيذ وإنجاز عمليات معالجة تنصب على معطيات ذات طابع شخصي، وتطبيقا لذلك جاءت المادة 12 من القانون 07/18 لتـ , خضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية لحماية المعطيات الشخصية[2]، وتتمثل الغاية الأساسية من هذا الإجراء في تمكين السلطة الوطنية من ممارسة مهامها المتعلقة بالمراقبة والتحقق من مدى إحترام المسؤول عن معالجة معطيات شخصية لمقتضيات القانون، لذلك يلزم على كل مسؤول عن المعالجة أو من يمثله قبل كل معالجه كلية أو جزئية لمعطيات شخصية أو مجموع معالجات لها غاية واحدة أو غايات مرتبطة، أن يقوم بإيداع هذا التصريح بالمعالجة

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص 97.

[2] تنص المادة 12 من القانون 07/18 " مالم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية... طبقا لأ حكام المنصوص عليها في هذا القانون".

لدى السلطة الوطنية، أو بإرساله إليها عبر البريد العادي أو الإلكتروني يتضمن تعهدا بتنفيذه لمعالجة المعطيات الشخصية وفقا لأحكام القانون، وهو نفس الإجراء الذي نص عليه المشرع الفرنسي في المادة 23 من القانون 17/78 [1].

وقد ميز المشرع في القانون 18/07 بين ثلاث أنواع من التصريحات المسبقة:

- **التصريح العادي** وهو الصنف الذي يشكل القاعدة لمثل هذا الإجراء، ويستوجب فيه القانون أن يتضمن البيانات المذكورة في المادة 14 من القانون 07/18 [*].

- **التصريح البسيط Une déclaration simplifiée :**وهو الإجراء الذي أجازته المادة 15 من القانون 07/18 ويتعلق بالمعالجات التي ليس من شأنها أن تحمل معها الإضرار بحقوق وحريات الأشخاص المعنيين بالمعالجة وحياتهم الخاصة، وقد سعى كذلك، لتخفيف المشرع من صرامة وثقل البيانات الواجب الإلتزام بها[2]كما هو الشأن في التصريح العادي، حيث يتضمن فقط الإ شارة إلى:

- إسم وعنوان المسؤول عن المعالجة.

- طبيعة المعالجة وخصائصها والغرض منها.

- تحديد الأشخاص المعنيين بالمعالجة وكذا المعطيات الشخصية محل المعالجة.

- تحديد الجهات التي يمكن أن ترسل إليها هذه المعطيات، وكذا تحديد المعطيات الشخصية التي يعتزم إرسالها الى دول أجنبية، بالإضافة الى تحديد مدة حفظ هذه المعطيات بنظم المعالجة.

---

[1] Article 23 de la loi 78/17 dispose que : « la déclaration comporte l'engagement satisfait aux exigences de la loi elle peut adresser à la commission nationale de l'informatique par voie électronique ».

[*] تتمثل البيانات الإلزامية التي يجب أن يتضمنها التصريح المقدم إلى السلطة الوطنية من طرف المسؤول عن المعالجة فيما يلي:

1- إسم وعنوان المسؤول عن المعالجة وعند الإقتضاء إسم وعنوان ممثله.

2- طبيعة المعالجة وخصائصها والأغراض المقصودة منها.

3- وصف للأشخاص المعنيين بالمعالجة وكذا وصف للمعطيات الشخصية محل المعالجة المتعلقة بهم.

4- تحديد الأشخاص الذين قد ترسل إليهم هذه المعطيات.

5- تحديد طبيعة المعطيات التي من المعتزم إرسالها إلى دول أجنبية.

6- تحديد مدة حفظ هذه المعطيات.

7- تحديد المصلحة أو الجهة التي يمكن للشخص المعني بالمعالجة صاحب المعطيات الشخصية أن يمارس لديها حقوقه المخولة له بموجب هذا القانون.

8- ذكر وصف عام للمعالجة، يمكن من خلاله للسلطة الوطنية أن تعد تقييما أوليا لمدى ملائمة وصلاحية التدابير المتخذة من طرف المسؤول عن المعالجة لضمان سرية وأمن المعالجة.

9- تحديد فيما إذا كان هناك شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين المعطيات المعالجة مع معطيات أخرى سواء التي يمسكها نفس المسؤول عن المعالجة أو مسؤولون آخرون عن المعالجة، وكذا سواء كانت معالجتها لنفس الغرض أو لأغراض أخرى.

10- بالإضافة إلى تحديد فيما إذا كانت هذه المعطيات الشخصية يمكن أن تخضع لمعالجة من الباطن سواء مجانا أو بمقابل.

[2] Etien-GNOAN N'Da brigitte, l'encadrement juridique de la gestion éléctronique des données médicales, Thèse pour obtenir le grade de docteur en droit, l'Université Lille 2- droit et santé, décembre 2014, p44.

ومن ثم يظهر أن المشرع لم يستلزم في هذا النوع من التصريح سوى بعض البيانات فقط من بين تلك التي اشترط أن يتضمنها التصريح العادي.

وقد أسند المشرع مهمة تحديد أصناف وفئات معالجات المعطيات الشخصية التي تخضع لهذا التصريح المبسط للسلطة الوطنية لحماية المعطيات[1] ، إنطلاقا من معيار درجة خطورة هذه المعالجات على الحياة الخاصة للمعنيين بالمعالجة، ويضيف المشرع الفرنسي أن إعداد اللجنة الوطنية للمعلوماتية والحريات (CNIL) قائمة بفئات المعالجات التي تخضع لمجرد التصريح المبسط يكون بعد تلقيها لمقترحات من طرف ممثلي الهيئات العامة أو الخاصة التي تتولى معالجة المعطيات الشخصية.[2]

وغالبا ما تندرج المعالجات التي تخضع لمجرد التصريح البسيط ضمن فئات المعالجات الأكثر شيوعا وتداولا، سيما تلك المستعملة في إطار المواقع الإلكترونية، وكذلك المعالجات الآلية المختلفة للمعطيات الشخصية المنفذة من قبل الإدارات المرتبطة بأنشطتها الإدارية اليومية المعتادة[3]، مثل معالجة المعطيات الشخصية المرتبطة بالتنظيم الإدراي والمحاسبي والتربوي للمؤسسات التعليمية[4]، أو المعالجات المرتبطة بالحوسبة الوثائقية كإعارات الكتب والإطلاع على وثائق الأرشيف العام.[5]

وهي مسألة أكدها المشرع الفرنسي في الفقرة الأولى من المادة 24 من القانون 17/78[6] ، مستلهما لها من المادة 18 من التوجيه الأوروبي 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية تداولها.[7]

ومن ثم فإن التصريح المبسط يرد على المعالجات التي تبدو فيها مخاطر المساس بالحريات والحق في الخصوصية لأصحاب المعطيات الشخصية أقل خطورة مما هو عليه الحال بالنسبة للمعالجات التي تستوجب تصريحا عاديا.

وسواء تعلق الأمر بالتصريح العادي أو بالتصريح المبسط فإن المسؤول عن المعالجة الذي ينجز العديد من المعالجات يخضع لتصريح واحد يشملها جميعا، شريطة أن تكون هذه المعالجات تنتمي لنفس الهيئة ولها

---

[1] تنص المادة 15 من القانون 07/18 على "أن السلطة الوطنية تحدد قائمة بأصناف معالجات المعطيات ذات الطابع الشخصي التي ... تكون محل تصريح مبسط..."

[2] Voir l'article 24-I de la loi 78/17.

[3] Nathalie MALLET-POUJOL Protection de la vie privée et des données personnelles, Pôle Droit de la Communication Université Montpellier I- UMR 5815 LEGAMEDIA Février 2004 p 49, disponible sur le site : https://eduscol.education.fr/chrgt/guideViePrivee.pdf

[4] La délibération de la CNIL n° 86- 115 du 2 décembre 1986 concernant les traitements automatisés des données personnelles relatifs à la gestion administrative, comptable et pédagogique des établissements d'enseignement du secteur privé, disponible sur le site : https://beta.legifrance.gouv.fr

[5] Délibération de la CNIL n° 99/27 du 22 avril 1999 concernant les traitements automatisés des données personnelles relatif à la gestion des prêts des livres du support audiovisuel œuvre artistique et la gestion de consultation de documents d'archives publiques, JORF n °121 du 28 mai 1999, legifrance.gouv.fr

[6] Article 24 de la loi 78/17 dispose que : " Pour les catégories les plus courantes de traitement de données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission Nationale de l'Informatique et des libertés établit et publie d'énormes destiner à simplifier l'obligation de déclaration."

[7] Voir l'article 18/2 de la directive 46/95 du 24 octobre 1995.

نفس الأغراض ذات الصلة،[1] حيث يمكن أن تكون المعالجات التابعة لنفس المسؤول عن المعالجة والتي تتم لنفس الغرض أو لأغراض مرتبطة، محل تصريح واحد[2].

وإذا كان هذا التصريحان العادي والمبسط إجراءان من طبيعة إلزامية يتعين على المسؤول على المعالجة التقيد بضرورة تقديمها لدى السلطة الوطنية قبل تنفيذ أي معالجة لمعطيات شخصية، فإن هناك بعض الأصناف من المعالجات أعفى فيها المشرع المسؤول عن المعالجة الإلتزام بهذا الإجراء، وذلك بسبب الطبيعة غير الضارة نسبيا لهذه المعالجات على الخصوصية المعلوماتية، ويرتبط أساسا هذا الإعفاء القانوني من التصريح المسبق بالمعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطلع عليه عموم الجمهور.[3]

غير أن المشرع استعاظ عن إعفاء المسؤول عن المعالجة من التصريح المسبق بإخضاعه لالتزامات أخرى، أي أن إعفاءه من الإلتزام بالتصريح المسبق لا يعفيه من التزامات أخرى تتمثل تحديدا في وجوب تعيين شخص يكشف للجمهور عن هويته، ويبلغ بها السلطة الوطنية،فيكون هذا الأ خير مسؤولا عن معالجة هذه المعطيات في إطار تطبيق الأ حكام المتعلقة بحقوق الأشخاص المعنيين بهذه المعالجة والمنصوص عليها في القانون 07/18[4]، كما يجب عليه أيضا أن يرسل إلى كل شخص معني بهذه المعالجة المعلومات المتعلقة بالغاية والغرض من المعالجة وهوية المسؤول عنها، وطبيعة المعطيات التي تتم معالجتها والجهات التي تكون قد أرسلت إليها هذه المعطيات، إذا طلب منه الشخص المعني ذلك.[5]

وينص المشرع الفرنسي[6] وكذلك المغربي[7] على أن من صلاحيات اللجنة الوطنية لحماية المعطيات الشخصية أن تعد قائمة بالمعالجات التي تستجيب لمستلزمات الإعفاء من التصريح المسبق، وهو ما لم ينص عليه المشرع الجزائري، ويكون هذا الاعفاء بقرار صريح منها[8].

---

[1] أنظر المادة 16 من القانون 07/18:" أو يطلع عليه كل شخص يثبت أن له مصلحة مشروعة في ذلك".

[2] المادة 3/13 من القانون 07/18 أنظر كذلك:

Guides de la CNIL, les avocats et la loi informatique et libertés, édition 2011. P 08 disponible sur le site/ http://www.droit-technologie.org

وتقابلها المادة II/23 من القانون الفرنسي 17/78:

"Les traitements relevant d'un même organisme et ayant des finalités indentiques ou liées entres elles peuvent faire l'objet d'une déclaration unique"

[3] Etien-Gnoan N'Da Brigitte, OP.CIT.P46.

[4] أنظر الفقرة 02 من المادة 16 من القانون 07/18.

[5] أنظر الفقرة 03 من المادة 16 من القانون 07/18.

[6] L'article 24/II de la Loi 78/17 dispose que : " la commission peut définir parmi les catégories de traitement mentionnees au I, celles qui compte tenu de leurs finalités de leurs destinataires ou catégories de destinataires, des données à caractère personnel traité de la durée de conservation de celle-ci et des catégories de personnes concernées sont disponsés de déclaration"

[7] تنص المادة 18 للفقرة الأخير من القانون المغربي 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي: "تحدد اللجنة الوطنية قائمة المعالجات التي تستجيب لعدم تطبيق إلزامية التصريح بموجب مقرر يخضع لمصادقة الحكومة".

[8] Les guides de la CNIL, guide les avocats et la loi informatique et libertés op, cit, p07.

ويضيف المشرع الفرنسي لأسباب الإعفاء من التصريح المسبق علاوة عن كون المعالجات من الفئات المعتادة و ليس من شأنها أن تحمل إعتداء على الحياة الخاصة والحريات الفردية لأصحاب المعطيات المعالجة، سببا آخرتعلق بالحالة التي يـ ،عين فيها المسؤول عن المعالجة مراسل حماية المعطيات الشخصية، والذي يكلف بشكل مستقل ضمان الإ متثال للإلتزامات الأخرى المنصوص عليها في القانون، لما له من دراية كافية بالمهام الموكولة إليه، ويتولى إبلاغ اللجنة الوطنية للمعلوماتية والحريات عن أي مساس بالمعطيات الشخصية، كما يلتزم بالقائمة المحددة للمعالجات المعفاة من التصريح والتي يتم إطلاع الأشخاص عليها بناء على طلبهم،[1]حيث تنص المادة 23 من القانون 17/78 على أن المعالجات التي يعين فيها المسؤول عنها مراسلا لحماية المعطيات الشخصية تعفى من الإجراءات الشكلية المنصوص عليها في المادتين 23 (المتعلقة بالتصريح) و24 (المتعلقة بالتصريح المبسط) باستثناء الحالات التي يتوخى فيها نقل المعطيات الشخصية إلى دولة أخرى ليست عضوا في الإتحاد الاوروبي.[2]

كما اعتبر المشرع الفرنسي أيضا أنه لا تخضع لإجراء التصريح المسبق المعالجات التي تتم طبقا للبند 03 من الفقرة II من المادة الثامنة من القانون 17/78 ،وهي المتعلقة بالمعالجات التي تقوم بها الجمعيات وكل الهيئات الأخرى التي لا تهدف إلى الربح، أو ذات طبيعة دينية وفلسفية وسياسية أو نقابية، شريطة أن تنصب هذه المعالجات على المعطيات الحساسة المذكورة في الفقرة I من المادة 08 والمرتبطة فقط بأعضاء هذه الجمعيات أو الهيئات، وإن لزم الأمر كذلك بالمعطيات الشخصية للأشخاص الذين لديهم اتصال منتظم معها، وذلك في سبيل تنفيذ أغراضها الشرعية، مع الإلتزام بعدم إرسال هذه المعطيات إلى الغير دون موافقة الأشخاص المعنيين.

وإذا كان المشرع الفرنسي قد أعفى هذه المعالجات بهذه الصورة من الخضوع لأي إجراء شكلي مسبق، فإن المشرع الجزائري نجده قد أخضع هذه المعالجات ليس لنظام التصريح فقط بل لنظام الترخيص، كما سوف نرى في حينه.

أما عن إجراءات هذا التصريح فإنه عبارة عن طلب يودع لدى السلطة الوطنية، أو يقدم بالطريق الإلكتروني، وفي فرنسا نجد أن اللجنة الوطنية للمعلوماتية والحريات (CNIL) وضعت نموذجا بمواصفات محددة على موقعها الإلكتروني يمكن للمؤسسات والهيئات والإدارات المضي قدما عبر الأنترنت لملئ ذلك النموذج تحت عنوان "أعلن عن ملف" «déclarer un fichier» عبر الرابط

. https://www.cnil.fr/fr/déclare-un-fichier

[1] أنظر في هذا الموضوع شريف يوسف خاطر، مرجع سابق، ص 62.

[2] L'article 22-III de la Loi 78/17 Prévoit que : " Les traitements pour les quels le responsable a désigné Un correspondant à la protection des données à caractère personnel... Sont disponsés des formalités prévues aux article 23 (déclaration) et 24 (déclaration simplifiée), Sauf lorsqu'un transfert de données à caractère personnel à destination d'un état non membre de communauté européenne et envisagé"

وتنص المادة 2/13 من القانون الجزائري 07/18 على أن السلطة الوطنية تسلم لصاحب التصريح وصلا بالإيداع، أو يرسل إليه بالطريق الإلكتروني فورا أو في أجل أقصاه 48 ساعة[1]، وحينها وبمجرد استلام المسؤول عن المعالجة لهذا الوصل يمكنه أن يباشر إجراءات المعالجة تحت مسؤوليته في احترام القواعد والضمانات التي تضمنها التصريح.

الفرع الثاني: الترخيص المسبق من طرف السلطة الوطنية لحماية المعطيات الشخصية

إنطلاقا من المادة 17 من القانون 07/18، فإن المشرع استثنى بعض المعالجات للمعطيات ذات الطابع الشخصي التي لا يكفي فيها مجرد التصريح لإنجازها، وإنما يستوجب فضلا عن التصريح بها لدى السلطة الوطنية، ضرورة الحصول على ترخيص مسبق من طرف هذه الأخيرة، وهذا الإجراء مخصص لأجل المعالجات التي قد تشكل مخاطر معينة على حقوق وحريات الأشخاص المعنيين بالمعالجة، وهو بمثابة رقابة قبلية للسلطة الوطنية على كل معالجة للمعطيات الشخصية قبل البدء في إنجازها.[2]

حيث تقرر السلطة الوطنية إخضاع معالجة المعطيات الشخصية لنظام الترخيص المسبق عندما يتبين لها عند دراستها للتصريح المقدم لها من طرف المسؤول عن المعالجة، أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة من شأنها المساس باحترام وحماية الحياة الخاصة والحقوق الأساسية للأشخاص، ويأتي هذا انسجاما مع حرص المشرع على احترام وتكريس المبادئ الأساسية التي تقوم عليها معالجة المعطيات الشخصية الواردة في المادة 02 من نفس القانون[3]، فإذا تقدم المسؤول عن المعالجة بتصريح لدى السلطة الوطنية فإن هذه الأخيرة عند تداولها وبحثها في طبيعة المعطيات الشخصية محل المعالجة، والغرض منها ومدى انطوائها على مخاطر في مواجهة الحق في الخصوصية، فان لها أن تقرر بعد ذلك إخضاع هذه المعالجة لنظام أكثر حماية يتمثل في نظام الترخيص المسبق، ولا يمكن على هذا الأساس للمسؤول عن المعالجة تنفيذ أي معالجة إلا بعد الترخيص له من طرف السلطة الوطنية .

بالإضافة إلى أن المشرع قد حدد حالات على سبيل الحصر تخضع معالجة المعطيات فيها إلى ضرورة الترخيص المسبق وتشمل مايلي:

أولا: معالجة المعطيات الحساسة: وهي المعطيات ذات الطابع الشخصي التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص أو حالته الصحية بما في ذلك معطياته الجينية.[4]

[1] المشرع الفرنسي لا يشترط أجلا معيا لتسليم وصل الإيداع، حيث تنص المادة 23 من القانون 17/78:

La commission délivrée sans délai un récépissé »

[2] Voir l'article 20 de la directive 95/46/CE Du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[3] تنص المادة 02 من القانون 07/18 على أنه "يجب أن تتم معالجة المعطيات ذات الطابع الشخصي في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم".

[4] أنظر المادة 03 من القانون 07/18.

وإذا كان المبدأ عند المشرع هو وضع قاعدة مقتضاها منع أي معالجة تنصب على مثل هذه الطائفة من المعطيات الشخصية،[1] فإنه استثنى من ذلك المعالجات التي تتم بناء على الموافقة الصريحة للشخص المعني صاحب هذه المعطيات، أو عندما يوجد نص قانوني يقضي بلزوم معالجتها لتنفيذ غرض معين، أو بترخيص من السلطة الوطنية.

وعلى هذا الأساس فمن دون الحالتين الأولتين، أي الموافقة الصريحة للشخص المعني بالمعالجة أو وجود نص قانوني يجيز معالجة المعطيات الحساسة*، فإن كل معالجة تتعلق بأي من هذه المعطيات لا تكون مشروعة إلا بلزوم الحصول على ترخيص مسبق من السلطة الوطنية، ويكون ذلك في حالات معينة نص عليها المشرع صراحة في المادة 18 من القانون 07/18 وتتعلق تحديدا بـ:

-معالجة المعطيات الحساسة لأسباب تتعلق بالمصلحة العامة، وتكون في نفس الوقت ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة.

- إذا كانت معالجة المعطيات الحساسة ضرورية لحماية المصالح الحيوية للشخص المعني.

- إذا كان الشخص المعني بالمعالجة في حالة عجز بدني أو قانوني يكون مانعا له عن الإدلاء بموافقته.

- تنفيذ معالجات تنصب على معطيات حساسة من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي في إطار نشاطاتها الشرعية، شريطة أن تخص المعالجة فقط أعضاء هذه المنظمة أو الأشخاص الذين تربطهم بها إتصالات منتظمة تتعلق بغاياتها، وألا ترسل هذه المعطيات إلى الغير دون موافقة الأشخاص المعنيين.

- إذا كانت المعالجة تنصب على معطيات شخصية حساسة سبق للشخص المعني وأن صرح بها علنا ويمكن استنتاج موافقته على معالجة هذه المعطيات من خلال تصريحاته هذه.

- إذا كانت المعالجة ضرورية للاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء، وأن تكون هذه المعالجة قد تمت حصريا لهذه الغاية، مثل المعطيات الشخصية التي قد يدلي بها المتقاضي لمحاميه أو لمساعدي العدالة الآخرون والتي قد تكون محل معالجة من طرفهم.

- معالجة المعطيات الجينية باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي، والقيام بتشخيصات طبية وفحوصات أو علاجات.

[1] تنص المادة 18 من القانون 07/18 على أنه "تمنع معالجة المعطيات الحساسة".

*وعلى سبيل المثال يجيز القانون 03/16 المؤرخ في 2003/06/19 الجريدة الرسمية العدد 35، ص05 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، معالجة المعطيات الجينية من خلال إنشاء قاعدة معطيات خاصة بالبصمة الوراثية على مستوى المصلحة المركزية للبصمات الوراثية، أنظ كذلك المرسوم 17/277 المؤرخ في 10/09 2017، الجريدة الرسمية عدد 60، المحدد لشروط وكيفيات تنظيم المصلحة المركزية للبصمات الوراثية وسيرها، ص14.

وفي هذا الصدد أيضا أخضع المشرع معالجة المعطيات الشخصية والتي يكون الهدف منها تحقيق مصلحة عامة للبحث أو الدراسة أو التقييم في مجال الصحة لنظام الترخيص، شريطة أن تتم هذه المعالجات في إطار احترام المبادئ المنصوص عليها في هذا القانون.

والملاحظ أن المشرع الجزائري لم يدرج المعالجات التي تنصب على المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن، والتي يمكن حسب نص المادة 10 من القانون 07/18 معالجتها من قبل أشخاص معنويين يسيرون مصالح عمومية وكذا مساعدي العدالة في إطار اختصاصاتهم القانونية، ضمن فئات المعالجات التي تخضع للترخيص المسبق، وهذا على خلاف ما جاء به المشرع الفرنسي الذي أخضع معالجة هذا النوع من المعطيات الشخصية لنظام الترخيص حسب البند الثالث من المادة 25 من القانون 17/78 مستثنيا منها تلك المعالجات التي يقوم بها أعوان القضاء لتلبية احتياجاتهم وتسهيل مهامهم في الدفاع عن الاشخاص المعنيين.[1]

كما نشير أيضا إلى أن المشرع الفرنسي أدرج ضمن هذه القائمة من المعالجات التي تخضع لنظام الترخيص المعالجات الإحصائية التي يقوم بها المعهد الوطني للإحصاء والدراسات الإقتصادية أو إحدى الخدمات الإحصائية الوزارية في إطار تطبيق القانون رقم 711/51 المؤرخ في 1951/06/07 المتعلق بالإلتزام بالتنسيق والسرية في الإحصاء، وكذلك المعالجات الآلية المتعلقة بالمعطيات البيومترية اللازمة للتحقق من هوية الأشخاص.*

ثانيا: الربط البيني لملفات إلكترونية: ويشمل هذا المقتضى حالتين:

- الحالة الأولى وتتعلق بالربط البيني لملفات تابعة لشخص أو عدة أشخاص معنويين يسيرون مرفقا عموميا لأغراض مختلفة مرتبطة بالمنفعة العامة، كما هو الشأن مثلا بربط الجهات القضائية والشرطة القضائية إلكترونيا بالقاعدة الوطنية للبصمات الوراثية[2]، وكذلك ربط المصالح الأمنية وبعض المصالح الإدارية بقاعدة المعطيات الوطنية لصحيفة السوابق القضائية التابعة لوزارة العدل، ورط الجهات القضائية بقاعدة المعطيات للحالة المدنية التابعة لوزارة الداخلية.

- الحالة الثانية تتعلق بالربط البيني للملفات التابعة للأشخاص الطبيعية الذي يتم لأغراض مختلفة.

---

[1] Article 25 de la loi 78/17 Prévoit que : " Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, … 3- Les traitements automatisés ou non portant sur des données relatives aux infractions, Condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense Des personnes concernées"

* المعطيات البيومترية هي المقاييس الحيوية التي يمكن من خلالها التعرف على الهوية انطلاقا من ملامح الوجه، الصوت، هندسة اليد، حدقة العين... وهذه المقاييس تعالج من خلال البرمجة والتشفير للسمات الفريدة لكل شخص وتخزن في قاعدة البيانات أنظر: مروة زين العابدين، مرجع سابق ص 98، وكذلك:

Délibiration de la CLIN n° 2019-01 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité, le contrôle d'accès par authentification biométrique aux locaux. disponible sur le site : https://www.ligifrance.gouv.fr

[2] أنظر المادة 14 من المرسوم التنفيذي رقم 277/17 المؤرخ في 09 أكتوبر 2017 المحدد لشروط وكيفيات تنظيم المصلحة المركزية للبصمات الوراثية وسيرها، الجريد ة الرسمية العدد 60، ص 14.

وإذا كان المشرع تحدث فقط عن الربط البيني لملفات تابعة لأشخاص معنويين يسيرون مرفقا عاما وهم إما أن يكونوا أشخاصا معنوية عامة (الإدارات العمومية) أو أشخاصا معنوية خاصة أسندت لهم مهمة تسيير مرفق عام في إطار عقد من العقود الإدارية كعقد الإمتياز مثلا، فإننا نراه قد أغفل ذكر حالة الربط البيني لملفات تابعة لشخص أو عدة أشخاص معنويين خاصة لا تسير مرفقا عاما وتدير أجهزتها الخاصة أغراضا مختلفة، كالربط الحاصل مثلا بين الوكالات السياحية ومجموعة الفنادق في إطار تنظيم العمليات السياحية وغيرها والتي يتم خلالها معالجة البيانات الشخصية لزبائنها.

لذلك كان نص المشرع الفرنسي في البند 05 من المادة 25 من القانون 17/78 أكثر وضوحا، حيث بعد ذكره الحالة الأولى، نص بعد ذلك على الربط البيني لملفات تتعلق بالأشخاص الأخرى والتي لها أهداف رئيسية مختلفة.[1]

ثالثا:حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية: حيث تنص المادة 44 من القانون 07/18 أنه لا يجوز لأي مسؤول عن معالجة معطيات ذات طابع شخصي نقل هذه المعطيات إلى دولة أجنبية إلا بترخيص من السلطة الوطنية، حيث يمكن الترخيص المسبق السلطة الوطنية من فرض رقابتها على طبيعة المعطيات الشخصية المزمع تحويلها إلى الدولة الأجنبية، فيما إذا كانت تؤدي إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة، بالإضافة إلى تأكدها من ضمان هذه الدولة الأجنبية لمستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجات التي قد تخضع لها هذه المعطيات الشخصية المحولة، وذلك بالإستناد على المقتضيات القانونية المعمول بها في هذه الدولة الأجنبية ووفقا لإجراءات الأمن المطبقة فيها، وكذا الخصائص المتعلقة بالمعالجة مثل غايات هذه المعالجة والغرض منها ومدتها وأصل ووجهة المعطيات المعالجة.[2]

في حين أن المشرع الفرنسي اعتبر أن عملية نقل المعطيات الشخصية إلى دولة أخرى لا يحتاج إلى ترخيص مسبق، عندما تتوفر الأطر القانونية المناسبة للحماية في البلد المعني بتلقي هذه المعطيات.[3]

وقد استثنى المشرع الجزائري تطبيق نظام الترخيص المسبق على حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية في حالات معينة وهي:

1- حالة الموافقة الصريحة للشخص المعني بنقل معطياته نحو دولة أجنبية.

2- إذا كان نقل المعطيات الشخصية ضروريا:

- للمحافظة على حياة صاحبها.
- للمحافظة على المصلحة العامة.

[1] « L'interconnexion de fichiers relvant d'autre personnes et dont finalités principales différents »

[2] أنظر المادة 44 من القانون 07/18.

[3] منى جبورالأشقر، محمود جبور، مرجع سابق، ص 101. أنظر كذلك المادة 68 من القانون الفرنسي 17/78.

- احتراما لالتزامات تسمح بضمان إثبات أو ممارسة حق الدفاع عن صاحب المعطيات أمام قضاء تلك الدولة.
- تنفيذا لعقد بين المسؤول عن المعالجة والشخص المعني.
- لإبرام أو تنفيذ عقد مبرم بين المسؤول عن المعالجة والغير لمصلحة الشخص المعني.
- تنفيذا لإجراء يتعلق بتعاون قضائي دولي.[1]
- للوقاية من إصابات مرضية أو تشخيصها أو معالجتها.

3- إذا تم نقل المعطيات الشخصية في إطار تطبيق اتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه.

غير أنه إذا تعلق الأمر بمعالجة معطيات شخصية تتطابق مع ما نصت عليه المادة 02 من القانون 07/18[2] فلن يكون نقل هذه المعطيات في كل الأحوال إلا بناء على ترخيص من السلطة الوطنية.

وتجدر الإشارة في هذا الصدد أن المشرع الفرنسي قد يعطي الإختصاص في منح الترخيص بالمعالجة لجهات أخرى غير اللجنة الوطنية المكلفة بحماية المعطيات الشخصية (CNIL) عندما يتعلق الأمر بمعالجة معطيات ذات طابع شخصي لحساب الدولة، ولا يكون لهذه اللجنة في هذه الحالات سوى إبداء رأيها فقط، ويتعلق الأمر بحالتين:

الحالة الأولى نصت عليها المادة 26 من القانون 17/78 يكون فيها الترخيص صادرا عن الوزير أو الوزراء المختصين بعد أخذ رأي اللجنة الوطنية للحريات والمعلومات (CNIL) ، وتتعلق تحديدا بمعالجة المعطيات الشخصية المرتبطة بأمن الدولة أو الدفاع الوطني أو الأمن العام، أو تهدف إلى منع الجرائم أو التحقيق فيها أو الكشف عنها أو ملاحقتها أو تنفيذ الإدانات الجزائية أو تدابير أمنية[3]، وهي ما يطلق عليها بمعالجات السيادة[4]، وإذا ارتبطت هذه المعالجات أي بما يسمى بمعالجات السيادة بالمعطيات الحساسة المنصوص

[1] أنظر المادة 23 من الإتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديموقراطية الشعبية وحكومة الجمهورية الفرنسية، الموقعة بباريس بتاريخ 05 أكتوبر 2016 والمصادق عليها بالمرسوم الرئاسي رقم 73/18 المؤرخ في 2018/02/25 ،ج ر عدد 13، ص 10.

[2] تنص المادة 02 من القانون 07/18 على أنه "يجب أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة،وألا تمس بحقوق الأشخاص وشرفهم و سمعتهم".

[3] Art 26-I de la loi 78-17 : "Sont autorisés par arrêté du ou des ministres compétents, pris aprés Avis motivé et publier de la Commission Nationale de l'Informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et :

1) Qui est intéressant la surete de l'état, La défense ou la sécurité publique

2) Qui a pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénal ou des mésures de sureté ».

La CNIL a notamment le 19 juillet 2012 pris une délibération pourtant un avis sur un projet de décret du ministre des Affaires sociales Et de la santé relative à la mise en œuvre de services en santé par les organismes de gestion des régimes obligatoires de base l'assurance maladie (www.ligifrance.gouv.fr) Et cet avis a conduit à la prise du décret n° 2012-1249 du 9 novembre 2012 Autorisons la création de traitement de données à caractère personnel pour la mise en œuvre de programme de prévention et d'accompagnement en santé des assurés sociaux

[4] Brigitte, OP, CIT, p 61.

عليها في المادة 08 من القانون 17/78 فإن مجلس الدولة هو المختص بالترخيص، بموجب مرسوم يكون مرفقا برأي اللجنة الوطنية للمعلومات والحريات.[1]

الحالة الثانية والتي نصت عليها المادة 27 وتتعلق بالترخيص الذي يصدره مجلس الدولة بخصوص المعالجات التي تكون لحساب الدولة والمنصبة على المعطيات الشخصية المتلعقة برقم تسجيل الأشخاص في الدليل الوطني لتحديد الأشخاص الطبيعيين، أو تلك المعالجات التي تنصب على المعطيات البيومترية اللازمة للمصادقة أو التحقق من هوية الأشخاص.

أما عن إجراءات الترخيص المسبق فإن المادة 20 من القانون 07/18 تستوجب أن يتضمن طلب الترخيص جميع العناصر التي أوردتها المادة 14 التي يستوجبها التصريح والسابق ذكرها، وعلى السلطة الوطنية أن تتخذ قرارها بمنح الترخيص من عدمه في أجل شهرين من تاريخ إخطارها، مع إمكانية أن يمدد رئيس السلطة الوطنية هذا الأجل بنفس المدة، ويعتبر سكوت السلطة الوطنية وعدم ردها على طلب الترخيص بعد انقضاء هذا الأجل بمثابة رفض الطلب[2]، وإذا تعلقت المعالجة بمعطيات مماثلة وبنفس فئات المرسل إليهم وكانت لها نفس الأغراض فإن الترخيص يكون بقرار واحد لجميع المعالجات المنصبة على هذه المعطيات[3].

المطلب الثاني: إلتزامات المسؤول عن المعالجة

فرضت التشريعات ومنها المشرع الجزائري على المسؤول عن معالجة المعطيات الشخصية إتخاذ مجموعة من التدابير و الإجراءات من أجل حماية المعطيات ذات الطابع الشخصي وضمان سلامتها وسريتها، ذلك أنه أثناء معالجة المعطيات الشخصية فانها تكون عرضة للعديد من المخاطر المرتبطة بهذه المعالجة خاصة مع شيوع استخدام شبكة الأنترنت التي تشكو نقصا فادحا في مستوى الأمن الفعلي فيها، نتيجة لعدة أسباب أهمها أن شبكة الأنترنت شبكة دولية و مفتوحة و لا تخضع لأي رقابة و لا لأي سلطة مركزية تدير التبادل المعلوماتي أو تراقبه، لذلك فقد برزت الحاجة إلى ابتكار وسائل تكنولوجية إلى جانب جرءات القانونية تساعد على تأمين وظائف الأمن و السرية للبيانات الشخصية

وترتبط سرية المعطيات ذات الطابع الشخصي بحق تحديد متى وكيف وإلى أي مدى يمكن مشاركة البيانات التي تم الإطلاع عليها، لذلك شرعت القوانين بمجملها على الإلتزام بسرية البيانات سواء في معرض التطرق إلى الواجبات المرتبطة على المسؤول عن المعالجة ومنفذيها، أو في معرض ذكر المبادئ التي تقوم عليها المعالجة.

ويعتبر هذا الإلتزام قريب من الإلتزام بضمان سلامة البيانات ومكملا له من الناحية المادية، ومن كونهما من الواجبات الأساسية للمسؤول عن المعالجة المرتبطة أساسا بضرورة الحفاظ على أمن المعلومات ومنع تسريبها والحد من مخاطر انكشافها، مع فارق في كون الإلتزام بسرية المعطيات يتعلق بالتزام الأشخاص

[1] L'article 26-II de la loi Francaise 78-17.

[2] أنظر المادة 20 من القانون 07/18.

[3] أنظر المادة 2/21 من القانون 07/18.

المأذون لهم بالإطلاع على البيانات الشخصية لسبب قانوني أو تنظيمي بعدم الإفصاح عما يطلعون عليه من بيانات شخصية، بينما يرتبط الإلتزام بضمان سلامة البيانات الشخصية باعتماد تقنيات تكنولوجية تمنع الإطلاع على من لا يحق لهم أصلا الإطلاع عليها وذلك بتوظيف التقنية ذاتها لتعزيز الخصوصية.

إن أي نظام أمن حاسوبي يجب أن يكون مبنيا على المكونات الأساسية التالية:

سرية البيانات، سلامة البيانات، إتاحة البيانات، وعملية تفسير هذه المكونات الأساسية الثلاث تتغير تبعا للسياق الذي تنبثق منه و إلى حاجات الأفراد، حيث تحتاج كل هيأة وكل شركة أن تقوم بعملية تنظيم وتنسيق ووضع قوانين صارمة للحفاظ على سرية وسلامة و إتاحة البيانات للمستخدمين الشرعيين، و هذا يحتاج إلى إدارة ناجحة واستراتيجية متينة وقوية يتم تطبيقها من أجل الوصول إلى مرحلة من النضج في نظام أمن الحاسوب، و إذا كان المشرع قد ألزم أي مسؤول عن معالجة البيانات الشخصية بالسرية، فهذا يعني أن هذا الأخير يحتاج إلى آليات للحفاظ على سرية هذه البيانات وعدم السماح بتداولها من قبل أطراف غير مصرح لهم بالوصول إليها، خاصة أن معظم المنظمات العامة و الخاصة منها (إدارات وشركات) في هذا العصر هي متصلة بشبكات الإتصال الإلكتروني و أهمها شبكة الأنترنت، وما يمكن أن يصاحب هذا الإتصال من مخاطر وتهديدات من قبل قراصنة الحاسوب و الذين يسعون دائما من أجل الوصول إلى الملفات السرية التي بحوزة الشركات أو الافراد، والحاجة الى الحفاظ على سرية البيانات يزداد عند استخدام الحاسوب في مجالات ذات حساسية عالية مثل المؤسسات الحكومية وما تقوم به من حفظ العديد من السجلات البالغة في السرية عن الأفراد وتحاول جاهدة الحفاظ على هذه السجلات بشكل سري.[1]

و أما سلامة البيانات فهي ضمان عملية انتقال البيانات بين الأطراف ووصولها سالمة دون أي تغيير، وذلك بعدم اعتراضها من قبل المخترقين والقيام بعملية التغيير فيها وإعادة إرسالها مرة أخرى إلى الطرف المستلم على غير حقيقتها، فالبيانات التي يتم نقلها عبر الأنترنت من الممكن اعتراضها بسهولة من طرف قراصنة الحاسوب، من خلال استخدام برامج لهذا الغرض ثم القيام بتغييرها والعبث فيها.

وترتيبا على ذلك فإن التزامات المسؤول عن المعالجة تجاه حماية المعطيات ذات الطابع الشخصي تقتضي منه اتخاذ التدابير والإجراءات الضرورية لتحقيق ذلك سواء أكانت تدابير تقنية أو تنظيمية، من خلال وضع حدود وقواعد وتقنيات تشمل حماية البيانات من أي تحوير أو إتلاف أو ضياع أو ولوج غير مرخص به، حتى بالنسبة للمعالجين، بحيث لا يسمح لهم بالوصول إلى المعطيات الشخصية إلا في حدود ما هو ضروري لتنفيذ مهام كل واحد منهم.

لذلك فقد أوجب المشرع الجزائري على المسؤول عن المعالجة الإلتزام بسرية وسلامة المعالجة في نص المادة 38 من القانون 07/18، وذلك من خلال إلزامه باتخاذ ووضع كافة التدابير التقنية والتنظيمية

[1] خضر مصباح إسماعيل الطيطي، أساسيات إدارة المشاريع وتكنولوجيا المعلومات، دار حامد للنشر والتوزيع، الطبعة الأولىعمان ـ 2002، ص242.

الملائمة لحماية المعطيات ذات الطابع الشخصي، مع وجوب أن تتضمن هذه التدابير مستوى ملائم من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها.[1]

فانطلاقا من المادة 38 من القانون 07/18، يلزم المسؤول عن المعالجة، وعند الإقتضاء في حالات معينة المعالج من الباطن[2] ، إتخاذ كافة الإجراءات والتدابير التقنية والتنظيمية لضمان سلامة محتوى البيانات الشخصية، كما يشترط أن تكون هذه التدابير على قدرٍ من المستوى الملائم الذي يتوافق مع درجة المخاطر التي تتعلق بطبيعة المعالجة من جهة، وبطبيعة المعطيات الشخصية محل المعالجة من جهة أخرى.[3]

وقد عدد المشرع بصفة خاصة أهم المخاطر التي من شأنها المساس بسلامة البيانات وهي: الإتلاف العرضي، الضياع العرضي، التلف، النشر أو الولوج غير المرخصين، خاصة إذا كانت معالجة المعطيات تستوجب إرسال هذه المعطيات عبر شبكة معينة مثل شبكة الأنترنت.

ومن الملاحظ أن الهيئة الوطنية للحريات والمعلومات بفرنسا CNIL تشدد حيال هذا الإلتزام حينما أصدرت قرارا بتغريم شركة فرنسية بمبلغ مئتين وخمسين ألف يورو بسبب عدم اتخاذ المسؤول عن معالجة البيانات التدابير والإجراءات الضرورية والمناسبة لطبيعة البيانات والمخاطر التي تهددها لضمان حماية سلامتها ومنع تحويرها أو تضررها ومنع الوصول إليها من طرف أشخاص آخرين غير مصرح لهم بذلك.[4]

الفرع الأول: التدابير التقنية لضمان سلامة وسرية المعطيات ذات الطابع الشخصي

إن مختلف الوثائق الدولية والإقليمية، وكذلك القوانين الوطنية تطلب من الجهات القائمة على معالجة المعطيات الشخصية أن تعتمد وسائل تقنية لحماية عمليات معالجة هذه المعطيات، فقد نص التوجيه الأوروبي 95/46 في المادة 17 منه على التزام الدول الأعضاء باتخاذ تدابير تقنية لحماية البيانات الشخصية ضد أي إتلاف عرضي أو غير مشروع أو ضياع أو نشر أو ولوج غير مرخصين، وضد كل شكل من أشكال المعالجة غير القانونية.

و قد برزت الحاجة ملحة لاعتماد مثل هذه الوسائل التقنية، خاصة مع الوتيرة المتسارعة التي تحولت فيها الشبكات المعلوماتية إلى فضاء جديد لتبادل المعلومات بكافة أشكالها على نطاق كوني، بحيث تتعرض الأسرار المعلوماتية للإنتهاك اللامتناهي، سيما بعد ارتباط الحاسوب بشبكة الأنترنت ضمن نطاق

[1] نص المادة 38 من القانون 07/18.

[2] عرف المشرع الجزائري المعالج من الباطن في نص المادة 13/3 من القانون 07/18 بأنه "كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر، يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة".

[3] Thibault verbiest et Etienne wery, le droit de l'internet et de la société de l'informatique, droit européen belge et francais, Revue internationale de droit comparé. Vol. 54 N°1, Janvier-mars 2002., Belgique, 2001, P 238

[4] La délibiration de la formation resteinte n° san 2018/002 du 07 mai 2018 de la commission nationale de l'informatique et des libertés. Pronocant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données, l'article 34 de la loi du 6 janvier 1978 disponible sur le site http://www.legifrance.gouv.fr/affichcnil

عمليات التبادل المعلوماتي، التي تمتد وتتزايد عبر هذه الشبكة يوما بعد يوم، وبالتالي فمن أجل تحقيق هذه الحماية التقنية تم تعميم تقنيات أوجدها المتعاملون مع المعطيات الشخصية، تساعد على تأمين وظائف الحماية الوقائية المسبقة لمنع وقوع اعتداءات على البيانات الشخصية وجعلها في مأمن، من خلال الحيلولة دون وقوع هذه الإعتداءات أو التخفيف من آثارها إذا وقعت[1]. كما يشترط لضمان توفر الحماية التقنية الكافية للبيانات أن تؤدي هذه الوسائل التقنية إلى ضمان السرية أو الموثوقية التكاملية، سلامة المحتوى، استمرارية تدفق وتوفير البيانات وكذا عدم الإنكار.

أولا: أهداف البرامج التقنية الحمائية

إن حماية الخصوصية المعلوماتية بواسطة النصوص القانونية لوحدها غير كاف*، لذلك يصبح من الضروري الإستناد إلى تقنيات متطورة أوجدها المختصون في شبكة الأنترنت والأنظمة المعلوماتية كأدوات تقنية متنوعة وتختلف باختلاف أهمية الغرض الذي وجدت من أجله، وهي في مجملها عبارة عن مجموعة من البرامج التي تستخدم في الوقاية من المخاطر أو تقليل الخسائر بعد وقوع الإعتداء على المعلومات وأنظمتها، ذلك أنه وأمام اتساع المخاطر التي تستهدف أنظمة الكومبيوتر التي تخزن البيانات الشخصية، وكذلك الشبكات التي يتم من خلالها تبادل هذه البيانات، بات يتحتم على الشركات العاملة في قطاع تكنولوجيا المعلومات توفير أدوات مبتكرة وفعالة لمكافحة هذه المخاطر، وكذا يتعين على القائمين على جمع المعطيات الشخصية ومعالجتها استعمال هذه المنتجات بغية تسهيل حماية أنظمة الكومبيوتر بشكل عام والبيانات الشخصية بشكل خاص.

ومن أهم هذه الوسائل التقنية الحمائية هي البرامج الإلكترونية، مع ملاحظة أن هذه الوسائل التقنية المتعين استخدامها في بيئة المعالجة الآلية لغرض حماية البيانات الشخصية تتعدد كما تتعدد أغراضها ونطاقات استخدامها، وتصنف هذه الوسائل التقنية على ضوء هدف وغرض الحماية إلى الوسائل التالية:

1) الوسائل المتعلقة بالتعريف بشخص المستخدم وموثوقية الإستخدام ومشروعيته: وهي الوسائل التي تهدف إلى ضمان استخدام النظام المعلوماتي أو الشبكة من قبل الشخص المخول بهذا الاستخدام، حيث يراد بها التحكم في الأشخاص المسموح لهم بالوصول للمعلومات والنظم العاملة عليها، ذلك أن الوصول إليها من طرف أشخاص غير مصرح لهم بذلك يؤدي لفقد سرية المعلومات وربما صحتها، وتضم هذه الطائفة كلمات السر بأنواعها، البطاقات الذكية المستعملة للتعريف، وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم و المتصلة ببنائه البيولوجي، كما تضم أيضا ما يعرف

[1] هلالي عبد الله أحمد، الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، 2003، ص71.

* وقد أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول بأن "الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل في التهديد بقانون العقوبات، ومع ذلك فإن هذا العرض لا يكون مكتملا دون تبني ووضع إجراءات أمنية فعالة". تم اعتماد الاتفاقية وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتها 109 في 08 نوفمبر 2001. وفتح باب التوقيع عليها في بودابست رومانيا في 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية وتسمى الاتفاقية رقم 185.

بالأقفال الإلكترونية التي تحدد مناطق النفاذ، وتعتبر هذه الوسائل وكأنها صمام الأمان للنظم الإلكترونية، وتختلف هذه الوسائل تبعا للتقنية المستخدمة في القطاع.[1]

2) الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة: وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة مشروعة، ومن أهم الوسائل الفنية المعتمد عليها في هذه الطائفة ما يعرف بالجدران النارية، وهي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات الشخصية من وإلى الجهاز أثناء التعامل مع شبكة الأنترنت، فيتم إجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها بأن تمر منعبر هذا الجدار الناري، والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة، وذلك عن طريق مراقبة الحزم التي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم، وعند مراقبة الجدار الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها فإن عليها السماح أو الإعتراض على دخول هذه البيانات أو خروجها وتنبه المستخدم لذلك.

3) الوسائل التي تهدف إلى منع إفشاء البيانات لغير المخولين أو المصرح لهم بذلك: وتهدف هذه الوسائل التقنية إلى ضمان سرية البيانات، وتشمل تقنيات تشفير البيانات والملفات، إجراءات حماية نسخ الحفظ الإحتياطية، برامج الفلترات (filtration) والموجهات.

4) الوسائل التي تهدف إلى حماية التكاملية وسلامة المحتوى: وهي الوسائل المناط بها ضمان عدم تعديل المعطيات من قبل جهة غير مخولة لذلك، ومن أهمها برامج تحري الفيروسات ومضادات الفيروسات.[2]

5) الوسائل المتعلقة بمنع الإنكار: وتهدف هذه الوسائل إلى ضمان عدم قدرة الشخص المستخدم على إنكار أنه هو الذي قان بالتصرف، وترتكز هذه الوسائل بصفة أساسية على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة من طرف ثالث.

6) **وسائل مراقبة الإستخدام وتتبع سجلات النفاذ والأداء**: وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الإستخدام، وهذه الوسيلة الأخيرة نجد أن المشرع الجزائري قد أشار إليها في المادة 10 من القانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما، حينما ألزم مقدمي خدمات الأنترنت العمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة المتعلقة بتاريخ ووقت ومدة كل إتصال، بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه الإتصال وعنوان الموقع المطلع عليه.

---

[1] فتحي عبد العزيز، الأمن الإلكتروني متوفر على الرابط: http://mubtakir.ae/mubtakir/uploads/1525242623713.pdf. أنظر كذلك: بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا (الاعلام والاتصال)، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، السنة الجامعية 2015/2014، ص 204

[2] بولين أيوب، مرجع سابق، ص227.

إن كل هذه الوسائل تساعد على تأمين وظائف الحماية والأمن والسرية المطلوبة بإلحاح في مجال تبادل البيانات الشخصية عبر الانترنت.[1]

ثانيا: أهم أنواع البرامج التقنية الحمائية للبيانات الشخصية

في مقدمة الوسائل والأدوات المبتكرة في مجال توفير أمن وسلامة وسرية البيانات الشخصية هي تقنية التشفير، كون هذه الوسيلة التقنية لا تقتصر فقط على توفير الحماية الرقمية للبيانات الشخصية، بل تتعدى ذلك لتشمل أيضا المساهمة بنسبة كبيرة في تدعيم الإثبات المعلوماتي،[2]بالإضافة إلى برامج أخرى كبرامج معاودة الإرسال وجدران النار واستخدام كلمات السر.

1) برامج التشفير المعلوماتي: يعتبر تشفير الرسائل والبيانات من الإجراءات والتدابير التقنية اللازمة لتأمين الشبكات ضد مخاطر الولوج والإختراق الوارد عن طريق الأنترنت وغيرها[3]، ويعد من الأساليب الأكثر شيوعا في التعامل عبر المنظومة المعلوماتية عامة وفي شبكة الأنترنت خاصة.

ويعد التشفير عملية تقنية يتم من خلالها تحويل المعلومات إلى شيفرات غير مفهومة، بحيث لو وقعت هذه المعلومات المرسلة في يد شخص آخر غير المستقبل المقصود، سيكون غير قادر على فهم محتواها لأنه غير مخول لقراءتها، وإذا وصلت هذه المعلومات المشفرة إلى المستقبل المعني فإنه يقوم بعملية عكسية من خلال ما يعرف بفك التشفير للحصول على النص الأصلي، وذلك باستخدام مفتاح سري يسمى مفتاح التشفير[4]، لذلك فالتشفير في أساسه هو علم إخفاء معنى ومفهوم المعلومة السرية وليس إخفاء وجودها، عن طريق تحويلها إلى رموز معينة غير مقروءة[5].

1-1) تعريف التشفير: من بين التعريفات العديدة للتشفير المستخدمة في ميدان المعلوماتية، التعريف الوارد في القانون الفرنسي حول تنظيم الإتصالات عن بعد[6]،الذي اعتبرها بأنها تشمل جميع التقديمات التي ترمي بفضل بروتوكولات سرية إلى تحويل معلومات مفهومة إلى معلومات وإشارات غير مفهومة، أو القيام بالعملية المعاكسة، وذلك بفضل استخدام معدات أو برامج مصممة لهذه الغاية.

[1] بولين أيوب، مرجع نفسه، ص227 وكذلك جمال عبد الله محمد، نظم المعلوماتالإدارية، دار المعتز للنشر والتوزيع، الطبعة الأولى، 2015، عمان الأردن، ص 204

[2] طوني عيسى، مرجع سابق، ص11

[3] عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي، دار النهضة العربية، الطبعة الأولى 2009، ص85

[4] رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الأنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2013، ص 288

[5] رشدي محمد علي عيد، نفس المرجع، 288

[6] أنظر المادة 28 من القانون الفرنسي رقم 1170/90 المؤرخ في 1990/12/29 المتعلق بتنظيم الإتصالات عن بعد. Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications

كما نجد أن المشرع التونسي قد عرف التشفير على أنه استعمال رموز أو إشارات غير متداولة، تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن وصول المعلومات بدونها.[1]

وقد عرفه المشرع المصري أيضا من خلال قانون التوقيع الإلكتروني بأنه منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة[2].

وفي نفس السياق نجد أيضا المشرع المغربي عرف التشفير على أنه "كل عتاد أو برمجة أو كلاهما معا، ينشأ ويعدل من أجل تحويل معطياته سواء كانت عبارة عن معلومات أو شعارات أو رموز استنادا إلى اتفاقيات سرية، أو من أجل إنجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها"[3]

والملاحظ أن المشرع الجزائري لم يعرف تقنية التشفير معتبرا إياه من بيانات إنشاء التوقيع الإلكتروني، واكتفى فقط بتعريف مفتاح التشفير في القانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني[4]، حيث نص على نوعين من مفاتيح التشفير وهما مفتاح التشفير الخاص وهو عبارة عن سلسلة من الأعداد التي يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي، وهذا الأخير عرفه المشرع بأنه عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني.

وعرف التشفير فقها بأنه عبارة عن برنامج يتولى فرض شفرة تحمي ظاهر المعلومات، بحيث تمنع الغير ممن ليس لهم الحق في التعامل مع الموقع أو الدخول إليه، ما لم يصرح له المالك بذلك، ويكون هذا التصريح للإطلاع على البيانات المشفرة باستخدام مفتاح إزالة التشفير، وهو عبارة عن برنامج تم تصميمه لكي يقوم بفك شفرة الدخول[5]

كما عرف التشفير أو الترميز أيضا أنه آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للإنعكاس، أي يمكن إرجاعها إلى حالتها الأصلية[6]، كما ذهب جانب من الفقه إلى تعريف التشفير بأنه عبارة عن تقنية قوامها خوارزمية رياضية ذكية تسمح لمن يمتلك مفتاحا

---

[1] المادة 12 من القانون 2000/83 المتعلق بالمبادلات والتجارة الإلكترونية، منشور في الجرائد الرسمية للجمهورية التونسية بتاريخ 29 ماي 2000

[2] أنظر القانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية تكنولوجيا صناعة المعلومات، الجريدة الرسمية عدد 18 مؤرخ في 22 أفريل 2004.

[3] أنظر المادة 12 من القانون المغربي رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، منشور في الجريدة الرسمية عدد 5584 مؤرخة في 06 ديسمبر .2007

[4] أنظر المادة الثانية من القانون 04/15 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، الجريدة الرسمية العدد 06، مؤرخة في 10 فيفري 2015

[5] عمر محمد أبو بكر يونس، مرجع سابق، ص 379

[6] بولين أيوب، مرجع سابق، ص231. نقلا عن:Valerie Sédaillan, droit de l'internet, collection AUI, 1997, page 171

سريا بأن يحول رسالة مقروءة إلى رسالة غير مقروءة، وأن يستخدم المفتاح السري لفك الشفرة وإعادة الرسالة المشفرة إلى وضعيتها الأصلية[1] .

وعرف فقهيا أيضا أنه "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها[2].

كما عرف أيضا بأنه فن حماية المعلومات عن طريق تحويلها إلى رموز معينة مقروءة، لا يمكن حلها إلا من خلال مفتاح سري يقوم بتحويل تلك الرموز إلى نص عادي مقروء[3].

وعرف التشفير في القانون العربي النموذجي[4] بأنه "تحويل البيانات المعالجة إلكترونيا إلى رموز لعدم تمكين الغير من انتهاك سريتها"[5]، وعرف أيضا بأنه مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات، حيث لا يمكن قراءتها من قبل طرف ثالث متطفل، وبالتالي هو عبارة عن فلسفة معينة يتم بها حصر معلومة في نطاق محدد، فيتم اللجوء إليه بقصد حجب تلك المعلومة عن التداول[6].

وقد كان للقضاء أيصادور في تعريف التشفير من خلال مجلس الدولة الفرنسي الذي عرفه بأنه كل عمل يوجه لتحويل –بمساعدة مصطلحات سرية- معلومات أو إشارات غير مفهومة للغير أو بإخراجها بطريقة عكسية بفضل وسائل مادية أو برمجية مخصصة لذلك.[7]

وعلى هذا الأساس يمكن القول بأن التشفير يعتمد على تغيير محتوى الرسالة الإلكترونية باستخدام أسلوب محدد، وبرنامج محدد يسمى مفتاح التشفير، وذلك قبل إرسال الرسالة، على أن يكون هناك قدرة لدى المستقبل على استعادة محتوى الرسالة وذلك في صورتها الأصلية قبل التشفير، باستخدام عملية عكسية لعملية التشفير encryption والتي تسمى الحل decryption [8]

2-1) تقنيات التشفير*: يمكن تصنيف تقنيات التشفير في ميدان المعلوماتية إلى فئتين رئيسيتين:

-الفئة الأولى والتي تستخدم المفتاح الخصوصي (cryptographie à une clé privée) وتسمى تقنية التشفير المتماثل (المتناظر)

---

[1] عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2009، ص74

[2] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، الطبعة الأولى، 2002، الإسكندرية، ص311.

[3] عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية ،2005 ص55

[4] القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والإتصالات.

[5] عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والأنترنيت في القانون العربي النموذجي. مرجع سابق، ص85

[6] عمر محمد أبو بكر يونس، مرجع سابق، ص379

[7] عمر محمد أبو بكر يونس، نفس المرجع، ص383

[8] رأفت رضوان، عالم التجارة الإكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، الطبعة الأولى، 1999، ص80

* تعتبر تقنيات التشفير في الولايات المتحدة الأمريكية من الأسلحة بعيدة المدى، لذلك كانت تصنف ضمن الأسرار القومية، وإلى غاية 1999 بدأت الحكومة الأمريكية تخفف من عملية التشديد على تصدير تقنيات التشفير، وفي سبيل ذلك رفعت هذه التقنية من قائمة الأسلحة التي تعد حيازتها من قبل الغير بمثابة تهديد للأمن القومي الأمريكي، حيث وضعت الحكومة قانون الأمن الإلكتروني الإفتراضي عام 1999 والذي تضمن السماح بتصدير تقنيات التشفير سواء كانت قطعا صلبة أو برامج، واشترط للموافقة على ذلك أن تحصل الحكومة الأمريكية على نسخة من المفاتيح الإستردادية لهذه التقنيات، وذلك من شأنه أنه يعطي الحكومة الأمريكية الحق في مراقبة استخدامات التشفير.

-الفئة الثانية والتي تستخدم المفتاح العمومي (cryptographie à une clé publique) وتسمى تقنية التشفير غير المتماثل (غير متناظر)

فأما بالنسبة لتقنية التشفير الخصوصي أو التشفير المتماثل (symétrique) فهو النظام الذي يستخدم فيه نفس المفتاح في عملية التشفير وفك التشفير، بمعنى أن نظام الكتابة المشفرة بالمفتاح الخصوصي يعمل بواسطة مفتاح واحد يمتلكه كل من مرسل الرسالة ومتلقيها، بحيث يتم استخدام نفس المفتاح بدون كشفه إلى أي طرف آخر، ومن ثم فأمن هذا النظام يعتمد على سرية المفتاح المستخدم.[1]

وقد عرف المشرع الجزائري هذا النوع من التشفير في المادة الثانية من القانون 04/15 المتعلق بتحديد القواعد العامة للتوقيع والتصديق الإلكترونيين، بأنه عبارة عن أعداد يملكها شخص الموقع فقط، وتستخدم كوسيلة أو آلية لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي، ومن بين أشهر أنظمة التشفير المتماثل نظام EDS [2]

و أما بالنسبة لتقنيات التشفير غير المتماثل*، أو التشفير بالمفتاح العمومي، فإنه يقوم على استخدام زوج من المفاتيح، مفتاح التشفير الخاص ومفتاح التشفير العام المستحدثان في نفس الوقت بعملية حسابية دقيقة عن طريق آليات إنشاء البيانات التي تقوم بتوزيع دور وعلاقة كل مفتاح بصاحب التصرف الإلكتروني،[3] ومن الناحية التقنية رغم اختلاف المفتاح العام عن المفتاح الخاص كونه متاح لأكثر من طرف، إلا أن هناك ترابطا في عملهما، فإذا تم استعمال المفتاح الخاص للتشفير، فلا يمكن فك التشفير إلا باستعمال المفتاح العام، وإذا عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر بطريقة حسابية.

ومن أجل زيادة فعالية التشفير في توفير الحماية للرسائل الإلكترونية، فإنه يمكن اعتماد طريقة الدمج بين ما يسمى بالبصمة الإلكترونية* والمفتاح العام، وهذه الطريقة هي أكثر أمانا حيث يتم أولا تمويه الرسالة لإنشاء بصمة إلكترونية لها، ثم تشفر البصمة الإلكترونية باستخدام المفتاح الخاص، مما ينتج عنه توقيع رقمي يلحق بالوثيقة المرسلة، وللتحقق من صحة التوقيع يستخدم المستقبل المفتاح العام المناسب لفك شفرة التوقيع، فإن نجحت عملية فك شفرة التوقيع، فهذا يعني أن المرسل قد وقع الوثيقة

[1] عيسى غسان ربضي، مرجع سابق، 2007، ص68

[2] DES (data encryptions standard) c'est un système de chiffrement par blocs conçu par « IBM » est fonde sur une clé de 56 bit

* لقد برزت هذه التكنولوجيا في نهاية السبعينات على إثر أبحاث قام بها العالمان الأمريكيان (diffce et hellman) والتي أثبتت فعاليتها في مجال توفير أمن الرسائل والبيانات المتبادلة داخل الشبكات المعلوماتية المفتوحة، وأول نظام تشفيري من هذا النوع أطلقه عام 1978 كل من leonard adeleman, adi shamir et ronald rivest وهم ثلاث باحثين من جامعة (MIT) الأمريكية تم تسميته بـ (RSA) وارتكازا على نظام (RSA) انطلقت معظم مجموعات برامج التشفير المعروفة في شبكة الأنترنت اليوم، لا سيما البرنامج المسمى (pretty good privacy) الذي تم تصميمه عام 1991 من طرف الأمريكي phil zimmerman أنظر بولين أيوب، مرجع سابق، ص233 و طوني عيسى، مرجع سابق، ص360

[3] دحماني سمير، التوثيق في المعاملات الإلكترونية، دراسة مقارنة، مذكرة لشهادة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص106.

* البصمة الإلكترونية للرسالة هي عبارة عن بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال أو اقترانات التمويه، حيث تطبق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة تمثل ملفا كاملا أو رسالة، وتدعى البيانات الناتجة عن البصمة الإلكترونية للرسالة، ومن غير الممكن اشتقاق البصمة الإلكترونية ذاتها من رسالتين مختلفتين، وتتميز البصمات الإلكترونية عن بعضها بحسب المفاتيح الخاصة التي أنشأتها، ولا يمكن فك شيفرتها إلا باستخدام المفتاح العام العائد لها.

بالفعل، وأي تغيير يحصل على هذه الوثيقة الموقعة يتسبب في فشل عملية التحقق، وتقوم برمجيات المستقبل بعد ذلك بتمويه محتوى الوثيقة لينتج عن ذلك بصمة الكترونية للرسالة، فإن تطابقت القيمة المموهة للتوقيع الذي فكت شفرته مع القيمة المموهة للوثيقة، فهذا يعني أن الملف سليم ولم يتعرض لأي تغيير أثناء النقل[1].

وقد عرف المشرع الجزائري هذه التقنية، معتبرا أن التشفير العمومي هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق في الإمضاء الإلكتروني وتدرج في شهادة التصديق الالكتروني.[2]

وبالرغم من إيجابيات هذه التقنية، فإن المسألة المتعلقة بضمان أن المفتاح العمومي صادر فعليا من المستخدم الذي يفترض أنه عائد إليه وأنه لم يصار استعماله من قبل الغير بشكل غير مشروع، قد جرت محاولات لمعالجتها عبر تدخل طرف ثالث محايد ومستقل سمي بمزود خدمات التصديق tiers certificateur [3] وذلك لضمان الأمان في عملية التشفير، بحيث يعمل هذا الطرف على تقديم شهادات إلكترونية تبين أن المفتاح العام يقود إلى شخص صاحبه الذي يدعي أنه هو من قام بإرسال الرسالة والتوقيع عليها، وذلك من خلال تولي مهمة إدارة المفاتيح العمومية، ويتحقق من هوية الحائزين عليها، ومن ثم إصدار هذه الشهادات الإلكترونية لحساب الحائزين على المفاتيح الخصوصية، والتي من خلالها يصادق على إصدار عمليات التشفير الحاصلة[4]، وبمقتضى هذه الشهادة الإلكترونية يؤكد الشخص الثالث المصادق عند كل عملية تبادل يجريها الحائز على المفتاح الخصوصي عبر شبكة الأنترنت، أن المفتاح العمومي يعود فعلا لمن يستخدمه، ويؤكد على هوية هذا الأخير وعلى السلطات الممنوحة له، وبدون القدرة على تأكيد هوية المتعاقد وعلى صحة توقيعه فإن أي صفقة إلكترونية تبرم عن بعد تبقى عرضة للشك ولاحتمال المنازعة في شأنها، لهذا السبب يستخدم البعض في تسمية الشخص المصادق بالموثق الإلكتروني le notaire electronique [5]

3-1) دور التشفير في حماية البيانات الشخصية: يعد استخدام التشفير كتدبير تقني من طرف المسؤول عن المعالجة من الإجراءات الهامة واللازمة لتأمين سلامة وسرية البيانات الشخصية عبر الشبكات وغيرها، وقد أثبتت هذه التقنية قدرتها في المحافظة على أمن وسلامة هذه البيانات، ويلاحظ أن وثيقة خصوصية المعلومات والبيانات يجب أن تتضمن مستويات معينة يتم التشفير بناءا عليها[6]:

[1] بن سعيد صبرينة، مرجع سابق، ص211

[2] أنظر المادة 9/2 من القانون 04/15 المؤرخ في 2015/02/01 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين، ج ر عدد 06 بتاريخ 2015/2/10

[3] ولقد أنشأ المشرع الجزائري بموجب المرسوم التنفيذي رقم 134/16 المؤرخ في 25 أفريل 2016 السلطة الوطنية للتصديق الإلكتروني، أنظر الجريدة الرسمية رقم 26 مؤرخة في 28 أفريل 2016.

[4] بولين أيوب، مرجع سابق، ص370

[5] طوني عيسى، مرجع سابق، ص370

[6] عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنيت في القانون العربي النموذجي، مرجع سابق، ص85.

-تشفير وصلات الإتصالات ويعني التشفير على مستوى الإرسال، وفي هذا المستوى يتم تشفير جميع البيانات بدءا من نقطة إرسال هذه البيانات وصولا إلى نقطة الإستقبال، فالتشفير على مستوى الإرسال يعد المرحلة الأولى التي يتم على مستواها إرسال رسالة أو معلومة مشفرة إلى المستقبل، وبهذا لا يمكن للغير الإطلاع على هذا المحتوى.

-تشفير مستوى التصفح: ويتم التشفير على هذا المستوى قصد حماية البيانات أثناء تنقلها عبر الشبكة، فيتم تشفير البيانات التي يتم تداولها بين برامج تصفح البيانات وبين مقر المعلومات، ويكون ذلك من خلال تشفير جميع الإتصالات، سواء التي تتم بين نوافذ الشبكة أو بين برامج التصفح أو المواقع الموجودة عليها، مما يؤدي إلى حماية جميع البيانات أثناء تنقلها.

-التشفير على مستوى التطبيق المستخدم في تنفيذ المعاملة الإلكترونية.

-التشفير على مستوى الملفات: وفي هذه الحالة فإن التشفير يرد على الملفات أو الرسائل التي يتم تبادلها ضمن النظام الإلكتروني بين المرسل والمستقبل، وهي المرحلة الأخيرة من مستويات التشفير فيكون الملف في طبيعة مشفرة وغير مفهومة لغير المخول له بالإطلاع على الملف.

ويجب أن تتضمن وثيقة خصوصية البيانات وسريتها في الإدارة الإلكترونية إجراءات إزالة التشفير (فك الشيفرة)، ذلك أنه بدون حل الشيفرة لا فائدة من الشفرة ذاتها، إذ تبقى الرسائل والبيانات مجرد رموز وأرقام وحروف صماء ليس لها دلالة معينة، لذلك فإن برمجيات التشفير[1] تتضمن نوعين من الإجراءات، الأولى تتعلق بتحويل البيانات إلى رموز، والثانية تتضمن إعادة هذه الرموز مرة أخرى في صورة معلومة أو بيان عن طريق إجراءات فك الشيفرة، ومن ثم يكون الهدف من التشفير كتقنية واضحا وهو أنه يجعل من المستحيل أو من الصعوبة بما كان فهم الرسائل المفتوحة والمتداولة بطريقة إلكترونية[2]، وبالنتيجة عدم السماح لأي مخترق من الحصول على البيانات المتضمنة في الرسالة، أو بإرسال رسالة أخرى إلى الشخص المستقبل أو التلاعب في مضمونها أو منع وصول الرسالة أو عدم وصولها بالشكل المطلوب[3]،

[1] من بين أهم برمجيات التشفير المستخدمة في تأمين البيانات سيما في مجال التجارة الإلكترونية:

*نظام المعاملات الإلكترونية الآمنة (SET) وهو بروتوكول يضمن أمن العقود والصفقات الإلكترونية على الأنترنت، يستخدم هذا البروتوكول نظام الأقفال والمفاتيح بالإضافة إلى رقم حساب معتمد لكل من الزبون والشركة التي تزاول أعمال التجارة الإلكترونية، والهدف منه هو ضمان الخصوصية بين المتعامل والموقع الذي يتعامل معه، وذلك عن طريق تشفير المعلومات المتبادلة على شبكة الأنترنت بطريقة سرية.

*نظام طبقة المداخل الآمنة(SSL) وهو برنامج تشفير يستخدم لنقل جميع المعلومات التي تتداول بين المتصفح وخدمات الواب عبر شبكة الأنترنت، ويعتمد هذا البرنامج على تشفير رزم من البيانات بالشكل الذي يمنع قراءتها إلا من قبل المرسل والمستقبل، وتتمثل طريقة عمل هذ البرنامج باستخدام خادم آمن (secure serveur) ويحصل الإتفاق بين خادمي الطرفين على رموز مشفرة محددة ومفاتيح خاصة، مع تزويد كل مستخدم وعميل بمفتاحين هما المفتاح العام والمفتاح الخاص، وعند دخول المتعامل للصفحة الآمنة التي يدخل فيها البيانات الشخصية الضرورية لعملية الشراء يقوم المتصفح المزود بهذا البرنامج بالإرتباط بجهات الخادم الآمن للموقع ويطلب منه الشهادة الرقمية ومصدرها، وكذلك تتم مقارنة بين إسم الموقع على الشهادة مع إسم الموقع للمتصفح مع التوقيع الإلكتروني. أنظر للتفصيل أكثر: ناصر وسام خليل، التجارة والتسويق الإلكتروني، دار أسامة للنشر والتوزيع، الطبعة الأولى، عمان، 2008، ص244

[2] بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنيت في القانون العربي النموذجي، مرجع سابق، ص86

[3] اسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون والكومبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ص10. متوفر على الرابط: http://www.almajlis.gov.ae أطلع عليه يوم 2019/12/28

وبالتالي ردع كل من لم يكن مصرحا له بالإطلاع على البيانات من فهم مضمون الرسالة التي تتضمنها أو التعرف على كنهها.

2) الجـدران النارية:[*] سبق الإشارة أن عملية تداول البيانات الشخصية ونقلها عبر الشبكات، خاصة شبكة الأنترنيت لا تخلو من المنغصات والمخاطر التي يتسبب فيها المتطفلون الذين يتلصصون على البيانات الشخصية للآخرين، ويلحقون الأذى بهم من خلال حذف هذه البيانات أو العبث بها أو استخدامها لغير الغرض الذي جمعت لأجله، لذلك فإنه من بين البرامج التقنية للحد من هذه المخاطر وأكثرها انتشارا الجدران النارية (firewalls)

2-1) تعريف برنامج الجدار الناري: يعرف الجدار الناري بأنه مجموعة أنظمة توفر أساليب أمنية بين نترنت وشبكة حواسيب المؤسسات والشركات وغيرها، بحيث تجبر جميع عمليات الدخول إلى الشبكة أو الخروج منها أن تمر من خلال الجدار الناري الذي يقوم بصد اختراقات المستخدمين المتطفلين، وهو يوفر في ذات الوقت حواجز أمنية قبل الدخول إلى الموقع المعني، مثل التحقق من المستخدمين المحليين والخارجيين ونظام الدخول والخروج[1]، لذلك فمن أجل توفير بعض الحماية لنفسها تقوم المنشآت والهيئات العمومية والخاصة بوضع جدار ناري لعزل شبكتها الداخلية عن الأنترنت، غير أن هذا العزل لا يكون كليا وذلك للسماح للجمهور بالاستفادة من الخدمات المقدمة، وفي الوقت ذاته منع المتطفلين والمخربين والبرامج الضارة من الدخول إلى الحاسوب الإلكتروني[2]، حيث يقوم البرنامج الموجود في الجدار الناري بمراقبة المعلومات بين الشبكة الداخلية للمنظمة والعالم الخارجي.[3]

كما يعرف الجدار الناري أيضا بأنه عبارة عن برنامج يقوم على حماية جهاز الحاسوب أثناء اتصاله بشبكة نترنت أو أي شبكة اتصال أخرى من المخاطر، حيث يتولى جدار الحماية فحص كل المعلومات والبيانات الواردة من الأنترنت أو من أي شبكة أخرى، ثم بعد ذلك يقوم بالسماح لها بالمرور والدخول إلى جهاز الحاسوب إذا كانت متوافقة مع إعداد برنامج الجدار الناري، أو يقوم باستبعادها وطردها إذا كانت من البرامج الخبيثة مثل الفيروسات وبرامج التجسس، أو كانت غير متوافقة مع إعدادات جدار الحماية، وبذلك فهذا البرنامج هو حد فاصل بين جهاز الحاسوب وشبكة الانترنت.

كما اعتبرت الجدران النارية (جدران الحماية) أنها عبارة عن برامج أو جهاز يوفر سياجا أمنيا ما بين الحاسب الآلي وشبكة الأنترنيت أو شبكة حاسبات وأخرى، حتى يتم إخضاع جميع عمليات الدخول

---

[*] ظهر أول جدار حماية للشبكات عام 1980 وكان يعمل على عدد محدد من الأشخاص المسموح لهم بالمرور، كما يعمل على تقسيم الشبكات إلى أجزاء وعزل الأجزاء المصابة منها لوقاية الأجزاء السليمة من أن تنتقل إليها الإصابة. أنظر منير محمد الجهني وممدوح محمد الجهني، أمن المعلوماتالإلكتروني، دار الفكر الجامعي، الإسكندرية 2005، ص65

[1] وليد الزيدي، القرصنة على الأنترنيت والحاسوب، التشريعات القانونية دار أسامة للنشر والتوزيع الطبعة الأولى، عمان الاردن 2003، ص101

[2] حسن طاهر داوود، جرائم نظم المعلومات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض 2000، ص109

[3] محمد عبد الله القحطاني، مقال متوفر على الرابط: http://www.boosla.com تم الإطلاع عليه في: 2019/12/28

والخروج من وإلى الشبكة لسيطرة الجدار الناري، فهو إذن جواز مرور للبيانات المتبادلة بين الشبكة الداخلية المحمية والشبكات الخارجية التي يخشى منها[1].

2-2) تقنيات وأشكال الجدار الناري: إن الوظيفة الأساسية للجدار الناري هي القيام بعملية مسح للمعلومات والبيانات التي تصل إليه من شبكة الأنترنت ثم يقوم بتحليلها، وعندما يجد أي شك في هذه المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة، فإنه يقوم بمنع هذه المحاولة وطردها خارج الشبكة، أما إذا كانت المعلومة عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول إلى الحاسبات الآلية، وتتم هذه الوظيفة من خلال التقنيات التالية[2]:

-غربلة حزم البيانات المرسلة packet filtering ويعمل هذا البرنامج في الطبقة الثالثة أو في المستوى المنخفض من جناح TCP/IP، حيث لا يسمح لحزم البيانات بالعبور إلا إذا كانت مطابقة للقوانين المحددة لها مسبقا، فالبيانات تنتقل عبر الأنترنت في صورة حزم إلكترونية، وإذا كان الجدار الناري مصمما بهذه الطريقة، فإنه يفحص كل الحزم التي تمر عبره ويتحقق من موافقتها لشروط معينة.

-غربلة حزم البيانات مع تغيير عناوين الحزم القادمة من الشبكة الداخلية proxies filtering وفي هذه التقنية يحجب الجدار الناري كل أجهزة الشبكة المراد حمايتها وينصب نفسه وكيلا proxy عنها، ومن ثم تأخذ حزم البيانات الواردة إلى الشبكة الداخلية عنوان الجدار الناري، ويقوم هذا الأخير عند استلامها بغربلتها ثم توجيهها إلى وجهتها النهائية، وفي هذه الحالة يحتفظ الجدار الناري بجدول متابعة يربط فيه بين عناوين حزم البيانات الصادرة والواردة، وهو بذلك يوفر حماية أكبر مقارنة بالتقنية الأولى، لأن الجدار الناري يحجب عناوين الشبكات الداخلية مما يصعب مهمة من أراد مهاجمتها.

-مراقبة السياق stateful inspections وهنا يقوم الجدار الناري في هذه الحالة بمراقبة حقول معينة في الحزم الإلكترونية ويقارنها بالحقول المناظرة لها في الحزم الأخرى التي هي في السياق نفسه، والمقصود بالسياق هو مجموعة الحزم الإلكترونية المتبادلة عبر شبكة الأنترنت بين أجهزة حواسيب لتنفيذ عملية ما، وتجري غربلة حزم البيانات التي تنتمي لسياق معين إذا لم تلتزم بقواعده، لأن في ذلك دليلا على أنها زرعت في السياق وليست جزءا منه، مما يولد عليه الظن أنها برامج خبيثة أو أنها حزم أرسلت من طرف مخترق.

ورغم مزايا جدران الحماية المتمثلة في توفير الحماية اللازمة للشبكات والبيانات والحد من تعرضها للاختراق، فإن لها عيوبا يتمثل أهمها في كونها تؤدي إلى بطء التعامل مع شبكة الأنترنت ورفض بعض المعلومات الآمنة التي يحتاج إليها المستخدمون داخل المؤسسات أو الشركات، كما لا يقدم الحماية الكافية

[1] ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي للنشر والتوزيع، الطبعة الأولى، القاهرة 2017، ص74

[2] خالد بن سليمان الغثير، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز للأمن المعلوماتي، جامعة الملك سعود، الطبعة الأولى، الرياض 2009، ص91 وما بعدها.

لمحتوى البيانات التي يتم تمريرها إلى الشبكة الداخلية، والتي تتضمن معلومات غير صحيحة أو برامج ضارة لوجوده خارج حدود الشبكة، كما لا يمنع المهاجم من الداخل والذي يريد سرقة بعض البيانات.[1]

3) تقنية الغفلية: نظرا لكون تبادل البيانات الشخصية عبر شبكة الأنترنت قد يؤلف عنصر تهديد أساسي للخصوصية المعلوماتية، فقد دفعت هذه المخاطر الجدية إلى ابتكار تقنيات متطورة تؤمن لمستخدمي هذه الشبكة تبادلهم البيانات والإتصالات بصورة مستترة، وذلك من خلال استخدام معدات يطلق عليها تسمية أجهزة معاودة الإرسال بشكل مغفل réexpéditeurs anonymes [2] وغالبا ما تتوفر هذه التقنية لدى موردي خدمات الإتصال عبر شبكة الأنترنت، ويعرضونها بمثابة خدمة إضافية للمشتركين.

ففي إطار المداخلات والحوارات التي تجرى داخل المنتديات أو المجموعات الإخبارية المخصصة لطرح ومناقشة بعض المواضيع سيما الطبية أو النفسية، قد يرغب الفرد في إبقائه مستترا لأسباب تتصل بالحياة الخاصة، إذ من المعلوم أن هذه المداخلات والحوارات تبقى موثقة ومحفوظة ويمكن لمن شاء وبعملية بحث بسيطة العثور على أسماء وعناوين أصحاب الرسائل المرسلة ومنذ مدة، لذلك ففي مثل هذه الحالات تكون تقنية الغفلية ذات منافع وإيجابيات تصب مباشرة في خانة حماية الحق في الخصوصية، لاسيما حقه في ألا تجمع أو تحلل أو تستعمل المعلومات المتعلقة بشخصه، والتي تسمح بالتعرف عليه بدون رضاه وموافقته،فهذه التقنية تقوم بمحو جميع العناصر المعرفة بأصحاب الرسائل الحقيقيين، وترسلها بعد ذلك إلى مقاصدها بعناوين مجهولة، وبذلك تمنح هذه التقنية الحماية للمستخدمين لاسيما الحريصين على أن تكون اتصالاتهم تتمتع بقدر من السرية، لكن وإن كانت تقنيات إخفاء الهوية في شبكة الأنترنت تضمن قدرا معينا من الحماية للحق في الخصوصية المعلوماتية، إلا أن لها مظاهر سلبية إذا ما تم إساءة استعمالها، كأن تسهل النشاطات الإجرامية وغير الشرعية على شبكة نترنت عن طريق حجب هوية مطلقي الرسائل الضارة، ويجد مرتكبوا هذه الأفعال أنفسهم مع هذه التقنية مدفوعين بشعور انعدام المعاقبة.[3]

فهذه التقنية تقوم في الحقيقة على مبدأ حق المستخدم في إخفاء هويته في مواجهة المستخدمين الآخرين عند استخدام تقنيات الإتصال، وهو الحق الذي دأبت المجموعة الدولية للعمل على حماية المعطيات الشخصية في مجال الإتصالات على الإهتمام به[4]، خاصة إذا تعلق الأمر بتقنية الغفلية المطلقة غير قابلة للتتبع، وهي تعني أن يستخدم مورد خدمة الأنترنت أجهزة معيدة للإرسال المغفل من النوع الذي يحقق غفلية كاملة، بحيث لا تحتفظ بأية بيانات أو معلومات تسمح بتعريف أصحاب الرسائل ولا تترك أي أثر

[1] ضرغام جابر عطوش آل مواش، مرجع سابق، ص77.

[2] بولين أيوب، مرجع سابق، ص250.

[3] طوني عيسى، مرجع سابق، ص410.

[4] Michel montazeau, les enjeux juridiques de l'anonymat sur internet, mémoire master 2, droit du numirique administration entreprise. Université Paris 1- Panthéon-Sorbonne, page 06

لأي عنوان أو لمنشئهذه الرسائل قبل أن تعيد إرسالها، فيصبح من المستحيل على أي كان معرفة الهوية الحقيقية لأصحابها، بمن فيهم مورد خدمات الإتصال.[1]

وفي هذا المجال نجد أن المشرع الجزائري ألزم مقدمي خدمة الأنترنت بحفظ المعطيات التي تسمح بالتعرف على مستعملي خدمة الانترنت لمدة سنة ابتداءا من تاريخ التسجيل.[2]

وفي الإتجاه المقابل فقد نادى البعض على عدم التشديد في استعمال الأجهزة المعيدة للإرسال التي تؤمن غفلية نسبية وقابلة للتتبع وذلك لتفادي احتمالات البوح عن المعلومات الشخصية من طرف موردي خدمات الإتصال، ذلك أن البوح بالبيانات الشخصية العائدة للمشتركين التي يكون مورد خدمة الإتصالات حائزا عليها يعتبر تعرضا للحق في الخصوصية المعلوماتية[3].

الفرع الثاني: التدابير التنظيمية لحماية البيانات الشخصية

رغم ما يتم توفيره من حماية تقنية لنظم المعلومات من خلال الإبتكارات المتنامية للوسائل التقنية، إلا أن هذه الحماية ليست كافية لضمان حماية البيانات والمعلومات ونظمها وتطبيقاتها، بالإضافة إلى أنها لم تؤد إلى توفير ثقة واسعة بنظم التقنية لدى المستخدمين الذين تسود عندهم قناعة أن أنظمة المعالجة والأنترنت ليست آمنة بقدر ما هو عليه الحال بالنسبة للوسائل التقليدية للأعمال القائمة على السجلات الورقية.[4]

لذلك فمن أجل دعم ثقة المستخدمين للنظم المعلوماتية وشبكات الإتصال، دفع الأمر باتجاه ظهور العديد من المبادرات للتنظيم الذاتي، كوسيلة قانونية تحظى باحترام المستخدمين تقوم على وضع مدونات سلوك ملزمة لقطاع معين وفق رؤية هذا القطاع.

وقد أصبح من المتفق عليه بين مختلف القطاعات أن تتجسد الحماية التنظيمية إما عن طريق التنظيم الذاتي بوضع سياسة خاصة بشأن حماية الخصوصية على مواقع الأنترنت، وإما عن طريق العقد عندما يتعلق الأمر بنقل البيانات الشخصية من إقليم إلى آخر بأمان.

أولا: التنظـيم الـذاتي من أجل حماية الخصوصية المعلوماتية:

إن التنظيم الذاتي هو النقيض لما يعرف بالتدخل التشريعي لتنظيم موضوعات تقنية المعلومات، وقد كان النموذج الأمريكي في التعامل مع تقنية المعلومات قد دعا إلى مزيد من تبني فكرة التنظيم الذاتي في حقول التجارة الإلكترونية،ومعايير الخدمات التقنية وحماية البيانات وأمن المعلومات[5].

[1] بولين أيوب، مرجع سابق، ص255.

[2] أنظر المادة 11 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، المؤرخ في 05 أوت 2009، ج رعدد 47.

[3] بولين أيوب، مرجع سابق، ص 255.

[4] عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والإقتصاد، الرياض، 2012، ص313.

[5] عبد الصبور عبد القوي علي مصري، مرجع نفسه، ص313.

فإزاء عجز القانون والتشريعات المختلفة عن توفير أمن قوي وحماية كاملة للبيانات الشخصية، ونظرا لاختلاف مستويات الحماية لهذه البيانات الشخصية بين دولة وأخرى، فقد برزت الحاجة إلى تجاوز النظام التقليدي في حماية البيانات الشخصية والتوجه نحو تصور أدوات وآليات تنظيمية أخرى تراعي طبيعة شبكة الأنترنت. وقد ظهر في هذا الإطار ما يسمى بالتنظيم الذاتي، الذي يعتمد كوسيلة لحماية البيانات الشخصية المعالجة إلكترونيا في شبكة الأنترنت.[1]

1) تعريف التنظيم الذاتي في حماية الخصوصية المعلوماتية: هو وسيلة قانونية تقوم على وضع مدونات سلوك ملزمة لقطاع معين وفق رؤية هذا القطاع نفسه، فيلزم نفسه بما يخدمه[2]، كما عرف أيضا بأنه تنظيم السوق نفسه بنفسه، مع إتباع سياسة الحد الأدنى من التدخل الحكومي، فهي سياسة شبه حتمية كالقوانين الداخلية في الدولة يجب عدم مخالفتها[3].

ويمكن أن تتحقق حماية البيانات من خلال أشكال عديدة للتنظيم الذاتي، التي من خلالها تؤسس الشركات الصناعية والتجارية نظاما خاصا للممارسة والمعايير يعد سياسة ذاتية لها جميعا.

ومن قبيل تجارب التنظيم الذاتي في بيئة أعمال الأنترنت لتعزيز الخصوصية، مبادرة الثقة الإلكترونية (treust. e) ، مجلس الأعمال لبرنامج الخصوصية على الخط واتحاد الخصوصية على الخط.[4]

ومع تزايد الشركات والجهات العاملة في بيئة الأنترنت، وكذا تزايد الجهات العاملة في حقل الأمن والخصوصية، نجد العديد من مبادرات التنظيم الذاتي، سيما على المواقع الإلكترونية التي تروج لخدمات حماية الخصوصية تحت عناوين متعددة تشير إلى تقديم منتجات وخدمات تحمي الخصوصية، كما أن كثيرا من الشركات التجارية تستخدم شعارات الخصوصية نفسها في خططها التسويقية وموادها الإعلانية وتتسابق في إظهار ما تستخدمه من تقنيات لحماية الخصوصية على الخط.[5]

وإذا طبق التنظيم الذاتي بجميع مقاييسه فإنه قد يعتبر حلا مثاليا وآلية مبتكرة في تنظيم استخدام شبكات التواصل في مجال احترامها للخصوصية المعلوماتية، ذلك أن الأعراف والعادات عندما تتكون تدريجيا على المستوى العالمي تمتاز بقدرتها على أن تكون مصدرا مرجعيا متجاوزا كل الحدود الإقليمية، كما أنها تتمتع بالمرونة والفعالية فيما تقدمه من حلول بشأن حماية البيانات الشخصية في نطاق

[1] بولين أيوب، مرجع سابق، ص260

[2] يونس عرب، موسوعة القانون وتقنية المعلومات والخصوصية، الجزء الثاني، الخصوصية وحماية البيانات في العصر الرقمي، إتحاد المصارف العربية، بيروت، الطبعة الأولى، 2002، ص448

[3] Pierre trudel, Quel droit et quelle régulation dans le cyberespace ? Centre de recherche en droit public, Faculté de droit, Université de Montréal, revue sociologie et sociétés vol. xxxii.2 Les Presses de l'Université de Montréal. 2000 p 191 disponible sur le site https://www.erudit.org/fr/revues/socsoc/2000-v32-n2-socsoc72/001806ar.pdf

[4] يونس عرب، الخصوصية وحماية البيانات في العصر الرقمي، مرجع سابق، ص449 وكذلك رولا جحا، حماية المستهلكين في عصر التجارة الالكترونية، مركز الحكمة للمعلوماتية القانونية، بيروت، 2001، ص69

[5] بولين أيوب، مرجع نفسه، ص264

المعلوماتية، لهذا يؤكد الفقه أن التنظيم الذاتي يعد أداة مكملة للتشريع، بل اعتبره البعض أنه وسيلة أولية تسبق التشريعات كلما وجدت صعوبة لإصدار التشريع أو الحاجة إلى وقت لإصداره.[1]

2) تقييم سياسة التنظيم الذاتي في حماية الخصوصيةالمعلوماتية: إن الحديث عن فكرة التنظيم الذاتي أمام فكرة التشريع الحكومي لا يعني أننا نتحدث عن فكرتين متناقضتين، إذ يمكن حقيقة إعمال السياستين مع غلبة إحداهما على الأخرى، بحسب طبيعة النظام القانوني العام في الدولة، فالنموذج الأمريكي يدعو إلى مزيد من تبني فكرة التنظيم الذاتي والحد من التدخل الحكومي في التعامل مع تقنية المعلومات، أما النموذج الأوروبي في شأن حماية المعلوماتية، يتجه نحو التنظيم الحكومي أكثر، لذلك نجد أن منظمات الإتحاد الأوروبي قد اتجهت دائما إلى توجيه الدول الأعضاء إلى إصدار تشريعات تتلاءم مع القواعد المقررة في الأدلة الإرشادية والتوجيهية الصادرة عن منظماته، كمجلس أوروبا، اللجنة الأوروبية والإتحاد الأوروبي، بل تم الإتجاه إلى التنظيم التشريعي الشامل عبر قوانين البرلمان الأوروبي، ومن ثم لم يكن لسياسة التنظيم الذاتي امتداد كبير نحو دول الإتحاد الأوروبي، والتي كانت تتجه في غالبيتها نحو التنظيم الحكومي عبر تشريعات تتلاءم مع القواعد المقررة في الأدلة الإرشادية والتوجيهية الصادرة عن منظماته[2].

وبذلك فقد تم الحديث على أن مسألة التنظيم الذاتي لا تصلح لكل الدول، فهو إن كان يصلح في الولايات المتحدة الأمريكية كونها تترك مسألة المعايير والمواصفات التقنية للتنظيم الذاتي للسوق، فإن دولا أخرى متطورة كانت أم غير متطورة قد لا يتوفر لها مثل هذا الإطار، ولا تستطيع الحكومات أن تغامر وتترك مسألة تنظيم معايير حماية الخصوصية للسوق، بل يبدو لها أنه من اللازم التدخل من أجل حماية المستهلك وضمان سلامة بياناته الشخصية خلال الخدمات التقنية الموجهة له.[3]

ومن ناحية أخرى فإنه وإن كانت جهود التنظيم الذاتي ساهمت من خلالها قطاعات الأعمال في تعزيز الثقة في شبكة الأنترنت لدى كثيرين ممن يتعاملون عبر هذه الشبكة، فإنها أيضا أثارت تساؤلات وتحديات كثيرة تتعلق بمدى ضمان الإلتزام بقواعد التنظيم الذاتي في بيئة غير مركزية كالأنترنت لا تتحكم بها سلطة مركزية، وعدم خضوعها إلى هيئة محددة تديرها وتنظمها على النطاق العالمي ولها سلطة الإجبار، بالإضافة إلى فشل العديد من جهود التنظيم الذاتي في الولايات المتحدة الأمريكية نظرا لتأثرها في كثير من الأحيان بالمصالح الخاصة، إلى جانب شبكة التواؤم مع هذه السياسات وتنفيذها في مختلف الحقول.[4]

وترتيبا على ذلك فقد ذهب البعض إلى التشكيك في جدوى هذه الوسيلة وفعاليتها معتبرين أنها سوف تقود إلى تعزيز نظام الرقابة الحكومية على شبكة الأنترنت، وإلى فرض قواعد ضيقة على الحريات

[1] يونس عرب، الخصوصية وحماية البيانات في العصر الرقمي، المرجع السابق، ص449.

[2] علي سعيد عبد اللطيف، الجرائم الناشئة عن استخدام الحاسب الآلي، كلية الشريعة والقانون، القاهرة، 1999، ص163

[3] طوني عيسى، مرجع سابق، ص348

[4] بولين أيوب، مرجع سابق، ص263

العامة، وأنه ليس من المؤكد مدى استطاعة أنظمة الخصوصية ذات التنظيم الذاتي لتحل محل التشريعات واللوائح العامة.[1]

لكن في مقابل هذا المنحى المشكك في إمكانية الإتكاء على التنظيم الذاتي في حماية البيانات الشخصية المتداولة عبر مواقع الأنترنت، هناك من يرى أنه لا يوجد ما يمنع تصور قواعد مهنية دولية تنسجم مع خصوصيات هذه الشبكة وتتلاءم معها، والتي يمكنها أن تؤلف أدوات تنظيمية في شبكة الأنترنت لا يستهان بها قد تتحول مع الوقت إلى مصدر فعلي للقانون.[2]

بالإضافة إلى أن حماية الخصوصية المعلوماتية أصبح خيار قطاع الأعمال بقدر ما هو خيار المستخدم ذاته، فليس المستخدمون أو الأفراد وحدهم من يهتمون بحماية خصوصيتهم، فمع ما أظهرته الدراسات المسحية في بيئة التجارة الإلكترونية من مخاطر عدم ثقة المستخدمين بالأنترنت بسبب الخصوصية، ظهر اهتمام عريض ومتزايد لدى قطاعات الأعمال التي أصبحت تأخذ موضوع الخصوصية على محمل الجد وتعمل على توفير الحماية له، لأنه أحيانا يعد كعامل خطير يهدد أعمالها باعتبار أن عدم الثقة بالتجارة الإلكترونية بسبب خشية وتخوف المستخدمين على خصوصيتهم، يمثل عائقا فاعلا لرواج التجارة الإلكترونية ذاتها في البيئة الرقمية[3]، فالشركات تحتاج إلى ثقة المستخدم، وأي خرق جسيم لثقتهم قد يضر بالشركة المخلة بهذه الثقة[4]. لذلك كانت سياسة التنظيم الذاتي كوسيلة تقوم على وضع مدونات سلوك يلزم بها القطاع نفسه وفق رؤية هذا القطاع، وهو الواضح من خلال جهود المنظمات الدولية المختلفة، وعلى رأسها غرفة التجارة الدولية التي قامت بجهود جبارة في هذا المجال[5]، وكذلك مبادرات شركات متخصصة في حماية الخصوصية وعلى رأسها الشبكة العالمية (GNI) التي تعتبر أشهرها[6].

ثانيا: عقود سياسة الخصوصية

غالبا ما تحتاج عملية توظيف شبكة الأنترنت في الأنشطة التجارية والخدماتية إلى نقل البيانات من بلد إلى آخر، أي خارج حدود الدولة، وهو أمر يحتاج إلى ضبط معيار متوازن بين حق تدفق البيانات وتنقلها وبين موجبات الحماية لها، ويتمثل هذا المعيار في ضرورة ضمان أن تتوفر في الدولة المنقول إليها البيانات الشخصية حماية ملائمة لهذه البيانات، تكفل عدم إهدار الحق في خصوصية البيانات الشخصية، وهو معيار قررته كافة الوثائق الأوروبية والتشريعات العالمية، ومنها المشرع الجزائري حينما قرر في المادة 44 من القانون 07/18 أنه لا يجوز لأي مسؤول عن المعالجة نقل المعطيات ذات الطابع

[1] بولين أيوب، مرجع نفسه، 363.

[2] بولين أيوب، مرجع سابق، ص267.

[3] يونس عرب، استراتيجيات وتقنيات الحماية من أنشطة الإعتداء على خصوصيات المعلومات، مقال منشور عبر موقع:
www.elmkz.hooxs.com/t54-topic

[4] توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الانترنيت وحرية التعبير، سلسلة اليونيسكو بشأن حرية الأنترنيت، مرجع سابق ص26

[5] بولين أيوب، مرجع نفسه، ص267

[6] توبي مندل وآخرون، مرجع نفسه، ص26

الشخصي إلى دولة أجنبية إلا إذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها.

ونظرا لعدم توفر الحماية التشريعية للبيانات الشخصية في كافة الدول أو عدم كفاية هذه الحماية في غالب الأحيان، ونظرا لموجبات الأداء المميز في العصر الرقمي، وما يقتضيه من تجاوب مع الأنماط المستجدة للإستثمار المعلوماتي الذي يتطلب ضرورة نقل البيانات وإجراء المعالجة في أكثر من إقليم، فإن عقود نقل البيانات* تكون هي الأداة التي تتجاوب مع معيار توفير قدر من الحماية للبيانات الشخصية، وتحل في نفس الوقت مسألة غياب الحماية التشريعية[1].

وفي إطار هذه العقود نجد أن سياسات الخصوصية المعتمدة على شبكة الأنترنت، تكيف من حيث طبيعتها القانونية بأنها عقود تندرج ضمن فئة نقل البيانات، وهذا بالنظر إلى ما تتضمنه من التزامات عقدية تلقى على طرفي المعاملات الإلكترونية، يتيح الإخلال بها إلى ترتيب المسؤولية العقدية على الطرف المخل بالتزاماته العقدية.

1) تعريف عقود سياسة الخصوصية: هي صفحة أو مجموعة من صفحات موجودة على مواقع الأنترنت، تصف البيانات الشخصية التي يجمعها الموقع وكيفية استخدامها والمواقع التي تتشارك معه في الإستخدام أو تنقل إليها هذه البيانات، ونطاق سيطرة المستخدم على استخدام بياناته الشخصية، والغرض من هذه السياسات هو إبلاغ المستخدم بما يجري جمعه من بيانات شخصية عنه خلال تفاعله مع الموقع، وسياسة الموقع بشأن التعامل معها واستخدامها ونقلها[2].

ومن ثمة فعقود سياسة الخصوصية تتمثل في وجود وثيقة العقد على الموقع الالكتروني متضمنة الحقوق والإتزامات لطرفيه (المستخدم وجهة الموقع) منتهية بمكان متروك لطباعة عبارة القبول أو للضغط على إحدى العبارتين (أقبل) أو (لا أقبل)[3].

لكن ليس بمجرد وجود سياسة الخصوصية على الموقع، يعني أن هذا الموقع يحمي خصوصية المستخدم وبياناته الشخصية، فحدود الحماية وفعاليتها لا يمكن إدراكها إلا بالقراءة التفصيلية لكافة بنود عقد سياسة الخصوصية، التي تظهر التزامات الموقع وما يقرره لنفسه من استثناءات وما يضعه من شروط، فهذه الطريقة وإن كانت في حقيقتها مقنعة للتعاقد، لكنها لم تكن طريقة واضحة، فغالبية السياسات تكتب موجزة وتحيل إلى سياسات تفصيلية عبارة عن شروط كثيرة تكتب بخط صغير، لا أحد يكون

* تسمى هذه العقود في أحيان أخرى اتفاقيات رخص النقل،وهي اتفاقيات تر افق البرامج وهي على شكلين: الأول رخص تظهر على الشاشة أثناء عملية تنزيل البرامج ويوجد على واجهة أي برنامج ويسبق عملية التنزيل، والثاني رخص تكون مع حزمة البرامج المعروضة للبيع، وهي عقود مصممة لبيئة النشاط على الأنترنت، أنظر مروة زين العابدين، مرجع سابق، ص 264-265.

[1] بولين أيوب، مرجع سابق، ص268

[2] بولين أيوب، نفس المرجع، ص271

[3] مروة زين العابدين، مرجع سابق، ص 271

مهتما بقراءتها قبل الموافقة، فالمستخدمون ورغبة منهم في سرعة التعامل مع الموقع فإنهم ينتقلون مباشرة إلى الأيقونة التي تتضمن قبولهم بالسياسة المعروضة دون قراءة شروط هذه السياسة.[1]

وحتى في الأحوال التي يقرأ المستخدم لمرات متتالية بعض سياسات الخصوصية الموجودة على المواقع، فقد تنشأ لديه نوع من القناعة بأن سياسات الخصوصية على المواقع تتشابه في مضمونها، فيقبلها دون التدقيق في محتواها في حين أن لكل موقع سياسته، ويمكن أن تتضمن استثناءات تجعل الحماية المعلن عنها غير فعالة، و تستخدم عقود سياسات الخصوصية كعقود إلكترونية على مختلف المواقع الإلكترونية محل الإتفاقات على الشبكة، و التي تتطلب بيانات شخصية من المستخدم للتفاعل معه، ويكون ذلك بشكل رئيسي في مواقع إنزال البرامج أو الملفات من الشبكة أو الدخول إلى خدمات المواقع، وتحديدا التي تتطلب اشتراكا خاصا في بعض الأحيان، أو لغايات التسجيل والإلتزام العقدي بإنفاذ الخدمة المعروضة مجانا بشروط الموقع، كخدمات البريد المجاني، وكذلك لإبرام التصرفات القانونية على الخط كالبيع والشراء، وطلب القرض وإجراء عمليات حوالة مصرفية[2]، كما في مواقع التجارة الإلكترونية والبنوك الإلكترونية.

2)أحكام عقود سياسات الخصوصية: كل أنواع عقود الأنترنت، ابتداء من عقود الإشتراك في الخدمة، مرورا بالعقود ذات المحتوى التقني أو عقود المستخدمين مع المواقع[3]، تتطلب أن يتنازل المستخدم عن بعض بياناته الشخصية، وأن يتخلى للجهة الإلكترونية غير مرئية والإفصاح لها عن بعض بياناته الشخصية، لذلك يجب أن يكون المستخدم على دراية أن مثل تلك البيانات لن تتوقف عند سجلات هذه الجهة أو الموقع، وأن احتمال إعادة استغلال بياناته الشخصية هو أمر حقيقي سواء لأغراض تسويقية أو سياسية، أو استخدامها في دراسات تحليلية، سواء من قبل شركات أو جهات حكومية، لذلك فإن مثل هذا الإفصاح الطوعي يجب أن يكون مشروطا في نطاق العقد[4]، وهو الأمر الذي غالبا ما يظهر في الشكل الذي تتخذه عقود سياسة الخصوصية وكذا ما تحتويه من بنود في سبيل تأمين الحماية للبيانات الشخصية.[5]

لذلك فاحكام عقود سياسة الخصوصية من حيث الشكل يجب أن تعكس الموقف القانوني من الخصوصية في نطاق يشعر المستخدم فيه بوجود مشروعية لما يطلبه الموقع وما يضعه من شروط، ذلك أن حماية خصوصية المعلومات تقوم على مبادئ تحكم عمليات جمع وتخزين ومعالجة واستعمال وتبادل البيانات الشخصية، وهي مبادئ تدور حول الإلتزام بعدم جمع البيانات في نطاق أوسع من الغرض الذي تجمع لأجله، وهو غرض ضروري ومشروع، وكذا الإلتزام بتحديد الإستعمال لهذه البيانات في نطاق الغرض منها، وخلال المدة الملائمة المحددة أو المتفق عليها، وعدم إساءة الاستخدام أو تعديه لأبعد من

[1] بولين أيوب، مرجع نفسه، ص271

[2] محمد أمين الرومي، التعاقد الالكتروني عبر الأنترنت، دار المطبوعات الجامعية، الطبعة الأولى، الإسكندرية، 2004، ص97.

[3] حسام الدين الأهواني،حماية حقوق الملكية الفكرية في مجال الأنترنت، ورقة عمل مقدمة إلى مؤتمر الملكية الفكرية، جامعة اليرموك، الأردن، الفترة 10، 2000/07/11 ص12.

[4] مروة زين العابدين، مرجع سابق، ص369.

[5] مروة زين العابدين، مرجع نفسه، ص 369.

ذلك، ومنح المستخدمين حقوقا منذ اللحظة الأولى لجمع البيانات تبدأ بإعلامهم بعملية الجمع وغرضها وإتاحة خيار الرفض أو القبول أو التراجع اللاحق عنه.[1]

ومن ثمة فإن مراعاة جهة الموقع الإلكتروني لهذه المبادئ وتجسيدها كبنود في عقود سياسة الخصوصية وتضمينها ما يعكس هذه المبادئ، من شأنه بناء الثقة لدى المستخدم في وجود حماية لخصوصيته، وفي سبيل ذلك فإنه من الغالب الأعم أن نجد سياسات الخصوصية تذهب إلى مراعاة جوانب شكلية لا تقل أهمية عن مضمونها، خاصة إذا كانت صياغة سياسة الخصوصية وفق بناء شكلي يمكن المستخدم من استيعاب مضمونها، وبالتالي فمراعاة العناصر الشكلية له أهمية بالغة، ومن أهم هذه العناصر:

- أن تكون السياسة مختصرة بقدر الإمكان دون إخلال بمحتواها، بحيث يكون هناك توازنا بين موجبات تغطية البناء الموضوعي من خلال عبارات واضحة مختصرة، فتكون بعيدة عن الإسهاب غير اللازم وفي نفس الوقت الإبتعاد عن الإيجاز المفرط إلى حد فقدان السياسة قيمتها ومضمونها، لكن من الطبيعي أن تختلف سياسات الخصوصية سعة أو تضييقا تبعا لاختلاف طبيعة المواقع وأغراضها، فالمواقع التي لا تجمع البيانات الشخصية إطلاقا هي ليست بحاجة في الأصل إلى سياسة الخصوصية، لكن عنصر الثقة اللازم يوجب عليها إشعار المستخدم بحقيقة عدم جمعها للبيانات وبالتزامها بعدم الجمع دون علمه عبر الوسائل الإلكترونية، و هنا تكون سياسة الخصوصية محددة ومختصرة، وأما المواقع التي تكون بطبيعتها مما يتعامل بالبيانات الشخصية، أو قد تزودها لجهات أخرى رسمية، كما في شركات الإتصال وشركات تزويد الخدمات التقنية ونحوها، فإنه لا يفي حاجتها الإ ختصار الذي يتعارض مع أغراضها، بل ولا يتناسب مع عناوين السياسة ذاتها التي تضعها على مواقعها.

- أن تتوفر الصفحة الرئيسية للموقع على أيقونة تكون في موضع تسهل مشاهدته والوصول إليه، تقود المستخدم وتنقله إلى سياسة الخصوصية.

-أن يتوفر في الموقع ملخص موجز لسياسة الخصوصية في أعلى النموذج، والذي يطلب تعبئته بالبيانات الشخصية مع مدخل إلى النص الكامل لسياسة الخصوصية.[2]

لكن ما يمكن أن يلاحظه أي متصفح للمواقع الإلكترونية التي تهتم بحماية الخصوصية وتعتمد على نظام سياسة الخصوصية، أنها غالبا ما ترد هذه الأخيرة في شكل لا يشجع إطلاقا على قراءتها، بحيث نجدها طويلة من حيث المتن، ومقسمة إلى صفحات تتطلب قراءتها الإنتقال من صفحة إلى أخرى، كما تكون مكتوبة بخط صغير يصعب قراءته، أو في مكان من الموقع قد لا يتم الإنتباه إليه.

ومن حيث أحكام عقود سياسة الخصوصية من الجانب الموضوعي فإنه يفترض أن تكون نماذج سياسة الخصوصية شاملة في تحقيقها للعناصر الموضوعية، ويكون ذلك إذا تضمنت المبادئ التي تهدف إلى تأمين حماية فعالة للبيانات الشخصية، مع مراعاة أن تتناسب في محتواها مع أغراض الموقع الخاص بها، بحيث

[1] بولين أيوب، مرجع سابق، ص273.

[2] بولين أيوب، مرجع سابق، ص 274.

يكون لكل موقع هويته الخاصة به، والتي تعكسها سياسة الخصوصية، وتتمثل أهم هذه العناصر فيما يلي:[1]

- تتضمن سياسة الخصوصية توضيحا عن البيانات الشخصية التي يتم جمعها سواء تلك التي يفصح عنها المستخدم طوعا ويقدمها مباشرة عن طريق تعبئة استمارات من أجل الحصول على الخدمة، أو تلك التي يتم جمعها عنه عن طريق برامج خاصة كرسائل الكوكيز.

- توضيح الأغراض التي تجمع لأجلها البيانات الشخصية، وغايات هذا الجمع، وذلك بشكل واضح بعيدا عن استعمال العبارات الغامضة.

-توضيح الأوجه الضرورية التي ستستخدم فيها هذه البيانات سواء بالنسبة للموقع نفسه أو الجهات المشتركة معه.

-تحديد الطرف الثالث الذي ستنقل إليه البيانات الشخصية، والإلتزام بعدم نقلها له دون موافقة المستخدم مع بيان أغراض نقلها بصورة دقيقة وشاملة، وهنا يحدد الموقع مدى التزامه بحماية البيانات لدى نقلها أو عدم مسؤوليته عن هذا النقل، مع إتاحة الخيار للمستخدم عندها لرفض نقل بياناته مستقلا عن باقي الشروط والإلتزامات، حتى يتسنى له ممارسة حقه في هذا الخيار.

-تحديد الأغراض الثانوية التي يريد الموقع استخدام البيانات الشخصية لأجلها، وإتاحة الحق للمستخدم برفض استخدام بياناته الشخصية إلا للغرض المعلن أو قبوله بالأغراض الثانوية، مع الإلتزام بعدم تجاوز هذه الأغراض تحت ذريعة انطواء أغراض أخرى ضمن الغرض الثانوي بصورة ضمنية.

-توضيح وتبيان ما إذا كان للمستخدم الحق في الوصول إلى بياناته الشخصية والعمل على تعديلها وتصحيحها أو المطالبة بإلغائها، وفي الحالة التي لا تتيح المواقع هذا الحق عليها أن توضح ذلك صراحة، حتى يتمكن المستخدم من توضيح موقفه من خلال حرصه على الدقة في الإدلاء بها أو رفضه الإدلاء بها أصلا.

-توضيح المدة التي يحتفظ خلالها الموقع بالبيانات، وما إذا كانت ستحفظ لمدة أطول من الغرض الذي جمعت لأجله.

توضيح الجهة التي يتصل بها المستخدم عند الإعتداء على خصوصياته ورغبته في تقديم شكوى والمطالبة بالتعويض عن الضرر، وكذا بيان آليات التعويض.

بيان وتوضيح ما هو القانون الواجب التطبيق في حالة حدوث أي نزاع، وما هي الجهة القضائية المختصة.

وانطلاقا مما سبق نخلص إلى القول أن الهدف الأساسي من وضع سياسات الخصوصية هو سعي الجهات التي تتعامل مع البيانات الشخصية في بيئة شبكات الإتصال إلى إقناع مستخدمي هذه التقنية بحرصها

[1] بولين أيوب، نفس مرجع، ص275-276.

على خصوصيتهم في هذا الفضاء الإلكتروني، وذلك من أجل كسب وتحقيق الثقة بينها وبينهم، لأنه بدون هذه الثقة لا وجود لأي نشاط استثماري على الشبكة الإلكترونية.

الفرع الثالث: الإلتزام القانوني بالسر المهني لضمان سرية البيانات الشخصية

لقد شددت القوانين بمجملها على الإلتزام بسرية البيانات الشخصية سواء في معرض التطرق إلى الموجبات المترتبة على مسؤول المعالجة ومنفذيها، أو في معرض ذكر مبادئ المعالجة.

وقد أكدت جميع التشريعات على بعض الإجراءات من قبيل الحرص على ضمان سرية البيانات كضرورة إتلاف البيانات بعد الإنتهاء من تحقيق هدف المعالجة، أو عندما يتوقف المسؤول عن المعالجة نهائيا من ممارسة أعمال المعالجة، وكذلك على التزام كل من اطلع على البيانات بمناسبة تنفيذ عمليات المعالجة بعدم الكشف عنها، حتى بعد انتهاء فترة عمله عليها، حيث يعتبر هذا الأمر بمثابة الإلتزام بالأسرار المهنية.[1]

والملاحظ أن القضاء الفرنسي قد سجل تشددا ملحوظا حيال هذا الإلتزام الملقى على عاتق المسؤول عن المعالجة، حيث اعتبرت المحكمة الكبرى لفرساي (TGI de Versailles)، أن المسؤول عن معالجة معطيات شخصية خاصة بملف تسيير الموظفين التابعين للمؤسسة، والذي سمح بتسرب عدد منها إلى الصحافة يبين أن المسؤول عن هذا الملف لم يتخذ جميع الإجراءات الضرورية لمنع هذا التسرب، مما استوجب الإعلان عن مسؤوليته.[2]

ولقد أوجب المشرع الجزائري في المادة 44 من القانون 07/18 على المسؤول عن المعالجة، وعلى كل الأشخاص الذين اطلعوا على المعطيات ذات الطابع الشخصي أثناء ممارستهم لمهامهم في مجال معالجة هذه المعطيات، الإلتزام بالسر المهني حتى بعد انتهاء مهامهم، ويعتبر هذا الموجب قريبا نوعا ما من موجب ضمان سلامة المعلومات، مع فارق في الأشخاص الموجه لهم هذا الإلتزام، وهم كل الأشخاص المأذون لهم بالإطلاع على البيانات الشخصية لسبب قانوني أو إداري*، إذ يتقيد هؤلاء بعدم الإفصاح عما يطلعون عليه من معلومات، بينما يرتبط الإلتزام بسلامة المعلومات باعتماد تدابير تقنية وتنظيمية تمنع الإطلاع على البيانات الشخصية على من لا يحق لهم أصلا الإطلاع عليها.[3]

أولا: مفهوم مبدأ الإلتزام بالسر المهني

يعتبر السر المهني من أهم الإلتزامات التي تقع على عاتق المهنيين الذي يتعين عليهم حفظ أسرار عملائهم الذين وضعوا ثقتهم فيهم، ولذلك فقد اشترط القانون بأن يكون السر مودعا لدى الأمناء عليه بمقتضى

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص131.

[2] منى الأشقر جبور، محمود جبور، مرجع سابق، ص131.

* الأشخاص المأذون لهم بالإطلاع على البيانات الشخصية هم: المسؤول عن المعالجة، المعالج من الباطن، من يقوم بمعالجة المعطيات، المرسل إليه المعطيات، رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، أنظر المادة 26، 40 من القانون 07/18 المتضمن تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] منى الأشقر، محمود جبور، مرجع نفسه، ص130.

وظيفتهم الدائمة أو المؤقتة، فهؤلاء وحدهم من يستطيعون بحكم مهنتهم أن يتعرفوا على أدق الخصوصيات، وليس لهم بحكم القانون خيانة الثقة الموضوعة فيهم.

وتكمن أهمية السر المهني في اتصاله الوثيق بالحياة الخاصة للفرد، فهو من أهم جوانب الحرية الشخصية، ذلك أن لكل فرد الحق في الإ حتفاظ بأسراره، وله إن شاء أن يدلي بها أو ببعضها إلى من يشاء ممن يثق بهم، ويتعين على المعهود إليه بالسر أن يكتمه.[1]

ولقد تضمنت كافة القوانين والشرائع واجب الحفاظ على السر المهني وتجريم إفشائه، وهذا ليس فقط لحماية صاحب السر ومكانته ومركزه وشرفه، فلكل شخص الحق في احترام حياته الخاصة، بل أيضا لصيانة وحماية المصلحة العامة في المجتمع، وعدم تعر يض المهن والمراكز السامية النبيلة للإهانة أو لعدم الثقة والاحترام.[2]

لذلك فإن المشرع يهدف من خلال حماية السر المهني إلى حماية مصلحتين: الأولى هي مصلحة صاحب السر، والثانية هي مصلحة المهنة ذاتها، فالثقة المفترضة في القائمين على المهنة والمفروضة عليهم هي التي تتيح لهم فرصة التعرف على خصوصيات الأفراد، ومن ثم قام الإلتزام في جانبهم بعدم خيانة هذه الثقة، فإذا أخلوا بهذا الإلتزام زالت عنهم الثقة، وتردد الناس في الإلتجاء إلى خدماتهم فتتعطل بذلك مصالحهم، كما تتعطل هذه المهن أيضا، وفي ذلك ضرر جسيم يصيب مصلحة أساسية للمجتمع كله.[3]

ورغم كتمان السر في الأصل واجب خ ، لقي تمليه قواعد الأخلاق العامة وتقتضيه مبادئ الشرف والأمانة، وإفشاؤه فعل ممقوت لا تقره قواعد السلوك القويم، إلا أن المشرع لم يجرم كل حالات الإفشاء وإنما قصر التجريم على إفشاء أسرار تودع لدى من يمارسون مهنا تفترض في عملائهم اضطرارهم إلى إيداع أسرارهم لديهم[4] شريطة أن تقوم الصلة بين السر والمهنة.[5]

وإذا كانت الحياة الخاصة في الماضي يكسوها الخفاء لاعتبارات أخلاقية ودينية، إلا أنها في العصر الحديث أصبحت مهددة بالكشف عنها وعن أسرارها، مما حذا بالتشريعات التدخل لاحتواء وتنظيم السرية، بل بات من الضروري أن يفرض القانون عقابا على كل من يقوم بإفشاء السر المهني الذي أؤتمن عليه، غير مكترث لما يترتب على ذلك من فضائح أو إساءة إلى السمعة والكرامة، غير مهتم بمبادئ الشرف والإ عتبار والأمانة.

---

[1] أحمد مصبح الكتبي، المسؤولية الجنائية الناشئة عن إفشاء السر المهني، مقال منشور بمجلة جامعة الشارقة للعلوم القانونية، المجلد 16، العدد الثاني، ديسمبر 2019، ص.302

[2] سعيد أحمد علي قاسم، السر المهني، مقال منشور بمجلة الفكر الشرطي، المجلد الرابع والعشرون، العدد 95، كلية الشرطة أبو ظبي، الإمارات العربية، أكتوبر 2015، ص02

[3] أحمد فاروق زاهر، الحماية الجنائية للأسرار المهنية- دراسة مقارنة بين القانونين المصري والإماراتي- مجلة الشريعة والقانون، كلية القانون، جامعة الإمار ات العربية المتحدة، العدد الثامن والخمسون، السنة الثامنة والعشرون، أفريل 2014، ص3.

[4] نعيم عطية، حق الأفراد في حياتهم الخاصة، مجلة هيئة قضايا الحكومة، القاهرة، العدد 04، السنة 21، ص97.

[5] لا يكون السر مهنيا في حالة إفشاء يصدر من صديق أودع لديه صديقه سره، طالما أنه لم يتلق السر بحسبانه يمارس مهنة ما، وكذلك إذا صدر الإفشاء من خادم أو مستخدم خصوصي فهؤلاء لا يضطر مخدوموهم إلى إطلاعهم على أسراره.

1)تعريف السر المهني: لقد خلت التشريعات المختلفة من أي تعريف للسر المهني، لذلك نجد أن الفقه قد عرفه بتعريفات مختلفة ومتعددة بتعدد المهن، فلكل منها تقاليدها وأعرافها، لأجل هذا قيل بأنه ليس هناك سر مهني واحد إنما العديد من الأسرار المهنية[1].

وقد عرف السر المهني بأنه كل أمر مطلوب كتمانه سواء كان يتعلق بشخص طبيعي أو معنوي معين، علم به شخص آخر بسبب مهنته وكان ملزما بحكم هذه المهنة بالمحافظة عليه وعدم الكشف عنه في الأحوال المحددة قانونا[2]

كما عرف السر المهني أيضا بأنه كل معلومة يعرفها صاحب المهنة أثناء أو بمناسبة ممارسة مهنته أو بسببها، وكان في إفشائه ضرر لشخص أو لشركة[3]

وذهب جانب من الفقه إلى تعريف السر المهني بأنه كل صفة لواقعة ما، يتضمن انحصار العلم بها في عدد محدود من الأشخاص، إذا كانت ثمة مصلحة لشخص أو أكثر في ذلك، فالسرية تقتضي ألا يعلم بالواقعة سوى أشخاص محددين، أما إذا كانت معلومة لدى عدد كبير من الأشخاص انتفت عنها تلك الصفة[4].

يبدو أن التعدد في تعاريف السر المهني راجع إلى اختلاف المعايير المعتمد عليها كأساس لتحديد صفة السرية للوقائع أو المعلومات التي يراد إضفاء الحماية عليها، حيث ذهب البعض إلى الأخذ بمعيار الضرر كأساس لتحديد السرية، وذهب البعض الآخر الى الإعتماد على إرادة مودع المعلومات واتجاهها إلى إبقائها سرا لدى المودع لديه، في حين ذهب اتجاه آخر إلى الأخذ بمعيار التفرقة بين الوقائع السرية والوقائع المعروفة من أجل تحديد ما يعد سرا ويستوجب حمايته وما يعد غير ذلك.[5]

وترتيبا على هذه الأسس يمكن تعريف السر المهني انطلاقا من أحد الإتجاهات الثلاث التالية:

1-1) تعريف السر المهني على أساس الضرر: يتجه أنصار نظرية الضرر في تعريف السر المهني إلى اعتبار أن المعلومة أو الواقعة لا تعتبر سرا إذا كان إفشاؤها أو البوح بها لا يشكل مساسا بسمعة وكرامة صاحبها، أما إذا كان إفشاء هذه المعلومة من شأنه إلحاق ضرر بصاحبها من خلال المساس بشرفه وكرامته وطمأنينته أصبحت من قبيل الأسرار وتقوم مسؤولية المؤتمن عليها، وإذا لم يكن هناك ضرر ينتج عن إفشاء المعلومة فلا تكون لها صفة السر.

---

[1] سليمان علي حمادي الحلبوسي، المسؤولية المدينة الناشئة عن إفشاء السر المهني، دراسة قانونية، منشورات الحلبي الحقوقية، بيروت2012، ص17

[2] أحمد مصبح الكتبي، مرجع سابق، ص306

[3] محسن عبد الحميد البيه، نظرة حديثة إلى خطأ الطبيب الموجب للمسؤولية المدنية في ظل القواعد القانونية التقليدية، مكتبة الجلاء الجديدة، المنصورة 1993، ص630

[4] الحاسي مريم، إلتزام البنك بالمحافظة على السر المهني، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2012، ص11.

[5] أحمد كامل سلامة، الحماية الجنائية للأسرار المهنية، دار النهضة العربية للنشر والتوزيع، القاهرة، 1988، ص39

وعليه يعتبر السر المهني "كل ما يعرفه الأمين أثناء أو بمناسبة ممارسته لمهنته، وكان في إفشائه ضرر للشخص أو عائلته، إما لطبيعته أو بحكم الظروف التي تحيط به[1]، كما يعد سرا مهنيا أيضا من هذا المنطلق كل ما يعرفه الأمين أثناء أو بمناسبة ممارسة وظيفته أو مهنته وكان في إفشائه حرج لغيره"[2].

وقد انتقد هذا المعيار على أساس أنه غير كاف للتأسيس عليه في تعريف السر المهني، فضلا عن كونه ليس السبب الوحيد الذي يجعل من المعلومة سرا مهنيا والبوح بها يشكل جرما[3]، كما أن هناك من المعلومات ما قد تكون سرا على الرغم من أن إفشاءها قد لا يضر بصاحبها، فالطبيب مثلا يعطي لغير المريض شهادة بخلو هذا الأخير من أي مرض، فهذه الشهادة السلبية من الطبيب ليس من شأنها الإضرار بالمريض، ويكون للطبيب في هذه الحالة سلطة تقديرية ما إذا كان للمريض مصلحة في حفظ السر، ويرجع الأمر إلى المريض نفسه الذي له وحده أن يقدر هذه الظروف.[4]

2-1) تعريف السر المهني على أساس التفرقة بين الوقائع المعروفة والوقائع المجهولة: إنطلاقا من هذا المعيار فإن الوقائع المعروفة تكون لها صفة العمومية بطبيعتها، ومن ثم فهي لا تصلح لأن تكون سرا، لأنها وقائع يعرفها الكافة، وإذاعتها لا تضيف أمورا جديدة بالنسبة للغير[5] ، والمعلومات التي تشكل سرا هي تلك التي لا يعرفها أحد، أو يعرفها عدد محدود من الأشخاص ولا يجوز لمن أودعت لديه بحكم مهنته البوح بها.

ومن هذا المنطلق عرف أصحاب هذا الإتجاه السر المهني أنه كل واقعة ينبغي أن تظل بعيدة عن علم الكافة، وينحصر العلم بها في شخص من تتعلق به أو أشخاص محددين ويحظر عليهم البوح بها، ولا يلزم لاعتبار الواقعة سرا أن ينحصر العلم بها في شخص واحد أو شخصين، بل قد يعلم بها عدة أشخاص وتبقى مع ذلك لها صفة السر[6]، شريطة أن لا تكون هذه المعلومات معروفة لدى جميع الناس، وبالتالي فالمعلومة المعروفة بطبيعتها والوقائع العامة لا تعد سرا.

واعتقد أن هذا المعيار هو الذي أخذ به المشرع في القانون 07/18 عندما ألزم في المادة 26 كلا من رئيس وأعضاء السلطة الوطنية بالمحافظة على الطابع السري للمعطيات الشخصية والمعلومات التي اطلعو عليها وكذلك عندما ألزم في المادة 40 المسؤول عن المعالجة بالسر المهني أثناء ممارسته لمهامه على معطيات شخصية، والتي الأصل فيها أنها معلومات غير معروفة لدى العامة.

---

[1] محمد صبحي نجم، شرح قانون العقوبات الجزائري –القسم الخاص- ديوان المطبوعات الجامعية، الطبعة الخامسة، الجزائر، 2005، ص111.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص (الجرائم ضد الأشخاص والجرائم ضد الأموال وبعض الجرائم الخاصة)، الجزء الأول، دار هومة، الجزائر، 2009، ص248

[3] أنظر في هذا المعنى: أحمد كامل سلامة، مرجع نفسه، ص41.

[4] عبد السميع أسامة السيد، التعويض عن الضرر الأدبي، دراسة تطبيقية في الفقه الإسلامي والقانون، دار الجامعة الجديدة، الإسكندرية، 2007، ص87

[5] محمود صالح العدلي، الحماية الجنائية لالتزام المحامي بالمحافظة على أسرار موكليه –دراسة مقارنة- دار الفكر الجامعي، الإسكندرية، 2005، ص68

[6] فتوح عبد الله الشاذلي، شرح قانون العقوبات القسم الخاص، الجزء الأول، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، 1996، ص852

3-1) تعريف السر المهني انطلاقا من إرادة صاحب المعلومة: ذهب جانب من الفقه إنطلاقا من هذا المعيار، إلى اعتبار أن الواقعة لا تكون سرا إلا بإرادة من أودعها، فلكي تعتبر الواقعة سرا ولا يجوز إفشاؤه للغير، يجب أن تكون قد أودعت من صاحبها لدى الأمين عليها واشترط عليه ألا يفشيها للغير وبقائها في الكتمان، وهذا يستلزم أن يكون صاحب السر قد عبر عن إرادته تعبيرا صريحا لكي تكون الواقعة سرا[1].

ومن هنا يعد السر المهني وفقا لهذا المعيار كل المعلومات التي يودعها صاحبها بإرادته لدى شخص معين بحكم مهنته فيعد أمينا عليها، ولا يجوز له بعد ذلك إفشاؤها. وهو المعيار الذي أخذ به المشرع الجزائري في قانون العقوبات حينما نصت المادة 301 على أنه يعاقب الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار، أدلي بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاؤها ويصرح لهم بذلك"

لكن هذا المعيار قد تعرض للنقد على أساس أن صاحب السر قد لا يعلم بالسر، وإنما يحصل اكتشافه من طرف الأمين، وبالتالي لا يكون للمعني مجال للتعبير عن إرادته بكتمان المعلومة لدى الأمين عليها طالما أنه لا يعلم بها أصلا ولم يدلي هو بها إليه، فالطبيب الذي يكتشف بعد فحصه للمريض أن هذا الأخير يعاني من مرض خطير يجهله، ومع ذلك يلتزم بعدم إفشاء الأمر، فكتمان هذا السر من قبل الطبيب لا يستوجب طلب المريض منه ذلك[2]، فضلا عن كون هذا المعيار لا يحقق الغاية من حماية السر المهني، ذلك أن بعض الوقائع تعتبر سرا بطبيعتها أو بحكم القانون، ولا دخل لإرادة المودع في ذلك، فلا مبرر لجواز إفشائها لمجرد إرادة المودع إلى بقائها سرا.[3]

2) أسس الإلتزام بالسر المهني: إذا كان السر المهني يجد أساسه في القانون، فإن الفقه كان له السبق في تأسيس هذا الإلتزام، غير أنه اختلف في تحديد أسسه، فبينما ذهب فريق إلى اعتماد نظرية العقد أساسا لهذا الإلتزام واعتباره التزاما تعاقديا مصدره الرابطة التعاقدية بين المهني وصاحب السر، ذهب فريق آخر إلى اعتماد نظرية النظام العام أساسا للإلتزام بالسر المهني.

1-2) نظرية العقد كأساس للالتزام بالحفاظ على السر المهني: يرى أنصار هذا الإتجاه أن التزام المهني أو الموظف بالسر المهني قائم على اتفاق المؤتمن (صاحب السر) والأمين على السر المهني، ومن ثم فإن أي شخص عندما يتجه للحصول على الخدمة فإنه حينها يكشف بعضا من أسراره للمهني في سبيل الحصول على هذه الخدمة، هنا يحصل أن يلتزم صاحب السر بتأمين سره للمهني أو الموظف، في مقابل أن يلتزم هذا الأخير بحفظه وعدم إفشائه، ويقرر هذا الإلتزام سواء نص عليه العقد صراحة أم لم ينص عليه*.

---

[1] عنان داود، التزام الطبيب بالحفاظ على السر الطبي، رسالة لنيل شهادة الماجستر، كلية الحقوق بن عكنون جامعة الجزائر، 2000-2001، ص21.

[2] بن سعيد صبرينة، مرجع سابق، ص73

[3] محمد عبد الودود عبد الحفيظ أبو عمر، المسؤولية الجزائية عن إفشاء السر المصرفي، دار وائل للطباعة والنشر، عمان الأردن، 1999، ص26

* من الاجتهادات القضائية التي اعتبرت أن الإلتزام بالسر المهني يرتكز على أساس العقد، نجد القضاء الفرنسي القديم في الحكم الصادر في قضية (walas) بتاريخ 05 ماي 1885 حين اعتبرت المحكمة أن السر المهني بمثابة عقد وديعة. أنظر عادل جبري محمد حبيب، مدى المسؤولية

لذلك فإن أنصارو منظري هذا الإتجاه يعرفون الإلتزام بالسر المهني بأنه التزام ناجم عن عقد بين المؤتمن (صاحب المهنة) وصاحب السر (الزبون) تترتب عنه التزامات متبادلة بين الطرفين، فصاحب السر يلتزم بالوفاء بالأجر و المؤتمن يلتزم بتلقي السر من صاحبه والحفاظ عليه.[1]

فالعميل مثلا الذي يتقدم أمام البنك قاصدا مساعدته فيدلي ببعض أسراره، ويعرض عليه البنك خدماته كنماذج عقد فتح الحساب أو عقد الإقتراض إلى غير ذلك من أنواع العمليات المصرفية، ويقبل العميل بالنموذج المقرر ويوقع عليه، فنكون في هذه الحالة أمام عقد والتزامات متبادلة، لا يحق للبنك من خلالها أن يتصرف في تلك الأسرار التي سبق وأن أدلى إليه بها العميل بخلاف ما يريده هذا الأخير[2]

ورغم محاولة أنصار هذه النظرية تفسير وتبرير الأساس القانوني للإلتزام بالسر المهني، إلا أنها لم تسلم من نتقاد، حيث لم تلق قبولا لدى العديد من الفقهاء مهما كان تكييف هذا العقد، فهذه النظرية تقوم على افتراض عقد بين العميل والأمين على السر، وهو أمر لا يتفق مع الواقع، لأن العقد يتطلب لقيامه توافر أركان معينة وهي الإرادة الحرة وأهلية المتعاقدين وسبب ومحل مشروعين، لكن السر قد يتعلق بشخص غير كامل الأهلية، كما قد يكون موضوعه غير مشروع،[3]كما قد يكون صاحب السر غير عالم به، كما في حالة المريض الذي يخفي عنه الطبيب بعض الأسرار المتعلقة بخطورة المرض، ومن ثم فإذا كان صاحب السر هو وحده الذي يملك الموافقة على إباحته و إفشائه وهو غير عالم به، فإن رضاه انصب على واقعة غير معلومة أو غير صحيحة ومن ثم أصبح محل الرضا منعدما.[4]

بالإضافة إلى أن القول بتأسيس السر المهني على أساس العقد يترتب عليه حسب القواعد العامة للعقود أنه يجوز لكل متعاقد منهما أن يمتنع عن أداء التزامه إلى أن يؤدي المتعاقد الآخر التزامه المقابل، وذلك ما لم يكن أحدهما ملتزما حسب الإتفاق أو العرف بأن ينفذ نصيبه من الإلتزام أولا، وعليه فإنه وإعمالا لهذه القاعدة جاز مثلا للمحامي إفشاء السر المعهود به إليه من طرف موكله إذا ما امتنع هذا الأخير عن دفع الأتعاب وهو أمر مخالف للواقع.

ووفقا لهذه النظرية أيضا يكون الإفشاء مباحا بموافقة صاحب السر، طالما أن المصلحة الشخصية لصاحب السر هي المبرر لوجوب الكتمان، إلا أن هذا الأمر مخالف للقانون، ذلك أن رضا صاحب السر

عن الأفعال بالالتزام بالسر المهني أو الوظيفي مع عرض لأهم الحالات التي يرتفع فيها الالتزام بالسر المهني دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر 2003، ص45

[1] أسامة بن عمر محمد عسيلان، الحماية الجنائية لسر المهنة في الشريعة الإسلامية والقوانين الوضعية وتطبيقاتها في بعض الدول العربية، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، كلية الدراسات العليا- قسم السياسة الجنائية- جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2004، ص107.

[2] الحاسي مريم، مرجع سابق، ص55

[3] أحمد كامل سلامة، مرجع سابق، ص84

[4] موفق علي عبيد، المسؤولية الجزائية للأطباء عن إفشاء السر المهني، الطلعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 1998، ص82

بإفشائه لا ينف عن هذا الفعل الصفة الجرمية لإضراره بالمجتمع من خلال زعزعته للثقة المتطلبة في ممارسة بعض المهن والوظائف.[1]

لذلك نعتقد أن الإلتزام بالسر المهني يتم بمجرد الدخول إلى المهنة وأداء اليمين القانونية بالمحافظة على السر المهني، أو استنادا إلى القوانين العقابية أو القوانين المنظمة للمهن، ومن ثم الإلتزام بالكتمان يكون قبل أي تعاقد، وبغض النظر عن إبرام أي عقد.

2-2) نظرية النظام العام كأساس للإلتزام بالحفاظ على السر المهني: إزاء قصور نظرية العقد كأساس للإلتزام بالسر المهني، وأمام الإنتقادات التي وجهت لها ذهب بعض الفقهاء إلى اعتبار أن النظام العام هو أساس الإلتزام بالسر المهني، والذي يجد مصدره في المصلحة الإجتماعية وتحقيق المصلحة العامة، ومن ثم فإنه وحسب هؤلاء لا يعتبر الإلتزام بالسر المهني نتيجة العقد بين العميل والأمين على السر، وإنما يتعلق الأمر بمسألة مرتبطة بالنظام العام، وهو بذلك التزام قانوني لا يتوقف على إرادة أي من الطرفين، فالقانون هو الذي يحمي السر ويعاقب على إفشائه[2]، على أساس أن إفشاء الأمين للسر الذي اطلع عليه بحكم مهنته أو أدلى به إليه صاحب السر يمثل اعتداء على المجتمع كله نتيجة إهدار الثقة في تلك المهنة، خصوصا في بعض القطاعات الحساسة، لذلك فإن المشرع الجزائي من وجهة نظر أصحاب هذه النظرية لا يتدخل لحمايةالمصالح الفردية أو من أجل ضمان تنفيذ اتفاقات الأطراف، وإنما يتدخل بالعقاب فقط في كل مرة يتعلق فيها إفشاء السر المهني بالنظام العام لما يقتضيه ذلك من تعريض المصلحة الإجتماعية للخطر.[3]

وقد ترتب عن الأخذ بهذه النظرية مجموعة من النتائج:

-أن السر المهني واجب مطلق ومستمر والتزام عام، وذلك لتعلقه بالنظام العام، حيث يكون الإلتزام بعدم إفشاء السر واجبا في كل الظروف، حتى ولو بإذن صاحب السر، والقضاء الفرنسي تمسك بالصفة المطلقة للنظام العام من خلال مجموعة من الأحكام والقرارات القضائية، مؤكدا أن واجب الإلتزام بالسر المهني في التشريع الفرنسي جاء عاما ومطلقا، مؤكدا أن قصد المشرع من فرض السر المهني على بعض الأشخاص كواجب عليهم بمقتضى الحالة أو المهنة، هو تأكيد للثقة المفروضة في بعض المهن[4].

-اتساع نطاق الإلتزام الموضوعي بالسر المهني، حيث أنه وفقا لهذا المعيار لم يعد السر يقتصر على ما يودع لدى الأمناء، وإنما يشمل بالإضافة إلى ذلك ما يصل إلى علمهم أثناء ممارسة المهنة أو بسببها، بغض النظر عما إذا كان قد طلب منهم المحافظة على السر أم لم يطلب منهم ذلك، على أساس أن مصدر السر ومكمنه هو الطبيعة الإئتمانية الكامنة في ممارسة بعض المهن باعتبارها حافظة للثقة العامة.

---

[1] أسامة عبد الله قايد، المسؤولية الجنائية للطبيب عن إفشاء سر المهنة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة 1986، ص13

[2] حسين محمد عبد الظاهر، المسؤولية المدينة للمحامي تجاه العميل، دار النهضة العربية للنشر والتوزيع، القاهرة طبعة 1993، ص140

[3] عادل جبري محمد حبيب، مرجع سابق، ص50

[4] أحمد كامل سلامة، مرجع سابق، ص89

-اتساع نطاق الإلتزام الشخصي بالسر المهني، حيث صار وفقا لهذا المعيار جميع أرباب المهن وحتى مساعديهم والموظفين ملزمين بالسر المهني على قدم المساواة، فحسبمنظري هذا الإتجاه أن نية المشرع في تحديده لنطاق السر المهني تقوم على ما اصطلح عليه "الأمناء بالضرورة" وربطوا هؤلاء بما أطلق عليه "بالأسرار المطلقة"

ونجد العديد من التشريعات أخذت بهذا الإتجاه كمبرر لحماية السر المهني، ومنها المشرع الجزائري طالما أن للنظام العام مفهوما مرنا عن طريق تبني فكرة النظام العام النسبي[1]، باعتبار أن هناك تدرجا في الإلتزامات المختلفة حتى ولو تعلق صميمها بالنظام العام، فعند التعارض بين التزامين متعلقين بالنظام العام فإن الإلتزام الأعلى درجة وأهمية هو الاجدر بالحماية،وهذا ما يفسر الإستثناءات في الخروج على مبدأ الإلتزام بالسر المهني.

ثانيا: موقف المشرع الجزائري من الإلتزام بالسر المهني في إطار حماية المعطيات الشخصية

لقد ألزم المشرع بموجب القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المسؤولين عن معالجة هذه المعطيات، وكل الأشخاص الذي يطلعون عليها أثناء ممارستهم لمهامهم بالمحافظة على السر المهني.

1) الأشخاص الملزمين بالسر المهني في ظل قانون 07/18: من المهم الوقوف على معرفة الأشخاص الذين يقصدهم المشرع في إطار حماية الأفراد من مخاطر المعالجة الإلكترونية لبياناتهم الشخصية بالإلتزام بكتمان السر المهني بمناسبة اطلاعهم على هذه البيانات الشخصية أثناء ممارستهم لمهامهم، ومن خلال نص المادة 40 و41 من القانون 07/18 فإن الأشخاص المعنيين بهذا الالتزام:

1-1) المسؤول عن المعالجة: عرفت المادة 03 من القانون 07/18 في إطار تحديد المقصود ببعض المفاهيم لأغراض هذا القانون، المسؤول عن المعالجة بأنه كل شخص طبيعي أومعنوي عمومي أو خاص أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها*، وبحسب المادة

[1] أنظر في هذا المعنى أحمد كامل سلامة، مرجع نفسه، ص99

* يعرف القانون المغربي المسؤول عن المعالجة في المادة 02 من القانون 09/08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي في إطار التعاريف ونطاق التطبيق، بأنه الشخص الذاتي أو المعنوي أو السلطة العامة أو المصلحة أو أي هيئة تقوم سواء بمفردها أو باشتراك مع آخرين بتحديد الغايات من معالجة المعطيات ذات الطابع الشخصي ووسائلها إذا كانت الغايات من المعالجة أو وسائلها محددة بموجب نصوص تشريعية أو تنظيمية، تجب الإشارة إلى المسؤول عن المعالجة في قانون التنظيم والتسيير أو في النظام الأساسي للهيئة المختصة، بموجب القانون أو النظام الأساسي في معالجة المعطيات ذات الطابع الشخصي المعنية"

يعرف القانون التونسي المسؤول عن المعالجة في الفصل الخامس من القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 بأنه كل شخص طبيعي أو معنوي يحدد أهداف معالجة المعطيات الشخصية وطرقها.

يعرف القانون الفرنسي المسؤول عن المعالجة من خلال القانون رقم 801/2004 المؤرخ في 06 أوت 2004 المتعلق بحماية الأشخاص الطبيعيين في إطار معالجة المعطيات ذات الطابع الشخصي ويعدل القانون 17/78 المؤرخ في 06 جانفي 1978 المتعلق بالمعلوماتية والملفات والحريات حيث تنص المادة 03 منه على:

Le responsable d'un traitement de données à caractère personnel, est sauf désignation expresse par les dispositions législatives ou réglementaires relatifs à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses fénalités et ses moyens »

الثانية من التوجيه الأوروبي رقم 46/95 المتعلق بحماية الأشخاص الطبيعيين في إطار معالجة المعطيات ذات الطابع الشخصي وحرية تدفق المعطيات الصادر عام 1995، فإن المسؤول عن معالجة المعطيات هو كل الشخص طبيعي أو اعتباري أو السلطة العامة أو المرفق، أو أي هيئة أخرى تحدد بمفردها أو بالاشتراك مع الآخرين أغراض ووسائل معالجة البيانات الشخصية، ويؤكد الفقه أن هذا المفهوم يعد أصيلا ومستقلا، فلا يمكن تفسيره أو الأخذ به إلا في إطار قانون حماية البيانات الشخصية، وأنه ذو مدلول وظيفي من جهة أخرى، لأنه يهدف إلى تعيين المسؤوليات بناء على دور الشخص وتأثيره في عمليات المعالجة، أي على أساس واقعي، أكثر منه نظري أو رسمي.[1]

والملاحظ أن تعريف المسؤول عن المعالجة الذي جاءت بها القوانين والأنظمة الوطنية ومنها المشرع الجزائري، يقوم على ثلاث عناصر مترابطة فيما بينها: الطابع الفردي من خلال استخدام عبارات الشخص الطبيعي أو المعنوي العمومي أو الخاص أو أي كيان آخر يقوم بمفرده، واحتمالات تعدد المسؤولية، من خلال استخدام عبارة الإشتراك مع الغير، بالإضافة إلى العناصر الأساسية التي تجعل من الممكن التمييز بين الشخص المسؤول عن المعالجة والأشخاص الآخرين الذين يتعاملون مع المعطيات الشخصية، وذلك من خلال عبارة تحديد الغايات من معالجة المعطيات ووسائل هذه المعالجة.

وقد كانت الإتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص في مجال المعالجة الآلية للمعطيات ذات الطابع الشخصي في مادتها الثانية أعطت للمسؤول عن المعالجة تسمية "صاحب الملف"، وعرفته بأنه الشخص الطبيعي أو المعنوي أو السلطة العمومية أو أي مصلحة أو جهاز مختص طبقا للقانون الوطني باتخاذ القرار في شأن الغاية من الملف الآلي، أصناف المعطيات ذات الطابع الشخصي التي ينبغي تسجيلها والعمليات التي ستخضع لها".

إن لمسألة تحديد صفة المسؤول عن المعالجة أهمية بالغة الأثر في تحديد المسؤوليات والإلتزامات الواقعة على هذا الأخير إنطلاقا من هذه الصفة، وبالتالي لابد لإقرار صفة المسؤول عن المعالجة من أن تقترن بقرار اتخذته جهة معينة للبدء في عملية المعالجة تحقيقا لأهداف معينة خاصة بها، لأن غياب هذا القرار يؤدي إلى إمكانية عدم انطباق القانون مع الواقع، كالحالة التي ينص فيها على تعيين جهة ما كمسؤول عن المعالجة، إلا أنها ليست هي من يقوم بغايات المعالجة وأهدافها حقيقة، لأنها تفتقر إلى السلطة التي تمكنها من تنفيذ مهمتها أو تكون غير قادرة فعليا على اتخاذ القرار، كما لو تم تعيين جهة ما لشخص بصورة رسمية بصفته كمسؤول عن المعالجة، بينما يكون في الواقع مجرد معالج يعمل لصالح جهة أخرى يكون لها هي وحدها إتخاذ القرار في تحديد أهداف المعالجة وغاياتها ووسائلها.[2]

وبالتالي فإنه ومن زاوية تحديد المسؤولية عن الإخلال بالإلتزام بالسر المهني لابد من معرفة المسؤول عن المعالجةفي الواقع، بغض النظر عن الصفة المستمدة من القانون والإعتماد على الجهة التي تقرر تحديد الغايات والأهداف من معالجة المعطيات الشخصية، بعيدا عن أي صفة أو مهمة رسمية، ولتأكيد مسألة

[1] منى الأشقر جبور، محمود جبور، مرجع سابق، ص109.

[2] منى الأشقر جبور، مرجع سابق، ص112.

اعتبار المسؤول عن المعالجة هو من يقرر الأهداف والغايات من المعالجة وليس من يعين قانونا، يمكن أن نستدل بالقضية المعروفة بـ(l'affaire swift) حيث تم التعاقد مع هذه الشركة بصفتها معالجا للمعلومات، بينما تبين في الواقع أنها كانت تمارس صلاحيات المسؤول عن المعالجة بسبب دورها الفعلي في جمع البيانات ومعالجتها وإرسالها إلى جهات أمنية أمريكية تعالج هذه البيانات وتستخدمها في إطار عملية مكافحة الإرهاب[1].

ومن جهة أخرى، فحسب التعريف القانوني، فإن من يكون مسؤولا عن معالجة البيانات الشخصية قد يقوم بمهامه إما بمفرده أو بالاشتراك مع الغير في معالجة هذه البيانات، فيكون في هذه الحالة اتخاذ قرار المعالجة وتحديد أهدافها ووسائلها وغاياتها بالإشتراك بين عدد من الجهات بشكل متلاحق أو متزامن وصولا إلى معالجة البيانات، ما يمكن أن ينتج عنه مسؤولية مشتركة، ففي هذا الوضع تعتبر كل جهة منهم مسؤولة عن المعالجة تجاه الأشخاص المعنيين ويمكن لهؤلاء مساءلة أي واحدة من هذه الجهات فيما يتعلق بحقوقهم في إدارة بياناتهم الشخصية.

وهو الأمر الذي يمكن أن يحصل بالنسبة للمنصات المشتركة التي تلجأ الشبكات الإ جتماعية إلى إنشائها، حيث تسمح لمستخدميها بتبادل المعلومات والتواصل فيما بينهم، ويعتبر مزودي الخدمة هنا أيضا مسؤولين عن معالجة البيانات، لأنهم يشتركون في تحديد أهداف المعالجة والوسائل التي تستخدم لهذه الغاية، ومن ثم يمكن مساءلتهم عن ضرورة الإلتزام بما يقع على المسؤول عن المعالجة من التزامات ومنها التزامه بالسر المهني.

2-1) الأشخاص الآخرين الذين يمكنهم الإطلاع على المعطيات الشخصية: ليس المسؤول عن المعالجة وحده من له إمكانية الإطلاع على المعطيات ذات الطابع الشخصي، بل يوجد أشخاص آخرون يكونون في موضع يسمح لهم بالإطلاع عليها، ويخضعون نتيجة لذلك إلى الإلتزام بالمحافظة على سريتها في إطار مبدأ المحافظة على السر المهني.

أ) المتعاقد من الباطن يعود للمسؤول عن المعالجة إقرار وجود معالج للمعطيات الشخصية وذلك عندما يختار أن يوكل جميع عمليات المعالجة أو جزء منها إلى جهة أخرى، تعمل لحسابه، ولكنها تتمتع باستقلال قانوني عنه وخارجة عن إطار مؤسسته، فتتوفر صفة المعالج من الباطن في الجهة التي تتمتع باستقلال كيانها القانوني عن المسؤول عن المعالجة وتقوم بهذه المعالجة لحسابه.

وتأسيسا على ذلك فقد نصت المادة 39 من القانون 07/18 على أنه عندما تجرى المعالجة لحساب المسؤول عن المعالجة، يجب على هذا الأخير اختيار معالج من الباطن، وهو نفس المقتضى الذي قرره

[1] Richard Montbeyre, le transfert de données bancaires à caractère personnel vers les états-unis : aspects juridiques de l'affaires SWIFT, master2 professionnel, droit de l'internet public administration entreprises, université paris 1, Pantheon-Sorbonne février 2008, p 25. Voir le site web : http://www.droit-tic.com

التوجيه الأوروبي 46/95[1]، وقد عرف المشرع هذا الأخير بأنه كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة.[2]

لذلك فحسب التشريعات المتعلقة بحماية البيانات الشخصية، فإن المعالج من الباطن ينفذ تعليمات المسؤول عن المعالجة، أقلها ما يتعلق منها بتحديد أهداف المعالجة والعناصر الأساسية لوسائلها، مع ترك بعض الحرية في اختيار الوسائل الأنسب باعتباره مفوضا يعمل لخدمة المسؤول عن المعالجة الذي فوضه، وعليه أن يؤدي هذه الخدمة بأفضل طريقة ممكنة، ويكون السند القانوني الذي يعطي لعمل المعالج من الباطن المشروعية هو العقد الذي يربطه بالمسؤول عن المعالجة.[3]

فإذا تجاوز حدود هذا العقد، وقام بالمعالجة لأهداف وأغراض خاصة به أو مختلفة عن تلك المحددة أساسا لعملية المعالجة، يصبح نشاطه غير قانوني، لذلك فقد أكد المشرع في نص المادة 39 من القانون 07/18 على ضرورة أن ينص العقد خصوصا بأن لا يتصرف المعالج من الباطن إلا بناءا على تعليمات المسؤول عن المعالجة.

ولضمان الحفاظ على المستوى المطلوب لحماية البيانات الشخصية، أقر المشرع لهذه الغاية ضرورة إلزام المسؤول عن المعالجة باختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها.[4]

ولأجل ضمان سرية البيانات الشخصية فإن المشرع أكد على منع كل من يعمل تحت سلطة المسؤول عن المعالجة وكذا الأشخاص الذين يعملون تحت سلطة المعالج من الباطن القيام بمعالجة البيانات الشخصية التي يصلون إليها إلا بناء على تعليمات المسؤول عن المعالجة.[5]

ب) الغير: يعتبر مصطلح الغير أو كما تطلق عليه بعض التشريعات الأخرى مصطلح الشخص الثالث، من المصطلحات التي استعملتها التشريعات في مجالات عديدة ومتباينة[6]، وقد تولى الفقه الفرنسي القديم تحديد المقصود به من خلال شرح القانون الفرنسي، حيث خلص إلى أن الغير هو وصف يطلق على الشخص للدلالة على أنه مستقل تماما بالنسبة لمركز قانوني معين، فلا يجوز أن يتأثر بهذا المركز ولا أن يؤثر فيه، ومن هنا كان الغير بالنسبة للعقد شخصا لا تمسه شريعة العقد ولا تنصرف إليه آثاره.[7]

---

[1] Article 17 de la directive 95/46 « les états membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant… »

[2] أنظر المادة 13/03 من القانون 07/18.

[3] أنظر المادة 02/39 من القانون 07/18

[4] أنظر المادة 01/39 من القانون 07/18

[5] أنظر المادة 41 من القانون 07/18

[6] استعمل الرومان مصطلح الغير في العبارة الشهيرة: «res inter alios acta alus neque nocere neque prodesse» وتعني أن العقود لا تتعدى أطرافها بنفع أو ضرر. وقد نصت المادة 113 من القانون المدني الجزائري على أنه "لا يرتب العقد التزاما في ذمة الغير ولكن يجوز أن يكسبه حقا".

[7] حليمي ربيعة، الغير في العقد-دراسة في القانون المدني وبعض القوانين الخاصة- أطروحة دكتوراه علوم في الحقوق، قسم القانون الخاص، كلية الحقوق، جامعة الجزائر، 2016-2017، ص01.

ومن ثم فقد جاء هذا المصطلح لكي يراد به التدليل على مبدأ قانوني يقضي باقتصار مفاعيل العقود على أطرافها دون انصراف آثارها لغيرهم سواء كان ذلك بالنفع أو الضرر، فمن لم ترض إرادته انصراف الأثر إليه يظل بعيدا عن هذا الأثر.[1]

ومن هذا المنطلق يمكننا فهم فئة "الغير" المقصودة في قانون حماية البيانات الشخصية، وهي فئة لا يدخل في إطارها كل من الشخص المعني بالمعالجة، المسؤول عن المعالجة، المتعاقد من الباطن أو من يعمل لحسابهما، لذلك فقد عرف المشرع الجزائري هذه الفئة بأنها كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر، غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.[2]

وهكذا يكون المقصود من هذا المصطلح في إطار قانون حماية البيانات، كل شخص لا يملك إذنا خاصا، أو حقا مشروعا في إطار رسمي لمعالجة البيانات الشخصية، بغرض تحديد المسؤوليات والصلاحيات في حال سلمت معالجة البيانات ذات الطابع الشخصي إلى جهة لم تكن في الأساس معنية بهذه المعالجة، فموظفو وكالة السفر التي تعالج البيانات الشخصية لزبائنها ليسوا من الغير، بينما يعتبر العاملون لدى وكالة سفر أو مؤسسة أخرى بالنسبة لهذه البيانات الشخصية من الغير إذا كانوا في موضع يسمح لهم بمعالجتها.

ومن منطلق حماية استقرار المعاملات القانونية والعلاقات في المجتمع، وحماية من اعتمدوا عن حسن نية على تصرف توافرت له مظاهر التصرف القانوني الصحيح، فإن الغير الذي يتلقى البيانات الشخصية بصورة مشروعة أو غير مشروعة يمكن أن يتحول إلى مسؤول عن المعالجة كلما توفرت عناصر تحديد هذه الصفة والتي سبق الإشارة إليها، ويصبح بالتالي خاضعا لأحكام قانون حماية البيانات الشخصية والإلتزامات المفروضة من خلاله.[3]

ومن الأشخاص الأخرى الذين يمكنهم الإطلاع على البيانات الشخصية بحكم مهامهم ويلتزمون في مقابل ذلك بالمحافظة على سريتها في إطار مبدأ الإلتزام بالسر المهني، نجد المرسل إليه و هذا الأخير هو كل شخص طبيعي أو معنوي أو السلطة العمومية أو المصلحة أو أي كيان آخر يتلقى معطيات ذات طابع شخصي أو يتوصل إليها[4]، وقد يكون المرسل إليه في حالات معينة من الغير و لا تعتبر السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وأعضاؤها كجهة مرسل إليها عندما تتوصل بالمعطيات الشخصية في إطار المقتضيات القانونية المتعلقة بممارسة صلاحياتها*، إلا أنه وفي سبيل ذلك يكون أعضاؤها ملزمين هم

---

[1] نبيلة اسماعيل رسلان، النظرية العامة للعلاقات الثلاثية، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 1986، ص76

[2] أنظر المادة 14/03 من القانون الجزائري 07/18.

وقد عرفه المشرع المغربي في القانون 09/08 المشار إليه سابقا، من خلال استعمال مصطلح "الأغيار" بأنه الشخص الذاتي أو المعنوي أو السلطة العامة أو المصلحة أو أية هيئة أخرى غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعين للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.

[3] منى الأشقر جبور، محمود جبور، مرجع سابق، ص120.

[4] أنظر المادة 14/03 من القانون 07/18.

* وهو الموقف الذي أخذ به المشرع الفرنسي في نص المادة 03 من القانون 2004/801 المؤرخ في 6 أوت 2004 المتعلق بحماية الأشخاص الطبيعيين في إطار معالجة المعطيات ذات الطابع الشخصي حيث نصت على:

أيضا بالمحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة حتى بعد انتهاء مهامهم.[1]

2 أحكام الإلتزام بالسر المهني في إطار القانون 07/18: يعد عدم إفشاء الأسرار من التطبيقات الهامة للحق في الخصوصية[2]، بل ويعد الإهتمام بالسر وحمايته جوهر حماية هذا الحق، ذلك أن الأسرار إطار ووعاء لحماية حقوق ومصالح أخرى عديدة، لذلك فإن الهدف المحوري والرئيسي من توخي المحافظة على السر المهني في مواجهة الأشخاص الذين بحكم مهامهم يطلعون على المعطيات ذات الطابع الشخصي، هو حماية الحق في الخصوصية المعلوماتية، حيث تعد حماية سرية المعطيات الشخصية من بين أهم الأهداف التي يرمي إليها التزام المهنيين في مجال معالجة المعطيات الشخصية بالسر المهني، فهؤلاء بحكم تخصصهم فهم يطلعون ويتعرفون بالضرورة على معطيات شخصية تعتبر بحكم خصائصها سرية لا يرغب أصحابها في اطلاع غيرهم عليها.

وتظهر حماية الحق في الخصوصية المعلوماتية من خلال الإلتزام بالسر المهني في الإتجاه الذي أخذ به المشرع الجزائري في المادة 40 من القانون 07/18[3] عندما أخذ بالتفسير الواسع الذي يمكن إعطاؤه لمفهوم هذا السر ليشمل كل ما يعلمه المهني أثناء تأديته لمهامه، بما في ذلك ما يطلع عليه من معلومات، وهو بذلك خرج عن التفسير الضيق لمفهوم السر المهني الذي أخذ به المشرع في قانون العقوبات المادة 301 حيث يكمن السر المهني فقط في المعلومات والوقائع التي قد أدلي بها للمهني من طرف صاحب السر"[4]

وهذا يأتي موافقا للمفهوم الواسع للسر المهني الذي تبناه المشرع الفرنسي في قانون العقوبات سنة 1992 عندما عوض في المادة 226- 13 عبارة "أسرار أدلي بها إليهم des secrets qu'on leur confie" بعبارة معلومات ذات طابع سري information à caractère confidentiel *

ومن ثم فإن المشرع في القانون 07/18في تعريفه للسر المهني كان موقفه الإعتماد على طبيعة المعلومة ذاتها في كونها سرية نظرا لارتباطها بالمعطيات ذات الطابع الشخصي، ولا ضرورة لأن تكون قد عهد أو أدلي بها

« Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoire communication de ces données… toutefois les autorités légalement habilitées dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires »

[1] أنظر المادة 26 من القانون 07/18.

[2] ممدوح خليل بحر، مرجع سابق، ص73.

[3] تنص المادة 40 من القانون 07/18 على أنه "يلزم المسؤول عن المعالجة والأشخاص الذي اطلعوا أثناء ممارسة مهامهم على معطيات ذات طابع شخصي بالسر المهني..."

[4] تنص المادة 301 من قانون العقوبات "يعاقب بـ.. وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة... على أسرار أدلي بها إليهم و أفشوها..."

* الإجتهاد القضائي الفرنسي توسع لاحقا في تفسير العبارة التي جاءت بها المادة 378 من قانون العقوبات الفرنسي القديم "...أسرار أدلي بها إليهم..." والتي أخذها قانون العقوبات الجزائري في المادة 301 ، حيث قضت محكمة النقض أنه لا يغطي مفهوم السر المهني فقط ما تم الإدلاء به للمهني من معلومات، سواء كان ذلك مصحوبا بتعليمات عدم إفشائها أو بدونه، بل إنه يجب أن ينصب السر أيضا على ما تمت معاينته وما تم فهمه من طرف الشخص أثناء ممارسة مهنته، أنظر نويري عبد العزيز، الحماية الجزائية للحياة الخاصة، دراسة مقارنة بين القانون الجزائري والفرنسي، دار هومة للطباعة و النشر والتوزيع، 2015، ص 531.

من طرف من تعلقت به إلى المؤتمن عليها، ومن هذا المنطلق اعتبر المشرع الجزائري أن المعطيات ذات الطابع الشخصي التي يطلع عليها المسؤول عن المعالجة سرا مهنيا ويلزم بكتمانه وعدم إفشائه، وهذا راجع ربما كما أسلفنا القول إلى طبيعة المعطيات الشخصية التي تتميز بالسرية، وكذلك إلى طبيعة المهمة التي يقوم بها المسؤول عن المعالجة، والتي تسمح له بمعرفة معلومات سرية عن المعني بالمعالجة حتى دون علمه أو اشتراط إرادته.

ويعد توسيع تطبيق مفهوم السر المهني في مواجهة المتعاملين مع المعطيات الشخصية على كل المعلومات التي يطلعون عليها، يدل على أن تجريم انتهاك السر لا يستجيب فقط لضرورة تأمين ما يمكن أن يدلي به الأشخاص المعنيون بالمعالجة من بيانات شخصية إلى المهنيين، بل يستجيب أيضا لضرورة المحافظة على كل ما يتعلق بالخصوصية المكتشفة من طرف هؤلاء أثناء ممارسة مهامهم.[1]

ومن جهة أخرى يمكن الإشارة إلى العبارة التي استخدمها المشرع الجزائري في المادة 40 من القانون 07/18 "... أثناء ممارسة مهامهم..." وهي عبارة قد ينحصر حسبها السر المهني على الأشخاص الذين يقومون بمعالجة المعطيات بصورة مباشرة ، وخلال الأوقات التي يؤدون فيها مهامهم بصفة نظامية، وهذا على خلاف المشرع الفرنسي الذي استعمل عبارة "بمناسبة" à l'occasion وهي عبارة واسعة لا ترم فقط إلى الأشخاص الذين يقومون مباشرة بمعالجة المعطيات بل يتعدى إلى أولئك الأشخاص الذين لهم علاقة بالمعالجة ولو بصفة غير مباشرة[2]، إلا أن القراءة الكلية لنص المادة 40 من القانون 07/18نجد أن المشر ع يبقي على الإلتزام بالسر المهني مستمرا على عاتق المسؤول عن المعالجة وعلى كل شخص اطلع على المعطيات الشخصية، حتى بعد انتهاء مهامه وانقطاع علاقته المهنية التي سنحت له بالإطلاع على المعطيات، طالما أنه علم بهذه المعطيات الشخصية بسبب ممارسته لمهامه.

وهو الأمر الذي يمكن أن نفهمه من المراسيم التنفيذية المتضمنة الموافقة على رخصة إقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية، حيث تضمن الملحق أحكاما في إطار شروط استغلال الخدمات مجموعة من الإلتزامات على عاتق صاحب الرخصة تتعلق باتخاذ الإجراءات التي من شأنها أن تضمن سرية المعلومات والمكالمات التي يحوزها عن مرتفقي شبكة GSMمع احترامه للسر المهني، أين جاءت هذه العبارة الأخيرة على إطلاقها دون إلحاقها بعبارة أثناء أو بمناسبة أداء المهنة.

المطلب الثاني: إلتزامات وسطاء خدمة الأنترنت في مجال حماية المعطيات الشخصية:

لقد أصبحت شبكات الأنترنت وسيلة مفتوحة لانسياب وتدفق وتداول كميات ضخمة من المعلومات، ذلك أنها قوة كامنة في توفير الخدمة لعدد غير محدود من الحاسبات على مستوى العالم تلبية لرغبة مستخدميها عن طريق الإتصال بها.

[1] أنظر في هذا المعنى نويري عبد العزيز، مرجع نفسه، ص 532.

[2] أنظر المادة ،23 24 من المرسوم التنفيذي رقم 313/14 المؤرخ في 10 نوفمبر 2014 المتضمن الموافقة على رخصة الإقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور جريدة رسمية عدد 70، ص 47.

ولما كانت شبكة الأنترنت عبارة عن أنشطة متعددة تتشارك كل واحدة منها في عملية تشغيل أجهزة تخزين المعلومات وبثها وعرضها، فإنها تتطلب في سبيل ذلك أشخاصا قائمين على هذه العمليات يطلق عليهم "الوسطاء في خدمة الأنترنت"، يتيحون للمستخدم الوصول إلى الشبكة وخدماتها، فهذه الخدمة هي ذات طبيعة فنية تتمثل في ربط المشتركين بالمواقع أو بالمستخدمين الآخرين في الشبكة.[1]

فالواقع العملي يثبت أن تداول المعلومات عبر شبكة الأنترنت بحاجة إلى تظافر جهود الأشخاص القائمين على إدارتها، فحتى يتمكن مستخدموا الأنترنت من الدخول إلى الشبكة والإبحار فيها بحرية والوصول إلى ما يصبون إليه من معلومات أو بثها، لا بد من وجود عدة أشخاص يطلق عليهم مقدمي خدمة الأنترنت أو الوسطاء في خدمات الأنترنت.

هؤلاء الأشخاص الفنيين أي الوسطاء في خدمة الأنترنت ينحصر دورهم في تمكين المستخدم من الدخول على شبكة الأنترنت والتجول فيها والإطلاع على ما يريد، لذلك فمنهم من ينقل الخدمة، ومنهم من يمكن المستخدم من الوصول إلى الموقع، ومنهم من يخزن المعلومات أو يوردها[2]، ومن ثم بدت الحاجة ماسة لإيجاد تنظيم تشريعي متكامل يحدد المركز القانوني لمقدمي خدمات الأنترنت ويبين في نفس الوقت مسؤولية كل منهم عما يرتكب من مخالفات عبر الشبكة، سيما ما تعلق منها بالمساس بالحق في الخصوصية المعلوماتية.

وقد كانت نواة عمل البرلمان الأوروبي الذي تبنى في 08 جوان 2001 التوجيه الأوروبي رقم 2000/31 [3] والمتعلق ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفة خاصة التجارة الإلكترونية في السوق الداخلي، والذي تم من خلال القسم الرابع منه تنظيم المركز القانوني للوسطاء في خدمة الأنترنت، حيث جاءت المادة 22 من هذا التوجيه الأوروبي لتلزم الدول الأعضاء في الإتحاد الأوروبي على نقل أحكامه إلى تشريعاتهم الداخلية، ومن الدول التي كانت السباقة في ذلك فرنسا التي أصدرت القانون رقم 2004/557 المتعلق بالثقة في الاقتصاد الرقمي بتاريخ 21 جوان 2004 .[4]

وعلى صعيد التشريع الوطني نجد القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كأول قانون يتحدث عن مقدمي خدمات الأنترنت في الجزائر.[5]

الفرع الأول: الطبيعة القانونية لخدمات الأنترنت وصفة مقدميها:

تتعدد طرق الوصول إلى الأنترنت سواء عن طريق الإتصالات النموذجية للاستخدام المنزلي والتي من أهمها:

[1] جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001 ص106.

[2] عبد الفتاح يومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، دار النهضة العربية، الطبعة الأولى 2009، القاهرة، ص93.

[3] Directive 2000/31/CE du parlement Européen et de conseil du 08 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, dans le marché interieur (directive sur le commerce éléctronique) journal officiel des communautés européennes L178/1 du 17/07/2000.

[4] Loi n° 2004/575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF 22 juin 2004.

[5] القانون 04/09 مؤرخ في 05 أوت 2009، جريدة رسمية عدد 47 لسنة 2009.

- الإتصال الهاتفي (Dial-up)، الإتصال اللاسلكي عريض النطاق، خط المشترك الرقمي DSL، كابل الأنترنت خدمة الألياف الضوئية للمنازل (FTTH)، الشبكة الرقمية للخدمات المتكاملة (ISOW)، الوي في (WI-FI) خط المشترك الرقمي المتماثل (SHDSL)، أو عن طريق خدمات متعاملي الهاتف النقال الذين يقدمون خدمات المواصلات اللاسلكية من نوع (GSM) * التي تضمن للمستخدمين الربط بشبكةالأنترنت.

إلا أنه وفي كل الأحوال يجب وجود وسطاء خدمة الأنترنت[1]، وإن كان لكل وسيط فني وظيفته إلا أن التطور التقني يؤدي إلى تشابك الأدوار وتنوعها، بحيث يجعل من اليسير على هؤلاء الوسطاء تتبع النشاط المعلوماتي غير المشروع وكشفه، وتحقيق ذلك يبقى رهن وجود ضوابط قانونية تحدد حقوق أطراف النشاط الإلكتروني والتزاماته في مواجهة بعضهم البعض من جهة، وفي مراجعة المجتمع الذي يعيشون فيه من جهة أخرى.

ولعل من أهم هؤلاء الوسطاء الفنيين في مجال خدمة الأنترنت هم متعهد الوصول، متعهد الإيواء، ناقل المعلومات، والذين بدون الإ ستعانة بخدماتهم لا يمكن حصول المستخدمين على خدمة الأنترنت.

إن اتصال الجمهور بشبكات الأنترنت والحصول على المعلومات منها أو بثها عبرها، لا يمكن أن يتم دون ستعانة بالأشخاص القائمين على إدارة الأنترنت وما يوردونه من خدمات.

ومن خلال التعريفات التي أوردها التشريع الوطني والمقارن بشأن هذه الفئة، ندرك بصفة واضحة تنوع الخدمات التي يقدمها القائمون على إدارة شبكة الأنترنت، وبالنتيجة اختلاف طبيعتها القانونية، وكذا تعدد صفة مقدميها، فمن هذه الخدمات ما هو مخصص لتوفير الوسائل التقنية اللازمة لربط شبكات الإتصال والتسهيل للعملاء وتمكينهم من الوصول إلى المادة المعلوماتية عبر شبكات الأنترنت، ومنها ما يهدف إلى تقديم المضمون المعلوماتي لجمهور مستخدمي الشبكة.[2]

أولا: الخدمات التقنية وصفة موردها: تتمثل هذه الخدمات بصفة أساسية في تمكين مستخدمي شبكة الأنترنت من الوصول إلى المادة المعلوماتية المتداولة عبر الأنترنت من خلال إيصال المستخدمين بالشكل الذي يمكنهم من النفاذ إلى الشبكة والدخول إلى المواقع الإلكترونية المطلوبة، فعملية الدخول إلى الأنترنت

* "GSM" (Global System for Mobile communication) تعني المنظومة الأرضية للاتصالات النقالة، المخصصة لضمان اتصالات نقالة باستعمال تقنيات رقمية خلوية، كما يعرفها المعهد الأوروبي لتقييس الاتصالات: GMPCS (Global Mobile Personal Communication by Satellite) وتعني كل منظومة المواصلات السلكية واللاسلكية عبر الساتل (ثابتة أو نقالة، بشريط واسع أو ضيق، عالمية أو جهوية، ثابتة أو غير ثابتة المدار، موجودة أو في طريق الإنجاز) توفر خدمات المواصلات السلكية أو اللاسلكية مباشرة للمستعملين النهائيين انطلاقا من سعة ساتلية، أنظر المادة الأولى من الملحق بالمرسوم التنفيذي رقم 313/14 المؤرخ في 10 نوفمبر 2014 المتضمن الموافقة على رخصة إقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور، ج رعدد 70 لسنة 2014 .

[1] محمد عبد الكريم حسين الداوودي، المسؤولية الجنائية لمورد خدمة الأنترنت، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت2017، ص 71.

[2] أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الانترنت، دراسة تحليلية مقارنة، قسم الدراسات القانونية، كلية الدراسات الفقهية والقانونية، جامعة آل البيت، مقال منشور على مجلة المنارة، المجلد 13، العدد 9، ص 328.

والإبحار فيها يحتاج بالدرجة الأولى إلى من يقدم هذه الخدمة، وهذه الفئة تسمى متعهدي الوصول les fournisseurs d'accès[1]

ويقصد بمتعهد الوصول أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدم أو الجمهور إلى شبكة الأنترنت، وذلك بمقتضى عقود الإ شتراك، يضمن توصيل العميل إلى المواقع التي يريدها[2]، وقد عرفه المشرع الفرنسي من خلال المادة 6 الفقرة الأولى البند الأول من قانون الإقتصاد الرقمي، بأنه كل شخص يتمثل نشاطه في توفير الوصول إلى خدمات الإتصال للجمهور عبر الأنترنت.

(Personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne)

وهو بهذا المفهوم يعد من مراكز التوزيع التي تتألف منها خدمات الأنترنت، فهو الممر الإلزامي لوصول المستخدم إليها[3]، لذلك اعتبره الفقه العامل في هذا المجال بأنه كل مشروع يتيح للعميل الوصول إلى الأنترنت عن طريق تقديم الوسائل الفنية اللازمة للحصول على هذه الخدمة[4] وتمكينهم من الإبحار فيها بكل حرية، ومن الوصول إلى المواقع الإلكترونية التي يرغبون في الإ طلاع على مضمونها، وقد يكون متعهد الوصول للأنترنت شخصا طبيعيا أو معنويا، وعمله ذو طبيعة فنية ينحصر في ربط المستخدم بشبكة الأنترنت وتوصيله إلى المواقع الإلكترونية أو البريد الإلكتروني للأشخاص الذين يريد مخاطبتهم في أي مكان من العالم[5]، فهو لا يقدم المعلومة أو محتوى المواقع الإلكترونية، بل تقتصر مهمته على إيصال المستخدم إلى الأنترنت عن طريق أجهزته الخاصة[6]، فهو ليس منتجا للمصنف،و لكنه يضطلع بتقديم خدمات ذات طبيعة فنية تمكن مشتركيه من استخدام شبكة الأنترنت، ومن ثم ليس له الإ طلاع أو التعرف على مضمون الرسائل والمعلومات المتبادلة عبر الشبكة التي تمر من خلاله .

ومن التشريعات التي تولت مهمة تعريف متعهد الوصول، نجد المشرع الجزائري الذي عرفه في المادة 02 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال السالف الذكر بأنه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات.

[1] باسم السيد، النظام القانوني لمزودي خدمة الأنترنت في سورية، مقال منشور في مجلة جامعة البعث، المجلد 39، العدد 50 لسنة 2017، ص 69.

[2] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، مرجع سابق، ص 94.

[3] رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم، تخصص جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2017، ص 70.

[4] أشرف صابر سيد، مسؤولية مقدمي خدمات الأنترنت عن المضمون الإلكتروني غير المشروع، دار النهضة العربية، القاهرة، 2010، ص 17.

[5] محمد عبد الكريم حسين الداوودي، مرجع سابق، ص 75.

[6] رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، مرجع نفسه، ص75

كما عرفه المشرع الفرنسي في المادة 09 من القانون رقم 2004/575 المتعلق بالثقة في الإقتصاد الرقمي على أنه "الشخص الذي يؤمن نشاطه خدمة التوصيل بشبكة إتصالات الكترونية" [1].

ومن التشريعات الأجنبية أيضا التي عرفت متعهد الوصول كمورد لخدمة الأنترنت، القانون المتعلق بحماية الحياة الخاصة في مجال الإتصالات الإلكترونية في الولايات المتحدة الأمريكية، والذي يتكلم عن نوعين من هذه الفئة: النوع الأول وهو كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الإتصالات السلكية والإلكترونية، والنوع الثاني يتعلق بكل من يقدم للجمهور خدمة معالجة البيانات عن بعد، بوسيلة من وسائل الإتصالات الإلكترونية.[2]

هذا بالإضافة إلى إتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001، التي عرفت متعهد الوصول في المادة الأولى منها بأنه "أي كيان عام أو خاص يقدم لمستخدمي الخدمة الخاصة به القدرة على الإتصال عن طريق منظومة كومبيوتر".[3]

ويقدم متعهد الوصول خدماته للمشتركين les abonnés بموجب "عقد تقديم خدمات الدخول" يربطه بهم، والذي من خلاله يتعهد بإيصالهم إلى شبكة الأنترنت وبتأمين التجهيزات اللازمة بمقابل، نظير أن يتعهد العملاء أيضا باحترام شروط الإستفادة من هذه الخدمة، وبذلك فاستنادا لهذا العقد الملزم للجانبين والذي يكون محله بالنسبة لمتعهد الوصول الإلتزام بتزويد المشترك (العميل) بالوسائل التقنية والبرمجيات التي تمكنه من الدخول إلى شبكة الأنترنت، ويكون على المشترك دفع قيمة الإشتراك المحددة في العقد للاستفادة من هذه الخدمة.

وعادة ما تتولى هذه المهمة مؤسسات عمومية متخصصة في مجال الإتصالات، مثل مؤسسة إتصالات الجزائر "Algérie télécom " التي تحتكر هذه العملية في الجزائر من خلال تقنية Idoom ADSL وتقنيات أخرى وفرانس تيليكوم في فرنسا "France Télécom».

وبالإضافة إلى النشاط المحوري لمتعهد الوصول السابق بيانه فإن هذا الأخير قد يتخطاه أحيانا فيقترح على مشتركيه خدمات إضافية، مثل اقتراحه لمضمون معلوماتي معين يتم بثه عبر الشبكة، أو التعهد بإيواء بعض المواقع، أو تخزين صفحات الواب التي يطلع عليها مشتركوه بصورة مؤقتة من أجل تسريع عملية وصولهم إليها عند طلبها مرة أخرى، غير أنه في هذه الحالة لا يقدم هذه الخدمات بوصفه متعهد الوصول و إنما يدخل في طائفة متعهدي الإيواء، ويخضع للأحكام الخاصة بهم[4].

[1] Voir l'article 09 de la loi n° 2004/575 du 21 juin 2004 pour la confiance dans l'économie numérique, crée l'aricle L 32-3-3 du code des postes et des communication éléctroniques. « Toute personne assurant une activité de transmission de contenus sur un réseau de communication électroniques ou de fourniture d'accès à un réseau de communication électroniques ne peut voir sa responsabilité civile ou pénale ... »

[2] رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، مرجع سابق، هامش رقم 1 الصفحة 447.

[3] أنظر المادة الأولى الفقرة "ج" من اتفاقية مجلس أوروبا رقم 185 المتعلقة بالجريمة الإلكترونية الموقعة في بودابست رومانيا، في 2001/11/23.

[4] أحمد قاسم فرح، مرجع سابق، ص 330.

لذلك نجد أن المشرع الجزائري عندما عرف خدمات الإتصالات الإلكترونية للجمهور في قانون البريد والإتصالات الإلكترونية[1] اعتبرها كل خدمة تتمثل كليا أو أساسا في تزويد الجمهور بالإتصالات الإلكترونية، وكذا الخدمات التي تستعمل قدرات شبكات الإتصالات الإلكترونية، والتي تتطلب زيادة على خدمة الإتصالات الإلكترونية القاعدية، وظائف المعالجة أو التخزين، وهذه المهام الأخيرة تدخل في إطار الخدمات المعلوماتية.

ثانيا: الخدمات المعلوماتية وصفة موردها: تختلف الطبيعة القانونية للخدمات المعلوماتية التي يقدمها وسطاء الأنترنت أو موردو الأنترنت باختلاف نوع الخدمة التي يقدمونها، فمن هذه الخدمات ما يقتصر على عملية التخزين الإلكتروني للمعلومات والبيانات المتداولة عبر شبكات الإتصالات الإلكترونية، وهي خدمات يسهر على تقديمها طائفة تعرف بمتعهدي خدمة الإيواء Hébergeurs، ومنها ما يتعلق بوضع هذه المعلومات تحت تصرف جمهور المستخدمين أو ما يعرف بتوريد المعلومات.

1) متعهدي الإيواء le fournisseur d'hébergement: إن الوظيفة الأصلية لموردي خدمة الأنترنت هي توصيل المستخدم بشبكة الأنترنت، لكن الى جانب هذه الوظيفة الرئيسية هناك خدمات أخرى يقدمها، و التي من أهمها خدمة الإيواء، وهي خدمة تتمثل في توفير مساحة محددة من ذاكرة تخزين المعلومات داخل ملقم مضيف خاص* (un serveur) لدى مورد خدمة الأنترنت يخصصه لتخزين المعلومات أو الخدمات التي ينشرها ويبثها المشتركون عبر مواقع الواب[2]، فمن هذا المنطلق يصبح مصطلح الإيواء (hébergement) بمعناه الإلكتروني الواسع، يشمل وضع الوسائل التقنية والمعلوماتية سواء بمقابل أو بالمجان تحت تصرف العملاء،ليتمكنوا من الدخول إلى شبكة الأنترنت في أي لحظة، بغية بث مضمون معلوماتي معين للجمهور وذلك من خلال قيام المتعهد بالإيواء بعرض إيواء صفحات الواب على حاسباته الخادمة (les servers) مقابل أجر، فهو إذن بمثابة مؤجر لمكان على الشبكة للمستأجر (الناشر)، الذي ينشر عليه ما يريد من مادة معلوماتية (صور، نصوص...)، أو ينظم مؤتمرات مناقشة أو ينشئ روابط معلوماتية مع المواقع الأخرى[3]، ويعمل كذلك على تخزين البيانات والمعلومات التي يبثها أصحاب المواقع الإلكترونية على حاسباته الإلكترونية المرتبطة على الدوام بشبكة الأنترنت، بحيث يتمكن أصحاب هذه المواقع من اطلاع الجمهور على مضمونها المعلوماتي على مدار الساعة،[4] وهذا دون عرض محتويات ومضمون تلك المعلومات

[1] قانون رقم 04/18 مؤرخ في 10 ماي 2018 المحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، جريدة رسمية عدد 27 مؤرخة في 13 ماي 2018.

* وهو عبارة عن جهاز يأوي ويستضيف تطبيقات وملفات ومعلومات يجري تقاسمها أو توزيعها بين مجموعة من المستخدمين ضمن شبكة اتصالات داخلية مغلقة، وكذا ضمن بيئة الشبكات الإلكترونية العالمية، وبشكل خاص شبكة الأنترنت، فتكون بذلك جميع التطبيقات والملفات والمعلومات مجمعة في مكان واحد داخل هذا الجهاز، وقد يكون في الغالب هذا الجهاز مجهزا ببرامج ووسائل حفظ منهجي ودائم للمعلومات المتقاسمة والمتبادلة، وكذلك مجهزا ببرامج رصد أو مراقبة.

[2] محمد عبد الكريم حسين الداوودي، مرجع سابق، ص 82.

[3] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، مرجع سابق، ص100.

[4] Christophe VERDURE, les hébergeurs de sites web : victimes ou régulateurs de la société de l'information ? publier sur le site : http://droit-technologie.org DCCR,2005 n°68, doctrine page 35.

والرسائل على متعهد الإيواء في كل مرة، وهذا ما يبرز أن متعهد الإيواء ليس له السيطرة على المادة المنشورة قبل بثها[1].

إلى جانب هذه التعريفات الفقهية اتجهت التشريعات أيضا إلى تعريف متعهدي الإيواء، ومن ذلك ما ذهب إليه المشرع الجزائري بموجب الفقرة الثانية من المادة الثانية من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها، على أنه أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال أو لمستعمليها، وهو التعريف الذي جاء مشابها إلى درجة كبيرة للتعريف الذي جاءت به اتفاقية بودابست المتعلقة بالجريمة الإلكترونية، حينما عرفت بدورها متعهد الإيواء بانه أي كيان آخر يقوم بمعالجة أو تخزين بينات الكومبيوتر نيابة عن خدمة الإتصالات المذكورة أو مستخدمي هذه الخدمة.

كما عرفه التوجيه الأوروبي حول التجارة الإلكترونية 31/2000 السالف ذكره في المادة 14 منه في بأنه شخص طبيعي أو معنوي يهدف إلى تخزين مواقع إلكترونية وصفحات الواب على حاسباته الآلية الخادمة بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع من خلاله تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تمكنهم في أي وقت من بث ما يريدون على شبكة الأنترنت[2].

وكذلك عرفه المشرع الفرنسي بموجب المادة 2-1/6 من القانون رقم 2004/575[3] على أنه كل شخص طبيعي أو معنوي يقدم ولو بالمجان خدمات بواسطة وسائل الإتصال عبر الخط، تخزين الرموز والكتابات والصور والأصوات أو الرسائل أيا كانت طبيعتها لفائدة مستعملي هذه الخدمات."

ويذهب الفقه إلى تفسير العلاقة التي تربط متعهد الإيواء بالمشترك بأنها علاقة تعاقدية في إطار عقد الإيجار، حيث يقوم متعهد الإيواء بإيجار بعض الفضاء الموجود على موزعه لكل من يريد خزن المعلومات فيها، حيث أطلق عليه البعض إسم عقد الإيجار المعلوماتي.*

وما يميز خدمات متعهد الإيواء عن الناقل الفني البسيط (cashing) هو قيام متعهد الإيواء بالتخزين المباشر والدائم للمواقع الإلكترونية ولصفحات الويب على الحاسبات الآلية والتي تكون مرتبطة بشبكة

---

[1] عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الالكترونية، دار الفكر الجامعي، الاسكندرية 2003، ص 344.

[2] أحمد فرح قاسم، مرجع سابق، ص325.

[3] Article 6-1-2 du loi n° 2004-575 du 21 juin pour la confiance dans l'économie numérique, modifié par la loi n° 2016-444 du 14 avril 2016 visant à renforcer la luttte contre le système prostitutionnel et accompagner les personnes prostituées « les hébergeurs de contenu sont les personnes physiques ou morales qui assurent, même à titre gratuit pour mise à disposition du public par des services de communication au public en ligne, le stokage de signaux d'écrits, d'images, de sons ou de message de toute nature fournis par des destinataires de ces services ... ».

* وقد عرف عقد الإيواء المعلوماتي بأنه العقد الذي يبرم بين طرفين أحدهما متعهد الإيواء الذي يمارس عمله على سبيل الإحتراف، والثاني هو مستخدم شبكة الأنترنت، حيث يلتزم بموجبه الطرف الأول أن يخصص جزءا من أجهزته وأدواته المعلوماتية في تصرف المستخدم وبذلك يتيح له الوصول إلى المضمون المعلوماتي من خلال تخصيص مساحة من القرص الصلب لحاسباته بشكل مباشر ودائم مقابل مبلغ مالي يلتزم به الطرف الثاني، للمزيد أنظر: حسين عبيد شعواط، عبد المهدي كاظم ناصر، عقد الإيواء المعلوماتي ، بحث منشور بمجلة الكوفة للعلوم القانونية والسياسية العدد 21 ،جامعة الكوفة، ديسمبر 2014،ص 130.

الأنترنت على الدوام، في حين أن الناقل الفني البسيط يتولى في سبيل توسيع عملية اتصال الجمهور بالشبكة الإ حتفاظ أوتوماتيكيا بنسخة مؤقتة عن كل صفحة واب ينقلها إلى طالبيها من المستخدمين[1].

وما يميز أيضا متعهد الإيواء عن متعهد الوصول أن الأول يمكن أن يكون وظيفة من وظائف الثاني، بينما متعهد الإيواء لا يقدم خدمة الإتصال بالشبكة التي هي جوهر وظيفة متعهد الوصول، وهذا يعني أن وظيفة هذا الأخير هي أوسع من وظيفة متعهد الإيواء.

ومن ثمة فإنه يفهم من خلال ما سبق أن متعهدي الإيواء يشكلون عنصرا رئيسيا من العناصر المكونة لشبكة الأنترنت، فالدور الهام الذي يضطلعون به في إدارة هذه الشبكة يفرض على كل من يرغب بالبث المباشر والدائم لمضمون معلوماتي ما على الانترنت اللجوء إلى هؤلاء للإستعانة بخدماتهم في إطار عقد الإيواء الذي يعد مصدرا مهما لتحديد التزامات أطرافه، إذ يمكن من خلاله إحاطة طالب الخدمة وإعلامه بوجوب عدم تجاوز الإطار الصحيح والمشروع لاستخدام الوسائل التقنية والمعلوماتية المخصصة له، وذلك تفاديا لإلحاق الضرر بمتعهد الإيواء وبالغير، وفي نفس الوقت تحديد التزامات مقدم خدمة الإيواء المتمثلة في تقديم الوسائل التقنية والمعلوماتية التي تمكن العملاء من بث ما يرغبون فيه من معلومات، بالإضافة إلى بعض الإلتزامات الإضافية كتقديم المساعدة الفنية للعملاء من أجل إنشاء مواقع إلكترونية خاصة بهم[2].

2) خدمات توريد المعلومات fournisseur du contenu: يعرف مورد المعلومات بأنه ذلك الشخص الذي يقوم بتحميل النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين، ومن ثم تكون له السيطرة الكاملة على المادة المعلوماتية التي تبث عبر الشبكة، فهو الذي يقوم بالاختيار ثم التجميع والتوريد حتى تصل إلى الجمهور في صورة مادة معلوماتية على الشبكة.[3]

فالمقصود إذن بتوريد المعلومات عبر شبكة الأنترنت، هو تحميل المساحة المستأجرة من القرص الصلب، أو من أجهزة التخزين المركزية التابعة لمتعهد الإيواء بالبيانات والمعلومات من طرف مورد المعلومات[4]، وقد اعتمد الفقه في تعريفه لمورد المعلومات، أو كما يسميه الفقه أيضا بالناشر الإلكتروني على عدة معايير متباينة، منها معيار القيام بنشر صفحات للجمهور عبر مواقع الأنترنت أو معيار تحقيق المنفعة الإقتصادية، أو معيار إنشاء وتنظيم المحتويات عبر مواقع الأنترنت، ومن ثم عرف بأنه الشخص الطبيعي أو المعنوي الذي ينشر للجمهور صفحات عبر مواقع الأنترنت"[5].

وهو بهذا المعنى تتحقق له السيطرة الكاملة على هذه المعلومات، لأنه هو من يملك توريدها من عدمه، وقد يكون مورد المعلومات متمتعا بصفتي المؤلف والناشر للمعلومات عندما يكون هو مؤلف هذه

[1] Christophe VERDURE, op, cit, p.38.

[2] أحمد فرح قاسم، مرجع سابق، ص 326.

[3] عبد الفتاح بيومي حجازي، الجرائم المستحدثة الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، مرجع سابق، ص 114.

[4] محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، 2003، ص 200.

[5] طارق جمعة السيد راشد، المسؤولية المدنية للناشر الإلكتروني – دراسة مقارنة- المركز العربي للدراسات والبحوث العلمية، القاهرة 2017، ص30.

المعلومات التي يقوم بنشرها عبر مواقع الأنترنت، أو يكون متمتعا فقط بصفة الناشر أو مدير الموقع عندما يكون دوره مقتصرا فقط على نشر المعلومات عبر الشبكة، حيث يقتصر دوره على جمعها من خلال التوسط بين مؤلف هذه المعلومات وصاحب البيانات ومستخدمي الشبكة الراغبين في الاطلاع على مضمونها، وكنتيجة لهذه الأدوار فإن مورد المعلومات يتخذ في الحالة الأولى في نفس الوقت صفة مؤلف المادة المعلوماتية والناشر لها، ويتخذ في الحالة الثانية صفة الناشر فقط، وفي كل الأحوال يكون مورد المعلومات هو صاحب السلطة الحقيقية في مراقبة المضمون المعلوماتي، وذلك انطلاقا من كونه هو من يغذي الشبكة بالمعلومات ويتولى توريدها عبر هذه الشبكة لتصل إلى الجمهور.[1]

أما عن التعريف التشريعي لمورد المعلومات (le fournisseur du contenu) ، فنجد من خلال التشريع المقارن أن قانون الثقة في الإقتصاد الرقمي في فرنسا أشار إليه في المادة 06 الفقرة الثانية البند الأول بأنه كل من شارك في إنشاء المحتوى المعلوماتي"، كما ذهب المشرع الفرنسي إلى تعريفه أيضا "بأنه كل من قام بإدخال أو استقبال نصوص أو أصوات أو صور في خدمات الإتصال بالجمهور عبر شبكة الأنترنت، كذلك عرفه القانون الأمريكي من خلال مصطلح مقدم المحتوى بأنه الشخص أو الكيان المسؤول كليا أو جزئيا عن إنشاء أو تطوير المعلومة التي يقدمها عبر شبكة الأنترنت.[2]

وكنتيجة مترتبة على تعريف مورد المعلومات يمكن ملاحظة الفرق بينه وبين متعهد الإيواء، حيث أن هذا الأخير كما سبق توضيحه لا يقوم بتأليف أو جمع المضمون المعلوماتي، ودائما ينحصر دوره على تخزين هذا المضمون على أجهزته بناءا على اتفاقه مع مورد المعلومات،ليتسنى في النهاية للجمهور الإ طلاع عليه في كل وقت،[3]في حين أنه لا يعد موردا للمعلومات إلا من كان يملك سلطة الرقابة والتحكم في المحتوى المنشور، وتتمثل مظاهر هذه الرقابة إما في المشاركة في اختيار المحتوى، وإما في إنشاء وتطوير هذا المحتوى، لذلك ومن هذا المنطلق فقد تم التوسع في تحديد مفهوم مورد المعلومات، ليصبح متمتعا بهذه الصفة، كل من يمارس وظائف النشر عبر شبكة الأنترنت ويقوم باختيار المادة المنشورة ويملك الرقابة والتحكم في جميع المحتويات المتاحة عبر موقعه على شبكة الأنترنت .

وتطبيقا لذلك يمكن اعتبار مستخدم الأنترنت أنه مورد للمعلومات لكنه غير مهني، على أساس أن هذا المستخدم للأنترنت كما يكون متلقيا للمعلومات ومستهلكا لها، يمكن أن يكون منشئا ومرسلا لها، ويلتزم في هذه الحالة بالإلتزامات القانونية التي يلتزم بها مورد المعلومات المهني، كالإلتزام بالكشف عن هويته عبر موقع الأنترنت وعدم انتهاك خصوصية الغير.[4]

---

[1] عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والأنترنت، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الأردن 2009، ص 58.

[2] طارق جمعة السيد راشد، مرجع سابق، ص 33، أنظر كذلك:

Michel Montazeau, les enjeux juridiques de l'anonymat sur internet, Mémoire Master 2-Droit du numérique adminstration-entreprise, université Paris 1 Panthéon-Sorbonne Page 13. disponible sur le site www.pantheonsorbonne.fr

[3] أحمد قاسم فرح، مرجع سابق، ص328.

[4] طارق جمعة السيد راشد، مرجع نفسه، ص39.

فالمستخدمون العاديون لشبكة الأنترنت لا يتصلون بها فقط لأجل الحصول على المعلومات بل بشكل أساسي لإرسال المعلومات عبرها، إما عبر البريد الإلكتروني أو عبر مواقع الواب أو من خلال منتديات المناقشة أو المجموعات الإخبارية وغيرها، وهم في هذا الموضع يصبحون منتجين للمعلومات في شبكة الأنترنت وليس في موقع المستهلك لها، ولا يكون الفرق بينهم وبين مورد المعلومات المهني سوى أنهم يتحركون في الفضاء المعلوماتي بصفتهم أفرادا وليس بصفتهم مهنيين، طالما أنهم مصدر للدفق المعلوماتي الذي يمد الحياة للأنترنت ويبقيها نشطة[1].

وكنتيجة مترتبة على ما سبق بيانه بشأن توضيح مفهوم الوسيط في تقديم خدمة الأنترنت أو ما يعرف بمورد خدمة الأنترنت، فإنه مصطلح يطلق على عدة متدخلين في عملية إدارة شبكة الأنترنت، يضطلع كل واحد منهم بتقديم خدمات تختلف في طبيعتها عما يقدمه الآخر، وهو الأمر الذي يثير مسألة البحث في طبيعة التزاماتهم تجاه المعطيات الشخصية المتعلقة بجمهور المستخدمين لشبكة الأنترنت.

الفرع الثاني: مسؤولية مقدمي خدمة الأنترنت تجاه الخصوصية المعلوماتية.

لقد اختلفت آراء الفقه وحتى أحكام القضاء بشأن تأصيل مسؤولية مقدمي خدمة الأنترنت بصفة عامة، نظرا لاختلاف التزاماتهم وتنوعها كنتيجة حتمية لاختلاف الطبيعة القانونية للخدمات التي يقدمونها بسبب تشعب أدوارهم وتعدد أنشطتهم، بدءا من تمكين المستخدم من الوصول إلى الموقع إلى تخزين المعطيات وتوريدها.

أولا: تحديد التزامات الوسيط الفني في تقديم خدمة الأنترنت:

يلتزم الوسطاء في تقديم خدمة الأنترنت بمجموعة من الإلتزامات تنبع خصوصيتها من تنوع مهامهم وتعدد أدوارهم المتبادلة، وهو ما يثير التساؤل حول كيفية تحديد التزاماتهم.

ولقد نص المشرع الجزائري في إطار تطبيق أحكام القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال على مجموعة من الإلتزامات، مع مراعاة طبيعة ونوعية الخدمات التي يوفرها مقدمو خدمات نترنت، حيث يلزم التشريع الجزائري هؤلاء بمجموعة من الإلتزامات تتعلق أساسا بحفظ المعطيات التي تسمح بالتعرف على مستعملي خدمة الأنترنت، والمعطيات التعريفية هي تلك المعطيات ذات الطابع الشخصي، أي المعطيات المتعلقة بشخص طبيعي معرف، أو قابل للتعرف عليه كما سبق بيانه، بالإضافة إلى حفظ معطيات أخرى تتمثل في :

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة في الإتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

[1] طوني مشال عيسى، مرجع سابق، ص419.

- المعطيات التي تسمح بالتعرف على المرسل إليهم ذلك الإتصال، وكذا عناوين المواقع المطلع عليها.[1]

وسواء تعلقت التزامات موردي خدمة الأنترنت بحفظ هذه المعطيات، و هي في جوهرها معطيات مرتبطة أساسا بحركة السير*، أو تعلق الإلتزام بجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات[2]، فإن غاية المشرع الأساسية من فرضها على موردي خدمة الأنترنت هو إلزامهم بتقديم المساعدة للسلطات المكلفة بالتحقيقات للحصول على الدليل التقني لإثبات الجرائم المعلوماتية، وهو ما أشار إليه قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 22 جانفي 2001 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية في المادة 01 الفقرة "و" ، حيث ألزم الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية وسرعة الحصول عليها[3]، وهو الشيء المؤكد من خلال اعتبار المشرع أن عدم احترام موردي خدمات الأنترنت لهذه الإلتزامات يؤدي إلى عرقلة حسن سير التحريات القضائية، مرتبا عقوبات إدارية وجزائية جراء ذلك[4].

غير أن هناك التزامات أخرى ترتبط بشكل أساسي بالحياة الخاصة لمستخدمي شبكة الأنترنت من شأن الإخلال بها وعدم احترامها أن يشكل اعتداء على حرمة الحق في الخصوصية، وهي مسائل لم نجد لها تنظيما كافيا من طرف المشرع الجزائري، إلا ما يمكن الإشارة إليه فيما يتعلق بالتزامات متعاملي الهاتف الناقل والذين يمكن اعتبارهم كمتعدي الوصول (fournisseurs d'accès)، على أساس أنه بإمكانهم ربط المشتركين معهم بشبكات الأنترنت، ومن ثم فإنهم يخضعون لأحكامهم ويلتزمون بما يلتزم به متعهد الوصول، حيث نصت المادة 23 من الملحق بالمرسوم التنفيذي 14/313 المتضمن الموافقة على رخصة لإقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور، أنه يلتزم المتعامل صاحب رخصة الإ ستغلال باتخاذ كل الإجراءات التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزها عن مرتفقي شبكة GSM، وكذا الإجراءات الكفيلة بضمان حماية وسرية المعلومات الإ سمية (المعطيات الشخصية) التي يحصل عليها والتي يعالجها أو يدرجها في

[1] أنظر المادة 11 من القانون 09/04.

* عرف المشرع الجزائري معطيات حركة السير وتسمى أيضا معطيات المرور، بأنها أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الإتصالات، توضح مصدر الإتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة". أنظر المادة 02/ه من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وعرفت المادة الأولى الفقرة (د) من اتفاقية بودابست هذا النوع من المعطيات بأنها أي بيانات كومبيوتر متعلقة باتصال عن طريق منظومة كومبيوتر والتي تنشأ عن منظومة كومبيوتر تشكل جزءا في سلسلة الإتصالات، توضح مصدر الإتصال والوجهة المرسلة إليها والطريق الذي تسلكه ووقت وتاريخ وحجم ومدة ونوع الخدمة المذكورة". وقد أشارت المذكرة التفسيرية لاتفاقية بودابست أن الإحتفاظ بكل أو ببعض المعطيات المجمعة لدى مزود الخدمات يهدف إلى تحديد خط سير الإتصال، بمعنى مصدر أو مكان وصول هذه الإتصالات والتي تعد من الأمور الجوهرية للتعرف على هوية الأشخاص الذين أرسلوا الفيروسات مثلا أو النجاح في اتمام الوصول إلى نظام المعالجة الآلية. أنظر المذكرة التفسيرية لاتفاقية بودابست، وكذلك هلالي عبد الله أحمد، مرجع سابق، ص 187.

[2] انظر المادة 10 من القانون 04/09.

[3] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، مرجع سابق، ص 446.

[4] تنص المادة 11 من الق 09/04 على أنه "...دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الإلتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ويعاقب الشخص الطبيعي بالحبس.."

وحدة التعرف على المشتركين أو على زبائنه.."، لذلك فلا بأس أن نستعين بما هو موجود في القضاء والتشريع الفرنسي لتوضيح هذه المسالة.

لقد كانت البداية في تحديد نطاق ومضمون الإلتزامات الملقاة على عاتق موردي خدمة الأنترنت بغية تحقيق حماية للحق في الخصوصية من طرف هؤلاء من القضاء الفرنسي، الذي اجتهد في التغلب على الصعوبات التي واجهته في فرض حد معقول من الإلتزامات على موردي خدمة الأنترنت لضمان ألا يكون الأنترنت فضاءا لانتهاك الخصوصية" في ظل غياب نصوص قانونية خاصة.

إن طبيعة الخدمة التي يقدمها متعهد الإيواء كأحد الوسطاء الفنيين المقدمين لخدمة الأنترنت تجعل منه الأقدر على معرفة مضمون أي نشاط معلوماتي متداول عبر شبكة الأنترنت، على خلاف متعهد الوصول الذي لا يمكنه ذلك، لتوقف دوره عند حد تمكين المستخدم من الوصول إلى الشبكة فقط، لذلك فقد ألزم القضاء متعهدي الإيواء بأخذ الحيطة والحذر تجاه ما يتم نشره من مضمون معلوماتي على المواقع الإلكترونية التي يستضيفونها، دون أن يشدد عليهم بممارسة الرقابة الدقيقة على هذه المحتويات.

وتطبيقا لذلك أصدرت محكمة باريس الكبرى في 09 جوان 1998 [1] حكما يضع على عاتق متعهد الإيواء التزاما ببذل العناية اللازمة لمراقبة احترام المواقع الإلكترونية المأوية لحقوق الآخرين وللآداب العامة، وذلك بمناسبة الدعوى القضائية التي رفعتها عارضة أزياء فرنسية ضد متعهد الإيواء، نتيجة إيوائه موقعا إلكترونيا نشر عليه تسع عشرة صورة تظهرها عارية، وقد اعتبرت نفس المحكمة أن متعهد الإيواء يجب عليه إثبات قيامه بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة مراعاة القوانين والأنظمة السارية، وبعدم الإعتداء على حقوق الآخرين، وإلا فإنه يتحمل المسؤولية الناجمة عن ممارسة هذا النشاط في حال انتهاك حقوق الغير.

وفي حكم آخر لمحكمة نانتير الفرنسية حدد القضاء الفرنسي صراحة في هذه القضية نوعية الإلتزامات الملقاة على عاتق متعهدي الإيواء، من خلال إلزامهم بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة احترام حقوق الآخرين، وبذل العناية للكشف عن أي مضمون معلوماتي غير مشروع والتوقف عن بثه حال اكتشافه[2]، وقد كانت هذه القضية بمناسبة الدعوى التي رفعتها عارضة الأزياء «lynda lacoste» ضد

[1] L'affiare (Estelle LEFEBURE epouse Hallydy, contre Valentin lacombre) TGI de Paris, réf 9 juin 1998_ JCP édition E 1998, n°21, Page 953 et CA Paris, 14ème chambre, section A réf 10 février 1999 Dalloz 1999 note Mallet-Poujol N.P - Droit à l'image et responsabilité des hébergeurs p.389.

"Par arrêt du 10 février 1999, la cour d'appel de PARIS, statuant en référé, a condamné M. Valentin LACAMBRE, à verser à Mme Estelle LEFEBURE épouse HALLYDAY, une provision sur dommages-intérêts pour avoir, début 1998, hébergé de façon anonyme sur le site ALTERN.ORG, qu'il a créé et qu'il gère, un site diffusant, sans y avoir été autorisé par l'intéressée, des photographies portant atteinte au droit qu'elle détient sur son image et à l'intimité de sa vie privée."

[2] TGI Nanterre, 08 décembre 1999, Gazette du Palais, Jur 11-12 février2000 page 2 « dans la décision, le tribunal de grande instance de Nanterre a relevé : « les sites présumés illisites sont aisément détectables par le moyen d'un moteur de recherche basé sur des mots-clé d'un nombre réduit évoquant l'univers de la nudité, la beauté, la célébrité, la féminité » il constate ensuite que les photographies de linda lacost ont été trouvées depuis le moteur de recherche Nomade sur les mots-clé « célébrités française » et depuis l'annuaire Yahoo sur les mots-clé « célébrités dénudées-photos, célébrités-photos sexe » .

متعهدي إيواء لقيامهم بإيواء واستضافة مواقع قامت بنشر وعرض عدد من الصور تظهرها وهي عارية بشكل فاضح دون الحصول على موافقتها.

وبالإضافة إلى الإلتزام بالإعلام أوجب القضاء الفرنسي أيضا على متعهدي الإيواء الالتزام باليقظة، والذي مقتضاه أن يتخذ متعهدوا الإيواء كافة الإجراءات التي من شأنها الكشف عن أي موقع إلكتروني يتضمن محتوى غير مشروع أو يمس بخصوصية الغير، وحينها يطلب من صاحب هذا الموقع تصحيح وضعه أو قطع الخدمة عنه إذا لم يلتزم بذلك، بحيث يعمل متعهدوا الإيواء بموجب هذا الإلتزام على اتخاذ الإجراءات الضرورية التي تمكنه من إرغام صاحب الموقع بإزالة المحتوى الذي يتضمن الإساءة وإجبارهم على احترام الآخرين وعدم الإساءة لهم.[1]

وتقريبا هي نفس الإلتزامات التي عمد المشرع الفرنسي على تقنينها من خلال القانون رقم 2004/575 حول الثقة في الاقتصاد الرقمي،[2]والذي جاء متوافقا مع أحكام ومقتضيات التوجيه الأوروبي حول التجارة الإلكترونية[3]، ومن أهم هذه الإلتزامات:

- الإلتزام بالتصرف "فورا": «l'obligation de réagir «promptement: إنطلاقا من نص المادتين 6-I-2 و 6-I-3 من قانون الثقة في الإقتصاد الرقمي (LCEN)، فإنه يتعين على المتعهد بالإيواء(المضيف) l'hebergeur أن يتصرف فورا عندما يتم إخطاره بالطبيعة غير القانونية للمحتوى وإزالته فورا، أو جعل وصوله للجمهور مستحيلا، مع ضرورة إخطار صاحب الموقع المورد للمعلومات بموضوع المشكلة واستدعائه للرد و وجعله في اتصال مع صاحب الشكوى حتى يتم التمكن من حل النزاع.

ويكون المحتوى غير مشروع إذا كان غير قانوني بشكل واضح كما لو كان يؤدي إلى نشر الكراهية أو العنف أو التمييز العنصري، أو انتهاك الخصوصية[4]، والمشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية أشار فقط إلى إلزام مقدم خدمة الأنترنت بمسك سجل تجرد فيه كل الإنتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي، وكذلك الإجراءات التي تم اتخاذها في مواجهة هذه الإنتهاكات.[5]

والملاحظ أن المشرع لم يتناول هذه المسائل بالتوضيح أو التنظيم الكافيين لإزالة أي غموض بشأن علم مورد خدمة الأنترنت بالإنتهاكات الماسة بخصوصية الأشخاص، خاصة إذا كان مورد الخدمة متعهد الوصول والذيلا يمكنه الإطلاع على المحتوى المعلوماتي، فكيف يتم اخطاره من قبل المتضرر، بالإضافة

[1] فرح قاسم، مرجع سابق، ص 335.

[2] Loi n° 2004/575 du 21 juin 2004 pour la confiance dans l'économie numérique JORF 22 juin 2004

[3] Directive du parlement européen et du conseil relative à certains aspects juridiques des services se la société de l'information et notament du commerce éléctronique dans le marché interieur (directive sur le commerce éléctronique).

[4] Michel Montazeau.op, cit, page 15. Voir aussi : Jérôme Huet, Emmanuel DREYER, Droit de la communication numérique, Lextenso edition L.G.D.J 2011, Page 121.

[5] تنص المادة 2/43 من القانون 07/18: " يجب على كل مقدم خدمات أن يمسك جردا معينا حول الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والا جراءات التي اتخذها بشأنها".

إلى عدم توضيح ما هي الإجراءات التي يتعين على مقدم الخدمة القيام بها لضمان حماية المعطيات الشخصية عند حدوث هذه الإنتهاكات.

لذلك فإن المشرع الفرنسي قد افترض وفقا للمادة 6-I-5 [1]من قانون الثقة في الاقتصاد الرقمي معرفة وعلم متعهد الإيواء بالمحتوى غير المشروع الماس بالحق في الخصوصية إذا تم إخطاره بالعناصر التالية:

- تاريخ الإخطار.

- سم وتاريخ ومكان الميلاد ومحل الإقامة والجنسية إذا كان المخطر شخصا طبيعيا.

- وإذا كان المخطر شخصا معنويا يذكر إسمه، شكله،والجهة التي تمثله قانونا ومقره الإ جتماعي.

- وصف الوقائع المتنازع عليها وموقعها بدقة.

- أسباب إزالة المحتوى.

- الإلتزام بتعريف المستخدمين: l'identification des internautes وذلك تطبيقا لما أوصى به التوجيه الأوروبي المتعلق بالتجارة الإلكترونية المؤرخ في 08 جوان 2000 في المادة 15-2 منه، حيث ألزم المشرع الفرنسي من خلال قانون الثقة في الإقتصاد الرقمي بنص المادة 6-11 المتعهدين بالإيواء وكذلك مقدمي الوصول بضرورة حفظ البيانات التي من المحتمل أن تسمح بتعريف وتحديد هوية أي شخص ساهم في إنشاء المحتوى، وهي البيانات التي يمكن أن تطلبها السلطات القضائية بمناسبة إجراءات التحقيق*.

وفي هذا الصدد أصدر المشرع الفرنسي المرسوم 2011-219 المؤرخ في 25 فيفري 2011 المتعلق بحفظ البيانات وإبلاغها[2] ، الذي يلزم بتعريف أي شخص ساهم في إنشاء محتوى تم نشره على الأنترنت من خلال تحديد البيانات المذكورة في المادة 06 من القانون المتعلق بالثقة في الإقتصاد الرقمي، فيما يتعلق بمقدمي خدمة الأنترنت، وتتمثل هذه البيانات خصوصا في تعريف الإتصال المعرف الذي خصصه مزود

---

[1] « La date de la notification :

- Si le notifiant une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance, si le réquérant est une personne morale : sa forme, sa dénomination, son siege sociale, l'organisme qui le représente légalement.
- Les noms et domicile du destinataire ou s'il s'agit d'une personne morale, sa dénomination et son siège sociale.
- La description des faits litigieux et leur localisation précise.
- Les motifs pour lesquels le contenu doit être retiré, comprenant la mention des position légales et des justifications de faits ».

*وقد مدد القانون الفرنسي رقم 2006/64 المؤرخ في 23 جانفي 2006 المتعلق بمكافحة الإرهاب ووضع مختلف الأحكام المتعلقة بمراقبة الأمن والحدود، سلطة الحصول على هذه البيانات كذلك من طرف ضباط الشرطة القضائية من شرطة ودرك تحت إشراف السلطة القضائية المختصة.

LOI no 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

[2] Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne JORF n°0050 du 1 mars 2011 page 3643

خدمة الأنترنت للمشترك (كلمة السر)، معرف الطرف النهائي للإتصال، أوقات البدء والإنتهاء من الإتصال، أنواع البروتوكولات المستخدمة في الإتصال بالخدمة[1] وطبيعة هذه العملية وأوقاتها، ومن دون أدنى شك فإن هذه البيانات،تعتبر من ضمن البيانات ذات الطابع الشخصي بالمعنى المقصود في قوانين حماية المعطيات الشخصية لقدرتها على تعريف المستخدم أو جعله قابلا للتعريف .

إلا أنه ومن جهة أخرى فإن كشف هذه المعطيات الشخصية لا شك أنه يتعارض مع رغبة مستخدمي الأنترنت في التخفي، ومع اتجاههم العام بضرورة ترك شبكة الأنترنت مجالا مفتوحا للتعبير بكل حرية[2]، لذلك اعتبر أنه إذا كان متعهد الإيواء ملزم بمطالة عملائه بالبيانات الشخصية التي تسمح بتحديد هويتهم، فانه ملزم أيضا وفقا لنص المادة 3/06-1 من قانون الثقة في الإقتصاد الرقمي الفرنسي بضرورة المحافظة على سريتها وعدم استخدامها أو الكشف عنها إلا للضرورة.

وهو في حقيقته التزام تبادلي، حيث يلتزم صاحب المضمون من جهته بتزويد متعهد الإيواء بالبيانات والمعلومات المطلوبة والتي تسمح بتحديد هويته، وبالمقابل على متعهد الإيواء المحافظة على سريتها.

وفي هذه المسألة بالذات يمكن أن نشير إلى أن المشرع الجزائري في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها قد ألزم مقدمي خدمة الأنترنت بإزالة المعطيات التي يقومون بتخزينها، وذلك بعد مرور سنة ابتداء من تاريخ تسجيلها، ويأتي هذا الإلتزام من موجبات حق النسيان المنبثق عن حماية الحق في الخصوصية.

وإلى جانب المشرع الجزائري، نجد كذلك المشرع الفرنسي مهتما بمسألة حرمة الحق في الخصوصية في نطاق التخزين التلقائي للمعطيات المتعلقة بالإتصالات الإلكترونية، وذلك من خلال نص المادة (L32-I-3) من قانون البريد والإتصالات الإلكترونية المضافة بموجب المادة 29 من القانون رقم 1062-2001 المؤرخ في 2001/11/15 المتعلق بالأمن القومي والمعدلة بموجب المادة 20 من القانون 2003/239 المؤرخ في 18 مارس 2003 المتعلق بالأمن الداخلي[3]، وهذا الإلتزام نص عليه أيضا المشرع التونسي في مواجهة المسؤولين عن المعالجة في القانون الأساسي عدد 2004/63 المتعلق بحماية المعطيات الشخصية، تحت مسمى إعدام المعطيات الشخصية حيث أوجب في المادة 45 منه إعدام(إزالة) هذه المعطيات بمجرد انتهاء الأجل المحدد لحفظها أو بعد تحقق الغرض الذي جمعت لأجله، أو إذا لم تعد ضرورية لنشاط المسؤول عن المعالجة.

وقد اعتبر الفقه الفرنسي أن الإلتزام بحفظ البيانات هو مقابل إعفاء متعهدي الإيواء من الإلتزام العام بالمراقبة[4]، ذلك أن نص المادة 7/1-6 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي يمنع فرض التزام عام على متعهد الإيواء بمراقبة المعلومات التي يتولى نقلها أو تخزينها، أو البحث النشط عن الوقائع

[1] اللجنة الوطنية للمعلوماتية والحريات في فرنسا (CNIL) تعتبرأن بروتوكول IPيعتبر من المعطيات ذات الطابع الشخصي.

L'adresse « IP » est une donnée à caractère personnel pour l'ensemble des CNIL européennes, voir le site : http://cnil.fr

[2] قاسم فرح، مرجع سابق، ص339.

[3] للإطلاع أكثر أنظر رشيدة بوكر، جرائم الإعتداء... مرجع سابق، ص451.

[4] Jérôme Huet, Emmanuel DREYER, Droit de la communication numérique, L.G.D.J, 2011, op cit page 131.

والظروف التي تكشف عن الأنشطة غير مشروعة[1]، ومن ثمة فبموجب هذا الإعفاء يجد متعهدو الإيواء أنفسهم معفون من ممارسة الرقابة السابقة على المضمون المعلوماتي غير المشروع، لكنهم ملزمين بالرقابة اللاحقة بعد إخطارهم بالمضمون أو المحتوى غير المشروع، وقد نصت على ذلك المادة 6-2 من القانون حول الثقة في الإقتصاد الرقمي، وكذلك المادة 15-2 من التوجيه الأوروبي حول التجارة الإلكترونية، حيث أكدتا على التزام متعهد الإيواء بإعلام السلطات العامة وبصورة عاجلة عن أي معلومات أو بيانات غير مشروعة عند ممارسة الرقابة اللاحقة على المضمون المعلوماتي غير المشروع ، والمشرع الجزائري أيضا نجده تناول الإشارة إلى هذا الإلتزام في المادة 43 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث ألزم مقدم الخدمات بأن يعلم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وكذلك الشخص صاحب المعطيات الشخصية، بكل فعل من شأنه المساس بالحياة الخاصة في شبكات الإتصالات الإلكترونية المفتوحة للجمهور (الأنترنت)، سيما معالجة المعطيات الشخصية على هذه الشبكة التي تؤدي إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها .

1) إلتزامات مورد المعلومات: أما بالنسبة لمورد المعلومات كأحد الوسطاء التقنيين «intermédiaires techniques» والذي يملك بهذه الصفة نشر المعلومات على المواقع الإلكترونية، فإنه مرتبط بالتزامين، ول يتعلق بالشفافية، وهو التزام يوجب على مورد المعلومات إطلاع مستخدم الأنترنت «les internautes» ومتعهدي الوصول les fournisseurs d'accès ومتعهدي الإيواء les hebergeurs على البيانات التي تعرف به، ومن عناصر التعريف الأساسية التي يلتزم مورد المعلومات تقديمها:

- إذا كان شخصا طبيعيا: يلتزم بالتعريف بإسمه ولقبه وكنيته وعنوانه.

- إذا كان شخصا معنويا فإنه يلتزم بتعريف إسمه وطبيعة نشاطه ومركز إدارته الرئيسي.

وغالبا ما تكون هذه المعلومات التعريفية الخاصة بمورد المعلومات منشورة على الصفحة الرئيسية للموقع الإلكتروني.

ومن شان هذه العناصر التعريفية أن تجعل من مورد المعلومات معروفا لدى المستخدمين، مما يتيح توفير طابع الشفافية على عمله.

أما الإلتزام الثاني فهو متعلق بإتاحة حق الرد، وهو الإلتزام الذي نجد مصوغه بنص المادة 6-2/3 من القانون الفرنسي حول الثقة في الإقتصاد الرقمي، حيث يتمتع كل شخص طبيعي أو معنوي بحق الرد على

[1] Article 6/1-7 « les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stokent, ni à une pbligation générale de chercher des gaits ou des circonstances révélant des activités illicites. »

وهذا النص القانوني جاء متوافقا مع أحكام المادة 15/1 من التوجيه الأوروبي حول التجارة الإلكترونية والتي جاء نصها كما يلي:

« les Etats membres ne doivent pas imposer aux préstataires pour la fournitures des services visée aux articles 12,13 et 14 une obligation générale de surveiller les informations qu'ils transmettent ou stokent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.»

أية معلومة منشورة على شبكة الأنترنت تمس شرفه أو تنتهك حقوقه، ومنها الحق في الخصوصية، وينطوي الإلتزام بإتاحة حق الرد على تحمل مورد المعلومات على عاتقه نشر رد الشخص المضرور مباشرة على موقعه، بالإضافة إلى تصحيح أو شطب المادة المعلوماتية غير المشروعة من على صفحات الويب[1].

ومن خلال التعريف الذي جاء به المشرع الجزائري لما يسمى بالمورد الإلكتروني في قانون التجارة الإلكترونية[2] 05/18 ، ندرك إمكانية اعتبار المورد المعلوماتي بمثابة مورد إلكتروني،[3] ويلتزم بما يلتزم به هذا الاخير، وعلى هذا الأساس وانطلاقا من المادة 26 من قانون التجارة الإلكترونية الجزائري 05/18 فإذا ما قام المورد المعلوماتي بجمع المعطيات ذات الطابع الشخصي المتعقلة بالزبائن، ألا يجمع منها إلا البيانات الضرورية لإبرام المعاملات التجارية، كما يجب عليه في هذا الإطار السعي إلى الحصول على موافقة المستهلكين الإلكترونيين* قبل جمع بياناتهم الشخصية وضمان الحفاظ على سريتها .

2) إلتزامات متعهد الوصول: من أهم التزامات متعهدي الوصول « les fournisseurs d'accès » والتي ترتبط بموضوعنا هو الإلتزام بالإعلام، وذلك من خلال القيام بإعلام مستخدمي الشبكة بالبيانات الخاصة بهم وبالمشتركين معهم، وإحاطتهم جميعا بضرورة احترام الأنظمة والقوانين وعدم الإعتداء على حقوق الغير وخصوصياتهم، وانطلاقا من نص المادتين 05 من التوجيه الأوروبي حول التجارة الإلكترونية و 1/3-06 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي، فإن متعهد الوصول يلتزم بالكشف لعملائه عن إسمه وعنوانه وبريده الإلكتروني، ومكان ورقم قيده التجاري، كما يتوجب عليه أيضا في مقابل ذلك أن يطالب عملاءه في مرحلة ما قبل التعاقد معهم بتقديم جميع المعلومات والبيانات الشخصية التي تمكنه من تحديد هويتهم[4].

ومن بين الالتزامات الأخرى الملقاة على عاتق متعهدي الوصول وهي ذات طبيعة تقنية، هو وجوب اقتراحهم على عملائهم الوسائل الفنية اللازمة لمنع الوصول إلى بعض المواقع الإلكترونية المشبوهة، فالمادة 6-1 من القانون الفرنسي حول الثقة في الإقتصاد الرقمي تلزم هؤلاء المتعهدين بتزويد المشتركين بالوسيلة الفنية التي تسمح لهم لفرض رقابة ذاتية على أنفسهم وعلى أفراد أسرتهم، مثل تقنية تصفية المعلومات

[1] Article 6-4 de la loi pour la confianc dans l'économie numérique modifié par loi n° 2018-898 du 23 octobre 2018- article 29, relative à la lutte contre la fraude, JORE n°246 du 24 octobre 2018 « le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffuson, alors qu'elle soit cette information inexate. »

Voir aussi Yves Poullet Jean-François Lerouge, Responsabilité des acteurs de l'internet, article disponible sur le site www.cride.be page 26.

[2] أنظر القانون 05/18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية عدد 28 لسنة 2018.

[3] تعرف المادة 06 من القانون 05/18 المورد الإلكتروني بأنه كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير سلع أو خدمات عن طريق الإتصالات الإلكترونية.

* يعرف المستهلك الإلكتروني بأنه "كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الإتصالات الإلكترونية من المورد الإلكتروني بغرض الإستخدام النهائي".

[4] أنظر المادة 2/15 من التوجيه الأوروبي حول التجارة الإلكترونية والمادة 6-2 من القانون الفرنسي حول الثقة في الإقتصاد الرقمي.

الإلكترونية (Filtrage)، وهي تقنية تمكن المستخدمين من استقبال إلا المعلومات التي تتفق مع قيمهم وتحترم حياتهم الخاصة.[1]

وتطبيقا للقواعد العامة فإن إخلال مقدمي الخدمة (الوسطاء الفنيين) بالإلتزامات القانونية الملقاة على عاتقهم يقابله قيام المسؤولية القانونية.

ثانيا: أساس مسؤولية الوسيط الفني في تقديم خدمات الأنترنت في مجال حماية الخصوصية المعلوماتية:

لقد اختلفت مسالك الآراء الفقهية في شأن تأصيل مسؤولية الوسطاء التقنيين في خدمة الأنترنت بين ثلاث جهات:[2]

الرأي الأول: يرى عدم مسؤولية مقدمي خدمة الأنترنت على الإطلاق لأن دورهم فني بحت، وبمقدورهم وفق هذه المهام وقف نشر المعلومات متى تضمنت مادة معلوماتية مخالفة للقانون.

الرأي الثاني: يرى مساءلة مقدمي خدمة الأنترنت على أساس قواعد المسؤولية المفترضة، ذلك أن المشرع أقام نظاما يتعلق بكيفية النشر على شبكة الأنترنت، لذلك يلزم على كل متدخل في سلسلة تقديم الخدمة أن يمنع أو يمحو المعلومات غير المشروعة، ولا يمكن أن يعتد بدفاعه أنه لا يعلم بذلك.

أما الرأي الثالث: فيرى باعتمدا المسؤولية المشروطة، حيث يتوقف أمر قيام المسؤولية من عدمها على طبيعة الدور الذي يقوم به مورد الخدمة، ووفقا لذلك فإذا كان دوره مجرد ناقل للمعلومات فلا تقام مسؤوليته على مراقبة المادة المعلوماتية التي يتم نقلها أما لو كان غير ذلك فإنه يسأل.

وبين رأي وآخر، ذهب الإتجاه الغالب إلى تقرير مسؤولية الوسطاء الفنيين أو مقدمي خدمة الأنترنت انطلاقا من طبيعة الخدمة التي يؤدونها، ودورهم في سلسلة الخدمات المتعلقة بإدارة الأنترنت لتقديم الخدمة النهائية للمستخدم، وبصفة خاصة مدى تمتعهم بالدور الرقابي على المحتويات غير المشروعة التي تمر عبر الخدمة.

إن هذه الحقيقة الواضحة أمامنا تقودنا إلى القول بأن هذا الجدل لا يمكن أن يؤدي بأي حال من حوال إلى استبعاد مسؤولية مقدمي خدمات نترنت، ذلك أن إقامة المسؤولية على هؤلا يزيد من حرصهم على فرض الرقابة الذاتية على مشروعية المعلومات لرد المسؤولية عنهم، وفي مقابل ذلك، فان عدم إقرار مسؤوليتهم من شأنه أن يؤدي إلى تداول معلومات غير مشروعة على الشبكة[3] من شأنها المساس بخصوصية الأشخاص.

---

[1] فرح قاسم، مرجع سابق، ص 348.

[2] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دراسة متعمقة ومقارنة، الطبعة الأولى، منشاة المعارف القاهرة.2009، ص 95،96.

[3] رشيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص 73.

ولذلك تختلف طبيعة مسؤولية مقدمي الخدمات باختلاف مضمونها، فقد تكون مسؤولية جزائية إذا تضمن المحتوى الإلكتروني ما يدخله في نطاق التجريم، أو قد تكون مسؤولية مدنية إذا احتوى هذا المضمون على تعد على حقوق الآخرين وأضر بهم،[1] أو نتيجة لإخلال مقدم الخدمة بالتزاماته العقدية.

وبالتالي تتنوع مسؤولية مزودي خدمة الأنترنت بين المسؤولية الجزائية والمدنية، وهذه الأخيرة إما مسؤولية عقدية أو تقصيرية.

و إننا لا نجد نصوصا قانونية على صعيد التشريع الجزائري تهتم بتنظيم موضوع مسؤولية مزودي خدمة الأنترنت، إلا أنه بالرجوع إلا التشريع المقارن نجد أن المشرع الفرنسي والذي جاء متفقا مع الإتجاه العام للتوجيه الأوروبي حول التجارة الإلكترونية، نصت المادة 3/I-6 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي، أن أفعال مقدمي خدمة الأنترنت الخاطئة لا يمكن أن تدخل في نطاق التجريم إلا إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، ولم يتخذوا على الرغم من علمهم الإجراءات اللازمة لشطبه أو على الأقل لمنع وصول الجمهور إليه، وهو نفس الموقف الذي نجد له سبيلا في القانون الأمريكي المتعلق بالحد من الإعتداءات على حقوق الملكية الفكرية في نطاق الأنترنت Digital Millenium) (Copyrightالمؤرخ في 28 أكتوبر 1998 والذي حصر إقامة مسؤولية مقدمي خدمة الأنترنت فقط في حالة علمهم بعدم مشروعية المضمون المعلوماتي ويقومون بنقله أو تخزينه، ويتحقق علمهم بعدم المشروعية هذه حسب هذا القانون، في حالة أن تكون عدم المشروعية ظاهرة إلى حد لا يمكن تجاهلها،أو في حالة قيام السلطة المختصة أو الشخص المتضرر من نشر المضمون المعلوماتي بإبلاغ مقدم الخدمة عن عدم المشروعية، ويعد مقدم الخدمة مخلا بالتزاماته القانونية مما يستوجب مسؤوليته، عند عدم مبادرته على اتخاذ موقف إيجابي بشطب هذا المضمون أو على الأقل منع وصوله لجمهور مستخدمي شبكة الانترنت[2] ، ولهذا السبب أطلق على مسؤولية مقدمي خدمة الأنترنت أنها مسؤولية مشروطة.

وقد كان المشرع الفرنسي قد قرر عدم مسؤولية موردي خدمة الأنترنت جزائيا من خلال القانون رقم 719/2000 المؤرخ في 01 أوت 2000 المعدل للقانون رقم 1067/86 المؤرخ في 30 سبتمبر 1986 المتعلق بحرية الإتصالات إلا في حالتين، وهما حسب نص المادة 8/43 من هذا القانون:

-حالة عدم تنفيذ الأمر القضائي الصادر بإلزامه بمنع الوصول إلى المضمون غير المشروع.

- حالة تبليغه من طرف الغير بوجود مضمون غير مشروع أو من شأنه الإضرار بحقوقه، ولا يقوم باتخاذ الإجراءات اللازمة لمنع بث هذا المضمون.

وقد أشار التوجيه الأوروبي حول التجارة الإلكترونية أن مقدم خدمة الأنترنت لا يسأل قانونا إذا كان عمله يقتصر على النقل أو التخزين، ولا يساهم بأي صورة كانت في إنشاء المعلومات المنقولة أو في تعديلها[3]، وهو الأمر الذي أكده المشرع الفرنسي من خلال قانون الثقة في الإقتصاد الرقمي، عندما ذهب إلى إعفاء متعهد

[1] فرح قاسم، مرجع نفسه، ص352.

[2] فرح قاسم، مرجع سابق، ص 354.

[3] رشيدة بوبكر، حماية التعاملات الإلكترونية، مرجع سابق، ص77.

الإيواء من المسؤولية المدنية والجزائية عن إيوائه لمضمون غير مشروع إذا لم يثبت علمه بعدم مشروعيته، أو قام بمجرد علمه بأسباب عدم مشروعية هذا المضمون باتخاذ الإجراءات الكفيلة لمنع وصوله إلى المستخدمين أو سحبه نهائيا.[1]

وعلى صعيد المسؤولية المدنية لموردي خدمة الأنترنت بشقيها العقدية والتقصيرية، فالملاحظ أن التوجيه الأوروبي حول التجارة الإلكترونية، وكذلك المشرع الفرنسي لم يتناولا المسؤولية العقدية لمقدمي الأنترنت إلا من خلال تنظيمه لأحكام المسؤولية في التجارة الإلكترونية، وهي في حقيقة الأمر تخضع للقواعد العامة للمسؤولية العقدية.

أما بالنسبة للمسؤولية التقصيرية، وكما سبق الإشارة فإن الإتجاه العام لنصوص القانون الفرنسي حول الثقة في الإقتصاد الرقمي (LCEN) وأحكام التوجيه الأوروبي حول التجارة الإلكترونية، تميل إلى إقامتها على عاتق مورد خدمة الأنترنت في حال ما إذا ثبت علمه الفعلي بالمضمون الإلكتروني غير المشروع، كأن يتضمن انتهاكا لخصوصية الأشخاص، ومع ذلك لم يقم باتخاذ الإجراءات اللازمة لسحبه أو لمنع وصوله للجمهور، أو إذا طلب منه محو هذا المحتوى أو منع وصوله إلى الجمهور من قبل السلطة القضائية ولم يستجب لذلك.

[1] Article 6-I-3 du loi fransaise pour la confiance dans l'économie numérique modifié par la loi n°2016-444 du 13 avril 2016 visant et renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées « les personnes visées au 2 ne peuvent voir leur résponsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites, ou si dés le moment ou elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou eu rendre l'accès impossible. ».

ملخص الفصل الثاني

تطرقنا في هذا الفصل إلى أن لمخاطر التي تهدد المعطيات ذات الطابع الشخصي كانت من العوامل الرئيسية والدوافع الأساسية نحو وجوب سن تشريعات تتضمن مجموعة من المؤيدات لحماية الأشخاص الطبيعيين المعنيين بمعالجة المعطيات ذات الطابع الشخصي، وذلك من خلال إقرار ضوابط تحكم عملية معالجة هذه المعطيات، تتمثل في الضوابط القانونية الموضوعية لمعالجة المعطيات ذات الطابع الشخصي، فقد وضع المشرع مجموعة من هذه الضوابط والضمانات التي تهدف إلى رقابة فاعلة على إنشاء نظم المعلومات وكيفية استخدامها، و في حماية الحريات الشخصية ومنها الخصوصية المعلوماتية، ويكون ذلك أساسا بإقرار عدد من المبادئ التي يتوجب احترامها عند كل معالجة لهذه المعطيات، كي لا ينتج عن ذلك أي إساءة إلى أصحابها، حيث يجب أن تقوم معالجة المعطيات الشخصية على مبدأ المشروعية في كل مرحلة من مراحل عمليات المعالجة الآلية لهذه المعطيات، وكذلك على مبدأ الشفافية من خلال توفير الإعلام الكافي عن عمليات المعالجة. ولقد أقر القانون الجزائري 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالة المعطيات ذات الطابع الشخصي عددا من المبادئ التي يتوجب احترامها عند كل معالجة لهذه المعطيات كي لا ينتج عن ذلك أي إساءة إلى أصحابها.

وعلى أساس ذلك حتى تتصف كل معالجة للمعطيات الشخصية بالمشروعية، يجب أن تتم وفق احترام المقتضيات القانونية اللازمة، والتي تستلزم أن تكون بحسن نية وبعلم من الشخص المعني، وتستند إلى مبررات كافية ومشروعة، أو أن تكون لازمة لحماية مصالح مشروعة للمعني بالمعالجة أو للمسؤول عنها، لذلك نصت المادة الثالثة "أ" من القانون 07/18 على أنه يجب أن تكون المعطيات الشخصية معالجة بطريقة مشروعة ونزيهة، وكذلك أن يكون الأساس الذي يقوم عليه جمع وتسجيل هذه البيانات حتى يكون مشروعا أن يتم بناء على موافقة الشخص المعني بالمعالجة والذي تتعلق به هذه البيانات، أو أن يتم بناء على نص قانوني صريح في الحالات الاستثنائية التي لا يتطلب الأمر فيها الحصول على موافقة هذا الأخير، كما تقتضي المشروعية أيضا أن يكون تخزين البيات الشخصية متناسبا مع الهدف من إنشاء قاعدة البيانات، وأن يكون محدد المدة، مع ضرورة الإلتزام بمبدأ الهدف المعلن والمحدد والمشروع طوال مدة المعالجة، ومن ثمة يقتضي الأمر أن يكون تجميع المعطيات ذات الطابع الشخصي قد تم لغايات محددة ومعلنة ومشروعة.

والمشرع الجزائري على غرار باقي التشريعات التي نظمت عملية معالجة المعطيات الشخصية أوجب في المادة 09 من القانون 07/18 أن تكون المعطيات الشخصية مجمعة لغايات محددة وواضحة ومشروعة، وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات، كما تطرق المشرع الجزائري بوضوح إلى هذه المسألة عندما نصت المادة 09 الفقرة "ج" على أنه يجب أن تكون المعطيات الشخصية ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها.

إضافة إلى مبدأ مشروعية المعالجة ترتكز القوانين المعمول بها في مجال حماية الخصوصية المعلوماتية بشكل كبير وأساسي على مبدا آخر يتعلق بموافقة صاحب المعطيات الشخصية بمعالجة هذه المعطيات،

وهذا الأمر من شأنه أن يعطي انطباعا بنوع من السيطرة للشخص المعني على معطياته الشخصية، وتأسيسا على هذا المفهوم أصبح رضا الشخص وموافقته المسبقة على معالجة معطياته الشخصية أحد أهم وأبرز الضمانات لتحقيق معالجة صحيحة ومشروعة.

غير أنه وبالرغم من إلزامية حصول المسؤول عن المعالجة الموافقة المسبقة للشخص المعني، فإن هذا المبدأ ترد عليه استثناءات، وهي حالات اعتبر فيها المشرع أن الرضا المسبق للشخص المعني ليس مطلوبا للقيام بالمعالجة، وذلك عندما ترتبط المعالجة أساسا بتحقيق مصالح مشروعة للشخص المعني أو المسؤول عن المعالجة، وكذا عند تنفيذ مصالح مرتبطة بالصالح العام، وقد حدد المشرع هذه الحالات في المادة السابعة من القانون 07/18.

كذلك من المبادئ الأساسية لحماية الحق في الخصوصية في مواجهة نظم المعلومات الشخصية، مبدأ الشفافية في معالجة المعطيات الشخصية، وتتعلق الشفافية بإمكانية الفرد من الوصول إلى بياناته الشخصية المحفوظة ضمن دائرة خاصة والإطلاع على دقة وصحة هذه البيانات بما يمكن له من القيام به من اعتراض على تجميع بياناته أو المطالبة بتصحيحها في حال كانت بياناته المخزنة غير صحيحة أو غير دقيقة، ويعتبر مبدأ الشفافية الأساس الذي يؤمن الثقة في ممارسة صاحب البيانات الشخصية للحقوق التي يقرها له القانون، وهي:

- الحق في الإعلام وهو أن يتم إعلام الشخص المعني بالمعالجة بأنه سوف يتم جمع بياناته الشخصية ويكون في حالتين، إما أن يتم الإعلام عند تجميع المعطيات لدى الشخص المعني، حيث يتم الإتصال به قبل البدء في عملية التجميع من قبل المسؤول عن المعالجة وإخباره بمجموعة من العناصر أهمها هوية المسؤول الذي يتولى عملية المعالجة وعند الإقتضاء هوية من يمثله، و أغراض المعالجة التي لأجلها يتم طلب البيانات الشخصية، وإما أن يتم الإعلام عند تجميع المعطيات ذات الطابع الشخصي لدى الغير أي لا يتم تحصيلها من المعني مباشرة وإنما من مصدر آخر، وفي هذه الحالة يلزم على المسؤول عن المعالجة أن يزود المعني بالمعالجة بتلك المعلومات قبل تسجيل معطياته أو قبل إرسالها إلى الغير، وقد رأينا أن هذا الحق ترد عله إستثناءات نصت عليها المادة 33 من القانون 07/18 من خلال مجموعة من الحالات ذكرت على سبيل الحصر استـ ، بعدت من نطاق الحق في الإعلام.

- الحق في الولوج، ويقصد به حق الشخص المعني في الوصول إلى بياناته الشخصية بغية الإطلاع عليها ومعرفة كل ما يتعلق به من بيانات شخصية تخصه تم تسجيلها على الكومبيوتر ومصادرها وطرق معالجتها، وكذا مضمون البيانات المتعلقة به بعد معالجتها، وقد عالج المشرع الجزائري حق المعني بالمعالجة في الولوج في المادة 34 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

- الحق في التصحيح، وهو قدرة كل شخص علم بأن هناك بيانات شخصية تخصه مخزنة لدى جهاز من الأجهزة الحكومية أو مؤسسة خاصة، وقام بالإطلاع على هذه البيانات، أو حصل على نسخة منها، أن

يطلب من الحائز لتلك البيانات الشخصية المتعلقة به والقائم عليها، أن يقوم بتصحيح الخاطئة أو الناقصة منها،ويعدل ما يشوبها من مغالطات لتتوافق مع الحقيقة، لكي لا يؤثر ذلك على مركزه لدى جمهور المتعاملين مع تلك الهيأة، بما قد يؤثر على سمعته ويسبب له خسائر لا سبيل له في تجنبها، وبهذه الصورة يعد حق التصحيح حقا أساسيا خوله المشرع للأشخاص المعنيين لغرض الرقابة على معالجة المعطيات الشخصية المتعلقة بهم، ومكملا للحق في الإعلام والحق في الولوج.

- الحق في الإعتراض، حيث يحق حسبه للشخص المعني بالمعالجة أن يعترض على معالجة معطياته الشخصية لأسباب مشروعة، كما يحق له أن يرفض استعمال هذه المعطيات لأغراض دعائية، لا سيما التجارية منها. وقد ميز المشرع بين نوعين من الإعتراض، الأول هو الاعتراض المشروط حيث يجب أن يكون مبررا بأسباب مشروعة، أما الثاني فلا يكون فيه الشخص المعني مجبرا على تقديم أي تبرير أو سبب. بالإضافة إلى إلى إعطاء المستهلك الحق في الإعتراض وبدون مقابل على معالجة بياناته الشخصية إذا استخدمت لأغراض التسويق المباشر، كما في أغراض الدعاية لخدمة أو سلعة تقدم عبر الأنترنت.

أما عن الضوابط القانونية الإجرائية لحماية المعطيات ذات الطابع الشخصي فتتمثل أساسا في ضرورة إتمام إجراءات مسبقة قبل البدء في أية عملية لمعالجة البيانات الشخصية، تتنوع هذه الإجراءات بين التصريح أو الإعلام البسيط أو ضرورة الحصول على الترخيص المسبق، وتعد هذه الإجراءات من أساسيات الشفافية في التعامل مع المعطيات ذات الطابع الشخصي، كونها تفتح أمام السلطة المختصة بحماية المعطيات الشخصية ليس فقط إمكانية ممارسة مهمتها في ضمان حماية حقوق الأشخاص أصحاب البيانات الشخصية، بل يتيح لها أيضا إجراء الرقابة اللازمة على مدى تقيد المسؤولين عن المعالجة بالأحكام القانونية المقررة والتوصيات والإجراءات.

فضلا عن اتخاذ المسؤول عن المعالجة مجموعة من التدابير التقنية والتنظيمية والإجراءات الملائمة لحماية المعطيات ذات الطابع الشخصي وضمان سلامتها وسريتها.

الفصل الثالث

آليات الحماية القانونية للحق في الخصوصية المعلوماتية

الفصل الثالث: آليات الحماية القانونية للحق في الخصوصية المعلوماتية:

لا يخف على أحد أن الحق في الخصوصية المعلوماتية أصبح واحدا من أهم حقوق الإنسان الرئيسية التي تتعلق بكرامته، وبقيم مادية ومعنوية ضمن ثقافات وأنظمة غالبية دول العالم، لذلك فقد جرت حمايته تقريبا في معظم الدساتير الحديثة التي تتضمن نصوصا صريحة تعترف بالحق في الوصول والسيطرة على المعطيات الشخصية وإدارتها.

ومن ثم اتجه الجهد التشريعي إلى وضع قواعد قانونية جديدة لمواجهة التحديات والمشكلات الجديدة الناشئة عن أثر التقنية المعلوماتية على خصوصية الأفراد في هذا المجال، وذلك انطلاقا من الحاجة الماسة إلى بناء الثقة في الفضاء المعلوماتي والإستخدام الآمن لتقنيات المعلومات والإتصالات الإلكترونية.

إلا أن الإطار القانوني وحده لا يعد فاعلا إلا متى تأمنت آليات وإمكانات الإنفاذ الفاعل، والتطبيق السليم للقانون، سواء عن طريق إيجاد جهة مستقلة ذات طابع إداري، تكون لها سلطات واسعة بما يكفل لها ممارسة دورها الإشرافي والرقابي بشكل يؤمن التطبيق الدقيق لأحكام القانون المتعلق بحماية المعطيات الشخصية، أو عن طريق آلية الردع الجزائي بتوفير مستويات من الحماية الجزائية، والوقوف على صور الإعتداء والإنتهاكات التي تطال الحق في الخصوصية المعلوماتية وصونه، وردع هذه الاعتداءات، وبالتالي اتباع حماية جزائية فاعلة على هذا الحق.

المبحث الأول: الحماية الإدارية للحق في الخصوصية المعلوماتية

إن التوفيق بين تطور الأنظمة المعلوماتية وضمان حماية الحق في الخصوصية المعلوماتية، يقتضي إضافة إلى وجود قانون ينظم المبادئ الخاصة بإنشاء نظم المعلومات ويحدد الضوابط المتعلقة بنشاطها المرتبط بمعالجة المعطيات ذات الطابع الشخصي، وجود جهات ذات طبيعة متميزة تتولى مراعاة التطبيق السليم للقانون المتعلق بحماية المعطيات الشخصية والسهر على مطابقة معالجة هذه المعطيات لأحكام هذا القانون [1].

ويعد إنشاء مرجعية تتولى الحرص على تطبيق قوانين الحماية للمعطيات الشخصية دليلا على النية الجدية في الحماية، وعلى وعي السلطة في الدولة التي سنت قوانينها الخاصة بالمعلوماتية على تضمينها نصوص قانونية تستحدث مثل هذه الجهات ذات الخلفية المهنية والعلمية والخبراتية، يمكنها التعامل مع متدادات المتنوعة والإنعكاسات المختلفة لظاهرة معالجة المعطيات الشخصية.[2]

وبالرغم من وجود اختلاف بشأن تسمية هذه الجهة أو القائمين بعملها الإشرافي أو الرقابي، إلا أن الإتفاق بين التشريعات المقارنة هو اعتبارها جهاز إداري متخصص يشرف على تطبيق قواعد وأحكام القانون وفقا للمبادئ والأهداف المعلنة فيه.

[1] بولين أيوب، مرجع سابق، ص 454.

[2] منى الأشقر جبور، محمد جبور، مرجع سابق، ص151.

المطلب الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

إن ضمان احترام قواعد و مبادئ معالجة المعطيات ذات الطابع الشخصي و التقيد بضوابطها وإلزام كل متدخل في عملية المعالجة لهذه المعطيات إحترام التزاماته القانونية، يقتضي وضع قواعد وقائية وحمائية لحرمة الحق في الخصوصية، وقد حرصت التشريعات في سبيل ذلك على تكريس مبدأ الإشراف و الرقابة غير المباشرة للدولة عن طريق إيجاد جهة مستقلة بصلاحيات واسعة ومضبوطة، بما يكفل لها ممارسة هذا الدور الرقابي والإشرافي بشكل يسمح بالتطبيق الصارم لقانون حماية المعطيات الشخصية، وذلك لما لها من قدرة على التوفيق بين ضرورة وجود الأنظمة المعلوماتية وتطورها وضمان الحق في الخصوصية للافراد.

والمشرع الجزائري إدراكا منه بأهمية وجود هيأة تتولى الإشراف والرقابة على أنشطة الأنظمة المعلوماتية، حرص على استحداث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب نص المادة 22 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تكلف بالسهر على مطابقة عملية معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون وضمان عدم انطواء استعمال تكنولوجيا الإعلام والاتصال على أية أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، كما تتولى هذه السلطة إعلام الأشخاص المعنيين بالمعالجة والمسؤولين عنها بحقوقهم وواجباتهم، وتقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، وإعلام أصحابها بمآلها والترخيص بنقل المعطيات الشخصية إلى الخارج، ومنح تراخيص معالجة هذه المعطيات وتلقي التصريحات المتعلقة بذلك [1].

ومن هنا تبدو رؤية المشرع من وراء إنشاء هذه السلطة، هو فرض احترام الحق في الخصوصية تماشيا مع أهداف القانون المحدث لها، والذي يسعى بدوره إلى إقرار الضمانات الكفيلة بحماية أي شخص طبيعي تكون معطياته الشخصية محل معالجة.

وفي القانون الفرنسي المتعلق بالمعلوماتية والحريات المؤرخ في 1978/01/16 تم إنشاء اللجنة الوطنية للمعلومات والحريات (CNIL) Commission nationale de l'informatique et des libertés.

وفي القانون التونسي المتعلق بحماية المعطيات الشخصية 2004/63 المؤرخ في 27 جانفي 2004 أستحدثت بموجب الفصل 75 الهيأة الوطنية لحماية المعطيات الشخصية.

وفي القانون المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي رقم 08/09 المؤرخ في 18 جوان 2009، أحدث بموجب المادة 27 منه اللجنة الوطنية لمراقبة حماية المعطيات الشخصية.

ولقد استلهم المشرع الجزائري حاجته في إنشاء هذه الهيأة الإشرافية المستقلة من تجربة معظم الدول التي لديها تشريعات في مجال حماية البيانات الشخصية، بالرغم من وجود اختلاف بشأن تسمية

[1] أنظر عرض الأسباب للقانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي 07/18.

هذه الجهة عنده، عندما اعتبرها سلطة على خلاف باقي التشريعات التي اعتبرتها إما هيئة (instence) أو لجنة (commission)، ويعبر هذا التوجه في إنشاء مثل هذه المرجعية التي تتولى السهر على تطبيق قانون حماية المعطيات الشخصية، دليلا على النية الجدية في توفير هذه الحماية في مواجهة المعالجات الهائلة للبيانات الشخصية والتقنيات المتخصصة التي تستوجب إضافة إلى وجود القانون والإلمام بمبادئه، وجود رؤية شاملة وواضحة في مواجهة التحديات التي تثيرها مسألة حماية المعطيات الشخصية في مجال معالجتها .

الفرع الأول: الطبيعة القانونية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

نصت المادة 22 من القانون 07/18 على أنه تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي، فالأكيد أن مجرد وجود قانون لحماية المعطيات الشخصية دون وجود جهة متخصصة مكونة من فنيين ومتخصصين في المعلوماتية وكذا قانونيين، يكون لها صلاحية الإشراف والرقابة على قيام الأنظمة المعلوماتية باحترام المعطيات الشخصية للأفراد أثناء ممارستها لأنشطتها المرتبطة بمعالجة هذه المعطيات، غير كاف لضمان توفير الحماية للمعطيات الشخصية عندما تكون محل معالجة، والملاحظ أنه بالرغم من وجود اختلاف بين التشريعات حول تحديد الطبيعة القانونية لهذه الجهة بين هيأة أو لجنة أو سلطة كما اعتبرها المشرع الجزائري، إلا أن صلاحياتها تبقى متعلقة بدورها الإشرافي والرقابي على عمليات معالجة المعطيات الشخصية .

أولا: النظام القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

اختار المشرع الجزائري التوجه الذي سارت عليه أغلب التشريعات التي جعلت من الجهة المكلفة بالرقابة والإشراف على حماية المعطيات ذات الطابع الشخصي سلطة إدارية مستقلة غير خاضعة في عملها إلا لرقابة القضاء، فقد نصت المادة 22 من القانون 07/18 على أنه تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي".

وقد بين المشرع في هذا النص القانوني تأثره بالقانون الفرنسي المتعلق بالمعلوماتية والملفات والحريات والذي نصت المادة 11 منه على أن اللجنة الوطنية للمعلومات والحريات كجهة يناط بها مسؤولية حماية المعطيات الشخصية تعد سلطة إدارية مستقلة.[1]

وقد كان البروتوكول الملحق[2] بالإتفاقية الأوروبية لحماية الأشخاص في مواجهة معالجة البيانات الشخصية [1] قد نص على التزام الدول الأوروبية بإنشاء سلطات إشراف على حماية المعطيات الشخصية تمارس مهامها

[1] Art 11 de la loi du 26 janvier 1978 relative à l'informatique aux fichies et aux libertés : « la commission nationale de l'informatique et des libertés est une autorité adminstrative indépandante ».

[2] Protocol additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractére personnel concernant les autorités de contrôle et les flux transfrantière de données, série des traités européens, n°181, strasbourg 2001, disponible sur le site : http://www.apda.ad .

باستقلالية تامة في مراقبة مدى الإلتزام بضمون هذه الإتفاقية.[2]

كما تولت المادة 28 من التوجيه الأوروبي 95/46/CE المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وحرية تداول هذه المعطيات، بإلزام الدول الأعضاء بأن تنشئ سلطة أو أكثر تتولى مراقبة التطبيق السليم لأحكام القانون المتعلق بحماية المعطيات، وتمارس مهامها المكلفة بها بكل استقلالية[3].

ويعتبر شرط الإستقلالية عاملا أساسيا في توفير الحماية الحقيقية والفعالة للبيانات الشخصية بما يسمح لهذه السلطة الموازنة بين مصالح الشخص المعني بالمعالجة والشخص المسؤول عنها مهما كانت صفته، دون خضوعها في ذلك لتأثير أي جهة أخرى.[4]

ومن هنا يبدو أنه وبشكل عام تنشأ الهيئات المتخصصة بحماية البيانات كجهاز إداري مستقل نظرا لطبيعة مهامها والصلاحيات التي تعطى لها، لتحقيق الهدف من حماية البيانات الشخصية المعالجة في القطاعين العام والخاص، إذ أن الحماية القانونية الفعالة للبيانات الشخصية لا تستقيم دون إنشاء جهاز إداري متخصص يشرف على احترام تطبيق قواعد وأحكام القانون وفقا للمبادئ والأهداف المعلنة فيه[5].

وانطلاقا من نص المادة 22 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[6] ، نكون أمام حقيقة واضحة ندرك من خلالها أن المشرع صنف الجهة التي كلفها بحماية المعطيات ضمن السلطات الإدارية المستقلة، وقد اعتبرها كذلك بالنظر إلى طبيعة مهامها والصلاحيات التي تعطى لها، لتحقيق الهدف من حماية البيانات الشخصية المعالجة في القطاعين العام والخاص.

وتعتبر السلطات الإدارية المستقلة هيئات جديدة مستمدة من النظام السياسي والقانوني الغربي القائم على أساس السوق الحرة التنافسية، وهي مرتبطة بتيار اجتماعي يدعو إلى تبني صنف طموح يتلخص في

---

[1] اتفاقية مجلس أوروبا رقم 108 المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي الموقعة في ستراسبورغ في 28 جانفي 1981.

[2] ورد في مقدمة هذا البروتوكول:

Convaincus que des autorités de controles exerçant leurs fonctions en toute indipendance sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel »

[3] Article 28 de la directive 95/46/CE du parlement Européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des ces données, dispose que : « chaque état membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire de dispositions adoptées par les états membres en application de la présente diricitve.

Ces autorités exercent en toute indépendance les missions dont elles sont investies. »

[4] Farid Bouguettaya, La protection des données personneles en droit communautaire, Mémoire master 2, Recherche droit européen des droits de l'homme Faculté de droit-IDEH, université de Montpellier 1, P112.

[5] منى الأشقر جبور، محمود جبور، مرجع سابق، ص151.

[6] تنص المادة 22 أعلاه "تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي".

تعويض مخطط إدارة عمومية عمودية بمخطط لإدارة أفقية، نتظر منها تنفيذ سياسات عمومية مع أنها لا ترتبط في سيرها بالإدارة التقليدية وليست موضوعة تحت إشراف حكومي.[1]

ومن ثمة فإن الهيئات الإدارية المستقلة أصبحت تعتبر إحدى ميكانيزمات الضبط الإداري، تعكس انتقال الدولة من وظيفة إدارية إلى مجموعة آليات مستلهمة من التسيير العمومي الجديد، كما تجسد فكرة عدم الجمع بين السلطة السياسية التي تحدد الإستراتيجيات والأهداف وبين الجهة المستقلة التي تجسد هذه الأهداف.[2]

وربما كان البعد الإجتماعي عاملا أساسيا ومبررا هاما لإنشاء مثل هذه الهيئات الإدارية المستقلة، نظرا للحاجة الماسة للأمن الإ جتماعي كشرط للتنمية، حيث تظهر هذه الهيئات كواق من تأثيرات التطورات المعقدة للمجتمع والتي تمس الإنسان بصورة مباشرة في خضم صراع المصالح والقوى، لذلك لها من الصلاحيات ما يمكنها من حماية الفرد، كطرف ضعيف في المعادلة في إطار محاولة التوازن من خلال منحها صلاحيات الضبط الإداري.

وعلى هذا الأساس فإن السلطات الإدارية المستقلة هي هيئات استحدثت في المنظومة القانونية الجزائرية بهدف تفعيل فكرة الضبط الإداري، وهي تتميز عن الهيئات الإدارية التقليدية بتمتعها بوصف "السلطة المستقلة"، خاصة إذا أدركنا أن فكرة الضبط أساسا هي تلك المهمة التي تتولاها بعض الهيئات والمتمثلة في ضمان تحقيق التوازن بين الحقوق والإلتزامات، والأكيد أن هذه المهمة لا يمكن لهذه الهيئات تحقيقها إلا إذا تم تزويدها بمجموعة من الصلاحيات و السلطات تجعلها تتدخل ليس فقط لحل النزاعات القائمة، ولكن تتدخل كذلك لتحقيق التوازنات المطلوبة من خلال تلك الإ متيازات التي تتمتع بها هيئات الضبط في ممارسة السلطة التنظيمية، مثل سلطة اتخاذ القرارات الإدارية، سلطة التحقيق وسلطة العقاب.

وترجع فكرة إطلاق تسمية السلطة لأول مرة على هيئات إدارية غير تلك الهيئات الإدارية التقليدية، في التشريع الفرنسي بمناسبة إنشاء اللجنة الوطنية للمعلومات والحريات (CNIL)، بموجب القانون 17/78 المؤرخ في 06 جانفي 1978 المتعلق بالمعلوماتية والملفات والحريات،[3] ثم تلتها بعد ذلك العديد من السلطات الإدارية المستقلة في مجالات مختلفة بنفس الصفات والخصائص.

إن مصطلح السلطة في مفهوم السلطات الإدارية المستقلة يوحي بأننا أمام هيئات لا ينحصر دورها في تقديم آراء استشارية فقط، وإنما يبرز أيضا تمتع هذه الهيئات بالعديد من الصلاحيات التي يعود

[1] سلطان عمار، السلطات الإدراية المستقلة في الجزائر، مقال منشور في مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العدد 33، ماي 2019 جامعة الإخوة منتوري، قسنطينة1، ص53.

[2] شيبوتي راضية، الهيئات الإدارية المستقلة في الجزائر-دراسة مقارنة- رسالة مقدمة لنيل شهادة الدكتوراه علوم في القانون العام، تخصص المؤسسات الإدارية، كلية الحقوق والعلوم الإدارية قسم القانون العام، جامعة الإخوة منتوري قسنطينة، 2015،2014، ص12.

[3] خرشي الهام، السلطات الإدارية المستقلة في ظل الدولة الظابطة، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون العام، كلية الحقوق والعلوم السياسية جامعة سطيف2، السنة الجامعية 2015/2014، ص04.

اختصاصها الأصلي للسلطة التنفيذية[1]، ومن بين أهم المعايير التي تكرس تمتع هذه الهيئات بالطابع السلطوي، هو تمتعها بسلطة إصدار الأنظمة واتخاذ القرارات الفردية، حيث يؤكد الفقه أن منح وصف السلطة لهيئة ما لا يمكن أن يكون مبررا إلا إذا كانت هذه الهيئة تتمتع بسلطة قرار فعلية بمناسبة ممارسة مهامها.

في حين ذهب مجلس الدولة الفرنسي[2]إلى تبني موقف يقرر من خلاله الإعتماد على معيار التأثير كعامل حاسم لتحديد الطابع السلطوي لأي هيئة، حيث يمكن اعتبار الهيئات التي تملك القدرة على التأثير بأنها سلطات حتى ولو كانت ذات طابع استشاري، إذا كان ذلك يؤثر في اتخاذ القرارات، والسلطة هنا في هذا الإتجاه لا ترتبط فقط بصلاحية القرار أو العقاب أو وضع قواعد تنظيمية عامة ومجردة بل ترتبط أيضا بالآراء والتوصيات والإقتراحات وهو ما أطلق عليه الفقه سلطة التأثير[3]، وهذا المعيار يعبر عن المقاربة السوسيولوجية لمفهوم السلطة إلى جانب المفهوم القانوني الأول .[4]

وترتيبا على ذلك يمكن القول أن مفهوم السلطة التي تتمتع بها هذه الهيئات تشمل:

-المعنى الضيق الذي يقوم على الإعتراف بوجود صلاحية القرار.

- المعنى الواسع الذي يقبل بفكرة السلطة المعنوية من خلال ممارسة تأثير محدد.

ومن هذا المنطلق فإن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تكتسي الطابع السلطوي سواء بالنص القانوني الصريح، حيث سماها المشرع بالسلطة الوطنية أو من خلال صلاحياتها في اتخاذ قرارات ضمن مجالها القطاعي، كالأمر بإغلاق معطيات أو سحبها، وإصدار عقوبات أو تقديم استشارات وهو ما سوف نعرج عليه بالتفصيل في الحديث عن صلاحيات هذه السلطة.

أما عن الطبيعة الإدارية لهذه الهيأة لا تثير أي شك بشأنها، فقد اعترف المشرع صراحة عبر النص القانوني بتصنيفها بأنها سلطة إدارية، ومن ثم فإن القرارات الصادرة عنها هي قرارات ذات طابع إداري تختلف عن تلك الصادرة عن الجهات القضائية.

لكن حتى في ظل غياب النص صراحة على الطابع الإداري لهذه الهيأة، فانه يمكن اعتبارها كذلك من خلال البحث عن المظاهر التي يمكن الإستناد عليها في تصنيف أي هيئة ضبط ما أنها ذات طابع إداري، وهي المظاهر المتعلقة بنشاط الهيئة، أو مدى خضوع القرارات الصادرة عنها لرقابة القضاء الإداري، ومن ثم فإذا عبر المشرع صراحة عن نيته في منح الصفة الإدارية لسلطة ضبط ما فلا يثور أي إشكال، أما إذا

[1]Rachid Zouaimia, les autorités adminstratives indipendentes et la régulation économique, revue Idara n°28, 2004. Page30.

[2]Conseil d'État, les autorités adminstratives indépandentes, rapport public, 2001 Jurisprudence et avis de 2000, ÉTUDES & DOCUMENTS N° 52, la documentation française, paris, p289. Disponible sur le site : http://www.conceil-etat.fr

[3] Michel Gentot, Les autorités adminstratives indépendentes, L.G.D.J La Librairie générale de droit et de jurisprudence (L.G.D.J) 2ème édition, sebtembre 1994 p 36.

[4] خرشي إلهام، مرجع سابق، ص85.

لم يبين المشرع موقفه ولم يضف عليها الطابع الإداري صراحة، فيثور الغموض والشك حول طبيعتها الإدارية وجب البحث حينها عن هذه المظاهر في النصوص القانونية المنشئة لها[1].

وتطبيقا لذلك فإن الصبغة الإدارية للسلطة الوطنية لحماية المعطيات الشخصية مقررة سواء بالنص القانوني الصريح، أو من خلال البحث عن العنصرين السابقين في القانون 07/18 المنشئ للسلطة الوطنية لحماية المعطيات الشخصية.

فمن حيث طبيعة النشاط، فإن كل هيئة تمارس نشاطات ذات طبيعة إدارية من خلال صلاحياتها القانونية وتكون غير تشريعية ولا قضائية ولا من القانون الخاص، فإنها تكتسي الصفة الإدارية، فهيئة الضبط ليست امتدادا للسلطة التشريعية ولا القضائية، بل تكون أقرب للسلطة التنفيذية خاصة إذا مارست الوظيفة التنظيمية بتفويض من المشرع في إطار وظيفة الضبط [2].

كما أن هذه الهيئات حتى وإن لم يحدد المشرع الطابع الإداري لها صراحة، فإنه وعند تفحص المهام الموكلة لها، يتضح أنها تشبه وإلى حد كبير تلك المسندة إلى هيئات الضبط المكيفة صراحة بأنها ذات صبغة إدارية، كاضطلاعها بمهمة السهر على احترام القوانين والتنظيمات المتعلقة بالتخصص الذي أنشأت لأجله، والحرص على مراقبة مطابقة أعمال الجهات المعنية لأحكام هذه القوانين، وكذا صلاحيتها في إصدار قرارات إدارية نافذة، كقرارات منح التراخيص مثلا، وهي نفس الصلاحيات التي أعطاها المشرع للسلطة الوطنية لحماية المعطيات الشخصية ، ومن شأنها إذن إضفاء الصفة الإدارية على هذه الجهة.

وأما من حيث اختصاص القضاء الإداري، فإنه انطلاقا من هذا المعيار، تصنف سلطة إدارية تلك الهيئة التي يحيل المشرع صراحة الإختصاص بالفصل في المنازعات التي تكون طرفا فيها إلى جهات القضاء الإداري، حيث يحدد القانون المنشئ لهذه الهيئة صراحة الجهة القضائية التي بإمكانها النظر في الطعون المرفوعة ضد القرارات الصادرة عنها سواء بسبب تجاوز السلطة أو بمراقبة المشروعية، لذلك فإن القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية نص صراحة بموجب المادة 46 منه على اختصاص مجلس الدولة للنظر في الطعون المرفوعة ضد قرارات السلطة الوطنية لحماية المعطيات الشخصية، وهذا تكريسا لنص المادة 901 من قانون الإجراءات المدنية والإدارية المحددة لاختصاص مجلس الدولة بالفصل في القضايا المخولة له بموجب القانون.

ثانيا: خصائص السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

لقد كانت رؤية المشرع من وراء إحداث السلطة الوطنية لحماية المعطيات الشخصية هي فرض احترام الحياة الخاصة والحريات الفردية والجماعية، تماشيا مع أهداف القانون المحدث لها، والذي يسعى إلى إقرار الضمانات الكفيلة بحماية كل شخص تكون معطياته الشخصية محل معالجة إلكترونية أو يدوية، وبهذا يكون لهذه الهيئة دور ذو أثر بالغ الأهمية في حماية أهم جانب من جوانب الحريات الأساسية للإنسان وهو حقه في الخصوصية المعلوماتية، ومن ثم فإنه من مصلحة جميع الأطراف سواء كمعنيين

[1] Rachid Khalloufi, les institutions de régulation en droit Algérien, Revue IDARA, (numéro spécial) n°2, 2004 page 196.

[2] خرشي إلهام، مرجع سابق، ص81.

بالمعالجة أو مسؤولين عنها، أن تمارس هذه الهيئة صلاحياتها في استقلال تام، وألا تخضع لتأثير أي جهة كانت، وبشكل عام فإن استقلالية الهيئة المختصة بحماية المعطيات هي أهم خاصية تتميز بها، نظرا لطبيعة مهامها ولدورها القيادي الموجه، الموضوعي، المشرف، التوعوي من جهة، ولطبيعة الصلاحيات التي تعطى لها لتحقيق الهدف من حماية المعطيات ذات الطابع الشخصي المحفوظة في ملفات رقمية أو ورقية في القطاعين العام والخاص من جهة أخرى ، وهذه الخاصية تستوجب ضرورة أن تتخذ قراراتها وتصدر توصياتها بشكل مستقل عن أي هيئة أو سلطة وصاية يمكن أن تؤثر عليها.[1]

و انطلاقا من حقيقة كون السلطة الوطنية لحماية المعطيات الشخصية هي من قبيل السلطات الإدارية المستقلة، فإنها بذلك تستمد استقلاليتها من الطبيعة القانونية لهذا الصنف من الهيئات الإدارية، لكن تقدير مسألة استقلالية مثل هذه الهيئات لا يظهر فقط من خلال التسمية، أي من خلال إطلاق وصف السلطة المستقلة عليها، بل يجد هذا المعني تبريره أيضا من خلال غياب كل وصاية أو رقابة رئاسية من قبل السلطة التنفيذية على هذه الهيئات*، لذلك يرى مجلس الدولة الفرنسي أن المشرع الفرنسي عندما كيف اللجنة الوطنية للمعلوماتية والحريات (CNIL) بأنها سلطة إدارية مستقلة لم يقصد أبدا خلق فئة قانونية جديدة في النظام الإداري، بل مجرد جعل هذه الهيئة تستفيد من أكبر قدر ممكن من الإستقلالية لا غير، وذلك من أجل حماية الحريات العامة في ظل تزايد استعمال الإعلام الآلي، لذلك فقد أكد الفقه الفرنسي أن فكرة الإستقلالية هي الخاصية والصفة المميزة للسلطة الإدارية المستقلة والتي منها اللجنة الوطنية للمعلوماتية والحريات، عن الهيئات الإدارية الكلاسيكية،وأن عنصر الإستقلالية، سواء ستقلالية العضوية أو الوظيفية، هو الذي يسمح للسلطة الإدارية المستقلة بتحقيق المهام الموكلة لها ، وهي الحقيقة التي أدركتها أغلب التشريعات الوطنية والدولية المنظمة لمسألة حماية المعطيات الشخصية.

وفي هذاالإطار نجد النظام الأوروبي العام رقم 2016/679 حول حماية المعطيات ذات الطابع الشخصي يؤكد في المادة 51 منه، على أن الهيئات التي ترصد لتطبيق أحكام هذا النظام من أجل حماية الحريات الأساسية وحقوق الأفراد فيما يتعلق بمعالجة وتسهيل التدفق الحر للبيانات الشخصية داخل الإتحاد الأوروبي تعد هيئات عمومية مستقلة.[2]

بالإضافة إلى المادة 28 الفقرة الثانية من التوجيه الأوروبي رقم 95/46، والمادة الأولى الفقرة الثالثة من البروتوكول الإضافي المتعلق بالاتفاقية الأوروبية لحماية المعطيات الشخصية اللتان أكدتا على أن

[1] منى الأشقر، محمودجبور، مرجع سابق، ص 154.

* السلطات الإدارية المستقلة هي عبارة عن هيئات إدارية، لا تخضع للسلطة الرئاسية ولا للوصاية الإدارية ، فهي عكس الإدارة التقليدية حيث تتمتع بالإستقلالية العضوية والوظيفية ولا تخضع إلا للرقابة القضائية .وعرفت كذلك بأنها هيئات عمومية غير قضائية استمدت من القانون مهمة ضبط قطاعات حساسة والسهر على احترام بعض الحقوق، وهي مزودة بضمانات تنظيمية وسلطات تسمح لها بممارسة وظائفها دون أن تكون خاضعة لتأثير الحكومة، كما اعتبر مجلس الدولة الفرنسي السلطات الإدارية المستقلة بأنها هيئات إدارية تتصرف باسم الدولة وتتمتع بسلطة حقيقية دون أن تخضع في ذلك إلى سلطة الحكومة أنظر:

Michel Géntot, op cit, page 16.

[2] Voir l'article 51 du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Journal officiel de l'union européenne L 119/1, applicable en europe depuis le 25 mai 2018.

السلطات المستحدثة لحماية المعطيات الشخصية تمارس صلاحياتها في سبيل هذه المهمة بكل استقلالية، وكذلك المشرع الفرنسي كان ملتزما بمبدأ استقلالية اللجنة الوطنية للمعلومات والحريات (CNIL)، عندما أكد على هذه الخاصية بنص المادة 11 من القانون 17/78 المؤرخ في 06 جانفي 1978 المتعلق بالمعلوماتية والملفات والحريات[1].

وقد جاءت هذه النصوص القانونية تدعيما لما جاءت به المادة 08 من ميثاق الحقوق الأساسية للإتحاد الأوروبي، التي أكدت على أن لكل شخص الحق في حماية البيانات الشخصية التي تتعلق به وفق قواعد محددة يخضع الإذعان لها لمراقبة هيئة مستقلة.[2]

والمشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية لم يحد عن هذا المسار، ولم يجانب موقف التشريعات المقارنة في تأكيده على استقلالية السلطة الوطنية لحماية المعطيات بالنص صراحة على ذلك، بالإضافة إلى تكريسه لمجموعة من المظاهر تبرز مدى تمتع هذه الهيأة بالإستقلالية العضوية والوظيفية.

1) ستقلال العضوي للسلطة الوطنية لحماية المعطيات الشخصية: تتحدد ستقلالية في جانبها العضوي لهذه الهيئة بناء على مجموعة من العوامل ترتبط أساسا بالتشكيلة الجماعية وطبيعة الأعضاء داخل هذه التشكيلة من ناحية، ونظام العهدة الذي يخضع له أعضاء هذه الهيئة من ناحية أخرى، ويشكل هذان الجانبان الأساس الذي يبنى عليه النظام الأساسي لهذه الهيئة والذي يحقق الهدف من ضمان استقلاليتها من جانبها العضوي، وهو عدم إمكانية التحكم في أعضاء هذه الهيئة والتأثير عليهم من طرف السلطات العمومية الأخرى.

1-1) ضمان استقلالية السلطة الوطنية لحماية المعطيات من خلال تشكيلتها: يطرح السؤال عن كيفية ضمان استقلالية السلطة الوطنية من خلال القواعد المتعلقة بتشكيلتها، وهي مسألة مرتبطة في كل الأحوال بأمرين أساسيين، الأول يتعلق بطبيعة هذه التشكيلة في حد ذاتها، ونوع الأشخاص المؤهلين ليكونوا أعضاء فيها، والثاني يرتبط بالجهة التي تملك الحق في تعيين هؤلاء.

إن المبدأ العام الذي يحكم تشكيلة مثل هذه السلطات هو أنها تشكيلة جماعية، وهي خاصية قانونية تفترض وجود مجموعة من الأشخاص من انتماءات وتخصصات ومؤهلات مختلفة ضمن هذه التشكيلة، وهو أمر من شأنه أن يخلق ثقافة الإستقلالية من خلال تمثيل مختلف القطاعات المعنية بمجال تخصص الهيئة، وذلك عن طريق توسيع التشكيلة الجماعية في سبيل تقوية شرعيتها الضامنة لاستقلالها[3]، على

[1] Article 11 la commission nationale de l'informatique et des libertés est une autorité adminstrative indépendente ... ».

[2] ميثاق الحقوق الأساسية للإتحاد الأوروبي، المحرر في مدينة نيس الفرنسية بتاريخ 07 ديسمبر 2000 عن البرلمان الأوروبي، عن الإتحاد الاوروبي وعن اللجنة الأوروبية متوفر على الموقع: http://www.hrlibrary.umn.edu

[3] Jean Pierre Moussy, des autorités de régulation financières et de concurrance, pourquoi, comment, Rapport du C.E.S.F note D EINA information du cnseil economique et social n 124 10janvier les éditions des journaux officiels, 2003, page 68.

اعتبار أن مبدأ تعدد الأعضاء داخل الهيئة ينتج عنه حتما التعدد في الآراء والأفكار، ويصعب في كثير من حيان التأثير على مجموعة كاملة من الأعضاء، بينما يسهل ذلك في مواجهة شخص واحد[1].

وقد كان موقف المشرع الجزائري محاكيا لنظرائه من التشريعات المنظمة لمجال حماية المعطيات الشخصية لاسيما المشرع الفرنسي، حينما تبنى مبدأ التشكيلة الجماعية للسلطة الوطنية لحماية المعطيات الشخصية، حيث تنص المادة 23 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية أن هذه السلطة تتشكل من:

- ثلاث شخصيات من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الإختصاص في مجال عمل السلطة الوطنية.

- ثلاث قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.

-عضو عن كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية.

- ممثل واحد عن المجلس الوطني لحقوق الإنسان.

- ممثل واحد عن وزير الدفاع الوطني.

- ممثل واحد عن وزير الخارجية.

- ممثل واحد عن الوزير المكلف بالداخلية.

- ممثل واحد عن وزير العدل حافظ الأختام.

- ممثل واحد عن الوزير المكلف بالبريد والتكنولوجيات الرقمية.

- ممثل واحد عن وزير العمل والتشغيل والضمان الاجتماعي.

وبهذا يكون عدد أعضاء السلطة الوطنية لحماية المعطيات هو 15 عضوا في حين حدد المشرع الفرنسي عدد أعضاء اللجنة الوطنية للمعلوماتية والحريات بـ 17 عضوا [2].

[1] Hubert delzangles, l'indépendance des autorités de régulation sectorielles communications éléctroniques, énergie et postes, thèse pour obtenir doctorat en droit, école doctorale de droit (E.D école doctorale n.41) université Montesquieu – Bordeaux 4, 2008 page 282.

[2] Voir l'article 13 de la loi 78/17 qui dispose « la commission nationale de l'informatique et des libertés est composée de dix-sept membres :

1) deux députés et deux sénateurs désignés respectivement par l'assemblée nationale et par le sénat

2) deux membres du conseil économique et social, élus par cette assemblée.

3) deux membres ou anciens membres du conseil d'état, d'un grade au moins égal à celui de conseiller. Elus par l'assemblée générale du conseil d'état.

4) deux membres ou ancien membre de la cour de cassation, d'un grade ou moins égal à celui de conseiller élus par l'assemblé générale de la cour de cassation.

ومن هذا المنطلق تعد التركيبة الجماعية للسلطة الوطنية لحماية المعطيات كإحدى السلطات الإدارية المستقلة معيارا فعالا لقياس درجة استقلاليتها [1] و أفضل ضمانة لتكريس هذه الإستقلالية.[2]

وما يزيد من تدعيم الاستقلالية في إطار التشكيلة الجماعية لهذه الهيئة، عامل آخر يتعلق بصفات الأعضاء، وطبيعة تخصصاتهم في المجال الذي ينتمي إليه نشاط السلطة الوطنية، ذلك أن التخصص العلمي من شأنه أن يـ ُ ضعف من سلطة تأثير جهات أخرى على هذه الهيئة، ويساهم في تأسيس مصداقيتها والتي تعني قوتها واستقلاليتها.[3]

وهي المسألة التي حرص المشرع الجزائري على التأكيد عليها، حيث نصت المادة 23 من القانون 07/18 على أن أعضاء السلطة الوطنية يتم اختيارهم حسب اختصاصهم القانوني والتقني في مجال معالجة المعطيات ذات الطابع الشخصي، ويبدو ذلك واضحا من طبيعة الشخصيات التي يختارها رئيس الجمهورية، إذ يكونون من بين ذوي الإ ختصاص في مجال عمل السلطة الوطنية لحماية المعطيات الشخصية، بالإضافة إلى الأعضاء الآخرين الذين هم من الشخصيات المؤهلة لكفاءتها في الميادين القانونية والقضائية من جهة، وتوفرها على خبرة واسعة في ميدان الإعلاميات وقضايا الحريات الفردية من جهة أخرى، وقد تميزت أغلب القوانين المنظمة لمثل هذه الهيئات المكلفة بحماية المعطيات الشخصية توجهها نحو تكريس معيار الخبرة والكفاءة في ذات المجال لدى أعضائها، وقد لاحظنا ذلك في تشكيلة اللجنة الوطنية للمعلوماتية والحريات في فرنسا.

لكن ما نعيبه على المشرع الجزائري أنه وعلى خلاف المشرع الفرنسي الذي لم يدرج من بين أعضاء اللجنة الوطنية للمعلوماتية والحريات (CNIL) أية شخصية تابعة للحكومة، في حين المشرع الجزائ ي نص على وجود 07 أعضاء تابعين لوزارات مختلفة، كممثلين لها داخل تشكيلة السلطة الوطنية لحماية المعطيات الشخصية، وهذا من شأنه إضعاف الإستقلال العضوي للسلطة الوطنية لحماية المعطيات، فالمشرع

---

5) deux membres ou ancien membre de la cour des comptes, d'un grade ou moins égal à celui de conseiller maitre, élus par l'assemblée générale de la cour des comptes.

6) Trois personnalités qualifiés pour leur connaissance de l'informatique, ou des questions touchant aux libertés individuelles nomées pour décrit.

7) deux personnalités qualifiées pour leur connaissance de l'informatique désignées respectivement par le président de l'assemblées nationale et par le président du sénat. »

[1] Aoun charbel, l'indépendance de l'autorité de régulation des communication éléctroniques et des postes, ARCEP thèse pour obtenir le doctorat en droit, université de Gergy Pontoise, Paris 2006, page 36.

[2] تنص المادة الثانية من المرسوم التطبيقي للقانون المغربي 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي أنه تطبيقا لنص المادة 32 من هذا القانون أنه تتكون اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي من 07 أعضاء:

- الرئيس يختاره الملك، و06 أعضاء يتم اقتراحهم كما يلي:
- عضوان من طرف الوزير الأول.
- عضوان من طرف رئيس مجلس النواب.
- عضوان من طرف رئيس مجلس المستشارين.

حسب المادة 28 من القانون الأساسي التونسي عدد 2004/63 المتعلق بحماية المعطيات الشخصية تتركب الهيئة الوطنية لحماية المعطيات الشخصية من 15 عضوا.

[3] Michel Gentot, op.cit page 54.

الفرنسي وزيادة في تدعيم هذا الجانب من الإستقلالية، نصت المادة 14 من القانون الفرنسي 17/78 على أنه لا يمكن لأي عضو أن يجمع بين صفته كعضو في اللجنة الوطنية للمعلوماتية وعضويته في الحكومة[1] لعدم التوافق بين المنصبين، ففي إنجلترا مثلا يعين الأعضاء من بين أصحاب الخبرة ومن شخصيات مستقلة عن السلطة السياسية التي تتولى الحكم، فالغالب أن الدول عموما تميل إلى اختيار الأعضاء من بين الأشخاص الذين يقدمون ضمانا للإستقلالية، ويستوفون الشروط بما يملكونه من خبرات وكفاءات، تمكنهم من إنجاز المهام المطلوب تنفيذها من خلال هذه الهيئة بحسب معايير موضوعية دون انحياز، استنادا إلى قاعدة استقلالية القرار.[2]

كما أنه كان يتوجب على المشرع الجزائري أن ينحو منحى بعض التشريعات التي زادت في تدعيم استقلالية الهيئات المكلفة بحماية المعطيات الشخصية، من خلال استقلال أعضائها وعدم تبعيتهم لأية جهة أخرى، وذلك بالنص على حالات التنافي، والتي تجسد استقلالية السلطة الوطنية لحماية المعطيات من الناحية الفعلية.

فمن الملاحظ أن الغالب الأعم من التشريعات حرصت على عدم تبعية أعضاء الهيئة المكلفة بحماية المعطيات لأي جهة مهما كانت، وذلك تكريسا لاستقلالية الهيئة، فلا يجوز لرئيس الهيئة أو لأي عضو من أعضائها أن يكونوا من الموظفين أو من أصحاب المصالح في المؤسسات أو الشركات العاملة في مجال الإتصالات ومعالجة البيانات، كما لا يجوز أن تتوافر لهم أية مصالح في مؤسسة تمارس هذه الأنشطة سواء كان ذلك بصورة مباشرة أم غير مباشرة.

وقد نصت المادة 26 من القانون 07/18 على ذلك مؤكدة على أنه لا يجوز لرئيس السلطة الوطنية وأعضائها أن يمتلكوا بصفة مباشرة أو غير مباشرة، مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي، مع ملاحظة أن المشرع الفرنسي قد أضاف على ذلك أنه يتوجب على كل عضو من أعضاء اللجنة الوطنية للمعلوماتية والحريات (CNIL) أن يخبر ويبلغ رئيس اللجنة بالمصالح المباشرة أو غير المباشرة التي حصل عليها أو قد يتحصل عليها بسبب وظيفة مارسها أو قد يمارسها، وعلى الرئيس اتخاذ التدابير المناسبة لضمان احترام الإلتزامات في هذا المجال، وهو ما يسمى بحالات التنافي المالي[3]، كما لا يجوز لأي عضو المشاركة في مداولة أو عملية تحقيق ذات صلة بهيئة اكتسب منها منفعة مباشرة أو غير مباشرة أو مارس بها انتدابا أو مهمة، إذا لم يمض أجل 36 شهرا من تاريخ توقف مهامه أو انتدابه بتلك الهيئات.[4]

[1] Article 14 : « la qualité de membre de la commission est incompatible avec celle de membre du gouvernement. »

[2] منى الأشقر، محمود جبور، مرجع سابق، ص 156.

[3] أنظر المادة 14 من القانون الفرنسي رقم 801/2004 المؤرخ في 06 أوت 2004 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ويعدل القانون 17/78 المؤرخ في 6 جانفي 1978 متعلق بالمعلوماتية والملفات والحريات.

[4] أنظر المادة II/14 من القانون الفرنسي 801/2004.

والمشرع المغربي أمعن في تجسيد هذه الإستقلالية من خلال اعتباره أن العضوية في اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، تتنافى*مع مهام متصرف أو مسير أو عضو مجلس إدارة، أو مدير عام وحيد أو عضو مجلس رقابة شركة معالجة للمعطيات ذات الطابع الشخصي،[1] وهو ما يسمى بحالات التنافي الوظيفي.

في حين المشرع الجزائري اكتفى فقط حسب مقتضيات المادة 26 من القانون 07/18 بالنص على عدم جواز امتلاك رئيس السلطة الوطنية وأعضائها بصفة مباشرة أو غير مباشرة، مصالح في أي مؤسسة تمارس نشاطها في مجال معالجة المعطيات ذات الطابع الشخصي، ونأمل أن يشايع المشرع الجزائري نظراءه في هذه المسألة، ويرفع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي إلى أقصى درجات ستقلالية، لارتباط مهامها بجانب مهم من جوانب الحقوق والحريات الفردية وهو حماية الحق في الخصوصية المعلوماتية.

2-1) ضمان استقلالية السلطة الوطنية لحماية المعطيات من خلال نظام العهدة: يعتبر نظام العهدة من خلال الخصائص الأساسية التي يتميز بها، والمتمثلة في تحديد مدة ممارسة الأعضاء لمهامهم وحصانتهم ضد العزل التعسفي من الأنظمة التي تضمن استقلالية السلطة الوطنية لحماية المعطيات الشخصية[2].

فتحديد المدة التي يمارس فيها أعضاء السلطة الوطنية لمهامهم يعد من بين أهم الركائز المعتمد عليها في إبراز طابع الإستقلالية لهذه السلطة من الناحية العضوية، حيث يمارس خلالها هؤلاء الأعضاء مهامهم دون الخوف من خطر عزلهم من طرف السلطة التي قامت بتعيينهم في حالة ما إذا كانت مواقفهم غير متوافقة معها.

ونجد أن أغلب التشريعات المقارنة تذهب إلى تحديد مدة ملائمة تتمكن من خلالها السلطة من الوصول إلى تحقيق أهدافها، وفي نفس الوقت ضمان استقلالية العضوية فيها، حيث أن طول مدة العهدة يكون له أثر سلبي بالنسبة للذين هم في بداية صناعة مسارهم المهني، ويبقى من دون أثر بالنسبة للذين هم في نهاية هذا المسار، وبالتالي لا يكون ذلك محفزا لهم للمحافظة على استقلاليتهم، أما قصر المدة سيكون حافزا لتسييس الأعضاء[3]، والخروج بهم عن الإستقلالية، فإذا كانت العهدة القصيرة لها سلبياتها على استقرار

*إن منطق الإستقلالية الذي يحكم السلطات الإدارية المستقلة في مواجهة السلطة السياسية يؤدي إلى إدراج مبدأ التنافي بين وظيفة العضو في السلطة الوطنية لحماية المعطيات الشخصية باعتبارها تندرج ضمن هذه الفئة من السلطات الإدارية وبين وظيفة حكومية أو برلمانية من جهة، وكذا بين العضوية في هذه السلطة والعمل في مؤسسات أو شركات في قطاع ذي صلة بمجال السلطة، وذلك لحماية العضو من خطر الإلتقاء مع المصالح في القطاع المعني أو امتلاك مصالح في هذا القطاع.

[1] أنظر المادة 35 من القانون المغربي 09/08 المؤرخ في 18 فيفري 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 5711 مؤرخة في 23 فيفري 2009.

[2] Rachid Khelloufi, les institutions de régulation en droit Algerien Revue Idara (numéro spécial) n°28, 2004 page 93. « Le mandat rest la garantie d'indépandance des autorités de régulation dans l'exercice de la fanction de membre d'une autorité de régulation »

[3] Marie José Guédon, le désordre des autorités adminstratives indépendantes : L'exemple du secteur economique et financier, recherche publiée avec le soutien de la maison recherche droit et jutice, sous la direction de nicole decoupman, universitée de pécardie jules verne, P 77. disponible sur le site : http://www.céprisca.fr

الأعضاء واستمرارية عمل الهيئة لتحقيق أهدافها، فإن المدة الطويلة لها أيضا مساوئ من خلال إمكانية قيام الأعضاء بنسج علاقاتتحيد بهم عن الإستقلالية في أداء مهامهم .

لذلك نجد المشرع الجزائري قد لجأ إلى مثل هذه الطبيعة في تعيين أعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، حيث تنص الفقرة الأخيرة للمادة 23 من القانون 07/18 على أن رئيس وأعضاء هذه السلطة يعينون بموجب مرسوم رئاسي لعهدة مدتها 5 سنوات، وهي نفس المدة التي حددها المشرع الفرنسي لعهدة أعضاء اللجنة الوطنية للمعلوماتية والحريات (CNIL)، ما عدا الأعضاء المقترحين من بين نواب الجمعية العمومية ومجلس الشيوخ والمجلس الإقتصادي الإجتماعي، والذين تكون عضويتهم باللجنة الوطنية مرتبطة بمدة عضويتهم بمناصبهم الأصلية*، مع الإشارة إلى أن المشرع الفرنسي ومن خلال المادة 1/1 من المرسوم 1309/2005 المؤرخ في أكتوبر 2005 المتعلق بتطبيق قانون المعلوماتية والملفات والحريات17/78، المعدل بالمرسوم رقم 356/2019 المؤرخ في 29 ماي 2019 نص على أن أعضاء اللجنة الوطنية للمعلوماتية والحريات المذكورين في الحالات 02 إلى 07 بالمادة 13 من قانون 17/78 يجدد نصفهم كل سنتين ونصف، وكان هذا استجابة لما ورد في اللائحة الأوروبية العامة لحماية المعطيات (2016/679) حيث نصت المادة 54 منها على أن مدة العضوية في السلطة المكلفة بحماية المعطيات الشخصية لا تقل عن 04 سنوات يكون جزء منها لفترة قصيرة من أجل ضمان تعيينات متداخلة تكون ضرورية لحماية استقلالية السلطة .

ولقد نص المشرع الفرنسي صراحة على الآثار المترتبة على عضوية اللجنة الوطنية للمعلوماتية للحريات استنادا على نظام العهدة، وهي عدم جواز إنهاء مهام العضو من أي جهة كانت، إلا في حالة عدم أهليته لأداء مهامه، ويكون ذلك من قبل السلطة نفسها[1]، وهو أمر من شأنه تقوية مركز الأعضاء داخل السلطة لممارسة مهامهم بحياد ونزاهة، إذ يكون أعضاء السلطة أو الهيئة المكلفة بحماية المعطيات متأكدين أنهم لن يعزلوا خلال عهدتهم المحددة، وهو أمر فيه طمأنة لأي عضو في السلطة بأنه يستطيع ممارسة مهامه بكل استقلالية ودون تخوف من تحكم السياسيين أو جماعات المصالح، وتضعه في منأى عن التأثير من أي جهة كانت، وبالمحصلة تكون السلطة بعيدة عن تلقي أي تعليمات من أي جهة ، كما لا يمكن معارضة أعمالها لأي سبب من الأسباب .

* Voir l'article 13/II de la loi 2004/801 du 06 aout 2004 relative à la protection des personnes physiques à l'égard des traitementes de données à caractère personnel et modifiant la loi n°78/17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés.
ونرى أن المشرع الجزائري كان ينبغي عليه أن يأخذ بمثل هذا النص ، ذلك أن العضوين المختارين من طرف رئيس المجلس الشعبي الوطني أو رئيس مجلس الأمة للإلتحاق بعضوية السلطة الوطنية لحماية المعطيات الشخصية (حسب الحالة الثالثة من المادة 23 من القانون 07/18) قد تكون المدة الباقية من عهدتهما بالمجلسين أقل من 05 سنوات، مدة العهدة بالسلطة الوطنية ومن ثم يكون تواجدهم كأعضاء في هذه السلطة بعد انتهاء صفتهم الأصلية غير مبرر قانونا، لذلك نقترح إضافة فقرة إلى المادة 23 يمكن أن تنص على أنه في حالة انتهاء عهدة النائب أو عضو مجلس الأمة المعينين في السلطة الوطنية، فانه يعوض بعضو آخر بنفس الشروط السابقة للمدة المتبقية من عضوية السلطة الوطنية .

[1] Voir l'article 13/II-3 « sauf démission, il ne peut être mis fin aux fonctions d'un membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit ».

وفي هذا الإطار أيضا نجد أن المشرع الفرنسي أشار إلى أن اللجنة الوطنية للمعلوماتية والحريات (CNIL) تعمل بحرية على انتخاب رئيسها والهيئة الدائمة المكونة من الرئيس ونوابه وثلاث أعضاء آخرين من بين أعضائها، وهو ما يجعل هذه الهيئة تتمتع بالاستقلالية الحقيقية[1]، وهذا على خلاف ما هو عليه الشأن في القانون الجزائري 07/18 أين يعين رئيس السلطة الوطنية لحماية المعطيات الشخصية بمرسوم رئاسي.

وتجدر الإشارة إلى أن عدم قابلية العهدة للتجديد فيه تكريس حقيقي لاستقلالية السلطة الوطنية لحماية المعطيات في مواجهة السلطة التنفيذية، حتى لا يطمع أي عضو في هذا التجديد عند انتهاء عهدته، وتكون هذه المسألة أداة ضغط في يد السلطات العمومية * يمكن أن تمارسها على الأعضاء، خاصة الراغبين منهم في الحصول على عهدة ثانية، وهي الرغبة التي تدفع بهؤلاء إلى البحث أو السعي إلى إرضاء السلطة التي تملك التعيين، لكن المشرع الجزائري خرج عن هذه الضمانة بالإشارة إلى إمكانية تجديد عهدة أعضاء السلطة الوطنية، وهو بذلك يكون قد ساير نفس الإتجاه الذي أخذ به المشرع الفرنسي، إلا أن هذا الأخير أكد على أن التجديد يكون لمرة واحدة فقط[2] وأن العهدة في كل الحالات لا يمكن أن تجاوز 10 سنوات، على خلاف الصياغة التي جاء بها المشرع الجزائري في الفقرة الأخيرة للمادة 23 من القانون 07/18 التي قد يفهم منها أن تجديد العهدة قد يكون لأكثر من مرة[3].

2) ستقلال الوظيفي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: كغيرها من السلطات الإدارية المستقلة، فإن من بين الأدوات التي يمكن من خلالها الكشف عن رغبة المشرع في منح السلطة الوطنية لحماية المعطيات استقلالا وظيفيا، هي تمتعها بالشخصية المعنوية وبالإستقلال الإداري والمالي.

ومن ثم فإن مظاهر ستقلالية الوظيفية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، منها ما يتعلق بالإستقلال القانوني من خلال تمتع هذه السلطة بالشخصية المعنوية وصلاحياتها لوضع نظامها الداخلي بنفسها دون تدخل أي جهة أخرى في ذلك، ومنها ما يتعلق باستقلالها من الجانب المالي، بحيث يكون لها ذمة مالية مستقلة عن ذمة الدولة وقدرتها على تمويل نشاطاتها بذاتها، بالإضافة إلى استقلالها الإداري من خلال غياب الرقابة الإدارية من قبل سلطة رئاسية أو وصائية عليها.

وعلى هذا الأساس نصت المادة 22 من القانون 07/18 أن السلطة الوطنية لحماية المعطيات الشخصية تتمتع بالشخصية المعنوية والإستقلال المالي والإداري.

---

[1] Voir Farid Bouguettaya, op.cit. page 103.

* وإذا قسنا على لجنة عمليات البورصة التي تعد من ذات الطبيعة القانونية للسلطة الوطنية لحماية المعطيات الشخصية (سلطة إدارية مستقلة) فإن المجلس الدستوري الفرنسي اعتبر أن المشرع قد استهدف بتكريسه قاعدة عدم جواز تجديد عهدة رئيس هذه اللجنة بمثابة ضمانة لاستقلالية هذه السلطة.

[2] L'article 13/II de la loi 2004/801

« Le mandat des membres de la commission – est de cinq ans il est renouvelable une fois »

[3] المادة 13/ الفقرة الأخيرة من القانون 07/18 " يعين الرئيس وأعضاء السلطة الوطنية لعهدة مدتها 05 سنوات قابلة للتجديد".

2-1) ستقلال القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: يتمثل الاستقلال القانوني للسلطة الوطنية لحماية المعطيات الشخصية في تمتعها بالشخصية المعنوية واستقلالها في وضعها لنظامها الداخلي.

أ) تمتع السلطة الوطنية لحماية المعطيات الشخصية بالشخصية المعنوية: إن اعتراف المشرع للسلطة الوطنية لحماية المعطيات بالشخصية المعنوية عامل هام ومؤثر في قياس درجة استقلالية هذه الهيئة ويساعد في إظهار هذه الاستقلالية من جانبها الوظيفي، وذلك بالنظر إلى الآثار المترتبة على التمتع بالشخصية المعنوية، ومن أهم النتائج المترتبة عن الإ عتراف بالشخصية المعنوية:

- الحق في التقاضي: إن تمتع السلطة الوطنية لحماية المعطيات بالشخصية المعنوية يكسب النائب الذي يعبر عن إرادتها وهو رئيس السلطة، صفة التقاضي باسمها، سواء كمدعية أو مدعى عليها في حالة ما إذا رفعت طعون ضد القرارات التي تصدرها أمام القضاء.

- الذمة المالية: يترتب أيضا عن تمتع هذه السلطة الوطنية بالشخصية المعنوية استقلال ذمتها المالية، مما يجيز لها التصرف في ممتلكاتها المالية المنقولة أو العقارية بكل حرية في حدود القانون وفي إطار تحقيق أغراضها.

ب) تمتع السلطة الوطنية بالحق في وضع نظامها الداخلي: نص المشرع الجزائري من خلال الفقرة الأخيرة للمادة 22 من القانون 07/18 أن السلطة الوطنية لحماية المعطيات الشخصية تعد نظامها الداخلي الذي يحدد كيفيات تنظيمها وسيرها وتصادق عليه، ويعتبر منح أي سلطة إدارية وطنية صلاحية إعداد نظامها الداخلي مظهرا جوهريا معبرا عن الإ ستقلال الوظيفي لهذه الهيئة عن السلطات العمومية،[1] وذلك اعتبارا بالأساس على ما يحتويه النظام الداخلي من قواعد تتعلق ببعض الإجراءات الداخلية الهامة مثل كيفية عزل العضو الذي يكون في حالة من حالات التنافي، أو تلك الإجراءات التي تبين كيفية سير المداولات ونظام التصويت وفترات المداولات، بالإضافة إلى تحديد طريقة التنظيم الداخلي وطريقة تسيير الهيئة والقانون الأساسي للمستخدمين ونظام الأجور، ومن هنا تتجلى استقلالية السلطة الوطنية من خلال حريتها في اختيار مجموع تلك القواعد لإدراجها ضمن نظامها الداخلي دون مشاركتها مع أي جهة أخرى، وبالخصوص السلطة المركزية.

ونجد في بعض الحالات أن القانون ينص على إشراك السلطة التنفيذية في عملية إعداد السلطات الإدارية المستقلة لنظامها الداخلي من خلال منحها صلاحية المصادقة على النظام الداخلي بعد إعداده، إلا أن المشرع الجزائري أعطى للسلطة الوطنية لحماية المعطيات الشخصية استقلالية كاملة لا تخضع فيها لأي رقابة من طرف السلطة التنفيذية في مجال إعدادها لنظامها الداخلي، بحيث تكون صاحبة السلطة في إعداده وكذا المصادقة عليه، في حين نجد المشرع المغربي مثلا يذهب إلى النص في المادة 39 من القانون رقم 08/09 المتعلق بحماية الأشخاص الذاتيين في مجال معالجة المعطيات الشخصية على أن اللجنة الوطنية لحماية المعطيات الشخصية تعد نظامها الأساسي الذي يعرض على الحكومة من أجل

[1] خرشي إلهام، مرجع سابق، ص184.

التصديق عليه، ومؤكدا ذلك من خلال المادة 06 من المرسوم التطبيقي 09/165 المتعلق بتطبيق القانون 08/09 حيث تضع اللجنة الوطنية نظامها الداخلي الذي يحدد على الخصوص شروط عملها وتنظيمها، وتبلغه إلى الوزير الأول أو إلى السلطة الحكومية التي يحددها، بهدف الموافقة عليه ونشره في الجريدة الرسمية .

2-2) ستقلال المالي للسلطة الوطنية لحماية المعطيات الشخصية: يعتبر الاستقلال المالي من بين أهم الركائز التي يقوم عليها الإستقلال الوظيفي لأي سلطة إدارية مستقلة، وقد نص المشرع في القانون 07/18 على أن السلطة المستقلة لحماية المعطيات لشخصية تتمتع بالإستقلال المالي، وتتجلى مظاهر هذا ستقلال المالي لأي سلطة إدارية مستقلة، في امتلاك هذه الهيئة لمصادر تمويل ميزانيتها خارج الإعانات التي تقدمها الدولة (التمويل الذاتي)، والإستقلالية في اقتراح ميزانيتها ثم تنفيذها وكذا ستقلالية في التسيير.

غير أن الإستقلال المالي للسلطة الوطنية لحماية المعطيات الشخصية لا يكاد يظهر إلا في الحالتين الأخيرتين، ذلك أن هذه الأخيرة تعتمد كليا على إعانة الدولة، ويقتصر مصدر تمويلها على الميزانية السنوية التي تمنحها الدولة في قانون المالية، وليست لديها مصادر تمويلية خاصة كالأتوات التي تحصلها بعض الهيئات من الأعمال والخدمات التي تقدمها، فالاستقلال المالي يلزم وجود تمويل كلي أو على الأقل شبه كلي بواسطة موارد ذاتية مغطاة أساسا من الإقتطاعات المالية التي تفرضها الهيئة، حيث نص المشرع صراحة في المادة 3/22 من القانون 07/18 على أن ميزانية السلطة الوطنية لحماية المعطيات تقيد في ميزانية الدولة، أي ارتباط تمويل هذه السلطة باقتطاع من ميزانية الدولة، وهو أمر من شأنه أن يمس بمظهر من مظاهر التكريس القانوني للاستقلال المالي للسلطة الوطنية لحماية المعطيات الشخصية.

وحتى بالنسبة لمسألة اقتراح الميزانية، فإنه وإن كانت للسلطة الوطنية لحماية المعطيات الشخصية الحرية في إعداد ميزانيتها إلا أن ذلك محكوم بالمبدأ العام في التشريع الجزائري وهو مرور اقتراح الميزانية عبر الحكومة للمصادقة عليه.

إضافة إلى ذلك فإن التسيير المالي والمحاسبي للسلطة الوطنية يخضع للمراقبة المالية البعدية طبقا للتشريع المعمول به[1]، وذلك من خلال الخضوع إما إلى رقابة المفتشية العامة للمالية[2]، أو لرقابة مجلس المحاسبة[3]، فرغم أن القوانين المنظمة لمجلس المحاسبة والمفتشية العامة للمالية لم تأخذ ضمن نصوصها

[1] تنص المادة 3/22 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:"تقيد ميزانية السلطة الوطنية في ميزانية الدولة وتخضع للمراقبة المالية طبقا للتشريع المعمول به".

[2] المادة 02 من المرسوم التنفيذي رقم 272/08 المؤرخ في 08 سبتمبر 2008 المحدد لصلاحيات المفتشية العامة للمالية على أن المفتشية العامة للمالية تمارس رقابة على التسيير المالي والمحاسبي لمصالح الدولة والجماعات الإقليمية وكذا الهيئات والأجهزة والمؤسسات الخاضعة لقواعد المحاسبة العمومية.

[3] تنص المادة 02 من الأمر رقم20/95 المؤرخ في 17 جويلية 1995 المعدل بالأمر رقم 02/10 المؤرخ في 26 أوت 2010 المتعلق بمجلس المحاسبة: على أن مجلس المحاسبة يعتبر المؤسسة العليا للرقابة البعدية لأموال الدولة والجماعات الإقليمية والمرافق العمومية، وهو بهذه الصفة يدقق في شروط استعمال الهيئات الموارد والوسائل المادية والأموال العامة التي تدخل في نطاق اختصاصه، ويقيم تسييرها ويتأكد من مطابقة عمليات هذه الهيئات المالية والمحاسبية للقوانين والتنظيمات المعمول بها.

صراحة هذه الفئة الجديدة من الهيآت الإدارية، إلا أنها غير مستثناة من رقابتها باعتبارها شخصا معنويا إداريا يستفيد من اقتطاع مالي تابع لميزانية الدولة، وإن كنا نرى أنه لإعطائها نوعا من الإستقلال المالي في هذا الجانب أن ينص المشرع صراحة على إخضاعها للمراقبة المالية من طرف مجلس المحاسبة فقط، دون المفتشية العامة للمالية لكون هذه الأخيرة تابعة لوزارة المالية[1]، على خلاف مجلس المحاسبة الذي يعد بمثابة هيئة قضائية [2]، وهذا ما اتجه إليه المشرع الفرنسي حينما نصت المادة 12 من القانون 801/2004 المتعلق بحماية المعطيات الشخصية، على عدم تطبيق أحكام القانون المتعلق بالمراقبة المالية المؤرخ في 10 أوت 1992 على التسيير المالي والمحاسبي للجنة الوطنية للمعلوماتية والحريات (CNIL) وأخضعها صراحة للرقابة المالية لمجلس المحاسبة فقط [3].

3-2) ستقلال الإداري للسلطة الوطنية لحماية المعطيات الشخصية:يتضح مدلول الإستقلال الإداري لهذه السلطة كغيرها من السلطات الإدارية المستقلة من خلال غياب الرقابة الإدارية عليها، حيث أن المشرع لم يخضع السلطة الوطنية لحماية المعطيات الشخصية لأي رقابة رئاسية أو وصائية من أي جهة كانت *، وإنما أخضعها فقط إلى الرقابة المالية وكذلك إلى الرقابة القضائية.

فبالرجوع إلى القانون 07/18 المنشئ للسلطة الوطنية لحماية المعطيات الشخصية، نلاحظ عدم وجود أية إشارة فيه لتمتع السلطة المركزية بحق إلغاء أو تعديل قرارات تلك الهيئة، أو الحلول محلها في اتخاذ قرارات تدخل في اختصاصها، كما أن مداولات السلطة الوطنية تعتبر صحيحة بمجرد استكمال إجراءات التداول والتصويت عليها، حيث لا نجد في طيات القانون 07/18 اشتراطه المصادقة على مداولاتها من أي جهة أخرى، ومن ثم فإنه يمكن القول بأن قراراتها تكون متمتعة بالقوة التنفيذية دون حاجة إلى تدخل السلطة السياسية، ناهيك عن كون أعضاء السلطة الوطنية يتمتعون بكامل الإستقلالية عن الجهات الأصلية التي ينتمون إليها، إذ يتداولون ويصوتون بكل حرية على المسائل المعروضة وفق ما يحدده القانون والنظام الداخلي للسلطة .

وتبقى الوسيلة الأساسية لفرض نوع من الرقابة الإدارية من قبل السلطة المركزية على السلطة الوطنية لحماية المعطيات الشخصية هي التقارير السنوية، والتي تعد إحدى الطرق الهامة والجوهرية التي يتم من خلالها توضيح كيفية سير النشاطات داخل هذه السلطة، وتفصيل الأمور والمسائل المتعلقة بأدائها لمهامها.

---

[1] تنص المادة 13 من المرسوم التنفيذي 272/08 المحدد لصلاحيات المفتشية العامة للمالية " تحدد عمليات الرقابة للمفتشية العامة للمالية في برنامج سنوي يعد ويعرض على الوزير المكلف بالمالية".

[2] تنص المادة 03 من الأمر 20/95 المتعلق بمجلس المحاسبة " مجلس المحاسبة مؤسسة تتمتع باختصاص إداري وقضائي في ممارسة المهمة الموكلة إليه".

[3] L'article 12 : « la commission nationale de l'informatique et des libertés dispose des crédits nécessaires à l'accomplissement de ses missions, les dispositions de la loi du 10 aout 1992 relative au contrôle financier ne sont applicables à leur gestion, les comptes de la commission sont présentés au contrôle de la cour des comptes ».

* تتجسد الرقابة الإدارية في إحدى الصورتين: إما أن تكون رقابة رئاسية سلمية تمارس داخل نظام المركزية الإدارية، وتأخذ عدة أوجه تتمثل في الرقابة السابقة من خلال توجيه التعليمات والأوامر للمرؤوس، والرقابة البعدية من خلال التصديق والإلغاء والسحب والحلول، وإما أن تكون رقابة وصاية تمارس من قبل السلطة المركزية على السلطات اللامركزية وتكون في إطار مبدأ لا وصاية إلا بنص قانوني.

والجهة التي ترفع إليها السلطة الوطنية لحماية المعطيات الشخصية تقاريرها، هي رئيس الجمهورية باعتبارها تنشؤ لديه[1]، وفي فرنسا تنشر المداولات والتقارير السنوية للجنة الوطنية للمعلوماتية والحريات (CNIL) في الجريدة الرسمية [2]، بالإضافة إلى رفع تقاريرها كل سنة إلى كل من رئيس الجمهورية والوزير الأول وكذا إلى البرلمان.[3]

الفرع الثاني: صلاحيات السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تضطلع السلطة الوطنية لحماية المعطيات الشخصية بدور رئيسي يرتبط بمواكبة ومرافقة من يقومون بمعالجة المعطيات الشخصية لمساعدتهم على الإلتزام بأحكام القانون، ومساعدة أصحاب البيانات الشخصية محل المعالجة في ممارسة حقوقهم التي يقرها لهم القانون، فضلا عن دورها في دراستها لتأثير التطورات التقنية واستخداماتها على الخصوصية المعلوماتية، بالإضافة إلى اهتمامها بوضع الأطر التنظيمية الأنسب و الأكثر فعالية لضمان خصوصية الأفراد في مواجهة المخاطر الناشئة عن معالجة معطياتهم الشخصية، وضمان عدم انطواء استعمال تكنولوجيا الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة .

إن فعالية هذا الدور المنوط بالسلطة الوطنية لحماية المعطيات الشخصية، يتوجب أن تكون لها سلطات واسعة تمكنها فعلا من الإشراف والرقابة السابقة واللاحقة على توفير حماية للمعطيات الشخصية، وفي سبيل ذلك منح المشرع الجزائري مجموعة من الصلاحيات ذات طبيعة مختلفة تقوم بها السلطة الوطنيةفي إطار عملها على حماية المعطيات الشخصية ذات الطابع الشخصي والمحددة بالقانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية، وهو ما سوف نوضحه فيما يلي:

أولا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في الإشراف والرقابة السابقة:

يتطلب توفير الضمانات الوقائية لحماية المعطيات الشخصية في مواجهة نظم المعالجة، وضع القواعد القانونية الموضوعية والإجرائية التي تمنح السلطة المكلفة بمهمة الإشراف والرقابة في مجال حماية المعطيات الشخصية صلاحيات واسعة للتأكد من استيفاء الشروط والضوابط المحددة قانونا لإنشاء هذه النظم وكذا تناسب أهدافها مع موجبات القانون.

والمشرع الجزائري في القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي أخذ بمبدأ الإشراف والرقابة السابقة على إنشاء نظم المعالجة الآلية للمعطيات الشخصية، حيث كلف السلطة الوطنية لحماية المعطيات الشخصية في هذا الصدد بالسهر على مطابقة

[1] تنص المادة 25/ الفقرة الأخيرة من قانون 07/18 أن السلطة الوطنية لحماية المعطيات تعد تقريرا سنويا حول نشاطها ترفعه إلى رئيس الجمهورية،

[2] Voir le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78/17 du 6 janvier relative à l'informatique, aux fichiers, et aux libertés.

[3] L'article 11 de la loi 2004/801 préscité.

معالجة المعطيات الشخصية لأحكام القانون، وذلك من خلال مجموعة من المهام والأدوار تتوزع على ما هو إداري، إعلامي، تنظيمي، رقابي واستشاري واستشرافي.[1]

1) المهام الإدارية والتنظيمية: تتمثل مهام السلطة الوطنية في هذا الإطار حسب المادة 25 من القانون 07/18

- تلقي التصريحات من الجهات المسؤولة عن المعالجة قبل إقدام هذه الأخيرة على أي عملية لمعالجة لمعطيات شخصية، وفق المضمون المحدد بنص المادة 14 من القانون 07/18.

- تحديد قائمة بأصناف المعالجات للمعطيات ذات الطابع الشخصي والتي ليس من شأنها الإضرار بالحياة الخاصة للأشخاص المعنيين.

- منح التراخيص المسبقة للمسؤولين عن المعالجة عند إخضاع المعالجة المعنية لهذا النظام في إطار أحكام المادة 17 من القانون 07/18.

- منح الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج، بحيث لا يجوز لأي مسؤول عن المعالجة نقل معطيات شخصية إلى دولة أجنبية دون ترخيص من السلطة الوطنية، ويكون لها في سبيل ذلك مهمة تقدير ما إذا كانت هذه الدولة الأجنبية تضمن قدرا كافيا من الحماية أم لا.

كما يكون في إطار منح التراخيص أيضا، من مهام السلطة الوطنية منح الترخيص المتعلق بالربط البيني للملفات التابعة لأشخاص معنوية تسير مرافقا عمومية لأغراض مرتبطة بالمنفعة العمومية.

ويدخل في إطار المهام الرقابية والإشرافية السابقة للسلطة الوطنية أن تحدد الشروط والضمانات المرتبطة بحقوق الشخص المعني بالمعالجة، والتي ينبغي على كل مسؤول عن المعالجة احترامها عندما ترتبط هذه المعالجة بمجالات متعلقة بحرية التعبير والصحة، والشغل والبحث التاريخي والإحصائي والعلمي.

والمشرع الفرنسي من خلال المرسوم 2005/1309 المؤرخ في 20 أكتوبر 2005 المتعلق بتطبيق القانون 17/78 يعطي لجنة المعلوماتية والحريات (CNIL) إمكانية وضع معايير للتصاريح حسب مقتضيات المادة 24 من القانون 17/78.

- نشر التراخيص الممنوحة والتصريحات المقدمة للسلطة الوطنية وحتى الآراء المدلى بها في سجل وطني، هذا السجل الذي تنص عليه المادة 28 من القانون 07/18 والذي تقيد فيه كذلك جميع الملفات التي تكون السلطة العمومية والخواص مسؤولين عن معالجتها، وفي إطار المهام التنظيمية أيضا منح المشرع السلطة الوطنية مهمة تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.[2]

[1] انظر المادة 25 من القانون 07/18.

[2] انظر المادة 25 من القانون 07/18.

وفي القانون الفرنسي 17/78 المتعلق بالمعلوماتية والملفات والحريات المعدل بالقانون 801/2004 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية، منح المشرع للجنة الوطنية للمعلوماتية والحريات (CNIL) مهمة إبداء الرأي المعلل عندما يتعلق الأمر بتنفيذ معالجة بيانات شخصية نيابة عن الدولة، تتعلق هذه المعالجة بأمن الدولة والأمن العام، أو التي تهدف إلى منع الجرائم أو التحقيق فيها، أو تنفيذ الإدانات الجزائية والتدابير الأمنية، كون الترخيص بشأن هذه المعالجات يكون من طرف مجلس الدولة[1] بعد ر أي من اللجنة الوطنية للمعلوماتية والحريات، و تقدم هذه اللجنة رأيها لمجلس الدولة قبل إصداره إذنا بالمعالجات المنفذة نيابة عن الدولة من طرف شخص اعتباري خاص يدير خدمة عامة.[2]

كما نجد المشرع المغربي أيضا في القانون 09/08 المتعلق بحماية الأشخاص الذاتيين في مجال معالجة البيانات ذات الطابع الشخصي يكلف اللجنة الوطنية لحماية المعطيات بمهام إبداء الرأي أمام الحكومة أو البرلمان بشأن مشاريع أو مقترحات القوانين أو مشاريع النصوص التنظيمية ذات الصلة بمعالجة المعطيات ذات الطابع الشخصي التي تعرض عليها، وكذا إبداء رأيها أمام السلطات المختصة بشأن مشاريع النصوص التنظيمية الصادرة من أجل إنشاء ملفات متعلقة بالمعطيات ذات الطابع الشخصي المجمعة و المعالجة من أجل الوقاية من الجرائم والجنح، وفي هذا الجانب التنظيمي أيضا تهتم السلطة الوطنية بأخلقة عمليات المعالجة للمعطيات الشخصية، من خلال مهمتها المتعلقة بوضع المعايير وقواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي تكون بمثابة مقاييس مرجعية للحماية يمكن الإ عتماد عليها في تقييم الإلتزام بحماية المعطيات الشخصية.

2) المهام علامية والإ ستشارية: تتمحور هذه المهام بدرجة أساسية حول توفير المعلومات الضرورية للمهنيين وأصحاب البيانات على السواء، لفهم مقتضيات القانون من أحكام تتعلق بحقوقهم والتزاماتهم والإحاطة بكافة أوجه وإمكانيات ممارسة الحقوق وأساليب تفعيلها، وتقديم استشارات في مجال اختصاصها للجهات المعنية بمعالجة المعطيات الشخصية، وذلك بغرض تبسيط بعض القواعد الإجرائية وشرح تقاطعات القوانين التي تطال حماية المعطيات الشخصية، وقد ألزمت المادة 28 من الإرشاد الأوروبي 46/95 السالف ذكره الدول الأوروبية بالنص في قوانينها الداخلية على ضرورة مراجعة هيئة حماية البيانات في كل مرة يتم اللجوء إلى اتخاذ تدابير إدارية أو وضع نصوص تنظيمية، يمكنها أن تؤثر على حماية البيانات الشخصية والحقوق والحريات، وقد منح المشرع الجزائري لهذه الغايات السلطة الوطنية حسب نص المادة 25 من القانون 07/18 :

- إعلام الأشخاص المعنيين بالمعالجة والمسؤولين عنها بحقوقهم وواجباتهم بطرق مختلفة، كأن تحفز أنشطة تربوية وتوعوية، أو إصدار منشورات أو كتيبات إرشادية توجه للمستخدمين العاديين، أو لفئة

[1] المادة 26 من القانون 17/78 المتعلق بالمعلوماتية والملفات والحريات المعدل بالقانون 801/2008 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي.

[2] المادة 27 من نفس القانون.

المسؤولين عن المعالجة، أو عن طريق تدخلها المباشر في حال بروز صعوبات على مستوى تطبيق القانون[1]، أو تنظيم دورات وملتقيات علمية بمشاركة مختصين في المجال، والخروج منها بتوصيات تخدم مجال حماية المعطيات الشخصية والتحسيس بخطورة الإعتداء عليها.

-تقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة، وهذا في سبيل مساعدتهم على التقيد بأحكام قانون حماية البيانات، والمشرع الفرنسي أشار في المادة 11 من القانون 2004/801[2] أن اللجنة الوطنية للمعلوماتية والحريات تلتزم بالإجابة على طلبات الرأي المقدمة إليها من السلطات العمومية وكذا القضائية، وتقديم النصائح للأشخاص والهيئات التي تعالج أو تباشر في معالجة آلية لمعطيات ذات طابع

ثانيا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في الإشراف والرقابة اللاحقة:

تستمد السلطة الوطنية صلاحياتها هذه من فلسفة وجودها كسلطة إشراف ورقابة على حماية المعطيات ذات الطابع الشخصي في مواجهة الأنظمة المعلوماتية، و لذلك فانه ينبغي أن لا تقتصر صلاحيات هذه السلطة على مجرد مهام إشرافية على إنشاء نظم المعالجة، بل يجب أن تمتد إلى ما بعد إنشائها، وذلك من خلال منح هذه السلطة مجموعة من السلطات اللازمة للإيفاء بدورها الإشرافي و الرقابي اللاحق لمراقبة مدى احترام الجهات القائمة بالمعالجة لأهداف المعالجة، ومن ثم اتخاذ القرارات اللازمة لتوجيه المعالجة وتنفيذها وفقا للقانون، وتلقي الشكاوى والطعون من المعنيين والتحقيق بشأنها وإبلاغ النيابة العامة في حال اكتشاف المخالفات ذات الطابع الجزائي.

والدراسات الفقهية تفيد أن العديد من الباحثين في هذا المجال يرحبون بالتحول نحو التركيز على الرقابة اللاحقة، بدلا من فرض ضوابط مسبقة ثقيلة محفوفة في كثير من الأحيان بالتفاصيل الشكلية التي من شأنها الإبطاء في معالجة المعطيات الشخصية في ظل مجتمع المعلومات، بسبب الكثير من الشكليات والمتطلبات الإجرائية، ومن ثم توفير العديد من التبسيطات الإجرائية السابقة على إنشاء نظم المعلومات في مقابل زيادة الضوابط اللاحقة ومن ثم الرقابة اللاحقة.[3]

والمشرع الجزائري في هذا الصدد منح السلطة الوطنية لحماية المعطيات سلطات نوردها كما يلي:

[1] أنظر البند 12من المادة 25 من القانون 07/18.

[2] منى الاشقر جبور، محمود جبور، مرجع سابق، ص158.

[2] « La commission nationale de l'informatique et des libertés... réponds aux demandes d'avis des pouvoirs publics et le cas échéant, des juridictions et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ».

[3] Guy braibant, données personnelles et société de l'information, Rapport au premier ministre sur la transposition en droit français de la directive 95/46, la documentation française 3 mars 1998, disponible sur le site :
https://www.vie-publique.fr/sites/default/files/rapport/pdf/984000836.pdf

1) سلطة التدخل واتخاذ القرارات: حسب نص المادة 25 من القانون 07/18 للسلطة الوطنية أن تأمر أي مسؤول عن المعالجة القيام بالتغييرات اللازمة في عمليات المعالجة بما يتوافق وتحقيق الحماية للمعطيات ذات الطابع الشخصي وذلك من أجل معالجة نزيهة للمعطيات.

- تأمر السلطة الوطنية بإغلاق المعطيات أو سحبها أو إتلافها، وذلك إذا ما تبين لها بعد التثبت أن معالجة معطيات شخصية قد تمت خرقا لأحكام القانون، كما لو تم جمعها دون موافقة الشخص المعني، أو انتهاء الأجل المحدد لحفظها بالتصريح أو الترخيص، وهنا يكون من صلاحياتها التدخل وإصدار قرارها بإلزام المسؤول عن المعالجة بتوقيف المعالجة غير شرعية للمعطيات، أو منع معالجة المعطيات الشخصية بصفة مؤقتة أو دائمة بما في ذلك المعطيات المتضمنة في شبكات مفتوحة لإرسال المعطيات انطلاقا من خادمات تقع داخل التراب الوطني.

كما يكون للسلطة الوطنية سلطة منع إرسال وتحويل معطيات ذات طابع شخصي إلى دولة أجنبية عندما يؤدي هذا الإرسال أو التحويل إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة.[1]

وقد أعطى القانون للسلطة الوطنية أيضا سلطة إصدار عقوبات إدارية وفق مقتضيات المادة 46 من خلال توجيه إنذارات أو إعذارات في حق المسؤول عن المعالجة حال خرقه لأحكام القانون، وقد يصل الأمر إلى درجة إصدارها قرارا بسحب وصل التصريح أو الترخيص مؤقتا لمدة لا تتجاوز سنة أو نهائيا[2]، فجميع القوانين تتفق على تمكين الهيئة المكلفة بحماية المعطيات الشخصية من إقرار عقوبات على مخالفة أحكام وضوابط حماية البيانات، حيث تتنوع هذه المخالفات بين ما هو متعلق بخرق أحكام المعالجة وجمع المعطيات وما هو متعلق بالإعتداء على حقوق الأشخاص المعنيين .

2) سلطة التحقيق والإخطار: تعترف أغلب التشريعات بتمتع الهيئة مكلفة بحماية المعطيات الشخصية بسلطات التحقيق، وتعمل بموجب هذه السلطات بالنظر فيما يقدم إليها من شكاوى وما يعرض عليها من قضايا، ويعطينا التوجيه الأوروبي لحماية المعطيات الشخصية 46/95 حسب المادة 28 منه بعض الأمثلة عن هذه السلطات، مثل القدرة على الوصول إلى البيانات التي تتم معالجتها وجمع كل المعلومات اللازمة لأداء مهام التحقيق[3]، كما تتمتع هذه الهيئة في هذا الصدد بصلاحية الدخول إلى المحلات والأماكن التي تتم فيها معالجة البيانات، سماع الأشخاص العاملين والمسؤولين وكل من ترى في سماعه فائدة للتحريات والتحقيقات التي تجريها، كما يمكنها طلب أية وثيقة تراها ضرورية للتحقيق.

ولقد منح قانون حماية المعطيات الشخصية 07/18 السلطة الوطنية فعلا صلاحية التحقيق (investigation) حيث نصت المادة 49 منه على إمكانية قيام هذه السلطة بالتحريات المطلوبة ومعاينة

[1] المادة 44 من القانون 07/18.

[2] أنظر المادة 46 من القانون 07/18.

[3] Article 28 de la directive 95/46 prévoit que : « chaque autorité de contrôle dispose : De pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle ».

المحلات والأماكن التي تتم فيها المعالجة، ولها في إطار ممارسة مهام التحقيق الولوج إلى المعطيات المعالجة وطلب جميع الوثائق والمعلومات أيا كانت دعامتها.

ونعتقد أن المشرع الجزائري لم يكن موفقا في توضيح كيفية ممارسة السلطة الوطنية سلطة التحري والتحقيق التي منحها إياها، حيث جاء بصياغة مبهمة في نص المادة 50 من قانون حماية المعطيات الشخصية 07/18 عندما تحدث عن قيام أعوان الرقابة الآخرون الذين تلجؤ إليهم السلطة الوطنية للقيام ببحث ومعاينة الجرائم[1]، فمن هم هؤلاء الأعوان الآخرون، وكيف تلجأ إليهم السلطة الوطنية.

غير أن المشرع الفرنسي كان واضحا في هذه المسألة، عندما اعتبر أنه يؤهل أعضاء اللجنة والأعوان التابعين لمصالحها المعينين وفق الشروط المحددة بالمادة 19 من قانون حماية المعطيات، للدخول إلى الأماكن، المحلات، المنشآت والمؤسسات التي تتم فيها معالجة المعطيات ذات الطابع الشخصي، والتي يتم استخدامها مهنيا وذلك من الساعة السادسة صباحا إلى الساعة التاسعة ليلا ما عدا الأجزاء المخصصة منها للسكن.[2]وهنا أوضح المشرع الفرنسي أنه في حالة اعتراض صاحب الأماكن المذكورة الدخول إليها، فإنه لا يمكن أن يتم ذلك إلا بموجب إذن من رئيس المحكمة التي يقع في دائرة اختصاصها المكان المراد زيارته، أو من القاضي الذي يفوضه، والذي يمكنه في أي وقت تعليق الزيارة أو إيقافها.

والمشرع الجزائري خول السلطة الوطنية لإنجاز مهمة التحقيق بموجب المادة 49 من القانون 07/18 سلطة الولوج لى المعطيات المعالجة و إلى جميع المعلومات والوثائق أيا كانت دعامتها، بالإضافة إلى معاينة الأماكن والمحلات التي تتم فيها المعالجة.

وكذلك أشار المشرع الفرنسي أنه يجوز لأعضاء اللجنة والأعوان التابعين لها طلب أي وثيقة مفيدة لاستكمال إجراءات التحقيق مهما كانت دعامتها، والدخول إلى برامج الكومبيوتر والمعطيات وطلب نسخها عن طريق أي معالجة مناسبة في مستندات قابلة للإستخدام مباشرة لحاجات التحقيق، ويمكن للجنة بطلب من رئيسها أن تستعين بخبراء في مجال المعلوماتية.

أما عن صلاحية الإخطار فهي مرتبطة ارتباطا وثيقا بسلطة التحقيق والتحري، حيث يجب أن تكون السلطة الوطنية قادرة على إبلاغ وعرض المخالفات ذات الطابع الجزائي التي تتوصل إليها من خلال ممارستها لسلطة التحري والتحقيق إلى الجهات القضائية المختصة.

وقد أشار قانون حماية المعطيات 07/18 أن السلطة الوطنية لحماية المعطيات لها في إطار ممارستها لمهامها أن تعلم النائب العام المختص فورا في حال معاينتها وقائع تحتمل الوصف الجزائي[3]، مع العلم أن

[1] تنص المادة 50 من القانون 07/18: "...يؤهل أعوان الرقابة الآخرون الذين تلجأ إليهم السلطة الوطنية للقيام ببحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون...».

[2] Art 44 de la loi 801/2004 : « les membres de la commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accés, de 6 heures à 21 heures, pour l'exercice de leurs missions aux lieux, locaux enceintes, installations ou établissement servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel à l'exclusion des parties de ceux-ci affectées au domicile privé ».

[3] المادة 25 الفقرة الأخيرة من القانون 07/18.

إجراءات التحري والمعاينات التي تقوم بها السلطة الوطنية تنتهي بإعداد محاضر توجه فورا إلى وكيل الجمهورية المختص إقليميا.[1]

وتجدر الإشارة أن سلطة الإخطار هذه ماهي إلا آلية إضافية تمنح للسلطة الوطنية من أجل إعلام الجهات القضائية بالمخالفات القانونية لأحكام قانون حماية المعطيات الشخصية ذات الوصف الجزائي، ذلك أن الشخص الذي يعتبر أن حقوقه فيما يتعلق بمعالجة معطياته الشخصية قد تم انتهاكها، بإمكانه أن يخطر الجهات القضائية مباشرة، وليس لزاما عليه أن يمر عبر السلطة الوطنية لحماية المعطيات[2]، وهذا ما يؤكده المشرع الجزائري في المادة 52 من القانون 07/18 التي تنص صراحة أنه يمكن لكل شخص يدعي أنه تم المساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية المختصة اتخاذ أي إجراءات تحفظية أو للحصول على التعويض.

وقد أشار المشرع الفرنسي أنه من صلاحيات اللجنة الوطنية للمعلوماتية والحريات (CNIL) إذا عاينت وجود معالجات لمعطيات شخصية من شأنها أن تشكل اعتداء على أمن الدولة والدفاع الوطني والأمن العمومي، أو عاينت وجود اعتداء على المعالجات التي تهدف إلى منع الجرائم والتحقيق فيها والكشف عنها وملاحقتها قضائيا، أن تخطر الوزير الأول بهذه الإعتداءات المعاينة لاتخاذ ما يلزم من إجراءات لوقفها ويقوم بإبلاغها بالإجراءات المتخذة من قبله في أجل 15 يوما من إخطاره.[3]

3) سلطة العقاب: تتفق جميع القوانين على تمكين الهيئة المكلفة بحماية المعطيات الشخصية من إقرار عقوبات على مخالفة أحكام حماية البيانات الشخصية، حيث تتنوع هذه المخالفات بين ما هو متعلق بخرق أحكام معالجة وجمع المعطيات، وبين ما هو متعلق بالاعتداء على حقوق الأشخاص المعنيين، وقد تكون المخالفات مقصودة أو ناتجة عن إهمال، كالقيام بمعالجات لمعطيات شخصية دون الحصول على الترخيص المفروض، أو الإستمرار في معالجة معطيات خارج المدة المصرح بالإحتفاظ بها، أو العمل على جمع بيانات شخصية بطريقة غير شرعية.

والمشرع الجزائري كان من بين التشريعات التي اعترفت للهيئة المكلفة بحماية المعطيات الشخصية بسلطة توقيع عقوبات إدارية على من يخالف أحكام القانون، حيث أعطى للسلطة الوطنية لحماية المعطيات الشخصية بموجب المادة 46 من قانون حماية المعطيات الشخصية 07/18 أن تتخذ في حق المسؤول عن المعالجة الذي لا يحترم الإلتزامات المفروضة عليه بموجب هذا القانون العقوبات التالية:

- الإنذار.

- الإعذار.

- السحب المؤقت لمدة لا تتجاوز السنة أو السحب النهائي لوصل التصريح أو الترخيص.

[1] المادة 51 من نفس القانون.

[2] Farid Bouguettaya, op.cit, page 107.

[3] أنظر المادة 45/II-3 من القانون الفرنسي 2004/801 المشار إليه سابقا.

- الغرامة، وتكون الغرامة ضد المسؤول عن المعالجة في حالات ذكرها المشرع على سبيل الحصر وهي:

*عندما يرفض المسؤول عن المعالجة دون سبب شرعي حقوق الإعلام والولوج أو التصحيح أو الإعتراض المنصوص عليها في المواد 32، 34، 35، 36 من هذا القانون.

* إذا لم يقم بتبليغ السلطة الوطنية بهوية ممثله المقيم في الجزائر الذي يحل محله في جميع حقوقه والتزاماته الناتجة عن أحكام هذا القانون، وهذا بالنسبة للمسؤول عن المعالجة غير المقيم في التراب الوطني ويلجأ إلى استعمال وسائل آلية أو غير آلية توجد فوق التراب الوطني بغرض معالجة معطيات شخصية.

* إذا لم يقم بتبليغ السلطة بأي تغيير للمعلومات المقدمة في التصريح أو بأي حذف يطال المعالجة.

* المسؤول عن المعالجة الذي لا يقوم بالكشف عن هويته للعموم، ولا يبليغ السلطة الوطنية بهذه الهوية في حالة ما إذا كانت المعالجة لا تخضع لإلزامية التصريح.

وعلى خلاف المشرع الجزائري فالملاحظ أن المشرع الفرنسي منح للجنة الوطنية للمعلوماتية والحريات اتخاذ هذه العقوبات الأخيرة في مواجهة المخالف بعد استدعاء المعني ومواجهته بالخروقات المعاينة ضده، وله في مقابل ذلك تقديم أوجه دفاعه بشأنها قبل إصدار العقوبة ضده، وهو أمر لم ينص عليه المشرع الجزائري فبالرجوع إلى القانون الفرنسي نجده أعطى للجنة الوطنية للمعلوماتية والحريات سلطة توجيه إنذار للمسؤول عن المعالجة الذي يعاين عدم احترامه لالتزاماته المفروضة عليه قانونا ، ولها أيضا أن توجه له إعذارا من أجل مطالبته بالتوقف عن خرق أحكام القانون في أجل تحدده له اللجنة، و إذا لم يلتزم المسؤول عن المعالجة للإعذار الموجه إليه فإن اللجنة الوطنية لها أن تصدر ضده بعد اتخاذ إجراءات الخصومة contradictoire une procédure après العقوبات الإدارية المقررة قانونا،[1] والعقوبات الإدارية التي قرر المشرع الفرنسي للجنة المعلوماتية والحريات CNIL اتخاذها هي:

- الغرامة الإدارية والتي يتناسب مقدارها حسب درجة خطورة و جسامة الخروقات التي ارتكبها المسؤول عن المعالجة، وهو ما لا نجده عند المشرع الجزائري الذي حدد غرامة واحدة مقدرة ب 500ألف دج مهما كانت طبيعة الإعتداء و درجة خطورته، كما أن المشرع الجزائري لا نجده يحدد مآل تنفيذ الغرامة الإدارية المنطوق بها من طرف السلطة الوطنية حول نفس الوقائع التي كانت محل متابعة جزائية وصدرت بشأنها غرامات جزائية، على خلاف المشرع الفرنسي الذي عالج هذه النقطة عندما نصت المادة 47 الفقرة الأخيرة من القانون 17/78 أن القاضي الجزائي الذي لم يفصل نهائيا في نفس الوقائع التي هي محل متابعة جزائية أمامه و التي سبق وأن صدرت بشأنها عقوبة مالية إدارية من طرف اللجنة الوطنية للمعلوماتية و الحريات، أن يخصم الغرامة المالية الإدارية التي حددتها اللجنة الوطنية من الغرامة الجزائية التي ينطق بها .

[1] Voir l'article 45 de la loi 801/2004.

-الأمر بتوقيف المعالجة في حالة عدم الإلتزام بأحكام المادة 22 من القانون والمتعلقة بالإجراءات المسبقة على عملية المعالجة، سيما ما تعلق منها بمسك سجل المعالجات، وتعيين مراسل لحماية المعطيات الشخصية.

-سحب الترخيص الممنوح بموجب أحكام المادة 25 من القانون.

وفي حالة ما إذا أدت المعالجة أو كان استغلال المعطيات المعالجة من شأنه أن يشكل اعتداء على الحقوق والحريات المحددة بنص المادة الأولى من القانون 17/78 يجوز للجنة بعد اتخاذ إجراءات الخصومة أن تقرر:

-قطع المعالجة لمدة أقصاها 03 أشهر، ما لم تكن المعالجة متعلقة بأمن الدولة والدفاع الوطني والأمن العمومي، أو التي تهدف إلى منع الجرائم والتحقيق فيها والكشف عنها وملاحقتها قضائيا، أو كانت المعالجات من التي ينفذها أشخاص معنوية عمومية أو خاصة منفذة لحساب الدولة.

-حظر معالجة بعض البيانات الشخصية لمدة أقصاها 03 أشهر مالم تكن من المعالجات المتعلقة بالحالتين الأولى والثانية.

وإذا كان الإعتداء على الحقوق المذكورة في المادة الأولى من القانون 17/78 حالا وجسيما، جاز لرئيس اللجنة الوطنية للمعلوماتية والحريات أن يتقدم بطلب لى القضاء الإستعجالي المختص من أجل إصدار أوامر بالإجراءات اللازمة للحفاظ على هذه الحقوق والحريات.

الفرع الثالث: هيئات حماية المعطيات الشخصية في القوانين المقارنة:

فضلا عن الهيأة المكلفة بالإشراف والرقابة على التطبيق السليم بالوضع الصارم لتدابير الحماية القانونية للمعطيات ذات الطابع الشخصي كما هو الشأن للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، فإنه انطلاقا من التوجيهات الأوروبية وكذا القانون الفرنسي في مجال حماية المعطيات ذات الطابع الشخصي، نجد هيآت أخرى تسعى بحسب المهام المسندة لها إلى تعزيز حماية هذه المعطيات، وذلك زيادة في الحرص على توفير أقصى درجات الحماية للمعطيات الشخصية.

أولا: هيئات حماية المعطيات الشخصية على مستوى الإتحاد الأوروبي:

حرص الإتحاد الأوروبي على وضع قانون موحد لحماية البيانات الشخصية، تلتزم جميع دول الإتحاد أن توافق قوانينها الداخلية مع أحكامه، وكان ذلك من خلال الإتفاقية الأوروبية لحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي رقم 108، وكذا من خلال التوجيه الأوروبي 95/46 المؤرخ في 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي وحرية تداولها، ثم اللائحة العامة 2016/679 المؤرخة في 27 أفريل 2016 المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والتي جاءت صادرة عن مجلس أوروبا والبرلمان الأوروبي.

وقد تضمنت هذه الإرشادات الأوروبية، النص على إنشاء كيانات قانونية مستقلة مسؤولة عن التطبيق المنسق لأحكامها على المستوى الوطني لدول الإتحاد، بالإضافة إلى هيئات أوروبية أخرى خارج هذه الإرشادات جاءت بها اتفاقيات ضمن إطار الإتحاد الأوروبي، وسوف نحاول أن نستعرض هذه الهيئات من خلال ما يلي:

1) هيئات حماية المعطيات الشخصية ضمن التوجيهات الأوروبية: تعتبر التوجيهات (les directives) الأوروبية في مجال حماية المعطيات الشخصية ترسانة قانونية للإتحاد الأوروبي، وعمادا مرجعيا للعديد من الهيئات الأوروبية لضمان حماية فعالة وكفؤة للبيانات الشخصية:

1-1) اللجنة الأوروبية لحماية المعطيات الشخصية: أنشئت هذه اللجنة بموجب المادة 31 من التوجيه وروبي CE/46/95 إستنادا على القرار الأوروبي لسنة 1987:[1] كهيئة مساعدة للمفوضية الأوروبية لحقوق الإنسان، ويأتي إنشاء هذه اللجنة في مجال حماية البيانات الشخصية ودورها المساعد على التنفيذ السليم لقانون حماية البيانات الشخصية، تأكيدا على الأهمية التي يوليها مجلس أوروبا والبرلمان الأوروبي لهذه البيانات.

تعد اللجنة الأوروبية لحماية المعطيات الشخصية هيئة مستقلة تتمتع بالشخصية القانونية، وتتكون من مجموع رؤساء الهيئات المكلفة بحماية المعطيات الشخصية للدول الأعضاء في مجلس أوروبا، بالإضافة إلى المراقب الأوروبي لحماية المعطيات الشخصية أو من يمثله قانونا، وهي حاليا تتكون من 28 سلطة مكلفة بحماية المعطيات الشخصية تابعة للدول الأعضاء في الإتحاد الأوروبي.

تنتخب هذه اللجنة رئيسها من بين أعضائها بالأغلبية البسيطة لعهدة مدتها خمس سنوات قابلة للتجديد مرة واحدة، وتعد نظامها الداخلي وإجراءات عملها، وتمارس مهامها وسلطاتها بكل استقلالية بعيدا عن تلقي أي تعليمات أو أوامر من أي جهة كانت.[2]

ولقد حددت المادة 70 من اللائحة الأوروبية العامة لحماية المعطيات الشخصية رقم 2016/679 مهام هذه اللجنة، والمتمثلة أساسا في ضمان التطبيق المنسجم لقواعد اللائحة الأوروبية العامة لحماية البيانات وتحقيقا لهذه الغاية فإن اللجنة تقوم بالمهام التالية:

-مراقبة وضمان التطبيق السليم للائحة العامة لحماية البيانات الشخصية من خلال مهمتها الإستشارية وتسوية النزاعات.

- تقديم المشورة في جميع المسائل المتعلقة بحماية البيانات الشخصية في الإتحاد الأوروبي، سيما ما تعلق منها بتبادل البيانات الشخصية بين المسؤولين عن المعالجة والسلطات المكلفة بحماية البيانات الشخصية التابعة للدول الأعضاء.

[1] Résolution du Parlement européen sur les compétences exécutives de la Commission (comitologie) et le rôle de la Commission dans les relations extérieures de la Communauté (13 décembre 1990) (JOCE). 28.01.1991, n° C 19, disponible sur le site : www.cvce.eu.

[2] Voir l'article 69 du règlement 679/2016,op,cit

- نشر المبادئ التوجيهية والتوصيات والممارسات الجيدة بشأن حماية البيانات الشخصية الموجودة في خدمات الإتصالات المتاحة للجمهور.

- تحديد الظروف الخاصة التي يتعين من خلالها على المسؤول عن المعالجة أو المعالج من الباطن الإبلاغ بكل اعتداء على المعطيات الشخصية.

- تحديد الظروف الخاصة التي من المحتمل أن يؤدي فيها اختراق البيانات الشخصية إلى مخاطر عالية.

- تحديد المعايير والمتطلبات المطبقة على نقل البيانات الشخصية.

- تقييم التطبيق العملي للمبادئ التوجيهية والتوصيات والممارسات الجيدة في مجال حماية المعطيات الشخصية.

- تقييم مدى كفاية مستوى الحماية التي توفرها دولة خارج الإتحاد الأوروبي أو منظمة دولية تحول إليها المعطيات الشخصية.

- صياغة قرارات السلطات المكلفة بحماية المعطيات الشخصية للدول الأطراف وفق آلية مراقبة مدى اتساق عملها مع اللوائح الأوروبية في مجال حماية المعطيات الشخصية، المشار إليها في المادة 64 من اللائحة العامة وإصدار قرارات ملزمة لها.

- تعزيز التعاون والتبادل الفعال الثنائي ومتعدد الأطراف للمعلومات والممارسات الجيدة بين السلطات المكلفة بحماية المعطيات الشخصية خارج الإتحاد الأوروبي.

- وتقوم اللجنة بإعداد تقارير سنوية حول التطبيق الفعلي للمبادئ التوجيهية والتوصيات والقرارات الصادرة عنها.

2-1) مجموعة المادة 29: (مجموعة سلطات الحماية الأوروبية) Groupes des autorités de protections européennes: بالإضافة إلى إلزامه الدول الأعضاء في مجلس أوروبا على إنشاء هيئة إشراف ومراقبة وطنية تكلف بحماية المعطيات ذات الطابع الشخصي، أنشأ التوجيه الأوروبي CE/46/95 بموجب المادة 29 هيئة مستقلة ذات طابع استشاري، أكسبها إسم مجموعة المادة 29 لحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي[1]، نسبة الى المادة 29 التي أنشئت بموجبها.

تتشكل مجموعة المادة 29 بشكل أساسي من ممثلين عن السلطات الوطنية لحماية المعطيات الشخصية التابعة لدول مجلس أوروبا، حيث تختار كل دولة عضوا يمثلها بالإضافة إلى المراقب الأوروبي لحماية المعطيات وممثل المفوضية الأوروبية لحقوق الانسان، و تنتخب المجموعة رئيسها من بين أعضائها لعهدة مدتها سنتين قابلة للتجديد مرة واحدة، وتعد نظامها الداخلي وإجراءات عملها وتتخذ قراراتها في إطار

[1] Article 29/1 de la directive 95/46 : « il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel ci-après dénommé « groupe ».

نظام المداولات بالأغلبية البسيطة، لمناقشة المسائل المتعلقة بحماية المعطيات الشخصية إما بطلب من رئيسها أو بطلب ممثل عن سلطة وطنية لحماية المعطيات.

ويشير التوجيه الأوربي CE/95/46 أن المجموعة تساهم في التنفيذ الموحد للأحكام الوطنية المعتمدة بموجب هذا التوجيه، وقد حددت المادة 30 منه مهام المجموعة والتي تقتصر على الوظائف الاستشارية والإعلامية المتعلقة بحماية البيانات الشخصية، وتقدم رأيها حول مستوى الحماية المضمونة في الدول، وتنصحها باتخاذ أي تعديل للتدابير في مجال حماية المعطيات الشخصية وهذا في إطار ضمان التجانس في تطبيق أحكام التوجيه الأوروبي، ولها أن تصدر توصيات في هذا الإطار.

بالإضافة إلى تقديم المشورة للدول الأعضاء بشأن أي تدابير إضافية أو محددة يتعين اتخاذها لتوفير حماية فعالة لحقوق وحريات الأشخاص فيما يتعلق بمعالجة البيانات الشخصية[1]، وتقدم المجموعة أيضا رأيها إلى المفوضية الأوروبية لحقوق الانسان حول مستوى الحماية الموفرة للبيانات الشخصية داخل الإتحاد الأوروبي والدول الاخرى خارج الإتحاد، وتقدم لها كذلك المشورة بخصوص أي مشروع قانون يخص حقوق وحريات الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية، وتعلمها بأي أفعال من شأنها المساس بحماية المعطيات الشخصية داخل الإتحاد الأوروبي.

كما تمتد مهامها إلى مجال الإتصالات الإلكترونية بموجب التوجيه الأوروبي CE/2002/58 المؤرخ في 12 جويلية 2002 المتعلق بمعالجة المعطيات ذات الطابع الشخصي وحماية الحياة الخاصة في قطاع الإتصالات الإلكترونية.

3-1) المراقب الأوروبي لحماية المعطيات الشخصية: le contrôleur européen de la protection des données (CEPD): وهو عبارة عن هيئة إشراف مستقلة تتمثل مهمته الأساسية في ضمان احترام المؤسسات والهيئات الأوروبية للحق في الخصوصية وحماية البيانات الشخصية أثناء المعالجة الآلية، ويعين المراقب الأوروبي من طرف البرلمان والمجلس (le parlement européen et le conseil de l'europe) بشكل مشترك لمدة 5 سنوات على أساس قائمة تقترحها المفوضية الأوروبية لحقوق الانسان*، تشمل جميع المهتمين بهذا المنصب بعد تقديم طلباتهم، وتكون هذه الولاية قابلة للتجديد مرة واحدة.[2]

ويمارس مهامه وسلطاته بكل استقلالية ولا يخضع لأي تأثير خارجي مباشر أو غير مباشر، ولا يتلقى أي تعليمات من أي جهة مهما كانت.[3] وانطلاقا من اللائحة الأوروبية 2018/1725،[1] يمكن تحديد مهام المشرف الأوروبي لحماية المعطيات الشخصية إلى ثلاث طوائف رئيسية:[2]

[1] Voir l'article 30 de la directive 95/46/CE

*المفوضية الأوروبية هي إحدى المؤسسات الرئيسية للإتحاد الأوروبي إلى جانب مجلس الإتحاد الأوروبي والبرلمان الأوروبي والمجلس الأوروبي، أنشئت بموجب معاهدة روما لعام 1957 (المواد من 155 إلى 163) تتكون من مفوض أوروبي لكل دولة عضو، وظيفتها الأساسية هي اقتراح مبادرات تشريعية، تنفيذ سياسات المجموعة الأوروبية من خلال المعاهدات وتشرف على تطبيقها، وهي تلعب دور الضامن المركزي تجاه المصلحة العامة للإتحاد الأوروبي،

[2] أنظر المادة 53 من اللائحة 2018/1725

[3] أنظر المادة 55 من اللائحة 1725/2018.

- **الدور الإشرافي**: تتمثل مهامه الإشرافية في مراقبة عمليات المعالجة للبيانات الشخصية التي تتم داخل المؤسسات والهيئات الأوروبية، وذلك بالتنسيق مع مفوض حماية المعطيات الموجود في كل مؤسسة أو هيئة أوروبية تقوم بمعالجة البيانات الشخصية، وذلك من أجل ضمان تطبيق أحكام اللائحة الأوروبية لحماية المعطيات الشخصية وأي قانون إتحادي آخر يتعلق بحماية الحقوق والحريات الأساسية للأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية.[3]

كما تقوم إدارة تطوير البرامج بإبلاغ المراقب بجميع المعالجات المتعلقة بالبيانات الشخصية الحساسة والذي يقوم بفحصها مسبقا، ليصدر بعد ذلك رأيه في سلسلة من التوصيات يتعين على المؤسسات أو الهيئات المسؤولة عن المعالجة بتطبيقها من أجل ضمان الإ متثال لقواعد حماية البيانات.

بالإضافة إلى قيام هيئة المراقب بالنظر في الشكاوى المقدمة من قبل موظفي الإتحاد الأوروبي أو أي شخص آخر يرى أن بياناته الشخصية لم تتم معالجتها بشكل صحيح من طرف مؤسسة أو هيئة أوروبية، وله في سبيل ذلك سلطات التحقيق التي تتمثل في:

- يطلب من المسؤول عن المعالجة أو المعالج من الباطن تزويده بجميع المعلومات التي يحتاجها في التحقيق، وكذا جميع البيانات الشخصية والمعلومات اللازمة لإنجاز مهامه.

- له سلطة الدخول إلى جميع محلات المسؤول عن المعالجة أو المعالج من الباطن، وكذا أي منشأة تتم فيها المعالجة، وإلى أي وسيلة معالجة وفقا لأحكام قوانين الإتحاد الأوروبي.

وله بعد ذلك سلطة اتخاذ الإجراءات التصحيحية التالية:

- إبلاغ المسؤول عن المعالجة أو المعالج من الباطن أن عمليات المعالجة التي يقوم بها من شأنها انتهاك أحكام هذه اللوائح.

- إلزام المسؤولين عن المعالجة أو المعالجين من الباطن بالامتثال إلى طلبات المعنيين بالمعالجة التي تهدف إلى ممارسة حقوقهم بموجب هذه اللائحة.

- إلزام المسؤول عن المعالجة أو المعالج من الباطن بجعل معالجاته متوافقة مع أحكام اللوائح، وإذا لزم الأمر وفقا للطريقة التي يحددها له في أجل معين.

- إلزام المسؤول عن المعالجة بالتواصل مع المعني بالمعالجة حول الإ عتداءات الماسة بالمعطيات الشخصية.

- الأمر بتصحيح أو محو البيانات الشخصية وتقييد المعالجة المخالفة لأحكام القانون.

---

[1] RÈGLEMENT (UE) 2018/1725 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE Journal officiel de l'Union européenne L 295/39

[2] Voir les articles 57-58 du règlement 2018/1725.

[3] أنظر المادة 3/52 من اللائحة الأوروبية 1725/2018.

- فرض غرامات إدارية في مواجهة المسؤول عن المعالجة الذي لا يمتثل للتدابير المأمور بها.

- **الدور الاستشاري**: في إطار هذه المهمة يقدم المراقب الأوروبي لحماية البيانات المشورة للمفوضية الأوروبية، البرلمان الأوروبي ومجلس الإتحاد الأوروبي بشأن المسائل المتعلقة بحماية البيانات الشخصية، ويكون لهذا الدور الإستشاري أثر مهم على الاقتراحات الخاصة بالتشريعات الجديدة التي قد تؤثر على حماية البيانات الشخصية داخل الإتحاد الأوروبي، ويكون هذا النشاط الإستشاري في شكل رأي رسمي أو في شكل ملاحظات كما يعمل المراقب الأوروبي أيضا في هذا الصدد على تعزيز الوعي العام وفهم المخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة المعطيات الشخصية.

- يقدم لأي شخص معني بالمعالجة بناء على طلبه معلومات تتعلق بممارسة حقوقه بموجب هذا النظام والتعاون لأجل هذه الغاية مع السلطات الإشرافية المكلفة بحماية المعطيات الشخصية لبلد ذلك الشخص.

- تقديم المشورة لجميع المؤسسات والهيئات التابعة للإتحاد بمبادرة منه، أو بناء على طلب هذه الهيئات وذلك فيما يتعلق بالتدابير التشريعية والإدارية المتعلقة بمعالجة البيانات الشخصية.

- الدور التعاوني: تتعاون هيئة المراقب الأوروبي لحماية البيانات (CEPD) مع جميع سلطات حماية البيانات للدول الأعضاء، من أجل تعزيز نهج ثابت لحماية البيانات الشخصية في أوروبا، ومن بين أهم الأدوار التعاونية الأساسية لـ CEPD، تعاونه مع مجموعة المادة 29 في التطبيق الموحد للوائح الأوروبية المتعلقة بحماية البيانات الشخصية وكذا تعاونه مع هيئة « Eurodac».*

4-1) مفوض حماية البيانات الشخصية le délégué à la protection des données personnels:

بعد دخول اللائحة الأوروبية العامة لحماية المعطيات الشخصية (RGPD) رقم 2016/679 السابق ذكرها حيز النفاذ، أصبحت الهيئات والمؤسسات والسلطات الإدارية داخل الدول الأوروبية بصفتها مسؤول عن المعالجة أو معالج من الباطن ملزمة بتعيين شخص تابع لها تسند له مهمة مفوض البيانات، حيث تنص في المادة 37 من هذه اللائحة على التزام المسؤول عن المعالجة أو المعالج من الباطن بتعيين مفوض لحماية البيانات في ثلاث حالات:

- عندما تتم المعالجة الآلية للمعطيات الشخصية من طرف سلطة أو هيئة عامة باستثناء الجهات القضائية خلال ممارستها للعمل القضائي، وهو الإستثناء المؤكد من خلال المادة 32 من التوجيه الأوروبي 2016/680 المؤرخ في 27 أفريل 2016.[1] والتي نصت على أنه يجوز للدول الأعضاء استثناء المحاكم وغيرها

* ,Eurodac هي قاعدة بيانات للتعرف على بصمات الأصابع (dactylogrammes) تم إنشاؤها في 15 جانفي 2003 بموجب اتفاقية "دبلن" بغرض التسهيل في التعرف على الأشخاص ومساعدة الدول الأعضاء في فحص طلبات اللجوء السياسي المقدمة إليها، أنظر: http://www.wikipedia.org

[1] Directive (UE) 2016/680 du parlement européen et du conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'éxécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du conseil, journal officiel de l'union européen L119/89.

من السلطات القضائية عندما يتصرفون في إطار ممارسة وظائفهم القضائية، الإلتزام بتعين مفوض لحماية المعطيات.

- عندما تكون الأنشطة الأساسية للمسؤول عن المعالجة أو المعالج من الباطن ذات طبيعة أو نطاق أو غاية تفرض مراقبة منهجية ومنتظمة على نطاق واسع للأشخاص الطبيعيين المعنيين.*

- عندما تكون الأنشطة الأساسية للمسؤول عن المعالجة أو المعالج من الباطن تتناول معالجة بيانات ذات طبيعة حساسة (البيانات الصحية، البيومترية، المعتقدات الدينية...) أو كانت البيانات موضوع المعالجة بيانات خاصة بالأحكام الجزائية.

و يعتبر مفوض البيانات (DPD) من أفضل الخطوات التي يمكنها أن تضمن التزام المؤسسات المختلفة بأحكام قوانين حماية البيانات، ذلك أن من أهم المهام الأساسية المنوطة به هي العمل على مراقبة التزام المؤسسة أو المنظمة أو الإدارة التي يعمل لديها باحترام تطبيق النصوص القانونية الخاصة بحماية البيانات الشخصية، كما يضمن مفوض البيانات للجهات التي يعمل لديها المشورة بشأن متثال لقواعد حماية البيانات الشخصية في إطار قيامها بالمعالجة الآلية لها، وهو بهذا الدور يكون بمثابة وسيط بين السلطة الوطنية الإشرافية المكلفة بحماية المعطيات الشخصية والأشخاص المعنيين بالمعالجة والمنظمة المسؤولة عن المعالجة التابع لها[1]، لذلك ألزمت المادة 38 من اللائحة العامة لحماية المعطيات (GPDR) كل مسؤول عن المعالجة أو معالج من الباطن بالحرص على أن يكون مفوض البيانات مرتبطا وفي الوقت المناسب وبالشكل اللازم بجميع المسائل المتعلقة بحماية المعطيات الشخصية ومساعدته على تنفيذ مهامه، من خلال توفير له كل الموارد اللازمة لذلك، بما فيها الموارد المالية والسماح له بالوصول إلى البيانات الشخصية وكذا عمليات المعالجة المتعلقة بها.

وفي المقابل يجوز للأشخاص المعنية بالمعالجة الإتصال بمفوض حماية البيانات فيما يتعلق بجميع المسائل المتعلقة بمعالجة بياناتهم الشخصية وممارسة حقوقهم بموجب هذه اللوائح.

غير أنه يفهم من نص المادة 37 من اللائحة العامة الأوروبية لحماية المعطيات الشخصية (RGPD) أن إلزامية تعيين مفوض حماية البيانات الشخصية من قبل المسؤول عن المعالجة أو المعالج من الباطن يكون فقط في الحالات الثلاث المذكورة على سبيل الحصر، وفي ماعداها يكون تعيينه اختياريا وخاضعا

*لم تحدد اللائحة المقصود بالعبارات: المراقبة المنهجية "واسعة النطاق"، والأنشطة الأساسية، لذلك فإن مجموعة المادة 29 نشرت بعض المبادئ التوجيهية حول تفسيرهذه العبارات، أنظر أكثر:

Lignes directives concernants les délégués à la protection des données (DPD), rapport du groupe de travail « article 29 » sur la protection des données, adaptées le 13 décembre 2016, WP243 rev 01 PP 6à9 disponible sur le site :

ww.ec.europa.eu/justice/data-protection

[1]Manuel de droit européen en matière de protection des données. Office des publications de l'union européenne, édition 2018 page197.disponible sur le site : https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_fr.pdf

لتقدير الجهة المعالجة للمعطيات الشخصية[1]، إلا أنه وبخلاف هذه الحالات الإلزامية الثلاث فقد أشارت المادة 4/37 من اللائحة على إمكانية إلزام المسؤول عن المعالجة أو المعالج من الباطن بتعيين مفوض لحماية البيانات في حالات أخرى إذا اقتضى قانون الإتحاد أو قانون دولة عضو ذلك، كما يجوز للدول الأعضاء أيضا أن تجعل هذا التعيين إلزاميا لأنواع أخرى من الهيئات والمؤسسات بخلاف تلك المشار إليها في المادة 37 من هذه اللائحة.[2]

ويتم تعيين مفوض حماية البيانات على أساس صفته المهنية، وعلى وجه الخصوص معرفته المتخصصة بقوانين وممارسات حماية البيانات وقدرته على إنجاز مهامه المحددة قانونا[3]، وقد يكون موظفا من بين الموظفين التابعين للمسؤول عن المعالجة، أو عنصرا خارجيا يؤدي مهامه في إطار عقود الخدمة، وفي كلتا الحالتين يتعين على المسؤول عن المعالجة أو المعالج من الباطن أن ينشر هوية المفوض ويبلغها إلى السلطة الوطنية لحماية المعطيات.

ويمكن إجمال المهام التي يكلف بها مفوض حماية البيانات الشخصية حسب نص المادة 39 من اللائحة العامة الاوروبية لحماية البيانات الشخصية فيما يلي:

- إبلاغ وإسداء المشورة للمسؤول عن المعالجة أو المعالج من الباطن حول التزاماتهم المتعلقة بمعالجة المعطيات الشخصية وفق أحكام هذه اللائحة وغيرها من أحكام قوانين الإتحاد ذات الصلة.

-مراقبة امتثال المسؤول عن المعالجة أو المعالج من الباطن لأحكام هذه اللائحة والأحكام الأ خرى لقوانين الإتحاد أو قانون الدول الأعضاء المتعلقة بحماية البيانات الشخصية وكذلك القواعد الداخلية للمسؤول عن المعالجة، سيما ما يتعلق منها بحماية البيانات الشخصية للموظفين وتدريب الموظفين المشاركين في عمليات المعالجة، لتمكينهم من تطوير مهاراتهم ومواكبة جميع التطورات في تشريعات حماية البيانات.

- التعاون مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

- العمل كجهة اتصال للسلطة الوطنية لحماية المعطيات مع المسؤول عن المعالجة أو المعالج من الباطن في إطار الإ ستشارة المسبقة التي يطلبها هذا الاخير من السلطة الوطنية وفقا لأحكام المادة 36 من اللائحة (RGDP).[4]

ولأجل ممارسة مفوض البيانات هذه المهام تلزم أحكام اللائحة (RGPD) المسؤول عن المعالجة أو المعالج من الباطن أن يضمن له جانب من الإ ستقلالية وتوفير قدر من الضمانات، كالحرص على عدم تلقي

[1] Voir L'article 37 du GPDR -désignation du délégué à la protection des données. le responsable du traitement et le sous traitant désignent en tout état de cause un délégué de la protection des données

[2] Voir art 37du RGPD, paragraphe 3 et 4.

[3] Voir l'article 37/5 du GPDR

[4] Article 36 : « le responsable du traitement consulte l'autorité de contrôle probablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque »

المفوض لأي تعليمات من أي جهة وعدم فصله من مهامه الأصلية، أو معاقبته في إطار ممارسته لمهامه المتعلقة بحماية المعطيات.

2) هيئات أوروبية لحماية المعطيات الشخصية خارج التوجيهات الأوروبية: بالإضافة إلى الهيئات السابق ذكرها هناك هيئات أخرى يدخل ضمن صلاحياتها حماية البيانات الشخصية نصت عليها الإتفاقيات المبرمة بين دول الإتحاد الأوروبي نذكر منها مايلي:

1-2) اللجنة الإستشارية للإتفاقية الأوروبية لحماية المعطيات الشخصية comité consultatif de la convention pour la protection des données à caractère personnel. إنطلاقا من الإتفاقية الأوروبية لحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي رقم 108، والتي نصت على إنشاء لجنة استشارية تتكون من ممثلين عن الدول الأعضاء في مجلس أوروبا، تم إنشاء هذه اللجنة ستشارية المنبثقة عن منظمة مجلس أوروبا وهي تضم حاليا أكثر من 50 دولة بصفة عضو، وأكثر من 25 دولة بصفة مراقب[1]، و تهدف هذه اللجنة إلى تعزيز فاعلية الإتفاقية الأوروبية في التعامل مع تحديات الخصوصية الناجمة عن التطور المستمر لتكنولوجيا المعلومات، بما يدعم الإتزام بتنفيذ بنودها ومستهدفاتها داخل الدول الأعضاء.

حيث تنص المادة 19 من الإتفاقية الأوروبية على أن اللجنة الإستشارية تعمل على تقديم كل اقتراح من شأنه تيسير أو تحسين تطبيق هذه الإتفاقية، والتي تهدف أساسا إلى توسيع الرغبة في حماية الحقوق والحريات الأساسية لكل فرد، لتشمل احترام الحق في الخصوصية عبر حماية المعطيات ذات الطابع الشخصي، وقد وضح التقرير التفسيري لهذه الإتفاقية أن إنشاء مثل هذه اللجنة أمر طبيعي طالما أن الإتفاقية تحتوي على حق من نوع جديد، وهو الحق في حماية المعطيات الشخصية، ومن ثم يأتي دورها في توقع المشاكل الجديدة المترتبة عن المعالجة الآلية لهذه المعطيات، وإعطاء المقترحات وإسداء المشورة للدول الأطراف لحل هذه المشاكل عند الضرورة.[2]

تجتمع اللجنة الإستشارية الأوروبية مرة كل سنتين على الأقل، وعند الإقتضاء بطلب من ثلث ممثلي الدول الأطراف، وذلك بدعوة من الأمين العام لمجلس أوروبا، وتنتهي اجتماعاتها بإعداد تقرير توجهه اللجنة الإستشارية إلى لجنة وزراء مجلس أوروبا.

[1] يحق لكل دولة عضو في المجلس وغير منظمة للإتفاقية أن تمثل داخل هذه اللجنة بواسطة مراقب، أنظر المادة 03/18 من الاإفاقية الأوروبية 108.

[2] Rapport explicatif concernant la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractères personnel, Conseil de l'europe, section des publications. disponible sur le site : http://rm.coe.int

والملاحظ أن منظور هذه اللجنة يتجاوز حدود الإتحاد الأوروبي لتكون أحد أفضل المنتديات العالمية التي تجمع بين الإهتمام بالحقوق الأساسية للإنسان والتنظيم المرن للتكنولوجيا، وذلك من خلال تقرير دور المراقب الذي يسمح لأي دولة خارج مجلس أوروبا أن تنضم إلى هذه اللجنة الإستشارية بهذه الصفة.[1]

2-2) السلطة المشتركة لمراقبة النظام المعلوماتي شينغن: في البداية نشير إلى أن اتفاقية شنغن المؤرخة في 14 جوان 1985 والإتفاقية المنفذة لها المؤرخة في 19 جوان 1990[2] جاءت لخلق منطقة حرة لتنقل الأشخاص عن طريق إلغاء المراقبة الحدودية الداخلية للدول الأعضاء، وإرساء نظام مراقبة حدودية موحد في هذه المنطقة، بغرض الحفاظ على مستوى مرضي من الأمن سيما من خلال التعاون بين الشرطة والقضاء لهذه الدول[3] ومواءمة سياسة التأشيرات، وكان من بين التدابير الهامة في هذا الصدد، اللجوء إلى إنشاء نظام المعلومات شنغن (SIS) système d'information schengen، وهو عبارة عن ملف معلوماتي مشترك بين جميع الدول الأعضاء في منطقة شنغن من أجل مركزية المراقبة لفئتين رئيستين من المعلومات تتعلق الأولى بالأشخاص المبحوث عنهم المفقودين والأشخاص تحت المراقبة، وتتعلق الفئة الثانية بالمعلومات المرتبطة بالسيارات كهوية وشهادات تسجيل السيارات ولوحات ترقيمها.[4]

ووفقا للمادة 114 من الإتفاقية المنفذة لاتفاقية شنغن، تلتزم الدول المتعاقدة بتعيين سلطة إشرافية على مستواها تكلف في إطار قوانينها الداخلية بعملية المراقبة المستقلة للجزء المتعلق بها من ملفات النظام المعلوماتي شنغن والتحقق من أن المعالجة والإستعمال للمعطيات الشخصية المدرجة في هذا النظام لا تحمل اعتداء على حقوق الأشخاص المعنية بالمعالجة، بعد السماح لكل سلطة إشرافية الدخول إلى هذا النظام المعلوماتي.

لنصل في الأخير إلى ما يهمنا في هذا الصدد وهو إنشاء سلطة مراقبة مشتركة بين الدول المتعاقدة في اتفاقية شنغن، تكلف بمهمة التحكم في وظيفة الدعامة التقنية لنظام المعلومات شنغن، ولها في إطار هذه المهمة سلطة التحقق من التطبيق السليم لأحكام هذه الإتفاقية، من خلال العمل على تحليل صعوبات تطبيق وتفسير نظام المعلومات شنغن (SIS) الناشئة عن استغلال هذا النظام، وكذا دراسة المشاكل التي تفرزها عمليات المراقبة التي تقوم بها السلطات الإشرافية الوطنية التابعة للدول المتعاقدة،

[1] Alessandro Mantelero, intelligence artificielle et protection des données : enjeux et solutions possibles, direction générale droits de l'homme et état de droit, conseil de l'europe, T-PD (2018) 09 Rev disponible sur le site : http://www.rm.coe.int/intelligence-artificielle

[2] Convention d'application de l'accord de s'chengen du 14 juin 1985 entre les gouvernements des Etats de l'union économique Bénélux, de la république fédérale d'Allemagne et de la république française relatif à la suppression graduelle des controles aux frontières communes, journal officiel des communautés européennes n° L239, 22 septembre 2000, p19.

[3] Voir l'article premier : de la décision-cadre 2008/977/JAI du conseil du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, Acte pris en application du titre VI du traité UE Journal officiel de l'union européenne n° L 350/60 du 30.12.2008.

[4] Le système d'nformation shengen, Mémonto sur l'éxercice du droit d'accès rédigé par l'autorité de contrôle commune de shengen, disponible sur le site : http://www.mzv.cz

أو بمناسبة ممارسة حق الوصول إلى هذا النظام، إضافة إلى عملها على وضع مقترحات تنسيقية وحلول مشتركة للمشاكل الناتجة عن عمل هذا النظام المعلوماتي بين الدول الأعضاء.[1]

وتتكون السلطة المشتركة لمراقبة النظام المعلوماتي شنغن من ممثلين عن كل سلطة إشرافية وطنية مستحدثة في إطار المادة 114 من هذه الإتفاقية، يكون لكل دولة صوت تداولي واحد داخل هذه السلطة.

وتعتمد أساسا في أداء مهامها حسب المادة 115 من هذه الإتفاقية على التوصية رقم 15 (87) R الصادرة عن لجنة الوزراء للدول الأوروبية، والمتعلقة بتنظيم استخدام البيانات الشخصية في قطاع الشرطة[2]، وتعد هذه السلطة المشتركةتقارير عن أنشطتها، ترسلها إلى الجهات الرسمية، التي ترسل إليها السلطات الإشرافية الوطنية تقاريرها.[3]

ثانيا: هيئات حماية المعطيات الشخصية على مستوى التشريع الفرنسي:

بالرجوع إلى النصوص القانونية في التشريع الفرنسي المتعلقة بمجال حماية المعطيات ذات الطابع الشخصي ألزم المشرع الفرنسي بموجب القانون 17/18 المتعلق بالمعلوماتية والحريات المؤرخ في 6 جانفي 1978 المؤسسات والهيئات التي تقوم بمعالجة المعطيات الشخصية أن تعين أشخاصا يعملون لديها، تسند لهم مهام المساهمة في حماية البيانات الشخصية داخل المؤسسة.

1) مراسل حماية المعطيات الشخصية: correspondant à la protection des données à caractère personnelles (CDP)

تنص المادة 3/22 من القانون 801/2004 المؤرخ في 6 أوت 2004 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة البيانات ذات الطابع الشخصي والمعدل للقانون 17/78 على أن "المعالجات التي يعين لها المسؤول عنها مراسل لحماية البيالت الشخصية يتولى بشكل مستقل ضمان الإمتثال للإلتزامات المنصوص عليها في هذا القانون، تكون معفاة من الإجراءات المنصوص عليها في المادتين 23،24 (المتعلقة بالتصريح والترخيص المسبق) باستثناء عمليات المعالجة التي يتم فيها نقل البيانات الشخصية إلى دولة ليست عضوا في المجموعة الأوروبية".

لقد كانت عمليات جمع ومعالجة البيانات ذات الطابع الشخصي تخضع للتصريح المسبق إلى اللجنة الوطنية لحماية البيانات، وقد خضع العديد من المسؤولين عن المعالجة إلى عقوبات جزائية نتيجة عدم احترام هذه الإجراءات[4]، إلى غاية صدور القانون 801/2004، الذي ابتكر ما يعرف بمراسل حماية

[1] Voir l'article 115 de la convention d'application de l'accord de shengen. Journal officiel n° L 239 du 22/09/2000 p. 0019 - 0062

[2] Recomendation n° R (87) 15 du comité des ministre aux états membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée par le comité des ministres le 17 septembre 1987 lors de la 410ème réunion des délégués des ministres.

[3] Voir l'article 115/4 de la convention d'application de l'accord de shengen.

[4] Eric A. Caprioli, le corespondant à la protection des données à caractère personnel : un nouvel arbitre pour l'entreprise, disponible sur le site : http://www.caprioli-avocts.com

البيانات كآلية لتبسيط الإجراءات وتسهيلها، خاصة فيما يتعلق بالتصريحات المسبقة من طرف المؤسسات المعالجة للمعطيات الشخصية إلى اللجنة الوطنية لحماية المعطيات، ويأتي ذلك استجابة إلى ما نصت عليه الفقرة الثانية من المادة 18 من التوجيه الأوروبي لحماية المعطيات الشخصية CE/95/46 والتي تنص على تبسيط الإلتزام بالإعلان عن المعالجة أو عدم التقيد به، عندما يعين المسؤول عن المعالجة مراسلا مسؤولا عن ضمان تطبيق مستقل للقانون المتعلق بمسائل حماية البيانات الشخصية والتأكد من أن المعالجة لا تحمل أي انتهاك لحقوق وحريات الأشخاص.[1]

وقد أكدت المادة 22 من القانون 2004/801 على أن مراسل البيانات الشخصية هو الشخص الذي يتمتع بمؤهلات يكون المسؤول داخل المنظمة عن ضمان الإ متثال الأنسب للإلتزامات المنصوص عليها في القانون فيما يتعلق بمعالجة البيانات الشخصية، وهو على هذا النحو يجب أن يحتفظ بسجل يحتوي على جميع المعالجات التي تتم ويمكن الوصول إليها على الفور من طرف أي شخص عند الطلب،[2] ويتعين حسب المادة 47 من المرسوم التنفيذي 1309 لسنة 2005[3] على المسؤول عن المعالجة أن يوفر لمراسل البيانات كافة العناصر التي تمكنه من إنشاء وتحديث سجل أو قائمة المعالجات الآلية المنفذة داخل المؤسسة أو الهيئة التي تم تعيينه فيها وذلك خلال ثلاث أشهر من تعيينه.

وبمجرد تعيين المسؤول عن المعالجة لمراسل حماية المعطيات الشخصية (CPD)، يتعين عليه إعلام اللجنة الوطنية بذلك فورا، ويصبح جراء ذلك معفى من الإعلان لهذه اللجنة بمعظم المعالجات الآلية للمعطيات الشخصية، في حين تبقى الجهات التي لا تعين مراسل لحماية البيانات خاضعة لإجراءات الإعلان المنصوص عليها في المواد 22 إلى 24 من القانون 2004/801.

ومن بين أهم المهام الرئيسية المنوط بمراسل البيانات القيام بها والتي حددتها المادة 49 من المرسوم التنفيذي 2005/1309

-يضمن مراسل حماية البيانات الإ متثال للإلتزامات المنصوص عليها في قانون حماية البيانات الشخصية عند إجراء المعالجات، ويجوز له في سبيل ذلك تقديم توصيات recommendations للمسؤول عن المعالجة.

- تتم استشارته بخصوص جميع المعالجات الجديدة قبل تنفيذها.

-يتلقى الطلبات والشكاوى من الأطراف المعينة، فيما يتعلق بالمعالجات الواردة في القائمة المنصوص عليها في المادة 47 من المرسوم، وإذا كان الأمر لا يدخل ضمن مسؤوليته يحولها إلى المسؤول عن المعالجة ويخطر الأطراف بذلك.

[1] Voir l'article 18 de la directive 96/46/CE du parlement européen et du conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[2] Voir l'article 22 de la loi 801/2004.

[3] Décret n° 2005/1309 du 20 octobre 2005 pris pour l'application de la loi n° 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés JORF n° 247 du 22 octobre 2005 page 16769.

- يبلغ المسؤول عن المعالجة بالخروقات والإعتداءات التي تمت معاينتها، قبل إحالتها على اللجنة الوطنية للمعلوماتية والحريات(CNIL) .

مع الإشارة إلى أن مراسل البيانات يمارس مهامه بطريقة مستقلة، ولا يمكن أن يخضع لأي عقوبة بسبب إنجاز مهامه، وإذا واجه صعوبات أثناء تأدية مهامه له أن يخطر اللجنة الوطنية للمعلوماتية والحريات (CNIL).[1]

2) اللجنة الاستشارية لمعالجة البيانات الشخصية في مجال البحوث الصحية:

(CCTRS) Le comité concultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé :

أنشئت هذه اللجنة بموجب المادة 20 من المرسوم 2005/1309 تحت الفصل الرابع بعنوان: أحكام خاصة بطلبات الترخيص بمعالجة البيانات الشخصية لغرض البحث العلمي في المجال الصحي، وذلك تطبيقا لأحكام المادة 64 من القانون 17/78المتعلق بحماية المعطيات ذات الطابع الشخصي.

وتتألف هذه اللجنة من 15 عضوا من المختصين بمهارات البحث في مجال الصحة وعلم الأوبئة وعلم الوراثة والإحصاء الحيوي، يعينون لمدة ثلاث سنوات قابلة للتجديد مرة واحدة بموجب قرار مشترك بين الوزير المكلف بالبحث العلمي والوزير المكلف بالصحة.

تختص هذه اللجنة الإستشارية بالنظر في أي طلب يتعلق بمعالجة البيانات الشخصية لأغراض البحث في المجال الصحي قبل إحالته إلى اللجنة الوطنية للمعلوماتية والحريات، وتبدي اللجنة رأيها خلال شهر من استلامها طلب الجهة المعنية.[2]

المبحث الثاني: الحماية الجزائية الموضوعية للحق في الخصوصية المعلوماتية:

ولدت فكرة حماية الحق في الخصوصية المعلوماتية من الناحية الجزائية انطلاقا من المخاطر الناشئة عن معالجة المعطيات ذات الطابع الشخصي، إذ كان لابد من تدخل المشرع لتحديد قواعد ومبادئ الحماية الجزائية لهذا النوع من المعطيات، و ذلك لما تقتضيه من أهمية بالنسبة لحق الأفراد في الحياة الخاصة عموما، ولقد احتدم الخلاف الفقهي حول مدى صلاحية النصوص الجزائية العقابية التقليدية المتعلقة بحرمة الحياة الخاصة في توفير الحماية الجزائية للمعطيات الشخصية، خاصة إذا تمت معالجتها آليا بواسطة أجهزة الكمبيوتر، إذ أن السؤال المطروح هو هل تكفي نصوص قانون العقوبات الحالي لمواجهة هذه الجرائم الجديدة المتولدة عن استخدام الحاسب الآلي في الإعتداء على

[1] Voir l'article 22 de la loi 2004/801

[2] انظر المواد 21،22 من المرسوم 1309/2005.

الحق في الخصوصية، خاصة إذا أخذنا في الحسبان أن القانون الجزائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا وكذا مهارة الذهن البشري في تسخير هذه المبتكرات في الإستخدام السيء.[1]

سواء أتمت معالجتها يدويا أم آليا، يذهب جانب من الفقه إلى الإقرار بفعالية هذه النصوص في توفير الحماية للمعطيات الشخصية، وبإمكانية استيعابها لحالات الإعتداء على هذه المعطيات باختراق الأنظمة المعلوماتية المخزنة فيها على أساس أن المشرع استخدم عبارة "... بأي تقنية كانت..." الواردة في المادة 303 مكرر من قانون العقوبات، وهي العبارة نفسها التي استخدمها المشرع الفرنسي في المادة 226-1 من قانون العقوبات الفرنسي « .... au moyen d'un procedé quelquonque ... » وبذلك يكون المشرع باستخدامه لهذه العبارة قد وسع من نطاق الحماية ومن شأنها أن تشمل أي اعتداء ضد الحق في الخصوصية، فتسمح بالعقاب على التقاط أو تسجيل أو نقل الأحاديث التي تجرى عبر الأنترنت، بالإضافة إلى العقاب على التقاط الصور الشخصية التي تخزن في النظم المعلوماتية أو الموجودة في ملفات معلوماتية شخصية بالبريد الإلكتروني، حتى ولو كانت موجودة لدى موزع الأنترنت.[2]

في حين يذهب اتجاه آخر[3] إلى اعتبار أن النصوص الجزائية التقليدية غير صالحة لتوفير الحماية للمعطيات الشخصية بسبب أن التجريم الذي تضمنته هذه النصوص متعلق فقط بالأفعال المتمثلة في الحصول على الصورة الشخصية أو تسجيل الحديث الخاص بطريقة غير مشروعة، في حين أن مقومات الحق في الخصوصية لا تتوقف عند هذا الحد، فهي ليست فقط صوتا لحديث يكون الفرد طرفا فيه، أو صورة للفرد في أي وضع كان عليه، بل إن مقومات الحق في الخصوصية أكثر بكثير من ذلك، حيث تشمل كذلك المعطيات الشخصية المخزنة في الأنظمة المعلوماتية أو المتداولة عبر شبكات وسائل الإتصال الإلكترونية، وهي الفئة من الخصوصية التي لم تشملها هذه النصوص الجزائية بالعقاب على الأفعال التي تشكل اعتداء عليها، لذلك فمن القراءة الأولى لهذه النصوص، يتأكد لنا وبلا أدنى شك عدم صلاحيتها لتوفير أدنى حماية جزائية للبيانات الشخصية والمحررة بالكتابة أو بأي وسيلة أخرى.[4]

لذلك كان الرأي الثاني راجحا فيما ذهب إليه من عدم صلاحية وكفاية النصوص السابقة في توفير الحماية الكاملة للمعطيات ذات الطابع الشخصي، ذلك أن الرأي الأول ارتكز على صيغة النص فيما يخص تقنيات الإعتداء، دون النظر إلى محل الإعتداء وهو المعطيات الشخصية خاصة تلك المعالجة آليا، والتي لم يشملها النص التجريمي إطلاقا ولا يمكن إعمال القياس لحالات واقعية على الحالات المنصوص عليها قانونا، لأن ذلك فيه خروج عن مبدأ الشرعية.[5]

---

[1] جميل عبد الباقي الصغير القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الآلي، مكتبة دار النهضة العربية، القاهرة، 1992، ص 12.

[2] مدحت رمضان عبد الحليم، مرجع سابق، ص.112

[3] فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الثانية، 2007، ص 300.

[4] عمر فاروق الحسيني، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الثانية، 1995، ص 121.

[5] رشيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص123.

وما يؤكد هذا الإتجاه هو النظر من زاوية أن النصوص التقليدية وضعت للتطبيق وفقا لمعايير معينة تركز على المحل المادي للجريمة (منقول، مادي)، في حين أن القيم في مجال المعطيات ذات الطابع الشخصي لها طبيعة غير مادية، بالإضافة إلى ما تتميز به الأساليب التقنية التي تستخدم في ارتكاب هذا النوع الجديد من الجرائم من ذاتية خاصة[1] ذلك أن البيانات المعالجة آليا يتم الإعتداء عليها باستخدام وسائل التقنية ذاتها، وبالتالي فإن هذه الإعتداءات تقع في صورها الغالبة ضمن نطاق الجرائم المعلوماتية والتي من منطلق مبدأ شرعية التجريم والعقاب تستوجب أحكاما ونصوصا تجريمية خاصة بهذه الأنواع الجديدة من الجرائم.[2]

لأجل ذلك فقد برز الجهد التشريعي الوطني في النظم المقارنة، من خلال إصدار تشريعات خاصة، أو تعديل لقوانين العقوبات للنص على تجريم الأفعال التي تشكل اعتداء على الخصوصية المعلوماتية، بعد أن أدركت أن النصوص التقليدية عاجزة عن استيعاب هذه الأفعال.[3]

ومن جهة أخرى أيضا لم تتفق التشريعات التي اتجهت إلى إفراد نصوص جزائية خاصة تختلف عن تلك النصوص القائمة في القوانين التقليدية، بين من أدرج هذه النصوص ضمن النص العقابي العام وهو قانون العقوبات في القسم الخاص منه، كما فعل المشرع الفرنسي[4]، وذلك في قسم مستقل تحت عنوان الإعتداءات على حقوق الأشخاص الناتجة عن الملفات والمعالجة المعلوماتية، وبين من نص على أحكام جزائية ضمن نص قانوني مستقل صادر في شأن حماية المعطيات الشخصية وتنظيم قواعد ومبادئ معالجتها، مثل المشرع الجزائري والمغربي والتونسي وغيرهم.

وإن كنا نرى أنه من الأجدر بالمشرع الجزائري أن يساير نظيره الفرنسي في هذه المسألة والإتجاه إلى إضافة صور التجريم الجديدة الماسة بالمعطيات الشخصية التي جاء بها القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي، إلى نصوص القسم الخاص من قانون العقوبات، وفي ذلك إقرار بانطباق الأحكام العامة عليها، ونجد أن هذا المسلك قد تبنته توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي.[5]

والحقيقة أنه إذا كان من الطبيعي بعد إقرار الحق في الخصوصية كحق عام، أن يستتبع ذلك بالتدخل التشريعي لتوفير مستويات من الحماية الجزائية تتصل بتكريس هذا الحق وصونه وردع الإعتداءات التي تطاله، فإنه من الطبيعي أن تكون هذه الحماية الجزائية متلائمة مع نطاق الإعتراف بهذا الحق ومشتملاته فإذا كان النظام القانوني يحصر حماية الحق في الخصوصية بحماية الشخص من الإنتهاكات المادية لشخصه وملكه، فستكون الحماية الجزائية مكرسة لهذا الفهم من خلال انحصارها في حماية المسكن والمراسلات وحماية حرية الإنسان من الأنشطة التي تستهدف بدنه أو كرامته أو سمعته، أما إذا كان الحق

[1] جميل عبد الباقي الصغير، مرجع سابق، ص12.

[2] بولين أيوب، مرجع سابق، ص383.

[3] مروة زين العابدين، مرجع سابق، ص 380.

[4] Article 50 de la loi 801/2004 : disposition pénale : les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

[5] مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها ومكافحتها) دراسة مقارنة، دار الكتب القانونية، 2005، ص37.

في الخصوصية يتجاوز هذا المفهوم إلى حماية السرية عموما، فسنجد النظام القانوني يضفي الحماية الجزائية ضد كل أنشطة التجسس والتنصت وغيرها، وإذا كان النظام القانوني يوسع من دائرة الحماية لتشمل البيانات الشخصية، فإن صور التجريم ستتسع لتشمل الإنتهاكات والإعتداءات التي تظهر في مجال جمع ومعالجة واستخدام ونقل البيانات الشخصية، و من ثم فتبعا لمستوى ونطاق ومحل الحماية الجزائية تحدد صور التجريم.[1]

وعلى هذا الأساس فقد سبق للمشرع الجزائري أن عمل على إصدار نصوص جزائية تحمي أنظمة المعالجة الآلية بشكل عام كيفما كان محتواها سواء معطيات شخصية أو غير ذلك، من خلال استحداث القسم السابع مكرر في قانون العقوبات بعنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004،[2]

ثم جاء مؤخرا بالفصل الثالث من القانون 07/18 المؤرخ في 10 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي بعنوان الأحكام الجزائية، من أجل تجريم صور عتداء على المعطيات الشخصية والمعاقبة عليها.

ولم يقتصر الأمر فقط على هذا النص القانوني الإطار، فمن أجل تحقيق حماية جزائية فعالة وناجحة للحق في الخصوصية المعلوماتية، نجد بعض النصوص القانونية الأخرى التي تحمل في طياتها أحكاما جزائية تضمن توفير الحماية الجزائية لهذا الحق في مجالها.

المطلب الأول: الجرائم الماسة بالحق في الخصوصية المعلوماتية في إطار القانون 07/18

لقد استهل المشرع الجزائري النص التشريعي المتمثل في القانون 07/18 بمبدأ أساسي يقوم على أن معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها، يجب أن تتم في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم[3]، مستندا في ذلك إلى نفس المبدأ الذي أوردته المادة الأولى من القانون الفرنسي 17/78 المتعلق بالمعلوماتية والحريات، وهو أن المعالجة الآلية للبيانات الشخصية يجب أن لا تحمل أي اعتداء على شخصية الأفراد أو حقوق الإنسان أو الحياة الخاصة أو الحريات الفردية أو العامة.[4]

وفي نطاق هذا المبدأ، جرى الوقوف على تحديد مجموعة من القواعد والمبادئ لضمان حماية الأشخاص الطبيعيين من صور الإعتداء التي تطال حقهم في الخصوصية عبر المساس بمعطياتهم الشخصية أثناء معالجتها، حيث عاقب المشرع من خلال قواعد التجريم والعقاب على مجموعة من الأفعال الماسة بهذا

[1] بولين أيوب، مرجع سابق، ص380.

[2] أنظر الجريدة الرسمية رقم 71 لسنة 2004 ص.11 و12.

[3] أنظر المادة 02 من القانون 07/18.

[4] Voir l'article 1er de la loi 78/17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par l'article 54 de la loi n° 2016/1321 du 07 octobre 2016.

الحق، وذلك بغرض تكريس حماية جزائية للمعطيات الشخصية في مواجهة نظم المعلومات، إدراكا منه لما يترتب على استخدام قواعد البيانات من آثار بالغة الخطورة على حق الأفراد في الخصوصية.

وباستطلاع نصوص التجريم التي تضمنها القانون 07/18 المحددة لصور السلوك الإجرامي التي تقع على الحق في الخصوصية في علاقته بمسائل معالجة المعطيات الشخصية، يمكن تصنيفها إلى فئات تنصب على القواعد الموضوعية للمعالجة، وأخرى تنطوي على مخالفة القواعد الإجرائية المنظمة لأنشطة المعالجة، ضمن تصنيفها إلى الفئات التالية:

الفرع الأول: الجرائم الماسة بالقواعد الموضوعية لمعالجة المعطيات الشخصية

تتعلق هذه الطائفة من الجرائم بالأفعال التي تشكل خرقا للقواعد الموضوعية التي يلتزم المسؤول عن المعالجة بمراعاتها عند القيام بكل معالجة للمعطيات الشخصية، وترتبط أساسا بالأفعال الماسة بالمعطيات الشخصية في حد ذاتها، كأن يصار إلى جمعها بطرق غير مشروعة أو جمعها دون علم صاحبها أو استخدامها في غير الأغراض التي جمعت لأجلها....

أولا: الجرائم الماسة بالمعطيات الشخصية ذاتها:

سبق الإشارة أن خصوصية الأفراد بصورتها المستحدثة والمرتبطة بالتقنية المعلوماتية أصبحت مهددة بالعديد من الإنتهاكات والإعتداءات من خلال المساس بحرمة البيانات الشخصية، لذلك فإن احترام حقوق وحريات الأشخاص المعنيين بمعالجة بياناتهم الشخصية يقتضي ضرورة جمع هذه البيانات بطريقة نزيهة ومشروعة وغير تدليسية، و أن تكون كل معالجة لهذه البيانات متوافقة مع الأغراض المصرح بها والمرخص لها، وأن تتم في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وكل ما يخالف ذلك يعتبر معالجة غير مشروعة يدخل ضمن دائرة التجريم والعقاب.

1)الجرائم المرتبطة بالمعالجة غيرالمشروعة: يدخل ضمن هذه الفئة من الجرائم:

1-1) جريمة جمع معطيات شخصية بطريقة تدليسية أو غير مشروعة أو غير نزيهة: تنص المادة 59 من القانون 07/18 على أنه يعاقب بالحبس من سنة (01) إلى ثلاث سنوات وبغرامة من 100 ألف إلى 300 ألف دينار، كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة.

نشير بداية قبل التطرق إلى مناقشة أركان هذا الجرم أن المشرع حصر وقوع الطرق التدليسية وغير المشروعة على عملية جمع المعطيات الشخصية فقط، في حين أن عملية الجمع ماهي إلا واحدة من بين عمليات عديدة تندرج ضمن نشاط المعالجة، كما سبق وأن عرفنا ذلك في المادة 03 من نفس القانون، فعدم المشروعية لا يقتصر فقط على عملية الجمع، بل يفترض أن يشمل جميع العمليات التي تدخل في إطار المعالجة المنصبة على المعطيات الشخصية، فقد تكون مثلا عملية تسجيل أو حفظ أو استخراج أو طلاع على المعطيات الشخصية غير مشروعة أو تتم بطرق تدليسية، ومن ثمة فإن النص القانوني بهذه الصيغة لا يحتمل هذه الأفعال، وقد يفلت مرتكبوها من العقاب انطلاقا من مبدأ الشرعية، لذلك نجد

أن بعض الفقه يذهب إلى القول أن المقصود هو جميع الأفعال من جمع أو تسجيل أو حفظ أو تخزين، وكل ما يتم في نطاق الأنشطة المعروفة بالمعالجة الآلية للبيانات الشخصية في نظم المعلومات[1]، وهو رأي نخالفه بحجة أن المشرع لم يكن صعبا عليه أن ينص على عمليات المعالجة بدل عملية الجمع فقط إن كان يقصدها كلها، ولا يمكن أن نحمل النص الجزائي أكثر مما يحتمل، وهو ما يتضح من موقف المشرع الفرنسي الذي جرم فقط عملية جمع المعطيات الشخصية التي تتم بطريقة غير مشروعة من خلال نص المادة 226-18 من قانون العقوبات الفرنسي التي تقابل نص المادة 59 أعلاه:

226-18 : « le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal, ou illicite est puni ... ».

1-1-1) أركان الجريمة:ويتعلق الأمر أساسا بالركنين المادي والمعنوي:

أ) الركن المادي: يقوم الركن المادي لهذه الجريمة عند توفر عنصرين أساسيين:

- سلوك إجرامي يتضمن عملية الجمع للمعطيات الشخصيةباستعمال طرق غير مشروعة في ذلك.

- عنصر مفترض يتعلق بمحل أو موضوع الجرم، وهو أن ينصب هذا السلوك الإجرامي على المعطيات الشخصية.

أما بالنسبة لعملية الجمع فيقصد بها أن يتمكن مرتكب الجريمة من الحصول على معطيات ذات طابع شخصي تخص شخصا أو عدة أشخاص، وهي عملية تكون في بدايات عمليات المعالجة وإحدى مراحلها فحسب نص المادة الثالثة من القانون 07/18 عرفت المعالجة على أنها "كل عملية أو مجموعة عمليات .... مثل الجمع أو....»، فمن أول الأنشطة التي يقوم بها المسؤول عن المعالجة هو السعي إلى تحصيل وتجميع المعطيات الشخصية للمعني بالمعالجة صاحب المعطيات الشخصية.

وقد تكون عملية الجمع يدوية أي منصبة على معطيات شخصية في ملفات أو سجلات ورقية موجودة مسبقا على مستوى الإدارات أو الهيئات، أو صرح بها طالب الخدمة من خلال ملئ الإستمارات الضرورية للحصول على هذه الخدمة، أو غير ذلك كما تكون عملية آلية automatisé باستعمال الأجهزة المعلوماتية عن طريق انتقائها وإدراجها في ملفات رقمية.

كما ترد عملية الجمع على عدة معطيات شخصية مختلفة تخص شخصا واحدا مثل رقم هاتفه، بريده الإلكتروني، تاريخ ومكان ميلاده... أو أن ترد على نفس المعطيات تخص عدة أشخاص.

أما بالنسبة لاستعمال طرق غير مشروعة في عملية الجمع، فلا خلاف بأنه مناط التجريم، ذلك أن القانون لا يجرم عملية جمع البيانات في حد ذاتها بغض النظر عن نوعها أو طبيعتها، ولكن التجريم جاء نتيجة الأساليب غير المشروعة وغير النزيهة المستعملة في الحصول على البيانات الشخصية.

[1] بولين أيوب، مرجع سابق، ص380

ويتحقق جمع المعطيات الشخصية بطريقة غير مشروعة من خلال الحصول عليها باستعمال وسائل تقنية متعددة كالتقاط الموجات التي تحدثها الأصوات عبر الجدران ومعالجتها بكمبيوتر مزود ببرنامج خاص لترجمتها إلى كلمات أو عبارات، أو تفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني، أو توصيل أسلاك بطريقة خفية إلى الكمبيوتر الذي تختزن فيه المعطيات الشخصية[1]، أو الحصول عليها أيضا بواسطة زرع فيروس (virus) في الكمبيوتر الخاص بالمستخدم للتطفل على معطياته الشخصية، حيث يكون بمقدور هذا البرنامج الفيروسي اختراق نظام إدارة قاعدة البيانات[2] ، ومن ثم السماح بالحصول على معطيات شخصية بطريقة غير مشروعة، أو يمكن أن يتم الجمع غير المشروع أيضا للمعطيات الشخصية بنصب مصائد بيانات لالتقاط وجمع بيانات شخصية خاصة بمستخدمي أنظمة "الفيديو تكس" دون أن يكون في مقدور أصحابها العلم بذلك.[3]

والملاحظ في هذا الصدد أن هذا العنصر من السلوك الإجرامي المكون للركن المادي لهذه الجريمة يطرح صعوبة كبيرة أمام عدم دقة المصطلحات التي استعملها المشرع وعدم توضيحه لما يقصده بالطرق التدليسية وغير النزيهة، ويبقى تقدير ذلك للقاضي الجزائي، وفي الغالب يشير الفقه الجنائي أن الطرق التدليسية تكون باستعمال أسماء وصفات كاذبة، أو باستعمال مناورات احتيالية من أجل خداع الشخص المعني، فيكون لها أثر في نفسه يدعوه لتصديق الجاني، ومن ثم يقدم له معطياته الشخصية، فيقوم هذا الأخير بجمعها.[4]

أما الطريقة غير النزيهة فتعني مخالفة المسؤول عن المعالجة لواجباته الأخلاقية في تعامله مع الجمهور أثناء جمع معطياتهم الشخصية كاستغلال النفوذ والتعسف في جمعها.

وإن كان مصطلح "بطريقة غير مشروعة" يكفي وحده ليتضمن الوسائل التدليسية وغير النزيهة لجمع المعطيات[5]، بحيث يمكن أن تتحقق عدم المشروعية في عملية الجمع للمعطيات بكل طريقة خفية لا تخلو من الإحتيال والغش والتدليس وهي من صور عدم المشروعية، كما لو كانت المعطيات الشخصية التي يقدمها الشخص لا تتناسب مع الخدمة التي يسعى إليها، ذلك أن عدم التناسب ينطوي على غش يعيب الرضا، كما يعتبر تدليسا تقديم وعود كاذبة من قبل المسؤول عن المعالجة في سبيل الحصول على هذه المعطيات.[6]

---

[1] بولين أيوب، مرجع سابق، ص 395.

[2] معالجة المعلومات القانونية في القرن الحادي والعشرين وتحدياتها، مركز الأبحاث والدراسات في المعلوماتية القانونية بيروت مكتبة صادر 2002، ص 365.

[3] يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، الجزء الثاني: الخصوصية وحماية البيانات في العصر الرقمي، اتحاد المصارف العربية، الطبعة الأولى، 2002، ص 506.

[4] أنظر في هذا المعني: أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص- دار هومة، الطبعة السادسة، 2016-ص 319.

[5] طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، مقال منشور في المجلة الأكاديمية للبحث القانوني، العدد 02، 2018 ص 32 متوفرعلى الرابط:https://www.asjp.cerist.dz/en/PresentationRevue/72

[6] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، تهميش رقم 03، مرجع سابق، ص 634.

وقد اعتبرت محكمة النقض الفرنسية في قرارها المؤرخ في 14 مارس 2006 أنه تعد عملية جمع غير نزيهة كل تجميع للعناوين الإلكترونية الشخصية للأشخاص الطبيعيين دون علمهم في الفضاء العام للأنترنت باعتبار هذه الطريقة تشكل عائقا أمام ممارسة حقهم في عتراض.[1]

كما اعتبر القضاء الفرنسي أيضا أن الجمع غير النزيه للمعطيات الشخصية، يتحقق أيضا بكل اطلاع على العناوين الإلكترونية واستعمالها ولو دون تسجيلها في ملف، من أجل إرسال رسائل إلكترونية لأصحاب هذه العناوين.[2]

أما بالنسبة للعنصر المفترض ويتعلق بمحل الجريمة، ويتمثل في المعطيات ذات الطابع الشخصي وهي موضوع كافة الجرائم التي سوف نتطرق إليها لاحقا.

وعليه لكي تقوم هذه الجريمة يجب أن تكون المعطيات موضوع الجمع بالطرق التدليسية أو غير مشروعة أو غير نزيهة، هي معطيات ذات طابع شخصي، وتكون كذلك إذا كانت هذه المعطيات من شأنها حسب تعريف المادة الثالثة من القانون 07/18 أن تؤدي بطبيعتها إلى التعرف على الشخص كإسمه وعنوانه ورقم هاتفه وبنفس الصيغة عرفها المشرع الفرنسي في المادة الثانية من القانون 2004/801 المعدل للقانون 17/78 المتعلق بالمعلوماتية والمفات والحريات بأنها كل معلومة تتعلق بشخص طبيعي بشكل مباشر أو غير مباشر...." وعرفتها أيضا لجنة المعلومات والحريات الفرنسية (CNIL) بأنها بيانات قد تتخذ شكل جملة، إشارة، رقما، كلمة، أو صفة معينة تجعل الشخص قابلا للتحديد أو من شأنها أن تجعله قابلا للتعرف عليه، كرقم تسجيل الضمان الإجتماعي، الرقم التعريفي الوطني، رقم الحساب البنكي، أو البيانات المتعلقة بالجوانب المهنية أو المالية أو الصحية ...

ومن خلال هذه التعاريف للمعطيات ذات الطابع الشخصي يمكننا القول أن مسألة اعتبار معلومة معينة تتعلق بالشخص الطبيعي تندرج ضمن بياناته الشخصية أم لا، هي مسألة موضوعية تخضع للسلطة التقديرية للقاضي.

ب) الركن المعنوي: يتحقق الركن المعنوي لهذه الجريمة بالقصد الجنائي العام الذي يتضمن عنصري العلم والإرادة، فهي جريمة عمدية، يجب أن يعلم مرتكب الجريمة أن المعطيات التي يقوم بجمعها هي معطيات شخصية تتعلق بشخص طبيعي، ويعلم بعدم مشروعية طرق وأساليب جمعها، ثم تتجه إرادته إلى القيام بهذه الأفعال بذاتها، وإلا انتفى القصد الجنائي وانعدم الركن المعنوي للجريمة.

---

[1] Myriam Quéméner, Yves Charpenel, cybercriminalité, droit pénal appliqué, collection pratique du droit, Economica, Septembre 2010, p66.

وتتلخص وقائع القضية في قيام إحدى الشركات سنتي 2002 و2003 بإرسال رسائل إلكترونية إشهارية إلى مجموعة من الأفراد كانت قد قامت بجمع عناوينهم الإلكترونية من شبكة الأنترنت ثم القيام بواسطة برنامج حاسوب (logiciel) بتسجيل المعلومات المتعلقة بهم في ملف إلكتروني بغية استعمالها لاحقا، ثم القيام في مرحلة أخرى بواسطة برنامج آخر بتوجيه رسائل اشهارية الى تلك العناوين المجمعة دون تسجيلها في ملف آخر. أنظر كذلك: Yves Mayaud, op,cit, p 674

[2] Myriam Quéméner, Yves Charpenel, op. cit, P 66.

مع الإشارة أن هذه الجريمة تقوم على القصد الجنائي العام، ولا تتطلب قصدا خاصا، فلا عبرة بالبواعث التي دفعت الجاني الى ارتكاب هذه الجريمة.[1]

2-1-1) العقاب: انطلاقا من المادة 59 والمادة 71 من القانون 07/18 فإن العقوبة المقررة لهذه الجريمة

أ) العقوبة الأصلية: تعاقب المادة 59 من القانون 07/18 على جنحة جمع معطيات شخصية بطريقة غير مشروعة بالحبس من سنة (1) إلى ثلاث سنوات وبغرامة من 100 ألف إلى 300 ألف دج.

ب) العقوبة التكميلية: حسب المادة 71 من القانون 07/18 يمكن أن يتعرض مرتكب هذه الجريمة إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات، وهكذا يجوز للجهات القضائية الحكم على الشخص المدان حسب المادة 09 من قانون العقوبات، بالعقوبات التكميلية الإختيارية التالية: الحجر القانوني، الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية، تحديد الإقامة، المنع من الإقامة، المصادرة الجزئية للأموال، المنع المؤقت من ممارسة مهنة أو نشاط، إغلاق المؤسسة، الإقصاء من الصفقات العمومية، الحظر من إصدار الشيكات، أو استعمال بطاقات الدفع، سحب جواز السفر، نشر أو تعليق حكم أو قرار الإدانة و زيادة على ذلك فإنه يجوز للقاضي حسب المادة 71 من القانون 07/18 أن يأمر بمسح كل جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب الجريمة .

ج) الشروع: يعاقب على محاولة ارتكاب هذه الجريمة بنفس العقوبة المقرر للجريمة التامة.[2]

2-1) جريمة الاستعمال التعسفي أو التدليسي للمعطيات الشخصية:

تنص المادة 69 من القانون 07/18 على أنه يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100 ألف إلى 500 ألف دينار كل مسؤول عن المعالجة وكل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل ولو عن إهمال الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك.

1-2-1) أركان الجريمة:

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة حسب نص المادة 69 المذكورة أعلاه بتوافر العناصر التالية:

- العنصر المفترض: وهو ارتكاب الجرم من قبل أشخاص معينين.

-أن يتم التسبب أو التسهيل للغير في الإستعمال التعسفي أو التدليسي للمعطيات الشخصية.

[1] عمار عباس الحسيني، مرجع سابق، ص 242.

[2] أنظر المادة 73 من القانون 07/18.

فبالنسبة لارتكاب الجريمة من قبل أشخاص معينين: فقد حددتهم المادة 69 بالمسؤول عن المعالجة والمعالج من الباطن، وكل شخص بحكم المهام المكلف بها يقوم بمعالجة معطيات شخصية، بحيث لا يمكن أن ترتكب هذه الجريمة من قبل أي شخص وإنما يلزم ارتكابها من:

* المسؤول عن المعالجة : وهو كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها[1]، وهو بهذا المعنى قد يكون مؤسسة عامة أو خاصة، سواء كانت تهدف لتحقيق الأرباح أم مجانية أو إدارة رسمية أو شركة تجارية أو جمعية أو مؤسسة استشفائية أو مكاتب أعمال أو غير ذلك ممن يرخص لهم بجمع ومعالجة معطيات شخصية، من خلال إنشاء ملفات إلكترونية تحتوي على معطيات تحدد هوية الأشخاص الطبيعية كالإسم ،الجنس ،السكن ، فصيلة الدم، الوضع الإجتماعي، الشهادات المدرسية، الوظيفة تاريخ الدخول و الخروج من الدولة وأي معلومات تتعلق بشخص الإنسان .[2]

* أما المعالج من الباطن فهو كما عرفه القانون 07/18 كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة، وهو بهذا المعنى قد يكون أي كيان يدخل في علاقة تعاقدية مع المسؤول عن المعالجة، يلتزم بموجب هذا العقد بالعمل على معالجة المعطيات الشخصية لحساب المسؤول عن المعالجة.

وفيما يتعلق بالشخص المكلف بمعالجة المعطيات الشخصية بحكم وظيفته ومهامه، فهو كل متدخل في عملية المعالجة بشكل مباشر أو غير مباشر، دون أن يتعلق الأمر بالمسؤول عن المعالجة أو المعالج من الباطن،مثل الموظفين الإداريين أو المكلفين بمصلحة الإعلام في الشركة ... ويكونون بحكم وظيفتهم ممن يعملون لدى المسؤول عن المعالجة أو المعالج من الباطن وخاضعين لسلطتهم.

-وبالنسبة للسلوك الإجرامي المتمثل في التسبب في الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو تسهيل ذلك، فيتعلق بمجموع التصرفات و السلوكات التي يأتيها الفاعل، فتؤدي إلى استعمال تعسفي أو تدليسي من قبل الغير للمعطيات الشخصية، ومن ثم فإن هذا السلوك الإجرامي يقوم أساسا على فعل ونتيجة وعلاقة سببية بينهما، فأما الفعل فهو أن يقوم المسؤول عن المعالجة أو المعالج من الباطن بأفعال سواء كان ذلك عمدا أو عن إهمال منه، وتكون نتيجتها التسبب والتسهيل للغير ستعمال التعسفي وغير المشروع للمعطيات الشخصية، وأن تكون هناك رابطة قوية بين تصرفات الفاعل المتسببة والمسهلة لوصول المعطيات الشخصية للغير وبين الأفعال التي يقوم بها هذا الأخير والمتمثلة في الإستعمال التعسفي والتدليسي لها ، ومن ثم يشترط لقيام الركن المادي لهذه الجريمة في حق المسؤول عن المعالجة أو المعالج من الباطن أن يكون هو االمتسبب المباشر في حصول الغير على المعطيات الشخصية سواء كان متعمدا في ذلك أو نتيجة إهمال منه .

[1] أنظر المادة 03 من القانون 07/18.

[2] نعيم مغبغب، مرجع سابق، ص149، 150.

والإهمال هو موقف سلبي من الفاعل عن القيام بما هو واجب عليه وتركه التزاما مفروضا في مسلكه الشخصي أو المهني، والتقاعسعن اتخاذ التدابير والإ حتياطات والوسائل الضرورية والمناسبة لتفادي وقوع الفعل وبالتالي حدوث النتيجة الضارة.

كما نشير أن المشرع في هذه الجريمة لم يشترط أن ينصب هذا الفعل على المعطيات الشخصية التي تمت معالجتها، بل يكفي فقط لمجرد أن تكون هذه المعطيات في مرحلة تسلمها ولم تدخل بعد في مراحل عمليات المعالجة بعد.[1]

والمقصود بالغير الذي يمارس فعل الإ ستعمال التدليسي أو التعسفي للمعطيات الشخصية، هو كل من ليس له الصفة القانونية وغير مؤهل للحصول على المعطيات الشخصية، ويكون الشخص غير مؤهل للحصول واستلام المعطيات الشخصية عندما لا يخوله القانون الحق في الإطلاع عليها، وهو ما أكده مجلس الدولة الفرنسي حينما اعتبر أن البيانات التي تجمعها عناصر الشرطة عن الأشخاص في إطار مهامها من أجل حماية من العام هي أساس عملهم، ومن ثم يلزم منع غيرهم من الوصول إليها[2]، كما نشير إلى القضية المتعلقة بشركة تأمين فرنسية التي تحصلت على بيانات شخصية تتعلق بعدد من زبائن شركة كهرباء فرنسا بتواطئ مع بعض العاملين في هذه الشركة، وتتلخص وقائعها في استلام عدد من الأشخاص كانوا قد انتقلوا إلى منازلهم الجديدة خطابات من إحدى شركات التأمين، تعرض عليهم إجراء التأمين الخاص لمنازلهم الجديدة لديها، وبعد التحري الذي قامت به اللجنة الوطنية لحماية المعطيات (CNIL) لمعرفة مصدر حصول شركة التامين هذه على معطيات هؤلاء الأشخاص ، تبين أن هذه الشركة قد حصلت عليها بطريق غير مشروع بمساعدة بعض العاملين بشركة الكهرباء نظير مبالغ نقدية، وقد أدانت محكمة باريس الإبتدائية شركة الكهرباء في حكمها الصادر في 1994/12/16 [3].

ب) الركن المعنوي: توسع المشرع في الركن المعنوي لهذه الجريمة حيث تعتبر من الجرائم العمدية التي تتطلب قصدا جنائيا، كما ترتكب أيضا عن طريق الخطأ، فالعمدية في ارتكابها تظهر من خلال اتجاه إرادة الفاعل بارتكاب أفعال يقصد من خلالها إيصال المعطيات الشخصية إلى الغير، أو تكون سببا في تسهيل وصولها إليهم، رغم علمه بأن القانون لا يخولهم الصفة ولا يؤهلهم لاستلامها، وأن من شأن أفعاله أن تؤدي إلى الإ ستعمال التعسفي والتدليسي لهذه المعطيات من طرفهم.

أما ارتكاب هذه الجريمة بالخطأ فيظهر من خلال استعمال المشرع لعبارة "ولو بفعل الإهمال"، والإهمال هو أحد عناصر الخطأ إلى جانب عناصر أخرى مثل عدم الحيطة والرعونة وعدم الإنتباه،[4] ومن ثم يكون الركن المعنوي قائما، إذا ظهر من ظروف الوقائع وملابساتها أن الفاعل اتخذ موقفا سلبيا ولم يقم بما يلزمه به القانون عن عدم تبصر و حيطة، وترتب على ذلك أن توصل الغير بالمعطيات الشخصية التي في

[1] المادة 69: ".... للمعطيات المعالجة أو المستلمة..."

[2] أسامة عبد الله قايد، مرجع سابق، ص 94.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية- الطبعة الأولى 2005، مشار إليه في الهامش 1 ص 238، 239.

[4] انظر حول عناصر الخطأ، أحسن بوسقيعة مرجع سابق، ص74،75،76.

حوزته، وإذا قامت الجريمة بركنيها المادي والمعنوي قامت المسؤولية الجنائية للفاعل، بصفته فاعلا أصليا، وليس التسهيل الذي يقوم به من قبيل عناصر المشاركة المنصوص عليها في المادة 42 من قانون العقوبات، وبالتالي لا يمكن اعتباره شريكا .

2-2-1) العقوبات المقررة قانونا:

أ) العقوبة الأصلية: نصت المادة 69 من القانون 07/18 على أنه يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100 ألف دج إلى 500 ألف دج.

والملاحظ أن المشرع قرر عقوبة واحدة لهذه الجريمة سواء ارتكبت عمدا أو عن طريق الخطأ، ولم يراعي في تقديره للعقوبة درجة الخطورة الإجرامية، فمن يرتكب هذه الجريمة بإهمال منه ليس بنفس درجة الخطورة الإ جرامية لمن يرتكبها متعمدا، ولهذا نجد المشرع الفرنسي يفرق في المادة 22/226 بين العقوبة المرصودة للفعل إذا كان عمدا وهي الحبس لخمس سنوات وغرامة 300 ألف أورو، وبين العقوبة لنفس الفعل إذا كان عن إهمال وهي الحبس لثلاث سنوات وغرامة 100 ألف أورو.

ب) العقوبات التكميلية: يقدر المشرع في العديد من الحالات عدم كفاية العقوبة الأصلية التي قررها كجزاء على اقتراف الجريمة في ردع الجاني، أو في حماية المصلحة التي قرر حمايتها، فينص على عقوبات تكميلية لتدعيم الحماية الجزائية[1]، وانطلاقا من المادة 71 من القانون 07/18 فإن القاضي الجزائي يمكن له أن ينطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 09 من قانون العقوبات، بالإضافة إلى الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي نتج عنها ارتكاب الجريمة.

3-1) جريمة إفشاء المعطيات الشخصية:

المقصود بفعل الإفشاء في هذه الجريمة هو نقل البيانات الشخصية من طرف المسيطر عليها بمناسبة معالجتها، إلى شخص أو جهة غير مختصة بتلقي هذه البيانات، وقد عاقب المشرع الجزائري في المادة 69 من القانون 07/18 كل مسؤول عن المعالجة أو كل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل في وصولها إلى غير المؤهلين لذلك، وهو الفعل الذي نصت عليه أيضا المادة 226-22من قانون العقوبات الفر [2]

وقد أشار الفقه إلى تبيان العلاقة بين هذه الجريمة المتعلقة بمعالجة المعطيات الشخصية وجريمة إفشاء الأسرار التي تعالجها قوانين العقوبات عموما، فهل من إمكانية لتطبيق نص المادة 301 من قانون العقوبات المتعلقة بتجريم إفشاء الأسرار التي علم بها الشخص بسبب أو بمناسبة مهنته أو وظيفته على

[1] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018، ص 232.

[2] تنص المادة 226-22 من قانون العقوبات الفرنسي "كل من تلقى بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الآلية معطيات شخصية من شأن إفشاءها الإضرار باعتبار صاحب البيانات أو حرمة حياته الخاصة وقام بنقلها دون موافقة المعني بها إلى من لا حق له في العلم بها يعاقب بخمس سنوات و300 ألف أورو.

وتكون العقوبة 03 سنوات حبس وغرامة 100 ألف أورو إذا كان الإفشاء نتيجة إهمال وعدم حيطة"

جريمة إفشاء المعطيات الشخصية المخزنة في أنظمة المعالجة من طرف من يعلم بها، لذلك فقد ثار التساؤل حقيقة حول مدى تطابق الجريمتان أم أن هناك اختلافا بينهما؟

إنه وبالنظر إلى موضوع الجريمة فإننا نجد أن جريمة إفشاء البيانات الشخصية موضوعها البيانات الشخصية المعالجة في الأنظمة المعلوماتية، أما جريمة إفشاء الأسرار المهنية فموضوعها المعلومات ذات الطبيعة السرية التي علم بها الموظف أثناء ممارسته وظيفته، كما أن الأسرار في هذه الجريمة الأخيرة يشترط فيها أن تكون رسمية أو متعلقة بمهنة معينة تفترض الثقة الضرورية للسرية، فهي تحرم على المستخدمين إفشاء الأسرار الخاصة بالمؤسسة التي يعملون بها والتي قد تكون متعلقة بالعمل، أو المصلحة الوطنية وليس فقط بالأشخاص.[1]

لذلك انتهى الفقه إلى القول بأن النصوص العقابية المتعلقة بجريمة إفشاء الأسرار المهنية لا تصلح لحماية البيانات الشخصية، خاصة إذا كانت محل معالجة آلية، فهما وإن كانا قد يتفقان في العلة التشريعية والمتمثلة في حماية البيانات والمعلومات المتعلقة بالأشخاص الطبيعيين، إلا أنهما يختلفان من حيث الموضوع والمحل[2]، وهناك من يذهب إلى القول أن النص العقابي المتعلق بجريمة إفشاء البيانات الشخصية يعد مخصصا ومقيدا للنص العقابي المتعلق بتجريم إفشاء السر المهني، ذلك أن النص الأول يعاقب على إفشاء سرية البيانات الشخصية المعالجة ضمن نظام معلوماتي من مالك النظام أو من له السيطرة عليه[3].

ويرى جانب آخر من الفقه أن جريمة إفشاء المعطيات الشخصية تقترب من جريمة إفشاء الأسرار المنصوص عليها في قانون العقوبات، والخلاف بينهما يكمن فقط في كون أن الإفصاح عن البيانات الشخصية المعالجة قد يتضمن بعض البيانات التي ليست من قبيل الأسرار، ومع ذلك تضل هذه البيانات محمية قانونا، ولذلك اعتبرت أن جريمة كشف البيانات الشخصية هي جريمة أوسع نطاقا من جريمة إفشاء الأسرار[4].

ومن جانبنا نؤيد الرأي الفقهي الذي يقول باختلاف كل من الجريمتين من حيث الموضوع والمحل.

1-3-1) أركان الجريمة: تتمثل أركان جنحة إفشاء البيانات الشخصية طبقا لأحكام المادة 69 من القانون 07/18 كما يلي:

[1] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي وشبكة الأنترنت، دراسة مقارنة، دار النهضة العربية، 2000، القاهرة ص 325.

[2] بولين أيوب، مرجع سابق، ص 403.

[3] علي جعفر، مرجع سابق ص 448.

[4] مدحت رمضان، مرجع سابق، ص 104.

ومن الحالات الواقعية التي يمكن أن نسردها في هذه المسألة هي الواقعة المتعلقة بالإعتداء على البيانات الشخصية المخزنة في النظم المعلوماتية التابعة لإحدى الدوائر الأمنية بالنمسا، حيث قام أحد ضباط شرطة العاصمة النمساوية فيينا بتزويد مخبر خاص ببيانات السجلات الجنائية وملفات معلومات البحث الجنائي وملفات الشرطة الجنائية الدولية –الأنتربول- المخزنة في الكمبيوتر العائد للشرطة عن بعض الأشخاص، وقد تمت إدانة ضابط الشرطة بجريمة إفشاء موظف عام للأسرار (وليس عن جرم إفشاء معطيات شخصية) انظر بولين أيوب، مرجع نفسه، ص406.

أ) الركن المادي: يستفاد من نص المادة 69 أن الركن المادي لهذه الجريمة يتحقق بتوافر عنصرين:

- صفة الفاعل.

- السلوك الإجرامي وهو النشاط المادي المتمثل في إيصال أو نقل المعطيات الشخصية للغير الذي ليس له حق الإطلاع على هذه البيانات.

فبالنسبة لصفة الفاعل هي أن يكون مسؤولا عن المعالجة أو معالجا من الباطن أو مكلفا بحكم وظيفته بمعالجة البيانات كما سبق بيانه، ومن ثم فإن إفشاء البيانات الشخصية في هذه الجريمة يقع من قبل الموكل لهم حفظها وتخزينها ومعالجتها وممن لهم سيطرة عليها.

وليس المقصود فيها ممن يتمكن من اختراق نظام المعلومات والحصول عليها من خارج دائرة المختصين بمعالجتها، إذ أن الفعل في هذه الحالة يقع ضمن جريمة إفشاء المعطيات المتحصل عليها بالدخول إلى نظام معلوماتي عن طريق الغش.[1]

وبالنسبة للسلوك الإجرامي، فهو النشاط المادي المتمثل في إيصال أو نقل المعطيات الشخصية لشخص غير ذي صفة قانونا وليس له حق الإطلاع عليها، أما إذا كان فعل الإفشاء بإيصال البيانات إلى شخص من حقه الإطلاع على هذه البيانات، انعدم السلوك الإجرامي ولا تتحقق الجريمة.[2]

وقد اعتبرت اللجنة الوطنية للمعلوماتية والحريات (CNIL) الفرنسية أن الشخص يكون مختصا وله أهلية في تلقي هذه البيانات عندما تقتضي ممارسته لمهنته أو وظيفته علمه بهذه المعلومات، أما الشخص غير المختص فهو الذي لا يكون هناك سبب مشروع أو مسوغ مهني أو وظيفي يتيح له الحق في العلم بهذه البيانات.[3]

لذلك نجد أن المشرع الجزائري اشترط على المسؤول عن المعالجة أن يحدد المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات في التصريح المقدم إلى السلطة الوطنية لحماية المعطيات، وكذلك نجد أن المشرع الفرنسي اشترط في كل من المادتين 19،20 من القانون 17/78 ضرورة إخطار اللجنة الوطنية للمعلومات والحريات (CNIL) بأسماء الأشخاص والجهات التي يتم إرسال البيانات الشخصية إليها.

ونشير إلى أن المشرع الفرنسي فضلا على ما تقدم فقد تطلب شرطين آخرين لقيام الركن المادي وهما النتيجة الإجرامية والمتمثلة في الضرر،أي أن يكون من شأن فعل الإفشاء للمعطيات الشخصية الإضرار بالمجني عليه صاحب هذه المعطيات الشخصية، وذلك بأن يؤدي فعل الإفشاء إلى الإعتداء على شرف الشخص واعتباره أو حرمة حياته الشخصية، وأن ترتبط النتيجة بفعل الإفشاء بعلاقة سببية، فإذا لم

[1] أنظر المادة 394 مكرر 3/2 من قانون العقوبات.

[2] علي جعفر، مرجع سابق، ص450.

[3] بولين أيوب، مرجع سابق، ص412.

يترتب عن هذا الفعل اعتداء على كرامة الشخص أو اعتباره، أو حرمة خصوصيته، فإنه لا تتوافر عناصر الركن المادي ومن ثم لا تقوم الجريمة.[1]

وهذا الشرط لم ينص عليه المشرع الجزائري، إذ يفهم من صياغة نص المادة 69 من القانون 07/18 أن جرم الإفشاء يتحقق بمجرد أن يوصل الفاعل المعطيات الشخصية إلى من ليس له الحق في الإطلاع عليها حتى ولو لم تستعمل من طرف هذا الأخير، أو لم يترتب عن ذلك أي ضرر يلحق الشخص المعني.

و إن كنانتفق مع نهج المشرع الجزائري في هذه المسألة و لا نرى أية حكمة من وراء أن يشترط المشرع أن يلحق بالشخص الذي تخصه البيانات الشخصية التي يتم إفشاؤها ضرر ما، كما فعل المشرع الفرنسي، لكننا نرى في مقابل ذلك حتمية أن يستثني المشرع صراحة من التجريم الإفشاء الذي يقوم على معيار تحقيق المصلحة العامة، وبالتالي يجوز الإفشاء للمعطيات الشخصية إذا كان بغية تحقيق الصالح العام الذي لا شك في أنه محقق في حالة تبادل هذه البيانات بين الجهات الحكومية.

الشرط الثاني أن يكون إفشاء البيانات دون موافقة صاحبها، ومن ثم ينتفي الركن المادي ولا تكون الجريمة، إذا كان نقل البيانات الشخصية إلى الغير برضا من الشخص المعني وموافقته، وهو أمر لا نجد له سبيلا عند المشرع الجزائري، ونعتقد أن المشرع الجزائري قد جانب الصواب في هذ النقطة، ذلك أنه بمفهوم المادة 2/7 من القانون 07/18 يمكن للمسؤول عن المعالجة إطلاع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة لديه، إذا وافق الشخص المعني بذلك ومن ثم لغاية التنسيق بين النصوص كان ينبغي على المشرع أن يرفع التجريم عن فعل إطلاع الغير على المعطيات الشخصية إذا كان بموافقة الشخص المعني.

ب) الركن المعنوي: يعتبر المشرع الجزائري أن إفشاء المعطيات الشخصية جريمة عمدية تقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة دون حاجة إلى قصد جنائي خاص، إذ يجب على الجاني أن يعلم أنه لا يحق له الإفضاء إلى الغير بالمعطيات الشخصية، وأنه يعلم أن من أفضى إليه بهذه المعطيات يعد من الغير الذي لا يؤهله القانون للاطلاع عليها، و أن القانون يعاقب على هذا الفعل، ومع ذلك تتجه إرادته للسلوك الإجرامي وهنا تقوم المسؤولية الجنائية في حقه.

أما المشرع الفرنسي حسب نص المادة 226-22 اعتبر أن الركن المعنوي لهذه الجريمة يقوم أيضا بصورة الخطأ نتيجة الإهمال أو عدم الحيطة، ومن ثم لا تكون الجريمة وليدة إرادة آثمة أخذت صورة العمد، وإنما كان الفعل وليد خطأ من الجاني بسبب عدم احترازه أو إهماله، ومثاله الموظف المكلف بمعالجة المعطيات الشخصية للمرضى بمستشفى و الذي يصرح للغير عن طريق الخطأ عن بيانات صحية تخص مريضا[2]، أو ترك بإهماله الغير للإطلاع عليها، ويشير الفقه الفرنسي أن من أثر رضا ذوي الشأن، نفي القصد الجنائي لدى الفاعل باعتباره سببا للإباحة، لأن الرضا ينفي عن الفعل عنصر الإعتداء وينفي

[1] أنظر المادة 226-22 من القانون 17/78.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص652.

الضرر، ومن ثم ينفي عن الفعل الصفة غير المشروعة، وذلك بشرط أن يتوفر للرضا شروط صحته التي تقضي بها القواعد العامة.[1]

2-3-1) قمع الجريمة:

أ) المتابعة: لا تخضع المتابعة الجزائية لهذه الجريمة في التشريع الجزائري لأي قيد أو شرط، ويجوز للنيابة أن تحرك الدعوى العمومية دون تقيدها بشكوى الطرف المضرور، لكن المشرع الفرنسي في نص المادة 22-226 من قانون العقوبات قيد الدعوى العمومية بشكوى الطرف المضرور أو من يمثله قانونا،[2] ومن ثم فإن النيابة لا يمكنها اتخاذ إجراءات المتابعة إلا إذا تقدم الشخص المضرور بشكوى أمامها، ويترتب على ذلك وفق القواعد القانونية العامة أن سحب الشكوى من الشخص المضرور يضع حدا للمتابعة الجزائية في أي مرحلة تكون عليها الدعوى الجزائية.

ب) العقوبة المقررة قانونا: حسب نص المادة 69 يعاقب المشرع الجزائري على جريمة إفشاء المعطيات الشخصية بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100 ألف دج إلى 500 ألف دج، بالإضافة إلى العقوبات التكميلية بالصورة التي سبق بيانها.

4-1) جريمة تجاوز الغرض من معالجة المعطيات:

عرضنا فيما تقدم أن المشرع يفرض التزاما على القائمين بعمليات معالجة المعطيات الشخصية يوجب من خلاله تحديد الغرض من عملية المعالجة في التصريح المودع لدى السلطة الوطنية لحماية المعطيات الشخصية.[3]

لذلك جاءت المادة 58 من القانون 07/18 لتعاقب بالحبس من 6 أشهر إلى سنة (1) وبغرامة من 60 ألف إلى 100 ألف دج، أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها."

1-4-1) أركان الجريمة:

أ)الركن المادي: يتحقق الركن المادي لهذه الجريمة بمجرد توفر السلوك الإجرامي وهو الإنحراف عن الغاية أو الغرض من معالجة المعطيات الشخصية، ويعد الغرض أو الغاية هي موضوع المعالجة، وهي المبرر القانوني لها، ومناط تحديد تجاوز الغرض أو الغاية من المعالجة و الإنحراف بها عن الغرض الأساسي الذي تمت من أجله[4]هو التصريح المقدم إلى السلطة الوطنية لحماية المعطيات الشخصية، حيث تفرض هذه الأخيرة سلطتها لرقابة هذا الإنحراف إنطلاقا من التصريح المقدم لها تبعا للأغراض المحددة في

[1] Jacques Francillon, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, revue internationale de droit pénale 64eme année 1993, p 291.

[2] L article 226-22 du code pénal français Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

[3] تنص المادة 14 من القانون 07/18: "يجب أن يتضمن التصريح ما يأتي: .... طبيعة المعالجة وخصائصها والغرض أو الأغراض المقصودة منها..."

[4] مروة زين العابدين، مرجع سابق، ص473.

النصوص التشريعية والتنظيمية، ومن ثم تفترض جريمة الإنحراف عن الغرض أو الغاية من معالجة المعطيات الشخصية الحصول ابتداء بصورة مشروعة على هذه المعطيات بالتصريح لدى السلطة الوطنية لمعالجة المعطيات وبترخيص منها، لكن الفاعل ينحرف عن هذا الغرض المقصود.[1]

ومن ثم فإنه وبمجرد الرجوع إلى التصريح المقدم إلى السلطة الوطنية مسبقا، والذي حدد فيه المسؤول عن المعالجة غايات وأغراض المعالجة وفقا لنص المادة 14 من القانون 07/18، يمكن إدراك حالات الإنحراف، فجمع البيانات الشخصية لا بد أن يكون له هدف وغرض معين، فنوع المعطيات التي يعطيها الإنسان عن نفسه وحجمها يختلف من جهة إلى أخرى، والغرض من المعالجة هو الذي يحدد ذلك، لأجل هذا يجب أن يتم الإلتزام بذلك للغرض المحدد مسبقا دون تغيير.

ومثال ذلك المسؤول عن المعالجة الذي يستعمل البيانات الشخصية التي جمعها عن شخص لإنجاز غرض معين في الكشف عن مصادر ثروته أو لمعرفة مركزه المالي أو في الإستدلال عليه لدى مصالح الضرائب[2]، أو استعمال المعطيات لغاية أخرى وهي الإساءة إلى السمعة، أو من أجل الضغط والإبتزاز السياسي ونحو ذلك[3]، أو أن يتم تغيير الغرض من معالجة المعطيات الشخصية المتصلة بالحالة الصحية في إطار التأمين الصحي لغرض آخر مثل الأبحاث الطبية.

وهدف الشرع من هذا التجريم هو حظر أي استخدام غير مشروع للمعطيات الشخصية من قبل حائزها ذلك أن جميع الإستخدامات غير المتوقعة من أي جهة كانت للمعطيات الشخصية يؤدي إلى إيذاء الفرد وتقليل فرص تمتعه بحقوقه على الوجه الأكمل.

ب) الركن المعنوي: تعتبر جريمة الإنحراف عن أغراض معالجة المعطيات الشخصية من الجرائم العمدية التي تقوم على توافر القصد الجنائي بعنصريه العلم والإرداة، فلا يعاقب عنها بوصف الخطأ.

ومن ثمة يتعين لتحقق الركن المعنوي أن يعلم الفاعل بأن من شأن سلوكه أن يشكل انحرافا عن الغاية أو الغرض من معالجة المعطيات الشخصية وأن تتجه إرادته نحو ذلك، كما يقوم الركن المعنوي لمجرد القصد الجنائي العام، ولا عبرة بالبواعث والدوافع التي جرت الفاعل لارتكاب هذه الجريمة سواء تمثلت في منفعة مادية أو معنوية له، أو دفع ضرر عنه أو تحقيق مصلحة للغير.[4]

2-4-1) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: تعاقب المادة 58 من القانون 07/18 على جريمة تجاوز الغرض من معالجة المعطيات الشخصية المصرح بها بالحبس من 6 أشهر إلى سنة أو بغرامة من 60 ألف دج إلى 100 ألف دج أو بإحدى هاتين العقوبتين، وهذا يعني أنه إذا تقرر إفادة الشخص الطبيعي غير المسبوق بظروف التخفيف جاز

[1] محمد أمين الشوابكة، مرجع سابق، ص 99.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 645.

[3] مروة زين العابدين، مرجع سابق، ص 473.

[4] بولين أيوب، مرجع سابق، ص 423.

تخفيض عقوبة الحبس إلى شهرين وعقوبة الغرامة إلى 20 ألف دج، حسب أحكام المادة 53 مكرر 4 من قانون العقوبات.[1]

ب) العقوبة التكميلية: حسب نص المادة 71 من القانون 07/18 فإنه يمكن أن يتعرض مرتكب هذه الجريمة إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات حسب ما سبق بيانه.

5-1)جريمة الإ حتفاظ بالمعطيات الشخصية بعد المدة المحددة قانونا:

تنص المادة 2/65 من القانون 07/18 على أنه يعاقب بنفس العقوبة المذكورة في الفقرة الأولى أي بالغرامة من 200 ألف دج إلى 500ألف دج كل من قام بالإ حتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص".

1-5-1) أركان الجريمة:

أ) الركن المادي: تقوم هذه الجريمة بتحقق النشاط الإجرامي المتمثل في الإ حتفاظ بالمعطيات الشخصية داخل النظام المعلوماتي لمدة أكثر من المدة التي سبق وأن تم التصريح بها لدى السلطة الوطنية لحماية المعطيات الشخصية، أو المدة المرخص بها من طرف هذه السلطة.

وعليه فإن هذه الجريمة تعالج فرضا هاما يتمثل في تجاوز الوقت المخصص لمعالجة أو حفظ المعطيات الشخصية، ذلك أن من ضوابط المعالجة لهذه المعطيات تأقيت عملية حفظها وتخزينها[2]، حيث أنه لا يمكن أن تحفظ لمدة غير محددة، إلا في حالات إستثنائية، يفترض أن تكون محددة صراحة بنص القانون.[3]

ويمكن أن تحدد مدة الإ حتفاظ بالمعطيات الشخصية بموجب نصوص قانونية، وهي الحالة التي تتحقق بصدور نصوص تشريعية تخول إحداث نظم معلوماتية في إطار القطاع العام والإدارات العمومية والجهات الحكومية لمعالجة المعطيات الشخصية، فيكون من أهم ما تتضمنه هذه النصوص هو تحديد مدة حفظ هذه المعطيات، كما هو الشأن في ما ورد بالمادة 14 من القانون 03/16[4] التي حددت مدة حفظ المعطيات الجينية المتعلقة بالبصمة الوراثية في القاعدة الوطنية للبصمات الوراثية بـ 25 سنة بالنسبة لأصول وفروع الأشخاص المفقودين وكذا المشتبه فيهم المتابعين المستفيدين من أمر بانتقاء وجه الدعوى أو الحكم بالبراءة و مدة 40 سنة بالنسبة للأشخاص المحكوم عليهم والمفقودين والمتوفين ومجهولي الهوية، أو أن تحدد هذه المدة في التصريح المقدم لدى السلطة الوطنية أو الترخيص الصادر عنها إذا كان مالك نظام المعالجة من مؤسسات القطاع الخاص[5]، ولقد نصت المادة 14 من القانون 07/18 أنه

[1] تنص المادة 53 مكرر 4من قانون العقوبات أنه "إذا كانت العقوبة المقررة قانونا في مادة الجنح هي الحبس أو الغرامة وتقرر إفادة الشخص الطبيعي غير المسبوق قضائيا بالظروف المخففة، يجوز تخفيض عقوبة الحبس إلى شهرين (2) والغرامة إلى 20 ألف دج.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي مرجع سابق، ص641.

[3] محمد أمين الشوابكة، مرجع سابق، ص96.

[4] القانون 03/16 المؤرخ في 2016/06/19 متعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، ج ر،عدد 37 صادرة في 19 جوان 2016.

[5] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي مرجع سابق، ص 642.

يجب أن يتضمن التصريح المسبق الذي يودع لدى السلطة الوطنية مدة حفظ المعطيات، وهو نفس الإلزام الذي كرسه المشرع الفرنسي في المادة 24 من القانون 2004/801 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي.[1]

ومن ثم فإن كل احتفاظ بالمعطيات الشخصية الذي يتجاوز المدة المحددة يعد حفظا غير مشروع للمعطيات الشخصية، إلا بإذن من السلطة الوطنية، ولذلك فقد نصت المادة 09 أنه يمكن للسلطة الوطنية في حالة وجود مصلحة مشروعة بناء على طلب المسؤول عن المعالجة أن تأذن بحفظ المعطيات ذات الطابع الشخصي لغايات تاريخية أو إحصائية أو علمية بعد المدة المشار إليها في الفقرة "هـ" من هذه المادة.

ونصت المادة 28من قانون المعلوماتية الفرنسي أنه لا يجوز الإ حتفاظ بالمعطيات الشخصية إلا للمدة المحددة في طلب إقامة نظم المعلومات أو المدة اللازمة لتحقيق الغرض من تجميع البيانات واحتياجات البرنامج، إلا إذا سمحت اللجنة الوطنية للمعلوماتية والحريات بالإ حتفاظ بهذه المعلومات أكثر من المدة المحددة".

ومن المنطقي أن تكون مدة حفظ المعطيات الشخصية مرتبطة بالمدة الضرورية لإنجاز الغايات التي تم من أجلها جمع هذه المعطيات ومعالجتها، وهذا ما تؤكده المادة 09 النقطة هـ من القانون 07/18 التي نصت "يجب أن تكون المعطيات الشخصية ..... هـ- محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها".

ويشير المشرع الفرنسي إلى إمكانية تجاوز المدة المحددة في الترخيص أو التصريح بناء على إذن من اللجنة الوطنية لحماية المعطيات بعد طلب من المسؤول عن المعالجة عند وجود مصلحة مشروعة تقتضي ذلك.

كما يفهم من نص المادة 226-20 من قانون العقوبات الفرنسي أنه استثنى شرط مدة الحفظ للمعطيات الشخصية، إذا كان هذا الحفظ من أجل معالجة المعطيات الشخصية لغايات تاريخية أو إحصائية أو علمية في إطار الشروط المحددة قانونا، أما إذا عولجت خارج هذه الغايات فيجب ألا تتجاوز مدة حفظها المدة المحددة قانونا.

والهدف التشريعي من هذا التجريم هو احترام حق الفرد في النسيان «le droit à l'oublie» من خلال محو البيانات الشخصية التي انتهى الغرض من تخزينها، سيما وأن حفظ البيانات إلكترونيا صار سهلا وبسيطا ويمكن من خلاله حفظ هذه البيانات للأبد في ذاكرة النظام المعلوماتي[2]، كما يمكن استرجاعها في كل لحظة وحين.

ب) الركن المعنوي: تعد جريمة حفظ المعطيات الشخصية بعد المدة المحددة قانونا من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام، والذي يتحقق بتوافر العلم والإرادة، بحيث

[1] Voir l'article 24 de la loi française 801/2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, « ... la durée de conservation des données à caractère personnel ».

[2] مدحت رمضان، مرجع سابق، ص 102.

لابد أن تنصرف إرادة القائم على النظام المعلوماتي إلى الإ حتفاظ بالمعطيات الشخصية لمدة تزيد عن المدة المحددة في القانون أو التصريح أو الترخيص، رغم علمه بتجاوزها، ويترتب على ذلك أن الركن المعنوي في هذه الجريمة لا يتحقق مع صورة الخطأ، إذ لا تقوم الجريمة إذا ثبت أن تجاوز مدة الحفظ القانونية للمعطيات الشخصية كان نتيجة إهمال أو نسيان، كما يفهم من النص القانوني أن هذه الجر يمة لا تتطلب القصد الجنائي الخاص.

2-5-1) العقوبة المقررة قانونا: انطلاقا من المادة 65 الفقرة الثانية يعاقب على جريمة الإحتفاظ بالمعطيات الشخصية بعد المدة المحددة قانونا بالغرامة من 200.000 دج الى 500.000دج كعقوبة أصلية بالغضافة إلى العقوبات التكميلية المقر رة قانونا في قانون العقوبات

6-1) جريمة معالجة معطيات ذات طابع شخصي متعلقة بالوضعية الجزائية للشخص المعني:

تنص المادة 68 من القانون 07/18 على أنه يعاقب بالحبس من 06 أشهر إلى ثلاث (03) سنوات كل من قام في غير الحالات المنصوص عليها قانونا بوضع أو الحفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن"

1-6-1) أركان الجريمة:

أ) الركن المادي: انطلاقا من نص المادة 68 المذكورة أعلاه فإن الركن المادي لهذه الجريمة يتحقق بتوفر العناصر التالية:

-العنصر الأول ويتعلق بالسلوك الإجرامي والمتمثل في عملية الوضع أو الحفظ للمعطيات الشخصية في الذاكرة الآلية، حيث تقوم الجريمة لمجرد قيام الجاني بعمليتين فقط من عمليات المعالجة وهي الوضع أو الحفظ، ولا يشترط لقيامها تحقق جميع أنشطة المعالجة المذكورة في المادة 03 من القانون 07/18، بل يكفي أن تتحقق مرحلة الوضع أو الحفظ لهذه المعطيات في الذاكرة الآلية، ويكتفي الجاني بهما فقط حتى ولو لم يقم بعمليات المعالجة الأخرى.

والمقصود بعملية الوضع هو إدخال أو إدراج تلك المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني في ملفات معلوماتية، أما الحفظ فيعني الإ حتفاظ بهذا النوع من المعطيات والإبقاء عليها داخل الذاكرة الآلية (la mémoire informatisée) لمدة غير محددة وعدم حذفها بعد تسجيلها، للتمكن من الرجوع إليها كلما تطلب الأمر ذلك وفي أي وقت، وخلافا للجرائم الأخرى التي تضمنها القانون 07/18، فإن هذه الجريمة تقوم فقط بواسطة المعالجة الآلية، حيث ذكر المشرع عملية الوضع أو الحفظ الذي يتم في الذاكرة الالية، ومن ثم يكون قد استبعد من نطاق التجريم عملية الحفظ التي تتم بشكل يدوي، كتدوين هذه المعطيات والاحتفاظ بها في سجلات يدوية يتم أرشفتها.

-أما العنصر الثاني فيتعلق بموضوع المعالجة، وهي المعطيات المتعلقة بالوضعية الجزائية للشخص المعني أو ما يعرف بالماضي الجزائي، وتتمثل هذه المعطيات أساسا حسب نص المادة 68 في الجرائم والإدانات وتدابير الأمن، والمقصود بالإدانات كل العقوبات التي تسلط على المحكوم عليه جزائيا لارتكابه جناية أو

جنحة أو مخالفة، سواء كانت عقوبات أصلية أو تكميلية أو بديلة كعقوبة العمل للنفع العام، أي كل المعطيات التي تدون بصحيفة السوابق القضائية، وهي حسب المادة 618 من قانون الإجراءات الجزائية:

-أحكام الإدانة الحضورية أو وفق إجراءات التخلف عن الحضور في المادة الجنائية أو الأحكام الغيابية غير المطعون فيها بالمعارضة المحكوم بها في جناية أو جنحة من أي جهة قضائية، بما في ذلك الأحكام المشمولة بوقف التنفيذ

– الأوامر الجزائية غير معترض عليها.

- الأحكام الحضورية أو الغيابية غير المطعون فيها بالمعارضة الصادرة في المخالفات، إذا كانت العقوبة المقررة قانونا تزيد على الحبس لمدة 10أيام أو بخمسة آلاف دج غرامة، بما في ذلك الأحكام المشمولة بوقف التنفيذ – عقوبات العمل للنفع العام.

- الأحكام الصادرة تطبيقا للنصوص الخاصة بالأحداث المجرمين، وتتعلق بتدابير الحماية والتهذيب الواردة في نص المادة 85 من القانون 12/15 المتعلق بحماية الطفل.[1]

- القرارات التأديبية الصادرة من السلطة القضائية أو من سلطة إدارية إذا ترتب عليها أو نص فيها على التجريد من الأهليات.

-الأحكام المقررة لشهر الإفلاس أو التسوية القضائية.

-الأحكام الصادرة بسقوط الولاية الأبوية أو بسحب الحقوق المتعلقة بها كلها أو بعضها.

- إجراءات الإبعاد المتخذة ضد الأجانب.

أما تدابير الأمن فهي الإجراءات التي تتخذ وفق أحكام المادة 19 من قانون العقوبات وتتمثل في:

- الحجر القضائي في مؤسسة إستشفائية للأمراض العقلية.

- الوضع القضائي في مؤسسة علاجية.

- ويتعلق العنصر الثالث بأن تتم المعالجة من جهات غير مخول لها قانونا معالجة هذه المعطيات، حيث أن المعطيات الشخصية المتعلقة بالجرائم والإدانات وتدابير الأمن لا يمكن معالجتها إلا من قبل السلطات القضائية والسلطات العمومية والأشخاص المعنويين الذين يسيرون مصلحة عمومية ومساعدي العدالة في إطار اختصاصاتهم القانونية[2]، ويحظر على من سوى هذه الجهات معالجة مثل هذه المعطيات بوضعها أو حفظها في الذاكرة الآلية للحواسيب الخاصة.

ولهذا تنص المادة 620 من قانون الإجراءات الجزائية على أنه توجد بوزارة العدل مصلحة مركزية لصحيفة السوابق القضائية يديرها قاض، و أن هذه المصلحة تختص لوحدها بمسك صحيفة السوابق

[1] القانون رقم 12/15 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل، جريدة رسمية عدد 39 الصادرة بتاريخ 19 جويلية 2015.
[2] أنظر المادة 10 من القانون 07/18.

القضائية للأشخاص المولودين خارج إقليم الجمهورية وذلك بغير مراعاة جنسيتهم، كما نصت كذلك المادة 620 مكرر من نفس القانون، المستحدثة بموجب القانون 04/14 المؤرخ في 10 نوفمبر 2004 على أنه تنشأ لدى وزارة العدل مصلحة لنظام آلي وطني لصحيفة السوابق القضائية مرتبطة بالجهات القضائية، و هذه الجهات تتمثل في المجالس القضائية أين يوجد على مستوى كل منها مصلحة لصحيفة السوابق القضائية، يديرها كاتب ضبط تحت إشراف النائب العام[1]. يتلقى رئيس هذه المصلحة قسائم السوابق القضائية رقم 01 المتعلقة بالأشخاص المحكوم عليهم المولودين في دائرة اختصاص ذلك المجلس[2]، ليتم إدراجها في قاعدة المعطيات المرتبطة بالنظام الآلي المركزي لصحيفة السوابق القضائية على مستوى وزارة العدل، بالإضافة إلى وجود صحيفة سوابق قضائية للأشخاص المعنوية تتعلق بالعقوبات والجزاءات الصادرة عن الجهات القضائية الوطنية، وكذا تلك الصادرة عن الجهات القضائية الأجنبية التي تخطر بها السلطات الجزائرية في إطار التعاون الدولي[3].

كما يناط أيضا لأشخاص معنوية أخرى مسك صحيفة السوابق القضائية حسب الفقرة الأخيرة من المادة 620 من قانون الإجراءات الجزائية والمادة 10 من القانون 07/18، وهي الإدارات العمومية التي تسير مصلحة عمومية مثل القيادة العامة للدرك الوطني والمديرية العامة لأمن الوطني، ووزارة الداخلية.

وترتيبا على ما سبق فإنه يمنع على أي مسؤول عن المعالجة من غير الجهات والسلطات العامة التي يسمح لها القانون الإ ضطلاع بمسك صحيفة السوابق القضائية أن يمارس معالجة آلية للمعطيات الشخصية تتعلق بالسوابق القضائية للشخص المعني على النحو الذي سبق بيانه، كإدراج تلك السوابق في ملفات آلية متعلقة بتسيير هيأة المستخدمين[4]، ومن ثم فإن هذه الجر يمة التي نحن بصددها تتحقق حين يقوم الجاني بمعالجة معطيات تتعلق بالجرائم والإدانات وتدابير الأمن من خلال وضعها أو حفظها في ذاكرة آلية دون أن يكون من الجهات القضائية والسلطات المختصة بتخزين هذه المعطيات[5].

والعلة من هذا الحظر هو حماية سمعة واعتبار الأشخاص، ذلك أن الإفصاح عن مثل هذه المعطيات عن طريق معالجتها من قبل القطاع الخاص دون أجهزة العدالة أمر يضر بمستقبل الأفراد، وكل هذه الاعتبارات هدفها نسيان الجريمة، سيما وأن القانون يحرص على ذلك من خلال إقراره لنظام تقادم الجريمة ورد الاعتبار وغيرهما.[6]

ب) الركن المعنوي: تعد هذه الجريمة من الجرائم العمدية، صورة الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة، ولذلك يجب أن يعلم الجاني أنه يعالج معطيات شخصية تتعلق بالوضعية

[1] أنظر المادة 619 من قانون الإجراءات الجزائية.

[2] أنظر المادة 618 من قانون الإجراءات الجزائية.

[3] أنظر المادة 646 من القانون 06/18 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عد 34 الصادرة بتاريخ 10 جوان 2018.

[4] Gassin Raymond, informatique et liberté, Encyclopédie juridique, Dalloz, répetoire de droit pénal et procédure pénal, tome 3 paris, 2003 p 09.

[5] بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 640.

[6] بيومي حجازي، نفس المرجع، ص 640.

الجزائية للشخص المعني، وأن القانون يحظر عليه ذلك كونه ليس من الجهات التي يخولها القانون هذا الاختصاص، ورغم ذلك تنصرف إرادته إلى إتيان هذا السلوك الإجرامي، ولا يعتد في هذه الجريمة بالقصد الجنائي الخاص، إذ لا عبرة بالدوافع والبواعث نحو ارتكاب الفعل، وهو ما يفهم من عبارات النص التجريمي للمادة 69 من القانون 07/18.

وإذا ما قامت الجريمة في حق الجاني بركنيها المادي والمعنوي يعاقب الجاني بحسب العقوبة المقررة قانونا.

2-6-1) العقوبة المقررة قانونا: إذا تحققت الأركان القانونة قامت المسؤولية الجزائية واستوجب العقاب

أ) العقوبة الأصلية: يعاقب مرتكب جريمة وضع أو حذف معطيات متعلقة بالوضعية الجزائية في ذاكرة آلية بالحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من 60 ألف دج إلى 300 ألف دج، ويلاحظ أنها عقوبة أقل من تلك التي رصدها المشرع لجريمة معالجة معطيات حساسة دون موافقة الشخص المعني المنصوص عليها في المادة 57، وهذا على خلاف المشرع الفرنسي الذي ساوى بين الجريمتين في العقوبة وتكريسهما في نفس النص القانوني، وهو المادة 226-19 من قانون العقوبات.

ب) العقوبة التكميلية: تتبع المحكمة عند قضائها بإدانة الجاني بالعقوبات الأصلية المحكوم بها واحدة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات، بالإضافة إلى وجوب الحكم بالمصادرة للأشياء المستعملة في ارتكاب جريمة حسب المادة 15 مكرر 1 من قانون العقوبات

2) الجرائم المرتبطة بخرق أحكام المادة 02 من القانون 07/18:

تنص المادة 54 من القانون 07/18 على أنه: "دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول يعاقب على خرق أحكام المادة 02 من هذا القانون بالحبس من سنتين إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج".

وبالرجوع إلى نص المادة 02 من نفس القانون فإنها تنص على أنه "يجب أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية، الحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم."

إن القراءة المتأنية لهذين النصين القانونيين تسمح لنا بالقول أن التجريم الذي جاءت به المادة 54 أعلاه إستنادا على خرق أحكام المادة 02 لا يستقيم من الناحية القانونية مع مبدأ الشرعية الجزائية الموضوعية، الذي يقتضي أن يحدد المشرع لكل جريمة نموذجها القانوني بأركان واضحة ومحددة العناصر، من خلال نص جزائي لا يترك مجالا لإعمال السلطة التقديرية للعاملين في مجال القانون في تحديد ما يدخل ومالا يدخل في دائرته.

فالملاحظ أن المشرع استعمل في المادة 02 مصطلحات عامة وغامضة أحيانا بمفاهيم متداخلة مثل الكرامة الإنسانية والحريات العامة وحقوق الأشخاص.

فالكرامة الإنسانية كقيمة متأصلة في الشخص الإنساني هي الأساس القانوني لجميع حقوق الإنسان، ولا يوجد أي مبرر لهذه الحقوق إن لم يكن هدفها هو صون كرامته[1]، وهذا أمر يجعل من الصعوبة بما كان وضع تعريف لمفهوم الكرامة الإنسانية والإ حتجاج به بشكل قاطع، لذلك فقد قيل بأن محتوى هذا الحق هو فضفاض ولا يمكن تحديده بدقة، والسبب في ذلك أنه يمس الطبيعة العميقة للإنسان ويشكل أهم خاصية من خصائص الشخصية الإنسانية.[2]

وأغلب النصوص القانونية سواء على الصعيد الدولي أو الداخلي التي تضمنت النص على هذا الحق قد كرست له الحماية القانونية دون تحديد مضمونه.*

ونفس الأمر بالنسبة للحريات العامة، والتي هي عبارة عن مكنات يتمتع بها الفرد بسبب طبيعته الإنسانية، ونظر العضويته في المجتمع يحقق الفرد من خلالها صالحه الخاص، ويسهم بها في تحقيق الصالح المشترك للبلاد ويمتنع على السلطة أن تحد منها إلا إذا أضرت بمصالح الآخرين.[3]

وتعتبر كذلك من الحقوق الأساسية التي هي مجموعة من الحقوق التي يخولها دستور الدولة لمواطنيها ويصونها ضد التجاوزات ومختلف ضروب التعسف التي قد تتعرض من قبل الأفراد أو السلطة، كما أن مدلول الحياة الخاصة قد بذل الفقه القانوني في شأنه محاولات عديدة لتحديد نطاقه الذي يرتبط بدرجة كبيرة بالمجتمع وما يسوده من أوضاع وعادات وتقاليد وقيم اجتماعية وأخلاقية، مما يترتب عليه اختلاف مفهومه من بلد لآخر ومن ثم يضيق هذا المفهوم ويتسع تبعا لهذه المعايير.

ولعل هذا ما يفسر أن مثل هذا النص التجريمي لا يوجد في التشريعات المقارنة التي عنيت بحماية المعطيات الشخصية إذ تضمنت فقط[4] ما يقابل نص المادة 02 والتي تحدد الأهداف العامة والغايات

---

[1] سوسن زهر، حسن جبارين، رولا سعيد، الكرامة الإنسانية في الممارسات القضائية، دراسة نظرية ودراسة حالة، إصدارات مركز القدس للمساعدة القانونية وحقوق الإنسان، جانفي 2012، ص 08 متوفر على الموقع:
http://lawcenter.birzeit.edu/lawcenter/attachments/article/1517/Dalel.pdf.

[2] فواز صالح، مبدأ احترام الكرامة الإنسانية في مجال الأخلاقيات الحيوية، دراسة قانونية مقارنة- مقال منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011 ص 254.

* أول إشارة إلى الحق في احترام الكرامة الإنسانية على الصعيد الدولي كانت مقدمة ميثاق الأمم المتحدة الصادر في 1945/06/26 التي جاء فيها "... وأن نؤكد من جديد إيماننا بالحقوق الاساسية للإنسان وبكرامة الفرد..." ويكرس الإعلان العالمي لحقوق الإنسان مبدأ احترام الكرامة الإنسانية في المواد 23،22،05 منه، العهد الدولي للحقوق الإقتصادية والإجتماعية والثقافية، المعتمد من الجمعية العامة للأمم المتحدة بتاريخ 1966/12/16 ودخل حيز النفاذ بتاريخ 1976/01/03 العهد الدولي للحقوق المدنية والسياسية الذي اعتمدته الجمعية العامة للأمم المتحدة بتاريخ 1966/12/16 ودخل حيز النفاذ بتاريخ 1976/03/23. إعلان طهران الصادر عن المؤتمر الدولي لحقوق الإنسان في طهران بتاريخ 1968/05/13. الإتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري المعتمدة من طرف الجمعية العامة للأمم المتحدة بتاريخ 1965/12/21. ودخلت حيز النفاذ بتاريخ 1969/01/04. إتفاقية منع التمييز ضد المرأة عام 1979. وكذلك إتفاقيات جونيف الأربعة المؤرخة في 2 أوت 1949 أنظر للإطلاع على هذه النصوص: محمود شريف بسيوني، محمد سعيد الدقاق، عبد العظيم وزير، حقوق الإنسان، الوثائق العالمية والإقليمية، المجلد الأول، الطبعة الأولى، دار العلم للملايين، بيروت، 1998، وكذلك: محمد يوسف علوان، محمد خليل الموسى، القانون الدولي لحقوق الإنسان، الحقوق المحمية، الجزء الثاني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثالث 2011.

[3] هاني سليمان الطعيمات، حقوق الإنسان وحرياته الأساسية، الطبعة الثانية، دار الشروق للنشر والتوزيع، 2003 ص 30.

[4] L'article 1er de la loi n° 78/17 du 6 janvier 1978 relative à l'informatique aux fichiers, aux libertés modifiées par l'article 54 de la loi n° 2016/1321 du 7 octobre 2016 : « ...Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

الأساسية من حماية المعطيات الشخصية، استهلت بها نصوصها القانونية كمبادئ أساسية في مجال حماية المعطيات الشخصية فقط، ولم تتضمن إطلاقا أيا من هذه القوانين نصا يعاقب على مخالفة أو خرق أحكامها.

2-1) أركان الجريمة:

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة لمجرد قيام الفاعل بمعالجة معطيات ذات طابع شخصي، ويترتب على ذلك مساس بكرامته الإنسانية أو حياته الخاصة، أو تقيدا لحرياته العامة أو اعتداء على شرفه وسمعته.

فإذا تمت معالجة المعطيات ذات الطابع الشخصي في غير إطارها القانوني وبشكل لا يضمن احترام الكرامة الإنسانية والحريات العامة، أو تمت خارج إطار احترام الحياة الخاصة وسمعته وشرف الأشخاص قام الفعل المجرم واستوجب المسؤولية الجزائية.

ولقد نص المشرع على الجرائم التي تشكل مساسا بشرف وسمعة الاشخاص في قانون العقوبات وتتمثل في الجرائم التالية: القذف، السب، الإهانة، الوشاية الكاذبة.

حيث يعتبر الفعل قذفا حسب المادة 226 من قانون العقوبات كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئات المدعى عليها بها، أو إسنادها إليهم أو إلى تلك الهيئة.

ويقصد بشرف الإنسان واعتباره، المكانة التي يحتلها الفرد داخل البيئة التي يعيش فيها، أو عند أفراد المجتمع الذين يخالطهم والتي يتحدد بمقتضاها درجة تقدير الناس لهذا الفرد واحترامهم له، كما يقصد بها أيضا المكانة التي ينالها الشخص في الجماعة والتي تتكون من رصيد تصرفاته الموروثة والمكتسبة وفق معيار موضوعي قوامه الرأي العام في المجتمع.[1]

ويعتبر الفعل سبا حسب المادة 297 كل تعبير مشن أو عبارة تتضمن تحقيرا وقدحا لا ينطوي على إسناد أية واقعة، كما يعتبر الفعل إهانة حسب المادة 144 كل فعل يقصد به المساس بالشرف والإعتبار والإحترام الواجب لسلطة الموظف.

ومن ثمة فإن أي معالجة لمعطيات شخصية أو استعمال معالجة هذه المعطيات لغرض القذف أو السب أو الإهانة يمكن أن يقع تحت طائلة أحكام المادة 54 من قانون 07/18.

أما الأفعال الماسة بحرمة الحياة الخاصة فقد نصت عليها أحكام المادة 301 مكرر من قانون العقوبات، بالإضافة إلى وجود نصوص قانونية في قوانين خاصة تعاقب على انتهاك الحق في الحياة الخاصة.

المادة الأولى من القانون المغربي رقم 09/08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي:"المعلوميات في خدمة المواطن وتتطور في إطار التعاون الدولي ويجب ألا تمس الهوية والحقوق والحريات الجماعية أو الفردية للإنسان، وينبغي ألا تكون أداة لإفشاء أسرار الحياة الخاصة للمواطنين"

الفصل الأول من القانون التونسي عدد 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية "لكل شخص الحق في حماية المعطيات الشخصية باعتبارها من الحقوق الأساسية المضمونة بالدستور ولا يمكن أن تقع معالجتها إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان..."

[1] علي جعفر، مرجع سابق، 311.

ب) الركن المعنوي: يتحقق الركن المعنوي لهذه الجريمة بالقصد الجنائي العام بعنصرية العلم والإرادة بحيث يعلم الفاعل وهو المعالج للمعطيات أو المسؤول عن معالجتها، بأن ما يقوم به من شأنه المساس بالكرامة الإنسانية للمعني بالمعالجة أو حياته الخاصة أو سمعته وشرفه، وتتجه إرادته رغم ذلك لإتيان الفعل، فلا تحصل هذه الجريمة إلا إذا تعمد الفاعل الإعتداء على هذه الحقوق من عمليات المعالجة للمعطيات ولا تقوم لمجرد إهمال أو عدم حيطة.

وإذا تحقق الركنان المادي والمعنوي قامت المسؤولية الجزائية واستوجب العقاب.

2-2) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: حسب نص المادة 54 من القانون 07/18 فإن العقوبة المقررة قانونا لهذه الجريمة هي الحبس من سنتين إلى خمس (5) سنوات وغرامة من 200 ألف دج إلى 500 ألف دج ، ويبدو أن المشرع قد أخذ في هذه المادة بمسألة تعدد وصاف المنصوص عليها في المادة 32 من قانون العقوبات عندما استهل نص المادة 54 بعبارة دون الإخلال "بالعقوبات الأشد" ، بحيث إذا كان الفعل المنصوص عليه في هذه المادة يحتمل نفس الوصف في نص قانوني آخر فلا يجوز متابعة نفس الشخص في آن واحد على نفس الفعل بالنصين معا بل يتابع بالوصف الأشد منهما .

ب) العقوبات التكميلية: يجوز الحكم على المدان بالعقوبة الأصلية بواحدة أو أكثر من العقوبات التكميلية الاختيارية التي يجوز الحكم بها عند الإدانة بالجنحة.

3) الجرائم المرتبطة بصاحب المعطيات الشخصية:

إنطلاقا من مجموعة الحقوق التي خولها المشرع للأشخاص المعنيين بمعالجة معطياتهم الشخصية في مواجهة المسؤول عن المعالجة أو المعالج من الباطن والتي تهدف إلى إعطائهم إمكانية السيطرة على بياناتهم في إطار تحقيق التوازن ما بين الإستخدام الحر والكامل للمعلوماتية من ناحية، وحماية الأشخاص باحترام معطياتهم الشخصية من ناحية أخرى، فإن كل معالجة يجريها المسؤول عن المعالجة دون احترام هذه الحقوق يدخل هذا الفعل دائرة التجريم.

والجرائم التي نص عليها القانون 07/18 المتعلق بحماية المعطيات الشخصية،والتي هي نتاج الإعتداء على حقوق الشخص المعني بالمعالجة

1-3) جريمة معالجة المعطيات ذات الطابع الشخصي دون الموافقة الصريحة للشخص المعني:

تنص المادة 55 من القانون 07/18 على أنه "يعاقب بالحبس من سنة (1) إلى ثلاث سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 07 من هذا القانون".

وباستقراء نص المادة 07 نجدها تنص على عدم إمكانية القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني.

1-1-3) أركان الجريمة: من خلال هذين النصين السابقين تقوم أركان هذه الجريمة كما يلي:

أ) الركن المادي: يقوم الركن المادي لجريمة معالجة المعطيات الشخصية دون موافقة الشخص المعني حسب أحكام المادة 07 و55 من القانون 07/18 بتحقق العناصر المكونة له بالشكل التالي:

- القيام بأي فعل من أفعال المعالجة.

- أن تكون المعالجة للبيانات الشخصية دون موافقة المعني بها.

- ألا تتعلق المعالجة بحالة من الحالات التي لا تكون فيها موافقة الشخص المعني واجبة.

فبالنسبة لإجراء معالجة لمعطيات شخصية، فيستلزم أن يقوم المسؤول عن المعالجة أو المعالج من الباطن بأحد العمليات أو أكثر المكونة للمعالجة التي تجرى على المعطيات الشخصية سواء كانت آلية أو يدوية، فلا يمكن أن نتصور قيام الجريمة إذا لم يقدم الفاعل على إجراء عمليات المعالجة.

- وبالنسبة لإجراء المعالجة دون موافقة الشخص المعني وهو السلوك المجرم، بحيث يقدم الفاعل على القيام بأي نشاط من الأنشطة التي تدخل في عملية المعالجة مثل جمع المعطيات أو تسجيلها أو حفظها أو إيصالها دون سعيه مسبقا للحصول على موافقة المعني بهذه المعالجة.

وقد عرفت اللائحة العامة لحماية المعطيات الشخصية (RGPD)[1] في المادة الرابعة منها الرضا على أنه أي مظهر من مظاهر الإرادة الحرة والمحددة والمستنيرة ولا لبس فيها، يقبل من خلالها صاحب المعطيات الشخصية أن تكون بياناته الشخصية محل معالجة سواء بالتصريح، أو من خلال أي فعل إيجابي واضح يهدف إلى ضمان أن الشخص المعني يرغب حقا في قبول استخدام معين لمعطياته الشخصية في سياق إعلان مكتوب، أو طلب الموافقة بشروط بسيطة وفي شكل يسهل فهمه والوصول إليه، ويبقى بعد ذلك للمسؤول عن المعالجة إثبات أن المعني بالمعالجة قد أعطى موافقته على معالجة بياناته[2]، كما تعتبر هذه اللائحة أن رضا المعني بالمعالجة هو أحد القواعد القانونية الأساسية التي تقوم عليها معالجة المعطيات الشخصية، وقد أكدت الإتفاقية الأوروبية لحماية المعطيات الشخصية المعدلة رقم 108 في مادتها الخامسة أن المعالجة الشرعية للمعطيات الشخصية تقوم على أساس الموافقة المسبقة لصاحب هذه المعطيات.[3] وقد جاء في القانون الأمريكي المتعلق بالخصوصية لعام 1974 أن الهدف منه هو حماية الحياة الخاصة للمواطن الأمريكي في مواجهة الحاسب الآلي الذي بات يهدد الحياة الخاصة وبشكل متزايد، لذلك نصت المادة 552/أ منه أنه لا يجوز لأي جهة أن تنشئ أي معلومات يتضمنها نظام للمعلومات بأي وسيلة

[1] Règlement (CE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[2] L'article 07 du règlement (CE) 2016/679

[3] L'article 05/2 de la convention 108 pour la protection des personnes à l'égard du traitement des données et qualité des données :
- « chaque partie prévoit que le traitement de données ne peut être éffectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne consernée ou en vertu d'autres fondements légitimes prévus par la loi ».

من وسائل الإتصال لأي شخص أو لأي جهة أخرى مالم يكن ذلك بناء على طلب كتابي وبموافقة صاحب الشأن الذي تتعلق به المعلومات.[1]

وللوقوف على مدى صحة الرضا المسبق للمعني بالمعالجة لابد من الرجوع إلى المتطلبات القانونية الواردة في القانون المدني مثل الأهلية القانونية وسلامة الإرادة.

وعلى هذا الأساس لا يمكن معالجة المعطيات الشخصية لأي فرد دون الحصول على موافقته المسبقة، وكل عملية معالجة يجريها المسؤول عن المعالجة على معطيات شخصية لأحد الأشخاص دون رضا صادر عن هذا الأخير، تشكل جريمة معالجة دون موافقة الشخص المعني.

- أما العنصر الثالث الذي يقوم عليه الركن المادي لهذه الجريمة فيتعلق بالحالات التي لا تكون فيها موافقة الشخص المعني واجبة، حيث حددت المادة السابعة حالات على سبيل الحصر لا تكون فيها موافقة الشخص واجبة لإجراء المعالجة، ومن ثم فإن هذه الجريمة تنتفي إذا تعلقت المعالجة بإحدى هذه الحالات رغم انعدام موافقة الشخص المعني، وتتمثل هذه الحالات عندما تكون المعالجة ضرورية:

-لا حترام التزام قانوني يخضع له الشخص المعني أو السؤول عن المعالجة.

- لحماية الشخص المعني بالمعالجة.

- لتنفيذ عقد يكون فيه الشخص المعني طرفا، أو لتنفيذ إجراءات سابقة لعقد اتخذت بناء على طلبه.

- للحفاظ على المصالح الحيوية للشخص المعني إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه.

- لتنفيذ مهمة تدخل ضمن مهام الصالح العام، أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة.

- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة.

وما يمكن أن نبديه كملاحظة بخصوص هذه الجريمة، تتعلق بحق الشخص المعني بالمعالجة في التراجع عن موافقته، فالملاحظ أن الشخص المعني بالمعالجة له الحق في أن يتراجع عن موافقته بمعالجة معطياته الشخصية التي سبق وأن أبداها للمسؤول عن المعالجة حسب أحكام المادة 07 من القانون 07/18، فما هو موقف المشرع الجزائري فيما يتعلق بالمعالجة التي يستمر المسؤول عن المعالجة القيام بها رغم تراجع الشخص المعني عن موافقته؟

لا نجد نصا قانونيا يجرم فعل الإستمرار في المعالجة من طرف المسؤول عنها رغم سحب وتراجع الشخص المعني عن موافقته السابقة، إلا أننا نرى أن هذا الفعل يخضع لأحكام المادة 55 وهو جريمة المعالجة دون موافقة، ويتحول عبئ الإثبات على المعني بالمعالجة بأنه قد قدم طلبا بسحب موافقته لدى المسؤول عن المعالجة.

[1] محمود أحمد عبابنة، مرجع سابق، ص 77.

ب) الركن المعنوي: يتحقق الركن المعنوي لجريمة معالجة معطيات شخصية دون موافقة الشخص المعني بالقصد الجنائي العام، على اعتبار أنها جريمة عمدية ولا تقوم بعنصر الخطأ، ويقوم القصد الجنائي بتوفر عنصر العلم، إذ يكون الفاعل عالما بأنه يقوم بإجراء معالجة لمعطيات شخصية لشخص ما، دون حصوله على موافقة هذا الأخير، ويعلم أيضا أن هذه المعالجة لا تندرج ضمن الحالات الضرورية التي يجيز فيها المشرع إنجاز المعالجات للمعطيات الشخصية دون اشتراط الموافقة المسبقة للشخص المعني، ورغم ذلك تتجه إرادته إلى القيام بالمعالجة وتحقيق نتيجتها.

3-1-2) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: حسب المادة 55 من القانون 07/18 فإنه يعاقب على جريمة معالجة المعطيات الشخصية دون الموافقة المسبقة للمعني بالمعالجة بالحبس من سنة (1) إلى ثلاث سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج.

وقد شدد المشرع العقوبة إذا تعلق الأمر بالمعالجة المنصبة على المعطيات الشخصية الحساسة، وهي المعطيات ذات الطابع الشخصي التي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الإنتماء النقابي للشخص المعني أو تلك المتعلقة بصحته، بما في ذلك معطياته الجينية[1]، حيث نصت المادة 57 من القانون 07/18 أنه "يعاقب بالحبس من سنتين(2) إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج كل من قام دون الموافقة الصريحة للشخص المعني وفي غير الحالات المنصوص عليها في هذا القانون بمعالجة المعطيات الحساسة."

فالقاعدة حسب نص المادة 18 من القانون 07/18 أن المعطيات الحساسة يمنع المشرع أصلا معالجتها إلا بناء على الموافقة الصريحة للشخص المعني، فإذا ما قام المسؤول عن المعالجة أو المعالج من الباطن بإجراء عملية من عمليات المعالجة على هذا النوع من المعطيات مثل تجميعها أو نقلها... دون الموافقة الصريحة للشخص المعني بها، كانت العقوبة أشد مما لو كانت المعالجة متعلقة بمعطيات شخصية عادية، وهي الجريمة التي نص عليها قانون العقوبات الفرنسي في المادة 226-19[2].

ومع ذلك استثنى المشرع الجزائري من نطاق جريمة معالجة معطيات حساسة دون موافقة الشخص المعني، بعض المعالجات التي تخضع لها هذه المعطيات، حيث يمكن للمسؤول عن المعالجة إجراء معالجات لمعطيات حساسة بطبيعتها دون اشتراط موافقة الشخص المعني ولا يكون الفعل مجرما، وهي الحالات الواردة في نص المادة 18 من القانون 07/18، فإجراء المعالجة على المعطيات الحساسة في

[1] أنظر المادة 03 من القانون 07/18.

[2] L'article 226-19 du code pénal français : dispose que : « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée sans le consentement exprés de l'intéréssé, des données à caractère personnel qui directement ou indirectement font apparaitre les origines raciales ou etheniques , les opinions politiques, philosophiques, ou relegieuses, ou les appartenances syndicales des personnes ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre de celles-ci est puni. »

مختلف هذه الحالات لا يشكل جريمة ولا يخضع القائم بها للعقاب حتى دون حصوله على موافقة الشخص المعني.

ب) العقوبة التكميلية: يمكن أن يتعرض مرتكب هذه الجريمة إضافة إلى العقوبة الأصلية المتمثلة في الحبس والغرامة، إلى عقوبة تكميلية اختيارية أو أكثر من العقوبات المنصوص عليها في المادة 09 من قانون العقوبات.

2-3) جريمة رفض أحد حقوق الشخص المعني دون سبب شرعي:

تنص المادة 64 من القانون 07/18 على أنه "يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة من 20 ألف دج إلى 200 ألف دج أو بإحدى هاتين العقوبتين كل مسؤول عن المعالجة يرفض دون سبب مشروع حقوق الإعلام أو الولوج أو التصحيح أو الإعتراض المنصوص عليها في المواد 32، 34، 35، 36 من هذا القانون.

يهدف قانون حماية المعطيات من وراء إقرار مجموعة من الحقوق لفائدة أصحاب البيانات الشخصية إلى إعطائهم مكنة السيطرة على بياناتهم هذه، لذلك يتعين على المسؤول عن المعالجة تمكينهم من ممارسة هذه الحقوق، وفي حال ممارسة أصحاب البيانات لحقوقهم التي خولها لهم القانون فإنه يفترض بالمسؤول عن المعالجة الإستجابة لمطالبهم، سواء تعلق الأمر بحق الإعلام (المادة 32) حق الولوج (المادة 34) الحق في التصحيح (المادة 35 الحق في الإعتراض (المادة36).

ومن ثمة فإذا رفض المسؤول عن المعالجة تمكين المعني بالمعالجة من حق أو أكثر من هذه الحقوق دون سبب مشروع قامت الجريمة في حقه بمفهوم المادة 64 من القانون 07./18

1-2-3) أركان الجريمة: تقوم الجريمة بتوفر ركنيها المادي والمعنوي.

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة بتوافر العنصرين التاليين:

- رفض المسؤول عن معالجة المعطيات ذات الطابع الشخصي تمكين الشخص المعني بالمعالجة من ممارسة حقوقه المقررة له قانونا والمتمثلة في حقه في الإعلام أو في الولوج أو رفض حقه في التصحيح، أو رفض حقه في الإعتراض.

- عدم وجود سبب شرعي يبرر هذا الرفض.

وعليه فإنه تقوم في حق المسؤول عن المعالجة جنحة رفض حق المعني في الإعلام (المادتين 32،64) إذا رفض إعلامه مسبقا بهوية المسؤول عن المعالجة أو من يمثله قانونا أو رفض إعلامه بأغراض المعالجة أو رفض إعلامه بنقل معطياته إلى بلد أجنبي.

ويتحقق رفض الحق في الولوج (المادتين 64،34) عندما يرفض المسؤول عن المعالجة تمكين الشخص المعني من الحصول على ما يفيد:

- تأكيد إن كانت المعطيات الشخصية المتعلقة به هي محل معالجة أم لا، أو رفض إفادته بشكل واضح عن المعطيات التي تخضع للمعالجة، أو رفض إفادته بمصدر حصوله على هذه المعطيات.

ويتحقق رفض الحق في التصحيح (المادتين 35،64) إنطلاقا من المادة 35 إذا رفض المسؤول عن المعالجة طلب الشخص المعني بتحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة للقانون، أو يمنع معالجتها قانونا مثل المعطيات الحساسة، كما يتحقق أيضا رفض الحق في التصحيح إذا لم يقم المسؤول عن المعالجة بتبليغ الغير الذي أوصلت إليه معطيات الشخص المعني بكل تحيين أو تصحيح أو مسح أو إغلاق يخص هذه المعطيات الشخصية.

كما يتحقق رفض الحق في الإعتراض (المادتين 36،64) إنطلاقا من المادة 36 إذا رفض المسؤول عن المعالجة الإستجابة لطلب الشخص المعني المتعلق باعتراضه المبني على أسباب مشروعة على معالجة معطياته الشخصية.

أما عن العنصر الثاني فيتعلق بعدم وجود أي سبب شرعي يبرر للمسؤول عن المعالجة رفضه لحقوق الشخص المعني، والأسباب المشروعة لرفض المسؤول عن المعالجة الإلتزام بموجبات الحق في إعلام الشخص المعني هي الحالات التي نصت عليها المادة 33 من القانون 07/18، حيث إذا توفرت حالة منها جاز له رفض الحق في الإعلام للشخص المعني بمقتضيات المعالجة حسب نص المادة 32، وتتمثل هذه الحالات

- إذا تعذر عليه إعلام الشخص المعني، ويلزم على المسؤول عن المعالجة في هذه الحالة إشعار السلطة الوطنية بهذه الإ ستحالة وتقديم أسبابها.

- إذا تمت المعالجة تطبيقا لنص قانوني.

- إذا تمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية.

وعليه تعتبر أي حالة من هذه الحالات سببا مشروعا ينتفي بوجوده الركن المادي للجرم.

أما الأسباب المشروعة لرفض حق الولوج هو ما نصت عليه الفقرة الأ خيرة من المادة 34 ويتعلق بالطابع التعسفي لطلب الولوج الذي يظهر من خلال تكراره بصفة مستمرة من طرف المعني بالمعالجة.

وأما بالنسبة للأسباب المشروعة لرفض حق الإعتراض حسب المادة 36 فهي تتعلق بكون المعالجة تستجيب لالتزام قانوني، أو إذا كان هذا الحق قد استبعد صراحة في الترخيص بالمعالجة.

وعلى هذا الأساس فإنه إذا تخلفت هذه الأسباب القانونية اعتبر عدم استجابة المسؤول عن المعالجة في تمكين الشخص المعني من حقوقه المذكورة بأنه رفض دون سبب مشروع، وبالتالي تحقق الركن المادي لجريمة رفض حقوق الشخص المعني حسب نص المادة 64 من القانون 07/18، وهي جريمة شكلية لا يتوقف قيامها على تحقق نتيجة معنية في صورة الإضرار بمصلحة المعني بالمعالجة، بل لمجرد تحقق

السلوك الإجرامي والمتمثل في رفض المسؤول عن المعالجة حقا من حقوق المعني بالمعالجة يقوم الركن المادي.

ب) الركن المعنوي: تعتبر جريمة رفض حقوق الشخص المعني بمعالجة المعطيات الشخصية جريمة عمدية تقوم لمجرد القصد الجنائي العام بعنصريه العلم والإرداة، ومن ثمة يتحقق القصد الجنائي لدى الفاعل بعلمه أنه يرتكب أفعالا تشكل رفضا لتمكين المعني بالمعالجة لحقه في الإعلام أو لحقه في الولوج أو لحقه في التصحيح أو لحقه في الإعتراض، ويعلم إضافة إلى ذلك أنه لا يوجد أي سبب مشروع يبرر له هذا الرفض، وتتجه إرادته إلى القيام بهذا السلوك.

2-2-3) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: يعاقب على جريمة رفض حقوق الشخص المعني بالمعالجة حسب نص المادة 64 من القانون 07/18 بالحبس من شهرين (2) إلى سنتين (2) وبغرامة مالية من 20 ألف دج إلى 200 ألف دج أو بإحدى هاتين العقوبتين، وهذا يعني أنه يمكن الحكم على الجاني بعقوبة الحبس فقط دون الغرامة، أو بالغرامة فقط دون الحبس، وإذا تقرر إفادته بظروف التخفيف جاز تخفيض عقوبة الحبس إلى شهرين.

ب) العقوبة التكميلية: كغيرها من الجرائم المنصوص عليها فيقانون 07/18، فإنه يجوز للقاضي أن يحكم على المدان بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

3-3) جريمة معالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني:

نصت الفقرة الثانية من المادة 55 على أنه "يعاقب بنفس العقوبة أي على النحو المذكور في الفقرة الأولى وهي الحبس سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري، أو عندما يكون الإعتراض مبنيا على أسباب شرعية".

1-3-3) أركان الجريمة:

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة بالسلوك الإجرامي المتمثل في عدم التفات المسؤول عن المعالجة لاعتراض الشخص على معالجة معطياته الشخصية والاستمرار في معالجتها رغم إبداء هذا الأخير لرفضه بشكل صريح القيام بمعالجتها، ولقيام ركنها المادي يجب توفر أحد الشرطين:

إما أن يكون اعتراض الشخص المعني على معالجة معطياته مبنيا ومؤسسا على أسباب مشروعة، لأنه وإن كان يحق لصاحب المعطيات الشخصية قانونا الإعتراض على معالجة معطياته إلا أن ذلك مرهون بوجود مبررات شرعية تحكم هذا الإعتراض.

وهذا يعني أن الإعتراض ليس حقا مطلقا يمارسه الشخص المعني في كل الحالات، بل لابد للمعني بالمعالجة أن يبني رفضه واعتراضه على معالجة معطياته الشخصية في مواجهة المسؤول عن المعالجة على سبب

شرعي، ويكون هذا الأخير حينها ملزما بحكم القانون الإستجابة لهذا الإعتراض والتوقف عن إتيان أي إجراء من إجراءات المعالجة تنصب على هذه المعطيات الشخصية.

وتعتبر مسألة تقدير مدى مشروعية الأسباب التي يبنى عليها الإعتراض مسألة موضوعيةتخضع لتقدير محكمة الموضوع[1]، وغالبا ما يتم ستناد في تقدير مشروعية هذه الأسباب على إثارة حرمة الحياة الخاصة كما يعتبر من بين الأسباب المشروعة ضرورة التناسب بين المعطيات الشخصية المطلوبة في المعالجة وبين الهدف من تجميعها، حيث لا يجوز وفق المبادئ الأساسية التي تحكم معالجة المعطيات الشخصية جمع وتخزين معطيات شخصية إلا بالقدر الذي تكون فيه مرتبطة بالغرض الذي لأجله يراد جمعها ومعالجتها دون مبالغة[2].

ولا يجوز للشخص المعني حسب نص المادة 36 من القانون 07/18 أن يعترض على معالجة معطياته الشخصية إذا كانت معالجتها استجابة لتنفيذ التزام قانوني وضرورية لإنجازه، كتجميع البيانات المتعلقة بالهوية ومعالجتها من طرف الإدارة لإعداد بطاقة التعريف البيومترية مثلا، كما لا يجوز له أيضا ممارسة الحق في الإعتراض إذا ما تم استبعاده صراحة في المحرر الذي يمنح الترخيص بالمعالجة للمسؤول عن المعالجة، اذ في هاتين الحالتين يعد اعتراض المعني بالمعالجة غير مشروع.

-الشرط الثاني وهو أن يكون الإعتراض منصبا على معالجة تستهدف الإشهار التجاري، فكما يمكن للمعني بالمعالجة أن يؤسس اعتراضه على أسباب مشروعة، يمكن له أيضا أن يبني اعتراضه على المعالجة التي يكون الغرض منها هو الإشهار التجاري، وهو ما أكده القضاء الفرنسي من خلال قرار محكمة النقض الفرنسية المؤرخ في 1999/06/29، حينما اعتبرت أن جريمة المعالجة الآلية للمعطيات الشخصية المتعلقة بأشخاص طبيعيين رغم اعتراضهم المبني على أسباب مشروعة والمعاقب عليها بالمادة 1-18/226 من قانون العقوبات تعد متحققة من خلال الإتجار في ملفات تم تكوينها انطلاقا من القوائم الإلكترونية للمشتركين في الهاتف دون حذف المعطيات الشخصية المتعلقة بالمشتركين الذين طلبوا التسجيل في القائمة المسماة اللائحة البرتقالية، وذلك من أجل توظيف هذه الملفات في عمليات دعائية واستطلاع الرأي*، وكذلك أكدت محكمة النقض الفرنسية أيضا في قرارها المؤرخ في 28 سبتمبر 2004 حينما أدانت الكنيسة السانتولوجية (légalise scientologique) لمعالجة معطيات شخصية رغم الإعتراض الشرعي لأصحاب هذه المعطيات.[3]

[1] Jean Pradel, les infractions à l'informatique, revue internationale de droit comparé, vol 42 n°2, Avril – Juin 1990, p233.

[2] بيومي عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 634.

* وتتلخص وقائع هذا القرار في أن أحد الأشخاص استغل طلبات مشتركي الهاتف لإدراجهم في قوائم تسمى (liste orange)، حيث قام بتجميع معطياتهم الشخصية من دليل الهاتف لغرض إنشاء سجلات للإشهار التجاري، فقام هؤلاء بالإعتراض على ذلك لأنه لم يقم بسحب بعض المعطيات الشخصية، ورغم ذلك استمر في المعالجة انظر: Yves Mayaud, op cit, p675.

[3] Myriam Quéméner, Yves charpenel, op cit, p67.

وينتفي الطابع الجرمي من على هذا الفعل إذا كان الشخص المعني قد أبدى موافقته المسبقة على استعمال معطياته الشخصية لاستقبال رسائل إشهارية ودعائية في إطار الإستكشاف المباشر.[1]

وتعد جريمة معالجة المعطيات الشخصية رغم الإعتراض على المعالجة، جريمة شكلية يتحقق الركن المادي فيها بمجرد قيام المعني بالمعالجة الاستمرار في معالجة معطيات شخصية رغم إبداء صاحبها اعتراضه على معالجتها واستعمالها، ولا يتوقف قيامها على تحقق نتيجة معينة.

واستنادا على ما أوضحناه فيما تقدم فإنه يمكن الإشارة إلى أن جريمة معالجة معطيات شخصية رغم اعتراض الشخص المعني طبقا للفقرة الثانية من المادة 55 تتداخل في وصفها مع جريمة رفض حقوق المعني بالمعالجة حسب المادة 64 في الحالة المتعلقة برفض حق الاعتراض، وهو مايطلق عليه بتعدد الأوصاف أو التعدد الصوري وهو انطباق أكثر من نص قانوني على فعل واحد.

إذ في كلتا الحالتين يتحقق رفض الإعتراض، ذلك أن استمرار المسؤول في المعالجة رغم اعتراض الشخص المعني هو أيضا رفض ضمني لاعتراضه، وفي هذه الحالة نطبق أحكام المادة 32 من قانون العقوبات.[2]

ب) الركن المعنوي: صورة الركن المعنوي لهذه الجريمة هي القصد الجنائي، لذلك فهي لا تقع عن طريق الخطأ بالإهمال أو عدم الإحتياط، بحيث تنصرف إرادة الجاني إلى الإستمرار في معالجة معطيات شخصية لشخص معين رغم الوصول إلى علمه باعتراض هذا الأخير لديه على معالجة معطياته.

ولا يتوقف تحقق الركن المعنوي لهذه الجريمة على توفر القصد الجنائي الخاص إلا في الحالة التي يستهدف فيها الجاني من وراء معالجة المعطيات الشخصية الإشهار التجاري، إذ يلزم في هذه الحالة أن تتجه نيته للقيام بعمليات الإستكشاف المباشر وإرسال إشهارات تجارية رغم اعتراض صاحب البيانات الشخصية على ذلك.

2-3-3) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: تعاقب المادة 2/55 من القانون 07/18على جريمة معالجة معطيات شخصية رغم عتراض بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج.

والملاحظ أن المشرع قد تشدد في عقاب هذا الفعل بالمقارنة مع فعل رفض الإعتراض.

ب) العقوبة التكميلية: علاوة على العقوبة الأصلية فإنه يجوز الحكم على الشخص المدان بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات، حسب ما يتوافق مع طبيعة الجاني (شخصا طبيعيا أو معنويا).

[1] انظر المادة 37 من القانون 07/18.

[2] تنص المادة 32 من قانون العقوبات: على أنه يجب أن يوصف الفعل الواحد الذي يحتمل عدة أوصاف بالوصف الأشد من بينها، وهو ما يسمى بحالة التعدد الصوري للجرائم الذي يعني تعدد الأوصاف القانونية للفعل الواحد، بمعنى انطباق عدة نصوص تجريمية إزاء فعل واحد، ولا يخضع في النهاية هذا الفعل إلا لنص واحد من بينها وهو النص الذي يحتوي على العقوبة الأشد.

4-3) جريمة عدم إعلام السلطة الوطنية والشخص المعني بالإنتهاك الحاصل على المعطيات الشخصية في مجال الإتصالات الإلكترونية:

تنص المادة 66 من القانون 07/18 على أنه "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج أو بإحدى هاتين العقوبتين فقط، مقدم الخدمة الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية خلافا لأحكام المادة 43 من هذا القانون".

وبمطالعة المادة 43 فإنها تلزم مقدم الخدمة بإعلام السلطة الوطنية والشخص المعني بالمعالجة فورا إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الإتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، وكان من شأن ذلك أن يشكل مساسا بالحياة الخاصة للشخص المعني، مالم تقرر السلطة الوطنية أن مقدم الخدمة قد اتخذ الضمانات الضرورية لحماية المعطيات.

بداية وقبل التطرق إلى أركان هذه الجريمة والعناصر المكونة لها نشير إلى خصائصها من حيث صفة مرتكبها ومجال ارتكابها، حيث ترتكب هذه الجريمة من طرف مقدم الخدمات، وهو أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات، كما يقصد به أيضا أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصالات المذكورة أو للمستعملين، وهو التعريف المقتبس كلية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

ويتضح من ذلك أن القدرة على استخدام وسائل الإتصال الإلكترونية يتطلب مجموعة من الأشخاص القائمين على تشغيل هذه الوسائل، وهؤلاء هم الذين يمكن أن نطلق عليهم الوسطاء في خدمة الأنترنت.[1]

وأساس المسؤولية الجزائية لمقدمي الخدمة في إطار القانون 07/18 هو المساس بالحق في الخصوصية انطلاقا من قدرتهم على معالجة المعطيات الشخصية للمستخدمين من جمع وتخزين وتحويل... وهو بذلك يختلف عن أساس مسؤوليتهم الجزائية وفق قانون العقوبات بخصوص الأفعال التي تشكل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في هذا القانون والمرتبط بنوع الخدمة المقدمة ومحتواها غير المشروع، لأجل هذا نجد معظم التشريعات تراعي التفرقة بين ما إذا كان مفهوم الخدمة مجرد ناقل للمعلومات أم يحق له مراقبة مشروعية محتوى ومضمون المعلومات التي تبث عبر الإتصالات الإلكترونية.[2]

[1] بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، مرجع سابق، ص93.
[2] بيومي حجازي، مرجع نفسه، ص93.

أما عن مجال هذه الجريمة هو شبكات الإتصالات الإلكترونية[1] والمقصود بها حسب الفقرة 21 من المادة 10 من القانون 04/18[2] أنها كل منشأة أو مجموعة منشآت تضمن إما إرسال أو إيصال إشارات إلكترونية، وكذا تبادل معلومات التحكم والتسيير المتصلة بها ما بين النقاط الطرفية لهذه الشبكة، وعند الإقتضاء الوسائل الأخرى التي تضمن إيصال الإتصالات الإلكترونية، وتعتبر هذه الشبكات هي أساس خدمة الإتصالات الإلكترونية الموجهة للجمهور، حيث تنص الفقرة 16 من المادة 10 من نفس القانون (04/18) أن المقصود بخدمة الإتصالات الإلكترونية وكذا الخدمات التي تستعمل قدرات شبكات الإتصالات الإلكترونية والتي تتطلب زيادة على خدمة الإتصالات الإلكترونية القاعدية ووظائف المعالجة والتخزين، ومن ثم فمجال هذه الجريمة هو وظائف المعالجة والتخزين المرتبطة بالمعطيات الشخصية .

1-4-3) أركان الجريمة:

أ) الركن المادي: يتمثل الركن المادي لهذه الجريمة في السلوك الإجرامي الذي يتحقق بعدم قيام مزود الخدمة بإبلاغ أو إخطار السلطة الوطنية لحماية المعطيات أو الشخص المعني صاحب المعطيات الشخصية بكل انتهاكات تطال هذه المعطيات بمناسبة معالجتها عبر شبكات الإتصالات الإلكترونية يتم اكتشافها من طرفه أثناء أداء خدمة الإتصالات الإلكترونية، وقد حددت المادة 43 من القانون مجموع الأفعال التي تشكل انتهاكا للمعطيات الشخصية وتتمثل في الإتلاف، الضياع، الإفشاء أو الولوج إليها دون ترخيص، كما يشترط أن تؤدي أفعال الإنتهاك هذه إلى المساس بالحق في الخصوصية للشخص المعني.

ويفهم من كلمة "فورا" الواردة في نص الماة 43 أن مقدم الخدمة يعلم السلطة الوطنية والشخص المعني بأية وسيلة تراسل إلكترونية دون انتظار أو تمهل.

ب) الركن المعنوي: تعد جريمة عدم إعلام السلطة الوطنية والشخص المعني بانتهاك المعطيات الشخصية في مجال الإتصالات الإلكترونية جريمة عمدية، صورة الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة، ولذلك يجب أن يعلم الجاني بوجود انتهاكات تطال معطيات شخصية لأحد المستخدمين لشبكة الإتصالات الإلكترونية قد تؤدي إلى إتلاف هذه المعطيات أو ضياعها أو إفشائها أو الولوج إليها بصورة غير مشروعة، وغالبا ما يكون ذلك عند تعرض نظام المعالجة الآلية للمعطيات الذي توجد به هذه المعطيات الشخصية للإختراق عبر القرصنة المعلوماتية، ولا يقوم رغم علمه هذا بإخطار السلطة الوطنية لحماية المعطيات الشخصية والشخص المعني بهذه الإنتهاكات .

وهي جريمة مادية تقوم لمجرد السلوك الإجرامي، ولا يعتد فيها بالقصد الجنائي الخاص، حيث يعاقب الفاعل عنها مهما كانت نيته أو غايته من وراء ذلك الفعل، إذ لا يهم أن يكون له باعث الإضرار بالشخص المعني، أو الإساءة إلى سمعته أو غير ذلك. ونشير إلى أنه لا يعد مقدم الخدمة مرتكبا لجريمة عدم إعلام

[1] المقصود بالإتصالات الإلكترونية حسب التعريف الوارد في المادة 03 من القانون 07/18 والمادة 02 من القانون 04/09 والمادة 10 من القانون 04/18 هي كل المراسلات والإرسالات التي تقع سواء في شكل علامات أو إشارات أو كتابات أو صور أو أصوات، أو بيانات أو معلومات مهما كانت طبيعتها يتم تبادلها أو إرسالها بطريق إلكتروني عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.

[2] القانون 04/18 مؤرخ في 10 ماي 2018 يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية عدد 27، صادرة بتاريخ 13 ماي 2018.

السلطة الوطنية أو للشخص المعني بانتهاك المعطيات الشخصية، إذا ما قررت السلطة الوطنية أن مقدم الخدمة قد اتخذ كافة الضمانات الضرورية لحماية المعطيات الشخصية.

2-4-3) العقوبة: إذا قامت الجريمة بركنيها المادي والمعنوي قامت المسؤولية الجزائية على الفاعل ويعاقب عنها طبقا لما يقرره القانون 07/18 من عقوبات.

أ) العقوبات الأصلية: يعاقب مورد الخدمات عن عدم إعلام السلطة الوطنية والشخص المعني بانتهاكات المعطيات الشخصية في مجال الإتصالات الإلكترونية بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج أو بإحدى هاتين العقوبتين.

وهنا يكون للمحكمة إما الحكم على الشخص المدان بالعقوبتين معا، وفي هذه الحالة يجوز إذا ما تقرر إفادته بظروف التخفيف، تخفيض عقوبة الحبس إلى شهرين والغرامة إلى 20 ألف دج، وإما إدانته بإحدى هاتين العقوبتين أي إما الحبس أو الغرامة، وفي هذه الحالة يجب ألا تقل العقوبة المحكوم بها عن الحد الأدنى المقرر قانونا للجريمة، أي ألا تقل العقوبة عن سنة حبس و100 ألف دج غرامة.

ب) العقوبة التكميلية: كغيرها من الجرائم المنصوص عليها في قانون 07/18، فإنه يجوز للقاضي أن يحكم على المدان بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

الفرع الثاني: الجرائم المرتبطة بمخالفة القواعد الإجرائية

تتعدد الإجراءات المرتبطة بمعالجة المعطيات الشخصية وتتكامل بطريقة تؤشر إلى أهمية هذه المسألة والتي تتوزع على أساسها المسؤوليات، ومن ثم اعتبرت أفعال المعالجات المنصبة على معطيات شخصية لا تحترم فيها هذه الإجراءات معالجات غير مشروعة تصل الى درجة التجريم.

أولا: الجرائم المرتبطة بالإجراءات المسبقة للمعالجة:

تعتبر هذه الجرائم التي تنص عليها تشريعات حماية البيانات الشخصية في إطار مخالفة القائمين بالمعالجة للقواعد الشكلية المحددة قانونا، حيث تقتضي المعالجة السليمة للمعطيات الشخصية ضرورة احترام مجموعة من القواعد الشكلية كرسها المشرع بهدف ضمان حماية الأشخاص الطبيعيين في مواجهة هذه المعالجة، ومن ثم تكون هذه الجرائم ناتجة عن مخالفة هذه القواعد الإجرائية والتي يلزم المسؤولون عن المعالجة بتطبيقها باعتبارها حماية احترازية واستباقية من المخاطر الناتجة عن معالجة المعطيات ذات الطابع الشخصي.

1) معالجة المعطيات الشخصية دون تصريح مسبق أو ترخيص:

تقع هذه الجريمة مخالفة لأحكام المادة 12 من القانون 07/18 التي أوجبت أن تخضع كل عملية معالجة لمعطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية لحماية المعطيات، أو بترخيص منها ما لم يوجد نص قانوني يقضي باستثناء عملية معالجة معينة من خضوعها لهذه الإجراءات.

لذلك نصت المادة 56 على أنه يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذلت طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون.

1-1) أركان الجريمة: تقوم الجريمة بتحقق الركنين المادي والمتمثل في النشاط الإجرامي من خلال إنجاز معالجة أو الأمر بإنجاز معالجة لمعطيات شخصية، دون مراعاة الإجراءات الأولية المتمثلة في التصريح لدى السلطة الوطنية أو ترخيص منها، والثاني ركن معنوي والذي يتخذ صورة القصد الجنائي العام وذلك كما يلي:

أ) الركن المادي: يتحقق الركن المادي للجريمة بتوفر عنصرين هما:

- إنجاز معالجة لمعطيات شخصية أو الأمر بإنجاز هذه المعالجة، حيث تنشأ الجريمة بداية بمباشرة القائمين على معالجة المعطيات الشخصية أنشطة المعالجة، وذلك من خلال تجميع هذه المعطيات أو تسجيلها أو تحليلها أو تعديلها أو تصنيفها أو حفظها أو محوها أو كل عملية من ذات الطبيعة، تحمل معالجة لهذه المعطيات بقصد الربط بينها للحصول على معلومات شخصية[1]، فإذا ما تم ذلك فإن فعل المعالجة الآلية للمعطيات يعد متحققا وفقا لأحكام القانون.[2]

- عدم التوفر على ترخيص أو تصريح مسبقينفهناك معطيات شخصية يكتفى في معالجتها بمجرد التصريح لدى السلطة الوطنية، وهناك معالجات تستوجب فضلا عن ذلك ضرورة صدور ترخيص من السلطة الوطنية.

والتصريح الذي بينت المواد من 13 إلى 16 من القانون 07/18 أحكامه هو عبارة عن إخطار يقدم أمام السلطة الوطنية، ولا يمكن للمسؤول عن المعالجة مباشرة أية معالجة معطيات شخصية مهما كانت طبيعتها دون أن يسبق ذلك تقديمه لتصريح لدى السلطة الوطنية، وأما الترخيص فهو بمثابة قرار تصدره السلطة الوطنية يتضمن الموافقة على القيام بعمليات معالجة المعطيات الشخصية، وذلك في بعض الحالات التي لا يكفي فيها مجرد التصريح لإنجازها، وإنما يستوجب زيادة على ذلك ضرورة الحصول على ترخيص من السلطة الوطنية، فإذا تم إجراء معالجات لبيانات شخصية أو تم الأمر بإجرائها دون التقيد بهذين الإجرائين، أي دون تقديم تصريح لدى السلطة الوطنية أو دون الحصول على ترخيص منها في الحالات التي يستوجب فيها القانون هذا الترخيص،[3] اعتبرت تلك المعالجة غير قانونية ومجرم إنجازها أو الأمر بإنجازها.

وقد قضت محكمة النقض الفرنسية بموجب القرار الصادر بتاريخ 30 أكتوبر 2001 بأن الجهة ستئنافية لما قضت بتوافر جميع أركان جريمة المعالجة دون تصريح مسبق من اللجنة الوطنية حسب مقتضيات المادة 16/226 من قانون العقوبات كانت على صواب، بعدما استخلصت من نتائج تحقيقها أن

[1] بولين أيوب، مرجع سابق، ص 416.

[2] محمد أمين الشوابكة، مرجع سابق، ص87.

[3] الحالات التي يشترط فيها القانون الحصول على ترخيص من السلطة الوطنية وردت في المواد 17،19،21 و14 من القانون 07/18.

المتهمين استعملوا نظاما للمعالجة الآلية للمعطيات الشخصية دون القيام بإجراء التصريح المسبق لدى اللجنة الوطنية للمعلوميات والحريات، وكذلك اعتبرت إحدى محاكم الدرجة الكبرى في فرنسا بموجب قرارها المؤرخ في 18 فيفري 2003 أن استعمال إسم أحد الأشخاص بموقع إلكتروني على شبكة الإنترنت يعد بمثابة معالجة آلية للمعطيات الشخصية حسب مفهوم المادة 5 من القانون 17/78 ، ومن ثم فإن المسؤول عن الموقع الإلكتروني الذي لم يقدم تصريحا مسبقا للجنة الوطنية للمعلوميات والحريات (CNIL) عند إنجازه معالجة آلية لهذه المعطيات الإسمية يقع تحت طائلة العقوبات المنصوص عليها في المادة 16/226 من قانون العقوبات.[1]

ويهدف المشرع من وراء هذا التجريم إلى فرض حق الدولة في الرقابة على تداول ونقل البيانات الشخصية، لأن عدم احترام إجراءات التصريح أو الترخيص يفقد جهات الرقابة عملها المؤسس على كفالة عدم الإعتداء على الخصوصية، وذلك لاحتمال تسهيل ارتكاب جرائم الإعتداء على البيانات الشخصية مع غياب رقابة الدولة على هذا النشاط.[2]

لذلك نجد في التشريع الفرنسي أن المادة 226-16 من قانون العقوبات تضمنت نفس الأحكام المنصوص عليها في المادة 56 من القانون 07/18 المتعلقة بالمعالجة دون ترخيص أو تصريح مسبق، غير أنه زيادة في تفعيل رقابة الدولة على احترام حق الخصوصية، اعتبر أنه في حالة ما إذا عاينت اللجنة الوطنية للمعلوماتية والحريات (CNIL) حالة اعتداء خطيرة وحالة على الحقوق والحريات المذكورة في المادة الأولى من القانون المتعلق بحماية البيانات، فإن رئيس اللجنة الوطنية للمعلوماتية والحريات يطلب من الجهة القضائية بموجب إجراءات الإستعجال الأمر باتخاذ أي إجراء تحفظي يكون لازما للحفاظ على هذه الحقوق والحريات.[3] وتعتبر مخالفة تلك الإجراءات المأمور بها من طرف القاضي الإستعجالي أفعالا مجرمة بموجب الفقرة الثانية من المادة 226-16 المذكورة أعلاه، ومعاقبا عليها بنفس العقوبات المقررة للمعالجة دون تصريح أو ترخيص مسبق[4].

وبالرجوع إلى المادة 14 من القانون 07/18 التي تلزم المسؤول عن المعالجة بضرورة إخطار السلطة الوطنية فورا بأي تغيير للمعلومات الواردة في التصريح المقدم لها أو بأي حذف يطال المعالجة، فالسؤال المطروح هنا يتعلق بمدى خضوع عدم الإلتزام بهذا الإخطار مخالفة لأحكام المادة 14 للتجريم، وليس فقط لعقوبة الغرامة الإدارية من طرف السلطة الوطنية لحماية المعطيات الشخصية حسب مقتضيات المادة47 من القانون 07/18.

يمكن القول إنه بالنسبة لعملية الحذف فقد اعتبر الفقه الفرنسي أنها عملية مناقضة لإنجاز المعالجة التي هي السلوك المادي للجريمة المنصوص عليه في المادة 56، وبالتالي لا يمكن أن يطال التجريم الوارد بهذا النص عملية الحذف دون إخطار السلطة الوطنية، أما التغيير فيعني إضافة معلومات جديدة غير

[1] Yves Mayaud, OP, CIT, P67.

[2] بولين أيوب، مرجع سابق، ص 414.

[3] Voir l'article 45/3-III de la loi n° 78-17 du 6 janvier 1978

[4]. Voir l'article 226-16/2 du code pénal français

تلك التي كانت موجودة، ومن ثم فيعتبر عملية أخرى لإنجاز المعالجة، وهو ما قد يؤدي بعدم الإخطار بها بمثابة عدم تصريح للسلطة الوطنية ويطاله التجريم،[1] وهو الأمر الذي ندعو المشرع الى تداركه وتجريم هذا الفعل بالنص على ذلك صراحة، وعدم الإكتفاء بخضوعه الى غرامة إدارية تسلطها السلطة الوطنية لحماية المعطيات الشخصية حسب ما تقضي به المادة 3/47 من القانون 07/18.

ب) الركن المعنوي: اعتبر المشرع الجزائري جريمة معالجة معطيات شخصية دون ترخيص أو تصريح مسبق من الجرائم العمدية التي يتحقق الركن المعنوي فيها بالقصد الجنائي العام، وذلك من خلال علم الجاني بأنه يباشر أو يأمر بمباشرة معالجة لمعطيات ذات طابع شخصي دون أن يكون قد سبق له أن قدم تصريحا بذلك لدى السلطة الوطنية، أو يعلم أن معالجته تنصب على معطيات شخصية تستوجب ترخيصا من السلطة الوطنية وهو لا يحوزه، ورغم ذلك تتجه إرادته إلى إجراء المعالجة دونهما في أي صورة من صورها المختلفة.

في حين اعتبر المشرع الفرنسي أن هذه الجريمة تقوم أيضا عن طريق الخطأ إذا أجريت المعالجة دون تصريح أو ترخيص نتيجة إهمال الفاعل[2] (par négligence)

وإذا كان الفقه الفرنسي قد اختلف حول طبيعة هذه الجريمة[3]، فإن محكمة النقض الفرنسية أكدت في قضائها[4] أن هذه الجريمة تعد من الجرائم المادية التي يفترض توفر القصد الجنائي فيها بمجرد ارتكاب السلوك المادي المكون لها، بإنشاء ملفات للبيانات الشخصية خفية دون ترخيص أو تصريح مسبق، ولا حاجة إلى البحث عن إقامة الدليل على توافر الركن المعنوي.[5]

1-2) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: يعاقب المشرع الجزائري على هذه الجريمة بعقوبة أصلية تتمثل في الحبس من سنتين إلى خمس سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج، كما يعاقب المشرع كل من أمر بإجراء المعالجة بذات العقوبة المقررة لمن قام بإنجازها، وذلك كفاعل أصلي للجريمة، ولم يميز بينهما.

ب) العقوبة التكميلية: إضافة إلى العقوبات الأصلية المتمثلة في الحبس والغرامة فإنه يجوز إخضاع المحكوم عليه بعقوبات تكميلية وفق نفس الشروط التي سبق بيانها.

---

[1] طباش عز الدين، مرجع سابق، ص 40.

[2] Voir l'article 226-16 du code pénal français.

[3] Pascal arrigo et Alain Benssoussan, la cyber criminalité vers une régulation internationale de l'internet, la gazette du palais, n°289 du 16 octobre 2001 p.35 disponible sur le site : http://www.labase-lextenso.fr/revue/GPL/2001L289 .

[4] نائلة عادل محمد فريد قورة، مرجع سابق، مشار إليه في الهامش رقم 01 ص 238.

- قرار المحكمة الإبتدائية الكبرى لـ كريتاي المؤرخ في 10 جوان 1987 وتتلخص وقائع القضية في قيام الشركة الفرنسية "SKF " بتخزين بيانات تتعلق بالحياة الخاصة والإتجاهات السياسية والعضوية النقابية العمالية لموظفيها، تحصلت عليها من الاستمارات التي قام الموظفون بتقديمها عند التقدم للوظيفة ، دون أن تحصل الشركة على إذن مسبق من اللجنة الوطنية للمعلومات والحريات (CNIL) وقد تقدمت اللجنة ببلاغ إلى النائب العام، وتمت متابعة الشركة حيث رأت المحكمة أن ذلك يعد مخالفة لأحكام المادة 42 من القانون 17/78، أنظر نائلة عادل محمد فريد قورة، مرجع نفسه، مشار إليه في التهميش رقم 01 ص 238.

[5] محمد أمين الشوابكة، مرجع سابق، ص 89.

ﻫ جريمة الإستمرار في معالجة المعطيات رغم سحب وصل التصريح أو الترخيص:

تنص الفقرة الثانية من المادة 56 أنه يعاقب بنفس العقوبات المذكورة في الفقرة الأولى أي الحبس من سنتين (2) إلى خمس (5) سنوات كل من واصل نشاط معالجة المعطيات الشخصية رغم سحب وصل التصريح أو الترخيص الممنوح له".

قبل التطرق إلى أركان هذه الجريمة لابد أن نشير هنا إلى أن سحب وصل التصريح أو قرار الترخيص يعد من صلاحيات السلطة الوطنية لحماية المعطيات الشخصية وفق أحكام المادة 46 من القانون 07/18، فهي الجهة القانونية الوحيدة المخولة بهذا الإجراء، حيث تتخذه بموجب قرارات إدارية قابلة للطعن أمام مجلس الدولة.

كما أن القرار بسحب وصل التصريح أو الترخيص قد يكون مؤقتالمدة لا تتجاوز سنة أو يكون نهائيا، وفي كلتا الحالتين يعد القرار بسحبهما بمثابة عقوبة إدارية تتخذها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في حالات معينة نصت عليها المادة 48 من القانون 07/18 وهي حالة ما إذا تبين أن المعالجة محل التصريح أو الترخيص من شأنها المساس بالإمن الوطني أو أنها منافية للأخلاق أو الآداب العامة.

1-2) أركان الجريمة: تقوم الجريمة بتحقق الركنين المادي والمعنوي معا.

أ) الركن المادي: ويتحقق بالسلوك الإجرامي المتمثل في قيام المسؤول عن المعالجة بمواصلة نشاط معالجة المعطيات الشخصية والإستمرار فيه، رغم أن السلطة الوطنية لحماية المعطيات أبلغته بقرارها حسبما تقتضيه القواعد العامة في تبليغ القرارات الإدارية الذي يتضمن سحبها لوصل التصريح أو الترخيص الممنوح له سابقا. ويشترط لقيام هذا النشاط المادي:

- أن يكون المسؤول عن المعالجة قد بدأ فعلا في ممارسة مختلف الأنشطة المتعلقة بالمعالجة بصورة قانونية بعد قيامه بالتصريح لدى السلطة الوطنية أو ترخيص منها.

- أن تصدر السلطة الوطنية قرارا يتضمن سحب وصل التصريح أو الترخيص لأي سبب من الأسباب في إطار ممارسة صلاحياتها.

- أن يواصل المسؤول عن المعالجة القيام بأنشطة المعالجة المنصبة على المعطيات الشخصية المعنية بهذا السحب، حيث قد لا يمس قرار السحب كل عملية المعالجة وينصرف إلى معطيات بعينها.

وفي حالة تحقق هذه الشروط يقوم السلوك الإجرامي وفق مقتضيات المادة 56 الفقرة الثانية.

ب) الركن المعنوي: تعتبر هذه الجريمة مثل جريمة المعالجة دون تصريح أو ترخيص، جريمة عمدية تقوم لمجرد القصد الجنائي العام الذي يقتضي علم المسؤول عن المعالجة بسحب السلطة الوطنية وصل التصريح أو قرار الترخيص له بمعالجة المعطيات الشخصية، وتتجه إرادته إلى إتيان فعل الإستمرار في المعالجة رغم ذلك.

ويكفي في هذه الجريمة شأنها في ذلك شأن جريمة المعالجة دون تصريح أو ترخيص لقيام ركنها المعنوي توفر القصد الجنائي العام فقط دون القصد الجنائي الخاص، إذ يفهم من صياغة النص التجريمي أنه لا يعتد بالنية الخاصة للجاني، حيث يستوي أن يكون باعثه هو الإضرار المادي بالشخص أو استغلال معطياته للإساءة بسمعته أو كان ذلك لمجرد الفضول وحب الإستطلاع، وهي جريمة مادية حيث يكون القصد الجنائي مفترضا وبالتالي تقوم لمجرد ارتكاب السلوك الإجرامي.

2-2) العقوبة المقررة قانونا:

أ) العقوبة الأصلية ساوى المشرع في العقوبة الأصلية بين جريمة الإستمرار في المعالجة بعد سحب وصل التصريح أو الترخيص وبين جريمة المعالجة بدون تصريح أو ترخيص، حيث يعاقب عليها بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج.

ب) العقوبة التكميلية: علاوة على العقوبات الأصلية يمكن كذلك إخضاع الجاني إلى العقوبات التكميلية الإختيارية المحددة بنص المادة 09 و09 مكرر من قانون العقوبات.

3) جريمة نقل معطيات ذات طابع شخصي لدولة أجنبية دون ترخيص: تنص المادة 67 من قانون 07/18 أنه يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500 ألف دج إلى مليون دج كل من قام بنقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من هذا القانون.

وتنص المادة 44 على أنه لا يجوز للمسؤول عن المعالجة نقل المعطيات الشخصية إلى دولة أجنبية إلا بترخيص من السلطة الوطنية ..."

ويشكل انتقال البيانات خارج الحدود الوطنية البعد العالمي لعملية معالجة المعطيات ذات الطابع الشخصي، ويعتبر هذا الإنتقال استنادا إلى مبدأ السيادة الإقليمية إخراج لهذه البيانات من نطاق تطبيق القوانين المحلية واختصاص السلطات الوطنية،[1] لذلك كان من البديهي وجود أطر قانونية مناسبة تكرس حماية جدية عند نقل هذه البيانات إلى بلد آخر، سيما من خلال ضرورة حصول المسؤول عن المعالجة على ترخيص من السلطة الوطنية لحماية المعطيات الشخصية حتى يتمكن من نقل هذه المعطيات خارج الدولة، وخلاف ذلك يشكل جريمة نقل معطيات شخصية إلى دولة أجنبية دون ترخيص.

1-3) أركان الجريمة:تقوم هذه الجريمة بتحقق كل من الركنين المادي والمعنوي:

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة بتوفر عنصرين هما:

- العنصر الأول ويتعلق بقيام المسؤول عن المعالجة أو المعالج من الباطن بتحويل معطيات ذات طابع شخصي إلى دولة أجنبية، والملاحظ أن المشرع الجزائري لم يأت على تحديد المقصود بعملية تحويل أو نقل معطيات إلى دولة أجنبية، وهو الأمر المشابه في التشريع الفرنسي والتوجيهات الأوروبية المتعلقة بحماية المعطيات، والتي لم تحدد هي أيضا مفهوم عملية تحويل المعطيات إلى دولة أخرى.

[1] منى الاشقر جبور، محمود جبور، مرجع سابق، ص102.

وحسب اللجنة الوطنية للمعلوماتية والحريات الفرنسية (CNIL) يعتبر نقل البيانات إلى بلد آخر أي اتصال أو نسخ أو تحويل معطيات بواسطة شبكة معلوماتية، أو أي اتصال من وسيط لآخر بغض النظر عن طبيعة الوسيلة أو نوع هذا الوسيط، كون هذه المعطيات من المقرر معالجتها في البلد المتلقي لها.[1]

وهناك العديد من المواقف التي تتطلب نقل المعطيات الشخصية إلى دولة أجنبية، مثل تحويل المؤسسات المالية (البنوك) معطيات شخصية متعلقة بزبائنها في إطار عمليات التوطين البنكي، عمليات التعاقد الإلكتروني المرتبط بالتجارة الإلكترونية، تبادل المعطيات الشخصية المتمركزة في قاعدة البيانات لإدارة الموارد البشرية للشركات متعددة الجنسيات، في إطار أنظمة صيانة تقنية المعلومات الدولية، في إطار ستضافة على شبكة الإتصالات الإلكترونية وتشغيل منصات تكنولوجيا المعلومات ....[2]

- أما العنصر الثاني أن يتم نقل المعطيات الشخصية إلى الدولة الأجنبية دون ترخيص من السلطة الوطنية، والملاحظ أن المشرع الجزائري في مسألة نقل المعطيات الشخصية نحو بلد أجنبي جاء غير منسجم مع باقي التشريعات المقارنة ،عندما اشترط فضلا عن ضمان الدولة المتلقية للمعطيات الشخصية لمستوى حماية كاف للحياة الخاصة وللحريات والحقوق الأساسية، أن يكون نقل هذه المعطيات بناء على ترخيص من السلطة الوطنية لحماية المعطيات*، وذلك بهدف تجنب التحايل على الحماية الممنوحة في هذه البلدان عن طريق التحويل، ومن ثم ضمان استمرار تمتع الأشخاص بالحماية فيما يتعلق بمعالجة معطياتهم الشخصية عندما تغادر هذه المعطيات إقليم الدولة.

وتبسط السلطة الوطنية رقابتها من خلال دراسة طلب الترخيص بنقل المعطيات الشخصية نحو بلد أجنبي معين، بالإضافة إلى تقييمها لمستوى الحماية الكافي الذي تضمنه تلك الدولة من خلال معايير تتفق مع المقتضيات القانونية المعمول بها في هذه الدولة وإجراءات الأمن المطبقة فيها، وكذا مع الخصائص المتعلقة بالمعالجة مثل غايتها ومدتها وكذا طبيعة المعطيات المعالجة ووجهتها.[3]

ومع ذلك فقد أجاز المشرع في حالات محددة على سبيل الحصر للمسؤول عن المعالجة نقل معطيات شخصية نحو دولة أجنبية دون ترخيص من السلطة الوطنية حتى ولو لم تتوفر فيها مستويات الحماية

[1] CHRISTIANE FÉRAL-SCHUHL, transfert à l'étrranger des données à caractère personnel article Publié le 07/01/2008, disponible sur le site : http://www.feral-avocats.com/fr/publication

[2] Commission Nationale de l'informatique et des libertés, rapport sur les transferts de données à caractères personnel vers des pays non membre de l'union européenne, mai 2005, p.5 disponible sur le site : http://www.frareg.com

« Constitue un transfert de données vers un pays tiers : « toute communication, copie ou déplacement de données par l'intermidiare d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quelque soit le type de ce support dans la mesure au ces données ont vacation à faire l'objet d'un traitement dans le pays destinataire. »

* لم يشترط المشرع الفرنسي في المادة 68 من القانون 17/78 الترخيص بنقل المعطيات الشخصية من طرف اللجنة الوطنية للمعلوماتية والحريات إلى دولة أجنبية تمنح الحماية الكافية للمعطيات الشخصية، ومع ذلك يجب إعلامها بوجود هذه التحويلات كجزء من الإجراءات الشكلية قبل تنفيذ المعالجة الرئيسية التي تنشأ منها هذه التحويلات. أنظر المواد 68،69 من القانون 17/78. وكذلك المشرع المغربي في المواد 43،44 من القانون 09/08.

[3] أنظر المادة 2/44 من القانون 07/18.

الكافية للمعطيات الشخصية[1]، إلا إذا تعلقت المعالجة بمعطيات ترتبط أساسا بالكرامة الإنسانية والحريات العامة، فلا يتم نقل المعطيات الشخصية في هذه الحالة إلا بناء على ترخيص من السلطة الوطنية لحماية المعطيات.

وبتوفر هذين العنصرين يكون السلوك الإجرامي المكون للركن المادي للجريمة المتمثلة في نقل معطيات شخصية إلى دولة أجنبية دون ترخيص من السلطة الوطنية متحققا، شريطة ألا يندرج ضمن الحالات المستثناة.

ب) الركن المعنوي: يقوم الركن المعنوي لهذه الجريمة بالقصد الجنائي العام، فهي جريمة عمدية يتطلب لقيامها أن يعلم الجاني أن فعله يعتبر نقلا لمعطيات شخصية نحو دولة أخرى، وأنه غير مرخص له بذلك من طرف السلطة الوطنية لحماية المعطيات الشخصية وإن عملية نقل هذه المعطيات الشخصية لا تندرج ضمن الحالات المستثناة قانونا، وذلك دون حاجة إلى قصد جنائي خاص، إذ لا عبرة للدوافع والبواعث التي حملت الجاني على القيام بهذا الفعل.

2-3) العقوبة: يعاقب المشرع الجزائري على جريمة نقل معطيات شخصية نحو دولة أجنبية دون ترخيص من السلطة الوطنية لحماية المعطيات وفق المادة 67 بالحبس من سنة إلى خمس سنوات وبغرامة من 500 ألف دج إلى مليون دج.

فضلاعن العقوبات التكميلية التي يجوز الحكم بها في مواجهة المحكوم عليه طبقا لأحكام المادة 9 و9 مكرر1 من قانون العقوبات.

ثانيا: الجرائم المرتبطة بإجراءات الحماية والتعاون مع السلطة الوطنية:

إنه وبالرغم من الإعتراف بالحماية التشريعية من قبل العديد من القوانين للمعطيات ذات الطابع الشخصي، إلا أنها تبقى عرضة للإعتداء ليس فقط نتيجة النقص التشريعي أو التنظيمي، وإنما كذلك نتيجة للإمكانيات التقنية الهائلة التي تتيحها النظم المعلوماتية والإتصالات الإلكترونية، لذلك فقد ألزم المشرع كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي بضرورة اتخاذ مجموعة من الإجراءات والتدابير التقنية والتنظيمية بهدف ضمان حماية هذه المعطيات من كل المخاطر التي يمكن أن تلحق بها، وعدم الإستجابة لهذا الإلتزام والتقصير في اتخاذ مثل هذه التدابير يعد فعلا مجرما، كما أن المشرع قد منح السلطة الوطنية لحماية المعطيات بعض الصلاحيات تقوم بها في إطار مهامها المرتبطة بتكريس الحماية الحقيقية للمعطيات الشخصية، وألزم في مقابل ذلك كل مسؤول عن معالجة المعطيات الشخصية بالإستجابة لمختلف الإلتزامات التي تتطلب منه التعاون مع هذه السلطة وعدم عرقلتها في أدائها لعملها.

[1] راجع المادة 45 من نفس القانون.

1) جريمة عدم اتخاذ التدابير التنظيمية والتقنية اللازمة لسلامة المعطيات الشخصية

تنص المادة 65 من القانون 07/18 على أنه "دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول يعاقب بغرامة من 200 ألف دج إلى 500 ألف دج المسؤول عن المعالجة الذي يخرق الإلتزامات المنصوص عليها في المادتين 38و39 من هذا القانون".

وبالعودة إلى هاتين المادتين، نجد أن المشرع ألزم من خلالهما كل من المسؤول عن المعالجة في المادة 38 والمعالج من الباطن في المادة 39 بوضع التدابير التقنية والتنظيمية الملائمة التي تضمن مستوى ملائم من السلامة للمعطيات الشخصية بالنظر إلى المخاطر المترتبة عن المعالجة، وبالنظر كذلك إلى طبيعة المعطيات الواجب حمايتها.

1-1) أركان الجريمة: وعلى أساس هذه النصوص القانونية فإن أركان هذه الجريمة هي:

أ) الركن المادي: لقيام الركن المادي لهذه الجريمة يقتضي الأمر توفر عنصرين هما:

العنصر الأول ويتعلق بقيام الجاني وهو إما المسؤول عن المعالجة أو معالج من الباطن بإنجاز معالجة لمعطيات شخصية عبر عملية أو مجموعة من العمليات التي تندرج ضمن نشاط المعالجة.

العنصر الثاني و يتعلق بعدم اتخاذ الجاني للإجراءات والتدابير التقنية أو التنظيمية حسب ما سبق بيانه كإجراءات التشفير أو وضع كلمات المرور أو وضع برامج أمنية تحول دون الدخول إلى النظام المعلوماتي الذي توجد به المعطيات ذات الطابع الشخصي، والهادفة جميعها إلى حماية المعطيات ذات الطابع الشخصي من كافة المخاطر التي من الممكن أن تتهددها خلال عمليات المعالجة، وقد حددت المادة 38 من القانون 07/18 أهم نماذج عن هذه المخاطر لا سيما الإتلاف العرضي أو غير المشروع، الضياع العرضي، التلف، النشر غير المرخص به، أو الولوج غير المرخص له، أو أي شكل من أشكال المعالجة غير المشروعة.

كما يجب أن تكون هذه التدابير على درجة من الفعالية وذات مستوى تقني يتلاءم مع درجة المخاطر التي تمثلها تلك المعالجة، خاصة إذا كانت المعطيات الشخصية تستوجب عملية معالجتها إرسالها عبر شبكات الإتصال الإلكترونية، أين يرتفع منسوب المخاطر فيها، ولقد حدد المشرع معيارين لتقدير مستوى الحماية وهما، درجة المخاطر المترتبة عن المعالجة، وطبيعة المعطيات الواجبة حمايتها، وبخصوص هذه الأخيرة أي طبيعة المعطيات الشخصية المعالجة، نجد أن المشرع الفرنسي يحدد للمسؤول عن المعالجة جملة من الإجراءات التقنية الملائمة، و التي تتخذ بموجب مراسيم بناء على رأي اللجنة الوطنية للمعلوماتية والحريات، حيث يجب اتخاذها عندما يتعلق الأمر بالمعطيات الشخصية الحساسة الواردة في النقطة 2 و6 في الفقرة II من المادة 08 من القانون 17/78، وهي التي أحالت عليها المادة 34 من نفس القانون، و يعد خرق هذه الإجراءات التي جاءت بها أساس التجريم الوارد في المادة 226-17 من قانون العقوبات الفرنسي، و كذلك نجد المشرع المغربي حدد في المادة 25 من القانون 09/08 المتعلق بحماية المعطيات الشخصية الإجراءات التقنية التي يتعين على المسؤول عن المعالجة اتخاذها عندما يتعلق الأمر بمعالجة معطيات

حساسة أو ذات الصلة بالصحة.* حيث يلزم قبل إجراء أي معالجة لمعطيات من هذا النوع اتخاذ كافة الإجراءات المحددة قانونا، وإلا وقع المسؤول عن المعالجة الذي يتقاعس عن اتخاذها في دائرة التجريم.

ولا يتوقف الأمر عند هذا الحد، بل نجد المشرع الجزائري في نص المادة 39 من القانون 07/18 يلزم المسؤول عن المعالجة عندما يتعلق الأمر بالمعالجة التي تكون لحسابه، ضرورة اختيار معالج من الباطن، يحرص هذا الأخير بدوره على أن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية ، ومن ثم يعتبر أي تقاعس منهما، أي من المسؤول عن المعالجة أو من المعالج من البطن عن اتخاذ التدابير الأمنية المطلوبة والملائمة لحماية المعطيات الشخصية أثناء عمليات المعالجة ضد أي فعل من شأنه الإضرار بالمعطيات وتهديد أمنها يعد فعلا مجرما، وهذا ما أكده القضاء الفرنسي حينما اعتبرت محكمة النقض الفرنسية في قراها المؤرخ في 30 أكتوبر 2001 أن قيام المتهمين باستعمال نظام معالجة آلية للمعطيات الشخصية دون اتخاذ كافة الاحتياطات اللازمة لمنع الموظفين الإداريين من الإطلاع على المعطيات الطبية باعتبارهم غير مرخص لهم بذلك، يشكل جميع العناصر المكونة للجريمة المنصوص عليها في المادة 226-17 من قانون العقوبات .[1]

والتساؤل المطروح في هذا الصدد، هل تقوم الجريمة فقط بعدم اتخاذ المسؤول عن المعالجة للإجراءات اللازمة لحماية سلامة وأمن المعطيات الشخصية محل المعالجة، أم يمكن أن تقوم الجريمة أيضا إذا كانت الإجراءات المتخذة لا تضمن مستوى كاف من الحماية للمعطيات، كعدم اختيار التدابير الملائمة والمناسبة التي تكفل هذه الحماية مثلا.

نرى أن المشرع نص في المادة 65 من القانون 07/18 على قيام هذه الجريمة في حق المسؤول عن المعالجة الذي يخرق الإلتزامات المنصوص عليها في المادة 38 من نفس القانون، وهذه الأخيرة توجب على المسؤول عن المعالجة أن يتخذ من التدابير التقنية ما يضمن مستوى ملائما من السلامة والأمن للمعطيات المعالجة، ومن ثم فإنه لا يكف أن يتخذ المسؤول عن المعالجة التدابير التقنية فقط، بل لا بد أن يختار منها ما يضمن مستوى معينا من الحماية يتماشى ودرجة المخاطر التي تتهدد المعطيات الشخصية، وذلك انطلاقا من طبيعة هذه المعطيات ونوعية المعالجة الخاضعة لها، وقد أشار الفقه الفرنسي إلى أنه لا يمكن

*تنص المادة 24 من القانون المغربي لحماية المعطيات الشخصية 08/09 على أنه يتخذ المسؤولون عن معالجة المعطيات الشخصية الحساسة أو ذات الصلة بالصحة الإجراءات الملائمة بغرض:

- الحيلولة دون ولوج أي شخص غير مأذون له على المنشآت المستعملة لمعالجة هذه المعطيات (مراقبة دخول المنشآت).

-الحيلولة دون قراءة أو نسخ أو تعديل أو سحب دعامات المعطيات من قبل أشخاص غير مأذون لهم (مراقبة دعامات المعطيات).

- الحيلولة دون الإدخال غير المأذون به وكذا التعرف على المعطيات ذات الطابع الشخصي تم إدراجها أو تغييرها أو الحذف غير المأذون به لهذه المعطيات (مراقبة الإدراج).

- منع استعمال أنظمة المعالجة الآلية للمعطيات بواسطة معدات إرسال معطيات من قبل أشخاص غير مرخص لهم (مراقبة الإستعمال).

- ضمان ولوج الأشخاص المرخص لهم فقط إلى المعطيات المعنية بالإذن (مراقبة الولوج).

- ضمان التحقق من الهيئات التي يمكن أن تنقل المعطيات ذات الطابع الشخصي التي تم إدخالها وتوقيت إدخالها، ولصالح من تم ذلك، وفي أجل يلائم طبيعة المعالجة ويحدد في النصوص التنظيمية المطبقة على كل قطاع على حدة (مراقبة الإدخال).

- منع قراءة أو استنساخ أو تغيير أو حذف معطيات ذات طابع شخصي أثناء إرسال المعطيات أو دعامات المعطيات بدون إذن (مراقبة النقل).

[1] Yves Mayaud, op, cit, p67.

للمسؤول عن المعالجة الإحتجاج بأنه يجهل التدابير الملائمة لنوع المعالجة التي يقوم بها للإفلات من المسؤولية[1].

ونشير إلى أن المشرع الجزائري قد حدد الجهة التي لها صلاحية تقدير مستوى الحماية التي توفرها التدابير التي اتخذها المسؤول عن المعالجة من حيث صلاحيتها وصمودها في مواجهة المخاطر التي تمثلها المعالجة الآلية للمعطيات الشخصية، وهي مسألة مخولة للسلطة الوطنية لحماية المعطيات، كما هو الشأن بالنسبة لما ورد في المادة 43 من القانون 07/18 التي تعطي للسلطة الوطنية صلاحية تقرير ما إذا كان مقدم الخدمة قد اتخذ الضمانات الضرورية لحماية المعطيات[2]، ويكون ذلك انطلاقا من التصريح الذي يقدمه المسؤول عن المعالجة إلى السلطة الوطنية، هذا التصريح الذي أوجب المشرع أن يتضمن وصفا عاما يمكن من خلاله تقييم أولي لمدى ملائمة التدابير المتخذة من أجل ضمان سرية و أمن المعالجة.

ب) الركن المعنوي: يشترط المشرع لقيام جريمة خرق التدابير اللازمة لحماية المعطيات الشخصية توفر القصد الجنائي العام لدى الجاني، والذي مضمونه أن يعلم هذا الأخير أنه يقوم بمعالجة معطيات شخصية دون أن يكون قد اتخذ مسبقا التدابير التقنية والتنظيمية التي تحول دون تعرض هذه المعطيات للأضرار الناجمة عن مخاطر المعالجة، وتتجه إرادته لمباشرة عمليات المعالجة رغم ذلك.

وإذا كان المشرع الجزائري قد حسم موقفه بشأن اعتبار هذه الجريمة من الجرائم العمدية، إلا أن هناك نقاشا فقهيا حول إمكانية قبول ارتكابها لمجرد الخطأ المتمثل في صورة الإهمال وعدم التبصر أو عدم الحيطة، وهكذا فإنه حسب هذا الرأي الفقهي يقوم الركن المعنوي لجريمة عدم اتخاذ التدابير اللازمة لحماية المعطيات الشخصية أيضا عندما لا يتخذ المسؤول عن المعالجة الإجراءات اللازمة لحماية أمن المعطيات الشخصية نتيجة إهمال أو عدم احتياط أو تبصر.[3]

2-1) العقوبة المقررة قانونا: كغيرها من الجرائم التي نص عليها المشرع في القانون 07/18 تسلط الجهة القضائية على المحكوم عليه بهذه الجريمة العقوبات الأصلية والتكميلية التالية:

أ) العقوبة الأصلية: يعاقب على جريمة عدم اتخاذ التدابير اللازمة لحماية المعطيات الشخصية حسب المادة 65 من القانون 07/18 بالغرامة فقط من 200 ألف دج إلى 500 ألف دج، ولم يقرر المشرع الجزائري لهذه الجريمة عقوبة الحبس، وهذا خلافا للمشرع الفرنسي الذي كان متشددا في العقوبة التي قررها لهذه الجريمة حسب المادة 226-17 حيث يعاقب عليها بالحبس خمس سنوات و300 ألف يورو.

ب) العقوبة التكميلية: يمكن أن يتعرض مرتكب هذه الجريمة حسب نص المادة 71 من القانون 07/18 للعقوبات التكميلية المنصوص عليها في المادة 09، 09 مكرر من قانون العقوبات.

---

[1] Malabat Valérie, droit pénale spécial 4ème édition, dalloz, paris, 2009. P.334.

[2] المادة 43 من القانون 07/18 "... ما لم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من قبل مقد الخدمات..."

[3] آدم عبد البديع آدم حسين، مرجع سابق، ص 577.

2) جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية:

تنص المادة 60 من القانون 07/18 على أنه يعاقب بالحبس من سنتين إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي".

2-1) أركان الجريمة:

أ) الركن المادي: يقوم الركن المادي لمجرد تحقق السلوك الإجرامي المتضمن فعل السماح للغير بالولوج إلى معطيات شخصية هي محل معالجة آلية ، فانطلاقا من استعمال المشرع لمصطلح الولوج والذي يعبر عن عملية الدخول إلى أنظمة المعالجة الآلية للمعطيات التي تحتوي على هذه المعطيات الشخصية، يفهم أن المشرع قصد في هذه الجريمة المعالجة الآلية دون اليدوية، ويمكن تصور اتخاذ فعل السماح للغير بالولوج إلى المعطيات الشخصية من خلال أي سلوك يفهم منه أن المسؤول عن المعالجة علم بدخول الغير إلى النظم المعلوماتي ورضي به ولم يتخذ ما من شأنه إيقاف هذا الدخول والإعتراض عليه، أو أي سلوك آخر يتيح للغير هذا الولوج، كأن يترك المسؤول عن المعالجة نظام المعالجة الآلي للمعطيات الشخصية مفتوحا يسمح للغير بالإطلاع على هذه المعطيات الشخصية المخزنة به، أو يمكنه من كلمات المرور أو رمز فك الشيفرة، أو قد يكون بعدم اتخاذ التدابير التقنية التي تمنع الولوج، وهو السلوك المادي الذي قد يشترك مع السلوك المادي المكون لجريمة عدم اتخاذ التدابير اللازمة لحماية المعطيات الشخصية، وهو ما يسمى بالتعدد المعنوي أو الصوري للفعل المجرم وهو الفعل الواحد الذي يحتمل أكثر من وصف، أو قد يكون كذلك عن طريق كشف التدابير التقنية المتخذة مما يسمح للغير بالولوج.

والغير كما سبق بيانه هم الأشخاص غير المؤهلين للدخول إلى المعطيات وليس لهم الصفة في الإطلاع عليها، والمشرع الجزائري حسب المادة 03 من القانون 07/18 يعتبر من الغير كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر غير الشخص المعني أو المسؤول عن المعالجة، أو المعالج من الباطن، والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.

كما يعتبر من الغير أيضا الذين لم يرد تعيينهم أو ذكرهم ممن ترسل إليهم المعطيات الشخصية حسب التصريح الذي يقدمه المسؤول عن المعالجة إلى السلطة الوطنية لحماية المعطيات الشخصية، والذي يجب أن يتضمن حسب المادة 14 الفئات المرسل إليهم الذين قد تصل إليهم المعطيات.

ومن ثم فأي سلوك يتخذه المسؤول عن المعالجة يسمح من خلاله لأي شخص طبيعي كان أو معنوي عمومي أو خاص، ليس مؤهلا للاطلاع على المعطيات الشخصية عن طريق الولوج إليها، يعد جريمة بمفهوم المادة 60 من القانون 07/18.

ب) الركن المعنوي: تعتبر جريمة السماح للغير بالولوج إلى المعطيات الشخصية جريمة عمدية يتحقق الركن المعنوي فيها بتوفر القصد الجنائي، وذلك من خلال علم الجاني أن سلوكه يؤدي إلى السماح بالولوج إلى المعطيات الشخصية التي له سيطرة عليها من قبل أشخاص ليسوا مؤهلين بحكم القانون طلاع عليها، ورغم ذلك تنصرف إرادته إلى إتيان هذا السلوك، وبذلك لا تقوم الجريمة في حق المسؤول

عن المعالجة الذي سمح للغير بالولوج إلى المعطيات الشخصية بالخطأ، اعتقادا منه أن هذا الأخير مؤهل للإطلاع عليها.

2-2) العقوبة المقررة قانونا: إذا قامت الجريمة بركنيها المادي والمعنوي معا قامت المسؤولية الجزائية في حق الفاعل واستوجب العقوبة المقررة قانونا.

أ) العقوبة الأصلية: يعاقب على جريمة التسهيل للغير بالولوج إلى المعطيات الشخصية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200 ألف دج إلى 500 ألف دج.

ب) العقوبة التكميلية: مثل باقي الجرائم التي ترتكب في إطار القانون 07/18 فإنه يمكن أن تسلط على الشخص المدان علاوة على العقوبات الأصلية، واحدة أو أكثر من العقوبات التكميلية المحددة في قانون العقوبات.

3) جريمة عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية:

تنص المادة 61 من القانون 07/18 على أنه "يعاقب بالحبس من 06 أشهر إلى سنتين (2) وبغرامة من 60 ألف دج إلى 200 ألف دج أو بإحدى هاتين العقوبتين فقط كل من عرقل عمل السلطة

-بالإعتراض على إجراء عملية التحقق في عين المكان.

- برفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب، أو عدم تقديمها بشكل مباشر وواضح."

1-3) أركان الجريمة:

أ) الركن المادي: حددت المادة 61 أعلاه مجموعة من الأفعال يعد ارتكاب الجاني لأحدها سلوكا إجراميا لجريمة عرقلة عمل السلطة الوطنية، وتتمثل فيما يلي:

-عرقلة عمل السلطة عن طريق الإعتراض على إجرائها لعمليات التحقق (la vérification): وتنصرف الأفعال التي يمكن أن تشكل اعتراضا على إجراء السلطة الوطنية لعملية التحقق، إلى كل فعل يحول دون تمكن اللجنة من القيام بمهامها سواء بأفعال إيجابية أو عن طريق الإمتناع عن القيام بعمل معين، ومن ثم فقد يتحقق فعل الإعتراض برفض الإستجابة للإلتزام القانوني الذي يفرض توفير الظروف المناسبة لأعوان الرقابة الذين تلجأ إليهم السلطة الوطنية للقيام بمهامها، سواء كان ذلك بشكل صريح أم ضمني، ومن أمثلة ذلك اعتراض المسؤول عن المعالجة أو شخص آخر ممن لهم السيطرة على المعطيات الشخصية على أعوان اللجنة في الولوج إلى المعطيات عن طريق الإمتناع عن منحهم كلمة المرور للدخول إلى النظام المعلوماتي، أو منعهم من دخول المحلات والأماكن التي تتم فيها المعالجة.

ولقد منح المشرع السلطة الوطنية دورا رقابيا يمكنها من خلال الصلاحيات التي يتضمنها هذا الدور من مراقبة مدى تقيد القائمين على معالجة المعطيات الشخصية بضوابط المعالجة المحددة قانونا في كافة الأنشطة المرتبطة بهذه المعالجة، ولأجل ذلك فانه يمكن للسلطة الوطنية حسب المادة 49 من القانون 07/18 القيام بالتحريات المطلوبة ومعاينة المحلات التي تتم فيها المعالجة، أو الولوج إلى المعطيات المعالجة وجميع المعلومات أيا كانت دعامتها، بالإضافة إلى منحها سلطة الأمر باتخاذ مجموعة من التدابير أو الأمر بتوقيف ممارسة بعض الأنشطة والتي من بينها ما نصت عليه المادة 35 من القانون 07/18، أين يجيز المشرع فيها للسلطة الوطنية بناء على طلب التصحيح المودع لديها من المعني بالمعالجة بعد رفض طلبه من المسؤول عن المعالجة، أن تكلف أحد أعضائها للقيام بكل التحقيقات الضرورية والعمل على إجراء التصحيحات اللازمة.

ومن ثم يجرم المشرع السلوك الذي يتخذه أي شخص يمنع من خلاله السلطة الوطنية من ممارسة هذه الصلاحيات المرتبطة بمهام التحري والبحث وكل أعمال التثبت والتحقيق، سواء داخل الأنظمة المعلوماتية إذا كانت المعالجة آلية، أو في السجلات والملفات الورقية إذا كانت المعالجة يدوية.

- رفض تزويد أعضاء السلطة الوطنية بالمعلومات أو الوثائق الضرورية أو إخفائها: ويتضمن هذا السلوك عدم الإ ستجابة لطلب أعضاء السلطة أو الأعوان الموضوعين تحت تصرفها بتمكينهم من جميع الوثائق والمعلومات الضرورية واللاز مة لتنفيذ مهامهم المرتبطة بالتحقيق والمراقبة، وغالبا ما يتجسد هذا الرفض في عدم القيام بإرسال هذه الوثائق أو عدم تسليمها عند طلبها من السلطة الوطنية أو إتلافها وتمزيقها إذا تعلق الأمر بمعالجة يدوية، أو بعدم إرسال المعلومات إلكترونيا أو حذفها أو مسحها من النظام المعلوماتي إذا كانت معالجة آلية، وقد تكون المعلومات شفوية ومن ثم لا يتصور إزالتها أو حذفها بل عدم الإدلاء أو التصريح بها[1] ومن ثم فإن امتناع المسؤول عن المعالجة عن تسليم الوثائق والمعلومات التي تطلبها السلطة الوطنية وتكون ضرورية في التحقيق، أو يقوم بإخفائها أو إزالتها يعد فعلا مجرما.

- إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديم هذه المعلومات بشكل مباشر وواضح: ويمكن أن نتصور تجسد عرقلة أعوان السلطة الوطنية في هذه الحالة بعدة أشكال كإرسال وثائق ناقصة،أو تحتوي على أخطاء عمدية أو معلومات لا تتسم بالدقة والوضوح، وتنطوي على لبس وغموض، أو إرسالها بعد انتهاء الأجل الذي حددته السلطة لإرسالها، أو يكون بتقديم محتوى التسجيلات بطريقة لا يمكن الوصول إليه بطريقة مباشرة ويحتاج كلمة سر من أجل التمكن من فتحه.

ونجد المشرع المغربي يضيف في هذا الصدد ضمن المادة 63 من القانون 09/08 المتعلق بحماية المعطيات الشخصية سلوكا آخر يندرج ضمن الأفعال المكونة للركن المادي لجريمة عرقلة عمل السلطة الوطنية، وهو عدم تطبيق قرارات اللجنة الوطنية (السلطة الوطنية في التشريع الجزائري) التي تدخل في إطار صلاحياتها المتعلقة بضمان حقوق الأشخاص المعنيين، وهي حالة لم يتطرق اليها المشرع الجزائري في القانون 07/18 ولكن يمكن أن نتصورها من خلال امتناع المسؤول عن المعالجة من تنفيذ مثلا تلك

[1] Raymond Gassin, informatiques et libertés, Répertoire pénal et procédure pénale, Dalloz, Janvier 1987 n°288, P56.

القرارات الموجهة له كقرار الزامه بإجراء التصحيحات اللازمة التي رفض القيام بها بناء على طلب المعني بالمعالجة، أو تلك الصادرة عنها في إطار سلطات المراقبة، كقرار إجراء التغييرات اللازمة لضمان حفظ نزيه للمعطيات، أو قرار إغلاق المعطيات أو إتلافها أو القرار بمنع المعالجات لبعض المعطيات ذات الطابع الشخصي...

ب) الركن المعنوي: يتضح جليا من خلال نص المادة 61 من القانون 07/18 أن الركن المعنوي لجريمة عرقلة أعمال السلطة الوطنية لا يتحقق إلا عن طريق القصد الجنائي، إذ لا يمكن تصور ارتكاب تلك السلوكات عن طريق الإهمال أو عدم الحيطة.

وبذلك يقوم الركن المعنوي عندما يكون الجاني على علم بأن الأفعال التي يقوم بها من شأنها أن تعرقل السلطة الوطنية لحماية المعطيات الشخصية في ممارستها لمهامها في التحري والتحقيق والمراقبة، وتنصرف إرادته رغم ذلك للقيام بها، وهي العناصر المكونة للقصد الجنائي العام الذي تتطلبه هذه الجريمة دون القصد الجنائي الخاص، إذ لا يتوقف قيامها على نية الجاني ودوافعه في عدم التعاون مع السلطة الوطنية وعرقلة أعمالها.

2-3) العقوبة المقررة قانونا: بقيام الركنين المادي والمعنوي للجريمة قامت المسؤولية الجزائية للجاني، واستوجب تبعا لذلك تسليط العقوبة المقررة قانونا.

أ) العقوبة الأصلية: يعاقب الجاني على ارتكابه أفعالا تعرقل عمل السلطة الوطنية لحماية المعطيات بالحبس من 06 أشهر إلى سنتين (2) وغرامة من 60 ألف دج إلى 200 ألف دج، أو بإحدى هاتين العقوبتين.

ب) العقوبة التكميلية: وهي العقوبات المنصوص عليها في قانون العقوبات التي يمكن أن يخضع لها الشخص المدان بعد معاقبته بالعقوبات الأصلية.

4) جريمة الولوج إلى السجل الوطني:

تنص المادة 63 من القانون 07/18 على أنه يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100 ألف دج إلى 300 ألف دج أو بإحدى هاتين العقوبتين فقط كل من يلج دون أن يكون مؤهلا لذلك إلى السجل الوطني المنصوص عليه في المادة 28 من هذا القانون.

1-4) أركان الجريمة: تقوم هذه الجريمة بتحقق الركنين المادي والمعنوي:

أ) الركن المادي: يتحقق بتوفر العناصر التالية:

- السلوك الإجرامي: والمتمثل في الولوج إلى السجل الوطني، حيث أشارت المادة 28 من القانون 07/18 إلى إنشاء سجل وطني لحماية المعطيات ذات الطابع الشخصي، والذي يتم مسكه من طرف السلطة الوطنية لحماية المعطيات الشخصية وتسهر هذه الأخيرة على أن تقيد فيه:

- الملفات التي تحتوي على معطيات شخصية يكون المسؤول عن معالجتها من السلطات العمومية.

- الملفات التي تحتوي على معطيات شخصية يكون المسؤول عن معالجتها من الخواص.

- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة أحداث ملفات عمومية.

- التصاريح المقدمة للسلطة الوطنية والتراخيص الصادرة عنها.

- المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في هذا القانون.

والولوج هو نشاط إيجابي يعبر به عن عملية الدخول إلى نظام معلوماتي والإطلاع على محتوياته، ومن ثم فإن السجل الوطني هو عبارة عن سجل إلكتروني.

وتقوم الجريمة فقط لمجرد فعل الولوج إلى هذا السجل الإلكتروني من طرف الجاني، دون اشتراط تحقق نتيجة معينة بسببه.

- صفة الجاني: لم يحدد المشرع على وجه الخصوص أشخاصا بعينهم يمنع عليهم الولوج إلى السجل الوطني حيث جاء النص عاما على إطلاقه، واستنادا إلى المادة 28 التي تحدد مضمون ومحتوى هذا السجل فإنه يمكن اعتبار أن شخصا غير مؤهل للولوج إلى السجل الوطني هو كل شخص طبيعي أو معنوي عمومي أو خاص ليس مسؤولا عن معالجة المعطيات الشخصية، وليس معالجا من الباطن أو ليس مكلفا بالمعالجة.

ب) الركن المعنوي: تعتبر هذه الجريمة كغيرها من الجرائم التي نص عليها المشرع في هذا القانون من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوفر القصد الجنائي، حيث يعلم الجاني أن سلوكه يؤدي به إلى الولوج إلى السجل الوطني لحماية المعطيات الشخصية الممسوك من طرف السلطة الوطنية وهو غير مؤهل قانونا لذلك، وتنصرف إرادته رغم ذلك لإتيان هذا السلوك، وهذا دون الاعتداد بنيته والبواعث التي دفعته إلى هذا الفعل.

2-4) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: وهي حسب المادة 63 الحبس من سنة (1) إلى ثلاث (3) سنوات حبس وبغرامة من 100 ألف دج إلى 300 ألف دج أو بإحدى هاتين العقوبتين.

ب) العقوبة التكميلية: وهي إحدى العقوبات المنصوص عليها في المواد 09 و09 مكرر من قانون العقوبات التي يمكن أن يحكم بها على الشخص المدان بعد معاقبته بالعقوبات الأصلية.

المطلب الثاني: الجرائم الماسة بالمعطيات الشخصية خارج إطار قانون 18/07:

مع الإنتشار الواسع والمتزايد لتطبيقات نظم المعالجة الآلية والإعتماد عليها بشكل رئيسي في التعاملات الإلكترونية بشتى أنواعها، أدى إلى تعاظم المصالح المرتبطة بها وبالمعطيات التي تقوم بتخزينها أو نقلها أو معالجتها، إلا أن هذا الدور قد استغل في أغراض أخرى غير مشروعة، وأصبحت نظم المعالجة الآلية والمعطيات التي توجد بداخلها محلا للعديد من الإعتداءات مهما كانت طبيعة هذه المعطيات، بما في ذلك

المعطيات ذات الطابع الشخصي المخزنة بالكمبيوتر والمتبادلة عبر الشبكة العالمية بمحوها أو تعديلها أو تغيير نتائجها، وذلك عبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

إن المتفق عليه أن أحكام هذه الجرائم سواء في التشريعات المقارنة أو التشريع الوطني جاءت لتحمي أهم المصالح المتعلقة بالمعطيات ونظم معالجتها، إقرارا بعجز النصوص التقليدية على توفير الحماية لها.[1]

وهي في الأساس جرائم ترتبط بكل سلوك غير مشروع موجه للمساس بنظم المعالجة الآلية بالإعتداء على سرية مكوناتها غير المادية أو في وفرتها أو إتاحتها أو في سلامتها وتكاملها، ومن ثم كان النظام في حد ذاته أي المحتوي (le contenant) وما يحتويه من معطيات (le contenu) محلا لها. وما يهمنا في هذه الدراسة هي اعتداءات الحاصلة على ما يحتويه نظام المعالجة من معطيات*، وهي تشمل كل ما يمكن أن يحتوي عليه نظام المعالجة من معطيات.[2]

وبالنسبة لهذه المعطيات فهي في حد ذاتها تختلف من حيث طبيعتها ونوعيتها إلى معطيات تتعلق بالأسرار الداخلية للشركات والهيئات، الأسرار التجارية، المعطيات المالية، المعطيات التقنية والفنية المستخدمة في الإنتاج، المعطيات الأمنية والأسرار العسكرية، بالإضافة إلى المعطيات ذات الطابع الشخصي للأفراد[3] وهذه الأخيرة هي المعطيات محل دراستنا.

لذلك فقد جرم المشرع الولوج أو الدخول إلى النظام المعلوماتي وهو الفعل الذي يسمح للمتدخل بالإطلاع على المعطيات الشخصية المخزنة في هذا النظام والحصول على كل مايريده منها، وشدد العقوبة إذا أدى ذلك إلى تعديل أوإزالة المعطيات الشخصية التي يتضمنها، كما جرم فعل التلاعب بهذه المعطيات وذلك بالإدخال أو التعديل أو الإزالة المقصودة غير المصرح بها للمعطيات الشخصية داخل نظام المعالجة الآلية.

وفي الحقيقة أن الإلتفات إلى هذه الطائفة من الأفعال والإهتمام بها، بدأ في وقت سابق على الإهتمام بالجرائم الإقتصادية للحاسب الآلي لما تشكله هذه الأفعال من تهديد معلوماتي للخصوصية، خاصة إذا ما قارنا بين النظم اليدوية لتسجيل وحفظ واسترجاع المعطيات الشخصية وبين المعالجة الآلية لهذه المعطيات عبر الأنظمة المعلوماتية، والتي تتيح إمكانيات فائقة لتخزين ومعالجة واسترجاع ومقارنة كم هائل من المعطيات الشخصية وفي أقصر وقت ممكن، مع قدرتها على حفظ هذه البيانات لفترة زمنية طويلة، مما يجعل فرص الوصول إلى هذه المعطيات على نحو غير مأذون به أو بطريق التحايل أو الغش

[1] رشيدة بوبكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، مرجع سابق، ص 157.

* وقد عرف المشرع الجزائري بموجب الفقرة "ب" من المادة 02 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، نظام المعالجة الآلية بأنه "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

وكذلك عرفته الإتفاقية الدولية لإجرام تقنية المعلومات في مادتها الأولى بأنه "كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للمعطيات.."

وعرفت المذكرة التفسيرية لاتفاقية بودابست المعالجة الآلية للمعطيات أنها "مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي".

[2] نعيم مغبغب، حماية برامج الكومبيوتر، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية بيروت، 2009، ص 234.

[3] حسن طاهر داوود، جرائم نظم المعلومات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 27،28.

أكثر من ذي قبل[1]، فضلا عن ذلك فإن هناك قوانين خاصة تضمنت نصوصا تجريمية، الغاية منها توفير حماية جزائية للمعطيات الشخصية في مجال بعينه مثل قانون التصديق الإلكتروني والقانون المتعلق بالتجارة الإلكترونية.

الفرع الأول: جرائم الإعتداء على المعطيات الشخصية في قانون العقوبات:

سوف نحاول أن نستعرض صور التجريم المعلوماتي الواردة في قانون العقوبات والمتعلقة بأنظمة المعالجة الآلية للمعطيات، ومدى انطباق نصوصه على حماية المعطيات التي تدخل في إطار الحياة الشخصية للأفراد.

وبالقراءة المتأنية لنصوص المواد الواردة في القسم السابع مكرر للفصل الثالث من قانون العقوبات تحت عنوان بالمساس بأنظمة المعالجة الآلية للمعطيات، يمكن تصنيف الجرائم الماسة بالمعطيات الشخصية الواردة في قانون العقوبات إلى صورتين:

الصورة الأولى تتعلق بجرائم الإعتداء على معطيات شخصية صحيحة داخل نظام المعالجة الآلية.

الصورة الثانية تتعلق بجريمة التعامل مع معطيات شخصية متحصلة عن جرائم المساس بأنظمة المعالجة الآلية.

أولا: جرائم الإعتداء على معطيات شخصية صحيحة داخل نظام المعالجة الآلية:

إن النظم المعلوماتية أو نظم المعالجة الآلية للمعطيات تشتمل على ثلاث عناصر هي المكونات المادية لنظام المعلوماتية، والبرامج التي يحتويها، وكذا المعطيات المسجلة على هذا النظام، لذلك فإن الجرائم المعلوماتية تقع على أحد عناصر نظم المعلوماتية أو جميعها.

وفي هذه الطائفة من الجرائم تكون نظم المعلومات ذاتها هي محل ووعاء الفعل الإجرامي، فالتزايد المستمر عتماد على الحاسبات الآلية في تخزين المعلومات جعل منها مستودع أسرار الأشخاص، سواء تلك المتعلقة بأموالهم أو نشاطاتهم الإقتصادية أو بحياتهم الخاصة، وهذا ما أدى الى ظهور أنماط جديدة من عتداء على تلك المعلومات، مما أظهر الحاجة الى توفير حماية قانونية لها[2]، وما يهمنا في دراستنا هذه هي الجرائم الواقعة على المعطيات ذات الطابع الشخصي المخزنة داخل أنظمة المعالجة الآلية والتي تكون محل معالجة بواسطتها ضمن نظم المعلوماتية، ومن ثم تكون هذه المعطيات بالتأكيد هي المحور الذي تدور حوله هذه الفئة من الجرائم ومحلا لها، كالتي تتعرض لها برامج الحاسوب مثل الإتلاف والحذف والتشويه وغيرها.[3]

حيث أن الكثير من المؤسسات الكبرى والشركات والإدارات الحكومية تجمع عن الأشخاص معطيات شخصية عديدة ومفصلة تتعلق بالوضع المادي، الصحي، العائلي أو التعليمي وتستخدم أنظمة المعالجة

[1] نائلة عادل محمد فريد قورة، مرجع سابق، ص 235.

[2] نائلة عادل محمد فريد قورة، مرجع سابق، ص 16.

[3] عمار عباس الحسيني، جرائم الحاسوب والأنترنت، الجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، الطبعة الأولى، 2007 ص 94.

الآلية لخزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه المعطيات على وجه غير مأذون أو عن طريق التحايل أكثر من ذي قبل ويفتح مجالا أوسع للتلاعب بها أو لإساءة استخدامها وتوجيهها توجيها خاطئا يترتب عنه تعرية خصوصياتهم.[1]

1) جريمة إتلاف المعطيات الشخصية: لقد حسمت العديد من الدول الخلاف الدائر حول وجود تشريعات تتعلق بحماية المعطيات بصفة عامة، وذلك بإصدارها لتشريعات خاصة لمواجهة حالات الإعتداء عليها بفعل الإتلاف العمدي لها.[2] والمشرع الجزائري كان واحدا من بين هذه التشريعات، حيث اعتبر هذه الجريمة بأنها جريمة مستقلة بذاتها.

والمقصود بالإتلاف في هذا المقام، ذلك الفعل الذي يوجه إلى الجانب المعنوي في النظام المعلوماتي وهي المعطيات التي يحتويها هذا النظام[3]، سواء بمحوها أو تدميرها إلكترونيا أو تشويهها.[4]

وقد نص على هذا الفعل الجرمي الفقرة الثانية من المادة 394 مكرر من قانون العقوبات،وهو الفعل المتمثل في الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، ويترتب عنه حذف أو تغيير لمعطيات المنظومة، ويقابل هذا النص الفقرة الثانية من المادة 323-1 من قانون العقوبات الفرنسي[5].

1-1) أركان الجريمة: يستفاد من المادة 394 مكرر من قانون العقوبات أن هذه الجريمة تتحقق بتوفر كل من الركن المادي القائم على فعل الدخول أو البقاء عن طريق الغش إلى النظام المعلوماتي، والنتيجة المترتبة على ذلك والمتمثلة في إتلاف المعطيات الشخصية الموجودة داخل النظام المعلوماتي، ثم توفر الركن المعنوي القائم على القصد الجنائي.

أ) الركن المادي: يتحقق الركن المادي بتوفر عنصرين هما:

- السلوك الإجرامي: والمتمثل في الدخول غير المصرح به إلى النظام المعلوماتي أو الدخول عن طريق الغش.

- النتيجة الإجرامية: والمتمثلة في حذف أو تغيير المعطيات الشخصية التي يحتويها هذا النظام.

فبالنسبة للدخول غير المصرح به إلى النظام المعلوماتي: accés non autorisé (frauduleux) فإن معنى مصطلح الدخول l'accè في إطار المعلوماتية بصفة عامة ينصرف ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي[6] والإ حاطة والسيطرة على المعطيات والمعلومات التي توجد بداخله.[1]

---

[1] بولين أيوب، مرجع سابق، ص 386

[2] فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الثانية 2007، ص 209.

[3] محمود أحمد عبابنة، مرجع سابق، ص 100.

[4] محمد أمين الشوابكة، مرجع سابق، ص 229.

[5] L'article 323-1 du code pénal français : « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni… Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système … »

[6] خالد ممدوح إبراهيم، مرجع سابق، ص 242.

ويعد الدخول أو الولوج غير المصرح به إلى نظام المعالجة الآلية للمعطيات، أو كما وصفه المشرع الجزائري الدخول عن طريق الغش المرحلة الأولى والسابقة على ارتكاب الجرائم المعلوماتية الأخرى وضرورية لها، وهو فعل ينطوي على تهديد الأمن المعلوماتي، بمعنى السرية والسلامة وإتاحة النظم والبيانات المعلوماتية، بما فيها الإعتداء على الخصوصية المعلوماتية، إذ من هذا الدخول يمكن أن يترتب عليه بعد ذلك الوصول إلى المعطيات الشخصية المخزنة في النظام والإضرار بها أو استخدامها في غير الغرض الذي تتواجد لأجله في هذه النظم المعلوماتية.

ونظرا لكون التشريعات في هذا المجال لم تبين بشكل واضح المقصود بمصطلح الدخول، فإن الفقه راح يستعرض آراءه حينما عرف البعض أن الدخول في المجال المعلوماتي هو عملية ولوج غير شرعي إلى نظام التشغيل في الحاسب الآلي من قبل أشخاص لا يملكون حق الدخول بهدف القيام بأعمال غير قانونية[2]، أو أنه إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعطيات والمعلومات المخزنة بداخله للإطلاع عليها.[3]

ولا يقصد بفعل الدخول الذي يشكل الركن المادي في هذه الجريمة، الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول الإلكتروني، لذلك فإن الدخول غير المصرح به إلى النظام المعلوماتي يتحقق بالوصول إلى المعطيات والمعلومات المخزنة داخل هذا النظام دون رضاء المسؤول عنه،[4] لذلك فلا شك أن مجرد الدخول إلى نظام المعالجة الآلية لا يشكل سلوكا غير مشروع في حد ذاته، وإنما يستمد هذا الدخول عدم مشروعيته من كونه قد تم عن طريق الغش وبدون وجه حق، ومن ثم فإن عدم مشروعية الولوج يرتبط أساسا بمعرفة من له الحق أو السلطة في الدخول الى النظام المعلوماتي، أو في التصريح بالدخول إليه، فمناط عدم المشروعية هنا هو انعدام سلطة الفاعل في الدخول إلى هذا النظام المعلوماتي، وفي الغالب الأعم يكون الولوج غير مشروع في حالتين:

-إذا كان دخول الفاعل إلى النظام المعلوماتي قد تم دون الحصول على تصريح من المسؤول على هذا النظام المعلوماتي.

-إذا كان دخول الفاعل إلى النظام المعلوماتي في غير الحالات المرخص له فيها ذلك، أي أن يتجاوز التصريح الممنوح له بالدخول إلى معطيات لا يشملها التصريح بها[5]، ويكون كذلك في حالة ما إذا كان ضد إرادة المسؤول عن النظام المعلوماتي[6].

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص 158.

[2] نسرين علم الدين، دراسة الحل الأمثل لبناء نظام مركز توليد الشهادات الرقمية المستخدمة في أمن المعلومات، رسالة ماجستير غير منشورة، كلية المعلوماتية، جامعة دمشق، 2009، ص 19 مأخوذ عن رشيدة بوكر، جرائم الإعتداء على نظم المعلومات، مرجع سابق، ص 178.

[3] نائلة عادل محمد فريد قورة، مرجع سابق، 326.

[4] خالد ممدوح ابراهيم، مرجع سابق، ص 243.

[5] نائلة عادل محمد فريد قورة، مرجع نفسه، ص 333.

4 ALAIN BENSOUSSAN, Fraude informatique, article publier sur le site https://www.alain-bensoussan.com/avocats/acces-non-autorise-systeme-informatique-dispositif-de-securite/2008/12/01/

والمسؤول عن النظام المعلوماتي هو كل من له سلطة أو سيطرة على هذا النظام le maitre de système، وهو بمفهوم المادة الثانية من الإتفاقية الأوروبية لحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي صاحب الملف، والمقصود به المسؤول عن معالجة المعطيات داخل النظام المعلوماتي.

وتكمن أهمية تحديد الشخص المسؤول عن النظام في حصر نطاق الأشخاص الذين ينطبق عليهم وصف الدخول غير المصرح به إلى النظام، على اعتبار أن هذا الأخير هو وحده من يملك حق الدخول إلى النظام أو من يحصل على ترخيص منه لأجل الدخول، وما سواهما يعد دخولا غير مصرح به، ومن ثم غير مشروع.

وعليه فإن المعيار الذي على ضوئه يمكن تحديد أن الدخول قد تم بطريقة غير مشروعة هو انعدام حق الشخص في الدخول إلى هذا النظام، سواء كان ذلك بصفة كلية أو جزئية، فقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام أو إلى أجزاء أخرى يـ ،حظر عليه الدخول إليها، وهذا الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي،[1] لذلك فقد اعتبر أن فكرة الدخول غير المشروع من حيث دلالة المكان هي عملية التسلل داخل النظم المعلوماتية، أما من حيث دلالة الزمان فيتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية،[2] أو الدخول إلى النظام المعلوماتي بعد انتهاء هذه المدة القانونية.

أما عن الوسائل التي يمكن اللجوء إليها والإعتماد عليها في عملية الدخول غير المصرح به إلى نظام المعالجة الآلية، فإن المشرع الجزائري كشأن نظيره الفرنسي لم يحدد وسيلة معينة للدخول إلى النظام المعلوماتي، وبالتالي يجوز الدخول إليه بأي وسيلة كانت، حيث جاءت المادة 394 مكرر شاملة لكل طرق الدخول ولم تحدد طريقة بعينها، فحسب مدلول كلمة "الدخول" "accès" التي استعملها المشرع في هذه المادة تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة والسيطرة على المعطيات والمعلومات التي يتكون منها، فلم يحدد المشرع طريقة معينة، ومن ثم يمكن تصور استعمال كل الوسائل المتاحة للدخول إلى النظام[3]، ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الحاسوب وفتح البرامج، وقد يتطلب اختراق النظام المعلوماتي الحصول على شفرات خاصة، أو استخدام فيروس يتم دمجه في إحدى البرامج الأصلية للحاسب الآلي كي يعمل كجزء منه ثم يقوم بتسجيل الشفرات التي يستعملها المستخدمون الشرعيون للدخول إلى الحاسوب[4] ، أو باستخدام أجهزة أو برامج فك الشيفرة [5] أو عن

---

[1] نهلا عبد القادر المومني، مرجع سابق، ص 159.

[2] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2000، ص 52.

[3] رابحي عزيزة، مرجع سابق، ص 148.

تتنوع أشكال اختراقات النظم المعلوماتية إلى عدة أشكل منها:

-إختراق الأمن المادي ومن أبرز تلك الإختراقات : الإحتيال بمختلف التقنية ، الإحتيال بالإلتقاط السلكي والإحتيال باستراق الأمواج.

-إختراق الأمن الشخصي للأفراد ومن أبرز تلك الإختراقات الإحتيال بانتحال صلاحيات شخص مفوض والهندسة الإجتماعية، الإزعاج وقرصنة البرمجيات.

- إختراق الحماية الخاصة بالإتصالات وأمن البيانات، ومن أبرز تلك الإختراقات: الإعتداء على البيانات والإعتداء على البرمجيات، الإحتيال على بروتوكولات الأنترنت، والتقاط كلمات السر، أنظر أكثر خالد ممدوح إبراهيم، مرجع سابق، ص 248.

[4] نعيم مغبغب، حماية برامج الكومبيوتر – الأساليب والثغرات – منشورات الحلبي الحقوقية، 2006، بيروت، ص 235.

[5] خالد ممدوح إبراهيم، ص 246.

طريق وسائل أخرى تعتمد على ضعف النظام المعلوماتي ذاته أو على بعض الأخطاء الناجمة عن عملية البرمجة.[1] وفي الغالب تكون كل محاولات اختراق الأنظمة المعلوماتية تتم من خلال برامج متوفرة على الأنترنت، يمكن لكل من له خبرة تقنية أن يستخدمها لشن هجماته على أجهزة الغير، لهذا يلاحظ أن الإختراق لا يطال أجهزة الكمبيوتر إلا إذا كانت موصولة بشبكة الأنترنت التي توصل الحاسوب بقراصنة* الأنترنت الذين عادة ما يقوم المخترق منهم بإجراء مسح (Scan) بحثا عن الأبواب أو المنافذ أو الثغرات المفتوحة في نظام المعالجة الآلية[2]، وهي تقنية تعمل بواسطة برنامج مخصص على المسح الآلي لسلسة من عدد معين من بروتوكول الأنترنت (IP) بهدف إيجاد وفحص المنافذ والأبواب المفتوحة في كل حاسوب آلي، ومن ثم استغلال هذه الثغرات الأمنية للدخول إلى النظام المعلوماتي.[3]

وأما بالنسبة للنتيجة الإجرامية فإنها تتعلق بالأثر المترتب عن سلوك الدخول إلى النظام المعلوماتي، حيث لجأ المشرع الى تشديد العقوبة في حالة ما إذا ترتب على الدخول نتائج ضارة بصور مختلفة بالمعطيات ومنها المعطيات الشخصية وفقا للفقرة الثانية من المادة 394 مكرر بقولها: تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة..."

والصور التي أشار إليها المشرع انطلاقا من نص المادة 394مكرر هي حذف المعطيات أو محوها، والذي يعني إتلافها أو تدميرها بصورة كلية أو جزئية، كما يشير هذا الفعل أيضا إلى إزالة المعطيات الموجودة داخل نظام المعالجة، وهو أقصى أنواع الضرر.

أما التغيير فيشير إلى كل العمليات التي تؤدي الى تحويل الملامح الأصلية للمعطيات وإحداث تعديلات عليها دون إزالتها، بحيث تظل المعطيات موجودة ولكن بدون معنى ولا فائدة بعد أن تم تشويهها والتلاعب فيها بصورة تؤثر في قيمتها، ويصبح غير ممكن استغلالها ومعالجتها وتحقيق الغرض الذي جمعت لأجله حتى يتحقق معنى الإتلاف عليها[4]، لأنها سوف تعطي معلومات غير صحيحة عن الشخص، فالحاسب الآلي ليست لديه ملكة التمييز بين المعطيات الحقيقية وغيرها، لأنه مجرد آلة.[5]

---

[1] نائلة عادل محمد فريد قورة، مرجع سابق، ص 316.

*القراصنة هم المخترقون ويمكن تصنيفهم إلى صنفين:

- الهاكرز (hackers) يملكون وسائل تقنية ومتخصصين في علم الشبكات ويتمتعون بالذكاء، والقرصنة بالنسبة لهم هي حياة ثانية، هدفهم مهاجمة مواقع الشركات والمؤسسات الكبيرة والمؤسسات الحكومية، ومواقع القواعد العسكرية، وهم ليسوا دائما سيئي النية، فهم يريدون بكل بساطة أخذ الخبرة بزيارة الأماكن الممنوعة على الشبكة، وأحيانا لا يقومون سوى بالإطلاع على المعطيات، وفي غالب الأحيان يترك الهاكر وراءه أثرا لاختراقه.

- الكراكرز(crackers) وهم مثل الهاكرز يتمتعون بالخبرة لكنهم يوصفون بأنهم حمقى ومخربين وتفكيرهم يتجه نحو التخريب وشن الهجمات والتزوير والتقليد، وهم يشكلون تهديدا أكبر للأنظمة المعلوماتية من الهاكرز لأنهم غير معروفين، وغالبا ما لا يكون هدفهم سرقة المعطيات أو تعديلها فقط بل تدميرها.

[2] خالد ممدوح إبراهيم، ص 246.

[3] رشيدة بوبكر، جرائم الإعتداء على نظام المعالجة الآلية، مرجع سابق، ص 188.

[4] فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص 211.

[5] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن الحاسب الآلي، مكتبة دار النهضة العربية، القاهرة ص 36.

ب) الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية التي يتخذ الركن المعنوي فيها صورة القصد الجنائي، والذي يتحقق بانصراف علم الجاني إلى كافة العناصر الداخلة في تشكيل الجريمة، ومن قبيل ذلك ضرورة علم الجاني أن فعله ينصب على الدخول إلى نظام المعالجة، وأنه ليس له الحق في الدخول إليه، فضلا عن ذلك فإن القصد الجنائي يتطلب أيضا أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على هذا الفعل، ذلك أن توقع النتيجة هو الأساس النفسي الذي تقوم عليه إرادة الفاعل، و النتيجة التي يجب أن يتجه إليها توقع الفاعل هي التي يحددها القانون،[1] وهي الآثار الضارة التي تلحق بالمعطيات الشخصية من محو و تعديل وتحريف.

وقد عبر المشرع في المادة 394 مكرر عن القصد العام المتطلب في هذه الجريمة باشتراطه أن يكون الدخول إلى النظام بطريق الغش، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله إلى النظام الآلي غير مصرح به وغير مشروع.[2]

وإضافة إلى وجوب توافر العلم بكافة العناصر المكونة للركن المادي للجريمة، ينبغي أن تنصرف إرادة الجاني إلى القيام بهذا الفعل رغم ذلك، ويمكن تصور ذلك بعزم الجاني على ارتكاب الجريمة وتنفيذها وإحداث النتيجة الجرمية وقبولها، كأن يقوم الجاني بالدخول إلى النظام نتيجة اختراقه لبرامج الحماية التقنية أو عن طريق استعمال الرقم السري أو فك الشيفرة، ثم يلحق ضررا بالمعطيات الشخصية الموجودة داخل هذا النظام، أما إذا كان الجاني قد سبق له وأن كان واحدا من بين المشتركين وانتهت مدة الاشتراك ودخل إلى النظام المعلوماتي اعتقادا منه بالخطأ أنه مازال له الحق في الدخول، فإن ذلك يعد جهلا بالواقع ينتفي معه القصد الجنائي.

وقد يدخل الجاني إلى النظام المعلوماتي بالخطأ ولكنه يبقي داخل النظام المعلوماتي ويطلع على المعطيات الشخصية التي بداخله، رغم إدراكه في لحظة ما أنه ليس له الحق في ذلك، فإن عنصر القصد الجنائي يصبح متوفرا ويسأل على فعله بالإعتداء على المعطيات الشخصية إذا ترتبت النتيجة.

غير أن ما يمكن أن نفهمه من نص المادة 394 مكرر أن المشرع الجزائري اعتبر النتيجة المتمثلة في الأضرار اللاحقة بالمعطيات الشخصية من حذف أو تغيير والمترتبة عن الدخول العمدي غير المرخص به إلى النظام المعلوماتي في هذه الجريمة بمفهوم المادة 394 مكرر من قانون العقوبات غير مقصودة، فالمقصود هو الدخول إلى النظام، أما النتيجة فهي عرضية وهذا ما يفهم من صريح نص المادة 394 مكرر/2 "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة " حيث تكون النتيجة في هذه الحالة ظرفا مشددا، تضاعف بتحققها العقوبة.

أما إذا قصد الجاني من وراء دخوله إلى النظام بداءة الإضرار بالمعطيات الشخصية، فلا تكون النتيجة في هذه الحالة ظرفا مشددا، و إنما تعد عنصرا مكونا لجريمة أخرى تدخل في دائرة التجريم الذي نصت عليه المادة 394 مكرر1.[1]

[1] نائلة محمد فريد قورة، مرجع سابق، ص 366.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 264.

2-1) العقوبة المقررة قانونا: بقيام أركان الجريمة تقوم المسؤولية الجزائية واستوجب الأمر توقيع العقوبة المقررة قانونا.

أ) العقوبات الأصلية: نصت الفقرة الثانية من المادة 394 مكرر من قانون العقوبات أنه "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"، وبالرجوع للفقرة الأولى التي حددت العقوبة على فعل الدخول إلى نظام المعالجة الآلية في حالته البسيطة المجردة من النتيجة، فهي تعاقب بالحبس من (3) أشهر إلى سنة وبالغرامة من 50 ألف دج إلى 200 ألف دج، ومن ثم تكون العقوبة المقررة لجريمة الدخول إلى نظام المعالجة المؤدي إلى محو أو تعديل المعطيات الشخصية (جريمة إتلاف المعطيات الشخصية) بمضاعفة الحدين الأدنى والأقصى للعقوبتين السالبة للحرية والغرامة، وهي بالنتيجة لذلك، الحبس 06 أشهر إلى سنتين وغرامة من 100 ألف دج إلى 400 ألف دج.

وقد اعتبر المشرع الفرنسي أن العقوبة تشدد إذا انصب فعل الحذف أو التغيير على المعطيات ذات الطابع الشخصي المتواجدة في أنظمة المعالجة الآلية للمعطيات التي تنفذها الدولة[2].

ب) العقوبات التكميلية: تتمثل في العقوبات التكميلية الإختيارية المنصوص عليها في المادة 09 من قانون العقوبات، بالإضافة إلى العقوبات التكميلية الوجوبية التي نصت عليها المادة 394 مكرر6، وهي المصادرة والغلق، وتشترك فيها جميع الجرائم المتعلقة بالإعتداء على نظم المعالجة الآلية للمعطيات، فبالنسبة للمصادرة فإنه وبعد إدانة الجاني بالعقوبات الأصلية يخضع هذا الأخير لعقوبة تكميلية تقضي بمصادرة الأشياء التي استخدمت في ارتكاب الجريمة، ويتعلق الأمر بالأجهزة والبرامج والوسائل المستخدمة، وهي عقوبة تكميلية وجوبية انطلاقا من نص المادة 15 مكرر1 من قانون العقوبات، و التي تقضي بأنه في حالة الإدانة لارتكاب جنحة أو مخالفة يؤمر بمصادرة الأشياء التي استعملت في الجريمة أو التي تحصلت منها وجوبا إذا كان القانون ينص صراحة على هذه العقوبة، وقد نصت المادة 394 مكرر 6 من قانون العقوبات على المصادرة صراحة عندما قضت بأنه "يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة..."

أما بالنسبة للغلق وهي أيضا عقوبة تكميلية وجوبية تتعلق بمحلين، الأول هو المواقع الإلكترونية التي تستعمل في الجريمة، والثاني هو المكان الذي كان يستغله الجاني في ارتكاب الجريمة، والذي قد يحتوي على الوسائل الإلكترونية التي استعملت في تنفيذ الجريمة، و أما بالنسبة لمدة الغلق فنرجع في تحديدها إلى القواعد العامة، حيث نصت المادة 16 مكرر1 من قانون العقوبات على أن عقوبة الغلق قد تكون بصفة نهائية أو لمدة لا تزيد عن خمس (5) سنوات في حالة الإدانة بجنحة، كما هو الحال بالنسبة لجميع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي تعد جميعها جنحا.

---

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية،2007، ص170.

[2] « Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'etat, la peine est portée à cinq ans d'emprisonnement et à 150,000 € d'amende »

2) جريمة التلاعب بالمعطيات الشخصية:

تنص المادة 394 مكرر 1 من قانون العقوبات على أنه "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500 ألف دج إلى 02 مليون دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، وهذا النص يقابل نص المادة 323-3من قانون العقوبات الفرنسي.[1]

إن صلاحية هذا النص القانوني لتوفير الحماية الجزائية للمعطيات الشخصية واستعاب مثل هذا النوع من المعطيات، هو إطاره العام الذي لم يميز بين نوعية المعطيات التي تضمنها، حيث جاء شاملا لكافة أنواع المعطيات بما فيها ذات الطابع الشخصي.

ويلاحظ أن هذه الجريمة لا يشترط لقيامها أن يكون التلاعب بالمعطيات الشخصية قد تم بعد الدخول غير المشروع إلى نظام المعالجة الآلية، بل تتحقق عندما يقوم الجاني بفعل التلاعب بالمعطيات المختزنة داخل النظام المعلوماتي، ولا يهم بعد ذلك إن كان الدخول إلى النظام مشروعا أم غير مشروع، بل إن كثيرا من عمليات التلاعب بالمعطيات يكون من الأشخاص المرخص لهم بدخول النظام المعلوماتي،[2] ويرجع سبب اعتبار المشرع هذه الجريمة مستقلة وغير مرتبطة بجريمة الدخول أو البقاء غير المرخص بهما في نظام المعالجة، وتمثل هذه الافعال الطريق الأول والعادي للوصول إلى المعطيات المتضمنة في النظام المعلوماتي ، ثم القيام بعدها بأفعال التلاعب من محو أو تعديل أو إدخال، بالإضافة إلى وجود طرق وأساليب تقنية أخرى تمكن من اقتراف هذه الأفعال عن بعد ولا حاجة إلى الدخول إلى نظام المعالجة*.

ويبدو واضحا أن المشرع في هذه الجريمة لا يحمي نظام المعالجة الآلية من الناحية المادية أو البرامج أو التطبيقات، وإنما يوفر الحماية للمعطيات الموجودة داخل هذا النظام ذاته ضد أي نشاط إجرامي يتمثل في أفعال الإدخال، الإزالة والتعديل، ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يقوم النشاط الإجرامي فيها، لكن القاسم المشترك بين هذه الأفعال جميعا هو انطواؤها على تلاعب بالمعطيات الشخصية التي يتضمنها نظام المعالجة الآلية، إما بإدخال معطيات جديدة وهمية وغير صحيحة، أو تعديل أخرى قائمة.[3]

[1] Article 323-3 du code pénal français : « le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qui'l contient est puni de cinq ans d'emprisonnement et de 150000 € d'amende »

[2] محمد خليفة، مرجع سابق، ص،178.

*يوجد العديد من الأساليب التقنية التي يمكن من خلالها التلاعب بالمعطيات المخزنة في النظام المعلوماتي وتأخذ عدة صور: التلاعب في البرامج التشغيلية عن طريق ما يسمى بالمصيدة، وتعني الولوج إلى البرنامج عن طريق المداخل المميزة والتي يستبعدها المبرمج بمجرد الإنتهاء من التصحيح النهائي للبرنامج، إصطناع برنامج وهمي ويكون القصد منه التخطيط لمراقبة وتنفيذ ارتكاب الغش المعلوماتي أو التلاعب في البرامج التطبيقية، وهذه ترتكب بأساليب متعددة أهمها زرع الفيروسات والقنابل المنطقية. أنظر في ذلك: بولين أيوب، مرجع سابق، ص 142،143.

[3] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر في القانون العربي النموذجي، مرجع سابق، ص 377.

1-2) أركان الجريمة: كغيرها من الجرائم تقوم هذه الجريمة بتحقق الركنين المادي والمعنوي:

أ) الركن المادي: من خلال نص المادة 394 مكرر1 من قانون العقوبات يتضح جليا أن الركن المادي لجريمة التلاعب بالمعطيات الشخصية الموجودة بنظام المعالجة الآلية يتحقق بالسلوك الإجرامي المتمثل في إدخال معطيات شخصية بطريق الغش في نظام المعالجة الآلية، أو إزالة أو تعديل هذه المعطيات بطريق الغش.

- محل الجريمة وهي المعطيات الشخصية التي يتضمنها النظام المعلوماتي.

- النتيجة الإجرامية، وهي تغيير في الحالة والملامح الأصلية التي تكون عليها المعطيات الشخصية المخزنة في بيئة النظام المعلوماتي.

-السلوك الإجرامي: إن الفكرة الأساسية لهذه الجريمة هي وجود معطيات ذات طابع شخصي مدخلة في ذاكرة النظام المعلوماتي بغرض معالجتها، ثم يتم التدخل فيها بطريقة غير مشروعة إما بإدخال معطيات شخصية أخرى في النظام المعلوماتي لم تكن موجودة أصلا وذلك بقصد التشويش على هذه المعطيات الموجودة سابقا مما قد يؤثر على صحتها[1]، أو كل فعل قد يؤدي إلى إزالة المعطيات الشخصية بصورة غير مشروعة، أو يؤدي كذلك إلى تعديل وتغيير مضمونها إما بالإضافة أو الشطب[2] ويؤثر بالنتيجة على سلامتها[3].

وعلى هذا الأساس فإن السلوك الإجرامي لهذه الجر يمة يقوم عند ارتكاب الجاني لفعل أو أكثر من الأفعال التي عددتها وذكرتها المادة 394 مكرر1.

- إدخال معطيات شخصية للنظام المعلوماتي عن طريق الغش: إن الأنظمة الآلية التي يتم من خلالها معالجة المعطيات الشخصية تعمل وفق أسلوب معالجة ينطلق من تغذية هذا النظام بالمعطيات عن طريق إدخالها وتجميعها وتخزينها داخل هذا النظام، ثم القيام بعد ذلك بمعالجتها بعمليات معينة يتم من خلالها استخراج النتائج المترتبة على هذه المعالجة بشكل آلي، لذلك فإن الجاني لا شك أنه يستطيع أن يغذي هذا النظام بمعطيات خاطئة ووهمية منذ البداية، وهو ما يطلق عليه التلاعب في المعطيات في مرحلة إدخال البيانات.[4]

[1] هدى حامد قشقوش، مرجع سابق، ص 569.

[2] بولين أيوب، مرجع سابق، ص 430.

[3] نصت على هذه الجريمة الإتفاقية الأوروبية رقم 185 المتعلقة بالجريمة الإلكترونية الموقعة في بودابست بتاريخ 2001/11/23 في المادة الرابعة منها تحت عنوان الإعتداء على سلامة المعطيات Atteinte à l'intégrité des données حيث جاء نصها كما يلي:

المادة 04: التدخل في المعطيات:

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني إذا ما ارتكبت عمدا: إتلاف معطيات حاسوبية، حذفها، إفسادها، تعديلها، أو تدميرها..."

[4] نائلة عادل محمد فريد قورة، مرجع سابق، ص 435.

وعملية الإدخال تتمثل في تغذية النظام المعلوماتي بالمعطيات المراد معالجتها آليا[1]، والمقصود بفعل الإدخال الذي يشكل السلوك الإجرامي في هذه الجريمةهو كل فعل يفضي إلى إدخال معطيات شخصية إلى نظام المعالجة الآلية بصورة غير مشروعة، كأن يتم إدخال معطيات محرفة ومغلوطة ومزيفة إلى نظام المعالجة الآلية لم تكن موجودة من قبل، الأمر الذي يؤثر على المعطيات الموجودة ابتداء في النظام ويحد من قيمتها[2]، ذلك أن جهاز الحاسب الآلي يقوم بتخزين أي معطيات تقدم إليه دون أن يكون بمقدوره أن يصنف الصحيحة من الخاطئة منها، فإذا ما أدرجت فيه معطيات شخصية خاطئة فإنه يعالجها ويخرج تبعا لذلك معلومات خاطئة، فلا شيء يمكن أن يوقظ حفيظة الكومبيوتر للتصحيح، حيث تتم جميع العمليات بالإستناد إلى ذلك بصورة خاطئة ومغلوطة[3].

وتعد الحالات التي تنطوي على التلاعب في المعطيات عند مرحلة الإدخال من أكثر الحالات شيوعا نظرا لما تتميز به من سهولة، حيث يكون من السهل تغذية النظام المعلوماتي بمعطيات غير معبرة عن الحقيقة فيكون من شأنها التشويش على صحة المعطيات القائمة، وقد تتم عملية إدخال المعطيات في النظام عن طريق خرق المنافذ والوصول إلى قائمة البيانات وإضافة المعطيات المغلوطة بهدف الإستفادة غير المشروعة.

- تعديل المعطيات الشخصية الموجودة داخل النظام المعلوماتي بطريق الغش، ويشير مباشرة مصطلح التعديل إلى تغيير المعطيات داخل نظام المعالجة الآلية واستبدالها بمعطيات أخرى، وكل فعل من شأنه أن يغير من حقيقة المعطيات الشخصية الأصلية التي هي مخزنة بنظام المعالجة وجمعت لغرض معين، وهذا ما يجعلها غير قابلة للإستعمال على النحو الذي جمعت لأجله، وتطرح عملية التعديل عدة أخطار أهمها الإستعمال غير المشروع للمعطيات، أي استعمالها في غير الوجه الذي جمعت لأجله تلك المعطيات، وهذا الإنحراف من شأنه أن يعرض الحياة الشخصية للخطر، لأن الهدف الثاني الذي حر ّفت وغيرت لأجله المعطيات الشخصية سوف يكون دون علم الشخص المعني، بل وقد يـ ُستعمل ضده.[4]

-إزالة المعطيات الشخصية و هو فعل المحو الذي يقصد به إزالة جزء من المعطيات المسجلة داخل نظام المعالجة الآلية، كما يقصد بالإزالة في مجال المعلوماتية أيضا اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، لذلك يتجه جانب من الفقه الجنائي إلى اعتبار أن محو المعطيات المعالجة قد يتم عن طريق التلاعب في الشرائط الممغنطة[5]، وقد تتحقق هذه الصورة من خلال زرع فيروس virus في النظام المعلوماتي بهدف التلاعب في البيانات الشخصية المخزنة في هذا النظام، وذلك عن طريق محو تلك البيانات الشخصية وإزالتها واستبدالها ببيانات أخرى مكانها، وقد يكون ذلك لتحقيق هدف معين كنسبة وقائع معينة

[1] نائلة عادل محمد فريد قورة، نفس المرجع ص 437.

[2] رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة، مرجع سابق، ص 252.

[3] جميل عبد الباقي الصغير، مرجع سابق، ص 33.

[4] بولين أيوب، مرجع سابق، ص 137.

[5] عبد الفتاح بيومي حجازي، جرائم الكومبيوتر في القانون العربي النموذجي، مرجع سابق، ص 384.

لأشخاص خلافا للواقع الحقيقي، الأمر الذي من شأنه تشويه سمعتهم من ناحية مركزهم المالي أو المهني أو حالتهم الصحية.[1]

كما نشير أيضا أن الأفعال السابقة سواء كانت الإدخال، الإزالة أو التعديل قد وردت على سبيل الحصر، ومن ثم لا يقع تحت طائلة التجريم أي فعل آخر غيرها، حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية، ومن ثمة فلا يخضع للتجريم وفق هذا النص القانوني فعل نسخ المعطيات الشخصية أو نقلها أو التنسيق أو التقريب فيما بينها، لأن كل هذه الأفعال لا تنطوي على إدخال أو محو أو تعديل بمفهوم المادة 394 مكرر 1 من قانون العقوبات.*

إضافة إلى إتيان الجاني لسلوك الإدخال أو الإزالة أو التعديل على المعطيات الشخصية المتواجدة بالنظام المعلوماتي، فإنه يشترط أن تكون هذه الأفعال قد تمت عن طريق الغش، أي دون رضا أو علم من يملك النظام المعلوماتي ويسيطر عليه، فالجريمة لا تتحقق إذا كانت هذه الأفعال قد تمت بعلم وبترخيص من طرف القائمين على النظام.

العنصر الثاني: وهو محل النشاط الإجرامي ويتعلق بالمعطيات الشخصية التي يتضمنها نظام المعالجة الآلية، حيث أن السلوك الإجرامي المتمثل في الأفعال السابقة ينطوي على التلاعب بالمعطيات التي يحتويها النظام، ومن بين أهم المعطيات التي تحتويها الأنظمة المعلوماتية الآلية، هي تلك المعطيات المرتبطة بالحياة الخاصة للأفراد، مثل تلك المتعلقة بحالتهم الصحية والمالية والمهنية والعائلية وكذا التي تتعلق بالأصل العرقي والمعتقدات الدينية و الإنتماء السياسي والنقابي، وكل المعطيات التي من شأنها أن تعرف بالشخص أو تجعله قابلا للتعرف عليه، فهي معطيات شخصية ذات طابع سري.

حيث تجمع أنظمة المعالجة الآلية العامة والخاصة عددا ضخما من المعطيات الشخصية، ويكون لأي شخص لديه قدر من المعرفة الفنية بأنظمة الكمبيوتر أن يقوم بالإعتداء على هذه المعطيات التي تمثل الحياة الشخصية لأصحابها.

والواضح من نص المادة 394 مكرر1 حينما أكدت على أن الاعتداء يكون على المعطيات التي يتضمنها النظام فإنها حتما تشترط لقيام الجريمة أن يقتصر وقوع النشاط الجرمي فقط على المعطيات المخزنة داخل النظام المعلوماتي والتي تشكل جزءا منه.[2]

---

[1] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992، ص 191.

* ومن الأمثلة التي تقدم في هذا الإطار قضية شركة TRW company credit data التي كانت تعمل على تزويد عملائها من بنوك، شركات ومتاجر من خلال أنظمتها المعلوماتية بمعطيات تتعلق بالمركز الإئتماني لأفراد الجمهور نظير اشتراك يدفعه هؤلاء العملاء، وكانت الشركة تحوز على معطيات تتعلق بحوالي 50 مليون شخص، وقد استغل أحد الموظفين في هذه الشركة بقسم علاقات المستهلكين هذا النشاط، وقام ببيع مراكز ائتمانية جديدة قام باختلاقها لذوي المراكز الإئتمانية الرديئة واستبدلها بمعطيات تحسن مركز الأشخاص المتعاملين معه، وتفيد بتمتع صاحبها بمركز ائتماني جيد، وذلك في مقابل مبالغ مالية يتم الإتفاق عليها، وقد قدر عدد السجلات التي تم التلاعب بها حوالي 100 سجل، وبناء على البيانات الإئتمانية التي تم إدخالها بالمحو أو التعديل أو بهما معا إلى نظام المعلومات الآلي للشركة قام عديد من عملائها بالدخول في معاملات مالية وتجارية مع أشخاص ذوي سمعة ائتمانية سيئة. أنظر عبد الفتاح بيومي حجازي، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 49 وكذلك نائلة عادل محمد فريد قورة، مرجع سابق، ص 236.

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة، مرجع سابق، ص 262.

وترتيبا على ذلك فانه يشترط لتجريم هذه الأفعال أن تكون المعطيات الشخصية محل الجريمة موجودة داخل النظام المعلوماتي[1] ، فالحماية الجزائية في مواجهة هذه الجريمة تكون مستمرة وقائمة طالما أن المعطيات المعالجة موجودة داخل النظام المعلوماتي أو في طريقها إلى المعالجة، أو المعطيات المعالجة والتي انفصلت عن النظام ثم أعيد إدخالها فيه، أما المعطيات غير المعالجة التي لم تدخل إلى النظام المعلوماتي، أو أدخلت ولم تبدأ مراحل معالجتها بعد، أو التي عولجت وانفصلت عن النظام، فهي خارج نطاق الحماية المشمولة بنص المادة 394 مكرر1 من قانون العقوبات، وإن كان يجوز حمايتها وفقا لنصوص جزائية أخرى.[2]

وتبقى الإشارة إلى مسألة الإعتداء على المعطيات الشخصية أثناء مرحلة نقلها عبر أنظمة المعالجة الآلية، حيث أن المادة 394 مكرر1 وكذلك المادة 323-3 من قانون العقوبات الفرنسي أشارتا فقط إلى أفعال التلاعب الذي يحصل على المعطيات التي يتضمنها النظام المعلوماتي، لكن ما هو الشأن بالنسبة للمعطيات الشخصية التي يتم تراسلها ونقلها والتي يمكن أن تطالها هذه الأفعال من خلال اعتراض عملية نقل المعطيات وإجراء تعديل أو محو عليها.

نرى أنه إذا أخذنا بالتعاريف القانونية لكل من النظام المعلوماتي والمعالجة الآلية للمعطيات معا، حيث الأول هو كل نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وأما المعالجة الآلية للمعطيات فهي العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات .... أو تغييرها أو مسحها أو استخراجها أو نشرها، فإننا ندرك بأن المشرع قد أخذ بالمفهوم الواسع لنظام المعالجة الآلية، ومن ثم تصبح المعطيات المنقولة عبره عرضة لأفعال التلاعب شأنها في ذلك شأن المعطيات المخزنة به[3].

العنصر الثالث ويتعلق الأمر بالنتيجة الإجرامية، وهي تغيير حالة المعطيات الشخصية من خلال الأفعال المكونة للنشاط الإجرامي، ومن ثم تحقق الضرر الفعلي الذي يهدد سلامتها، وذلك بإفنائها وتدميرها عن طريق فعل المحو، أو تشويهها عن طريق فعل الإزالة.

غير أن الفارق بين النتيجة المنصوص عليها في المادة 394 مكرر وهذه النتيجة المنصوص عليها في المادة 394 مكرر1يكمن في أن هذه الأخيرة تقع مقصودة، أي يريدها الفاعل وتتجه إرادته بداءة لإحداثها من خلال السلوك الإجرامي، أما في الجريمة المنصوص عليها في المادة 394 مكرر، فان النتيجة قد تترتب عن السلوك الإجرامي من دون أن يكون للجاني قصد لإحداثها.

ب) الركن المعنوي: إن هذه الجريمة من الجرائم العمدية، وبالتالي لابد من توفر النية الإجرامية المتمثلة في القصد الجنائي العام، الذي يتطلب أن يعلم الجاني أنه يقوم بإحدى الأفعال التي تشكل تلاعبا بالمعطيات الشخصية المنصوص عليها قانونا، أي أنه يقوم بإدخال معطيات وهمية وغير صحيحة في

[1] بولين أيوب، مرجع سابق، ص 431.

[2] بيومي حجازي، جرائم الكمبيوتر في القانون العربي النموذجي، مرجع سابق، ص 377.

[3] أنظر في هذا المعنى رشيدة بوبكر، جرائم الاعتداء على نظم المعالجة الآلية، مرجع سابق ص 267.

النظام المعلوماتي أو يعدل معطيات شخصية قائمة داخل النظام المعلوماتي دون أن يكون مصرحا له القيام بذلك وغير مسموح به، ورغم ذلك تتجه إرادته إلى ارتكاب هذه الأفعال قاصدا تحقيق نتيجة الإضرار بهذه المعطيات وتغيير حقيقتها.

أما عن القصد الخاص فهو غير مطلوب لتحقق الركن المعنوي، إذ لا يوجد في صياغة نص المادة ما يستفاد منه اشتراط المشرع لنية خاصة لدى الجاني، كنيته إلحاق ضرر بصاحب المعطيات أو سعيه لتحقيق غاية ربحية، بل اكتفى المشرع لقيام الجريمة بالقصد الجنائي العام بعنصريه العلم والإرادة على النحو السابق بيانه.

2-2) العقوبة المقررة قانونا:

أ) العقوبة الأصلية: يعاقب المشرع على جريمة التلاعب بالمعطيات الشخصية حسب نص المادة 394 مكرر1 من قانون العقوبات بالحبس من 06 أشهر إلى ثلاث سنوات وغرامة من 500 ألف إلى 2 مليون دج، وهي عقوبة غير مشددة بالمقارنة مع العقوبة التي أقرها المشرع الفرنسي على نفس الجريمة في المادة 323-3 من قانون العقوبات الفرنسي، حيث تصل عقوبة الحبس إلى 05 سنوات، ويشددها أكثر عندما تكون أفعال التلاعب من إدخال أو محو أو تعديل ترتكب ضد المعطيات ذات الطابع الشخصي والموجودة داخل أنظمة المعالجة الآلية التي تنفذها الدولة لتصل العقوبة إلى 07 سنوات.

ب) العقوبة التكميلية: علاوة على العقوبات الأصلية، فإن الجاني في هذه الجريمة يخضع لعقوبات تكميلية وجوبية وأخرى اختيارية.

فأما العقوبات التكميلية الإلزامية فهي التي نصت عليها المادة 394 مكرر6 والمتمثلة في المصادرة والإغلاق.

- حيث يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة، كما يحكم أيضا بإغلاق المواقع التي تكون محلا للجريمة، ونعتقد أن المشرع يقصد المواقع الإلكترونية التي استعملت في تنفيذ الجريمة، لأن المواقع التي تكون محلا للجريمة هي المواقع التي توجد بها المعطيات الشخصية الضحية محل عتداء، بالإضافة إلى إغلاق المكان أو المحل الذي كان يستغل في ارتكاب الجريمة.

ثانيا: جريمة التعامل في معطيات شخصية غير صحيحة

تعد هذه الجريمة من بين جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتي ترتبط بأفعال تصب كلها في إطار التعامل مع معطيات شخصية مخزنة أو معالجة في النظم الآلية، وتكون إما صالحة لأن ترتكب بواسطتها إحدى الجرائم التي تمس بسرية المعطيات وسلامتها، وإما أن تكون متحصلة عن إحدى الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات، فقد حرص المشرع على التخفيف من آثار الإ عتداءات على المعطيات الشخصية والتصدي لها قبل وقوعها، وذلك من خلال تجريم مجموعة من الأفعال تصب كلها في إطار التعامل مع معطيات شخصية صالحة لأن ترتكب بها إحدى الجرائم المنصوص عليها في المواد 394 مكرر و394 مكرر1 من قانون العقوبات، فإذا لم تنجح الحماية الجزائية التي يوفرها التجريم الذي يمس مباشرة المصالح المرتبطة بالمعطيات الشخصية المكفولة بهذه النصوص القانونية، ولم يرتدع الجناة

عن القيام بمثل هذه الجرائم، فقد عمد المشرع على التقليل من الضرر الذي يمكن أن تسببه جرائم المعطيات ما أمكن، ومن ثم فعلى الأقل التخفيف من آثار هذه الإعتداءات التي تمثل أفعالا تعبر عن ستعمال لمعطيات شخصية تم الحصول عليها بطريقة غير مشروعة، ومن ثم فكل معطيات شخصية غير صحيحة أو غير مشروعة سواء كانت صالحة لأن ترتكب بها جريمة أو كانت متحصلة من جريمة، حرص المشرع على تجريم التعامل فيها من خلال المادة 394 مكرر2، سعيا منه لمنع وقوع الجريمة أو للتخفيف من آثارها إن وقعت.[1]

1) جريمة التعامل في معطيات شخصية صالحة لارتكاب جريمة:

تناول المشرع هذه الجريمة في الفقرة الأولى من المادة 394 مكرر2 حيث تنص على أنه "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 01 مليون إلى خمسة (5) ملايين دج، كل من يقوم عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم".

1-1) أركان الجريمة: تقوم هذه الجريمة كغيرها من الجرائم على تحقق الركنين المادي والمعنوي، وهو ما سوف نعرضه كما يلي:

أ) الركن المادي: نشير بداية أن المقصود بالتعامل في المعطيات الشخصية في هذه الجريمة هو كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة، أو كل سلوك من شأنه أن يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، وهي الصلة التي تظهر في القيام بأحد أنواع السلوك المنصوص عليها في البند الأول المادة 394 مكرر 2.[2]

وهذه الأفعال تشمل كافة العمليات السابقة على استخدام المعطيات في ارتكاب جريمة معينة، وتمثل السلوك الإجرامي ابتداء من تصميمها وبحثها، مرورا بتجميعها وصولا إلى توفيرها أو نشرها أو الإتجار بها.[3]

وعلى هذا الأساس فإن السلوك الإجرامي لجريمة التعامل في معطيات شخصية صالحة لارتكاب جريمة حسب المادة 394 مكرر2 البند الأول، هو مجموعة من الأفعال لو تركت دون تجريم لأدت إلى حدوث جرائم أخرى وهي تشمل أفعالا تعبر عن التعامل مع معطيات شخصية سواء المخز نة داخل نظام المعالجة الآلية أو المرسلة منه، أي مهما كانت حالتها، ثابتة (مخزنة) أم متحركة (مرسلة)، وهذا خلافا لجريمتي الإتلاف أو التلاعب بالمعطيات المذكورتين سابقا واللتان ينحصر السلوك الاجرامي فيهما على المعطيات المخزنة التي يتضمنها نظام المعالجة فقط.[4]

---

[1] محمد خليفة، مرجع سابق، ص279.

[2] رابحي عزيزة، مرجع سابق، ص 156.

[3] رشيدة بوبكر، جرائم الاعتداء على نظم المعالجة الآلية، مرجع سابق، ص 279.

[4] وهذا واضح من نص المادة 394 مكرر2 "... ي معطيات مخزنة، أو معالجة أو مرسلة..." بينما نص المادة 394 مكرر1 تنص "... المعطيات التي يتضمنها...

إن هذه الأفعال التي جاءت بها المادة 394 مكرر2 من شأنها أن تجعل من المعطيات صالحة لأن ترتكب بها الجريمة وقابلة لاستعمالها في ذلك، وكأن الأمر يتعلق بتهيئة معطيات شخصية عبر عمليات مرحلية تبدأ بتصميم هذه المعطيات والبحث فيها ثم تجميعها وصولا إلى جعلها في متناول الغير وتحت تصرفه من خلال نشرها أو توفيرها أو الإتجار بها.

كما لا يشترط أن تقع هذه الأفعال مجتمعة لكي يقوم الركن المادي للجريمة، بل يكفي لتحقق النشاط الإجرامي قيام الجاني بإحدى هاته الأفعال، والتي تتمثل حسب نص المادة 394 مكرر فيما يلي:

* **التصميم** : وهو عملية إعداد معطيات صالحة لارتكاب جريمة بواسطتها، وذلك باصطناعها وإخراجها للوجود أو إنتاجها*، ويعد هذا الفعل أي عملية في سلسلة التعامل في المعطيات التي تدخل ضمن لائحة الوسائل التقنية والمعلوماتية المستخدمة في جرائم الإعتداء على الأنظمة المعلوماتية وما تحتويه من معطيات، وغالبا ما يقوم بعملية التصميم المختصون في مجال التقنية كالمبرمجين ومصممي البرامج، مثل برنامج القنبلة المعلوماتية (bombe informatique) الذي هو عبارة عن برنامج يصمم ويثبت بداخل النظام المعلوماتي، وتكون الغاية بعد ذلك تدمير ومحو البيانات التي يتضمنها.

***البحث:** وهو عملية تستخدم بشكل أساسي على شبكات الأنترنت من أجل مساعدة المستخدمين على التنقل بين المصادر الهائلة والمتاحة على هذه الشبكة، وذلك عبر ما يسمى بمحركات البحث، وكما هو معروف فإن أغلب خدمات الأنترنت تقدم بصورة مجانية، لكن المقابل هو إدلاء المستخدم ببعض من بياناته الشخصية التي يطلبها الموقع لتقديم الخدمة، وكلما كانت المعطيات الشخصية كاملة وجيدة كلما زادت فعالية تقديم الخدمة، وقد يمكن البحث في هذه البيئة عن معطيات شخصية تخص الغير ومن ثم استخدامها على نحو غير مشروع، وكذلك هو الحال بالنسبة لأنظمة المعالجة الآلية للمعطيات التابعة للمؤسسات العمومية والخاصة، و التي تحتوي بدورها على كم هائل من المعطيات الشخصية للأفراد الذين تتم معالجة معطياتهم الشخصية في سبيل تسيير شؤونهم وتقديم خدماتها، ومن ثم فمن المتصور أن يعمد الجاني على البحث والتنقيب عن المعطيات الشخصية سواء المخزنة أو المعالجة في هذه الأنظمة أو المرسلة عبرها تكون بالنسبة له صالحة لأن يرتكب بواسطتها جريمة أخرى، كمن يبحث في النظام المعلوماتي التابع لمؤسسة استشفائية عن معطيات شخصية صحية تخص الغير واستخدامها فيما بعد على نحو غير مشروع كإفشاء مرضه الخطير، أو البحث عن معطيات شخصية تخص ذمته المالية المخزنة لدى نظام معلوماتي تابع لمؤسسة مالية يكون هذا الغير عميلا (زبون)لديها قصد الإساءة إلى مركزه المادي أو المعنوي.

وهذا رأي قد أخالف فيه من ذهب إلى اعتبار أن المقصود بعملية البحث في هذه الجريمة ينصرف إلى البحث عن كيفية تصميم هذه المعطيات وإعدادها.[1]

---

*وهو المصطلح الذي استعملته المادة 09 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في القاهرة بتاريخ 2010/12/21، متوفرة على موقع جامعة الدول العربية. http://www.lasportail.org/ar

[1] أنظر في ذلك محمد خليفة، مرجع سابق، ص 201، وكذلك رشيدة بوكر، جرائم الإعتداء على نظم المعالجة، مرجع سابق، ص 281.

* **التجميع :** وهي عملية تقوم على جمع أكبر قدر ممكن من المعطيات الشخصية المخزنة في أنظمة المعالجة الآلية والمرسلة منه، ليتمكن الجاني بعدها من استخدامها في إحدى الجرائم الأخرى كالتلاعب في المعطيات أو إتلافها، ومن الأدوات والوسائل التقنية التي صممت لتجميع المعطيات نجد ملفات تعريف الإرتباط (cookies) وملفات التجسس، بالنسبة للمعطيات المخزنة، أو عن طريق برامج الإعتراض بالنسبة للمعطيات المرسلة.

والملاحظ أن المشرع الفرنسي استعمل مقابل ذلك المادة 323-2-1 مصطلح الحيازة Détenir متأثرا باتفاقية بودابست، وما من شك أن هناك فرقا بين من يحوز على المعطيات وبين من يجمعها، إذ توحي حالة التجميع بسعى الجاني إلى جمع عدد كبير من المعطيات وهو الأمر الذي من شأنه أن يرفع من درجة الخطورة التي تشكلها هذه العملية وهي أوسع نطاق من حيث عدد المعطيات المحازة.[1]

***التوفير:** ويقصد المشرع بهذا السلوك وضع المعطيات تحت تصرف الغير وجعلها في متناوله، وإتاحتها لمن يريد أن يستخدمها في ارتكاب جريمة الدخول أو التلاعب في المعطيات، وكذا تقديمها له وعرضها عليه، وتفيد هذه العملية أن استخدام المعطيات لا يقتصر على من قام بتجميعها، بل يتعداه إلى أشخاص آخرين ومن ثم تزداد خطورة هذه العملية بازدياد هؤلاء.[2]

وقد استعملت اتفاقية بودابست عبارة "أي أشكال أخرى للوضع تحت التصرف" d'autre forme de mise à dispposition، ومن قبيل ذلك إتاحة كلمات المرور أو شفرة الولوج التي تسمح بالدخول إلى النظام المعلوماتي غير المصرح به، وقد توسع القضاء الفرنسي في تفسير مدلول مصطلح التوفير ليشمل الكشف أو الإفشاء العلني للثغرات الأمنية في النظام المعلوماتي، ومن قبيل فعل التوفير أيضا إفشاء من تكون المعطيات الشخصية تحت سيطرته باعتباره مسؤولا عن النظام المعلوماتي إلى الغير بهذه المعطيات، لتستخدم بعد ذلك في ارتكاب إحدى الجرائم.

***النشر :** يقصد بهذه العملية إذاعة المعطيات الشخصية التي يمكن أن تستخدم في ارتكاب الجريمة وتمكين الغير من الإطلاع عليها بأي وسيلة يمكن أن تتم عملية النشر بها، لتشمل كل نشاط من شأنه نقل المعطيات إلى الآخرين، وهو سلوك ينطوي على درجة كبيرة من الخطورة كونه كفيل بأن ينقل المعطيات الشخصية إلى علم عدد كبير من الأشخاص ممن ليس لهم الحق في الإطلاع عليها.

* **الإتجار :** ويقصد به كل أنواع التعاملات التي تقع على المعطيات الشخصية والتي تكون صالحة لأن ترتكب بها جريمة من جرائم المعطيات، نظير مقابل معين لا يشترط أن يكون نقديا، وهو مناط الفرق بين عملية الإتجار و عملية التوفير التي يكون دائما دون مقابل.

ونخلص بعد هذا التوضيح للأفعال التي يقوم عليها السلوك الإجرامي في جريمة التعامل في المعطيات الشخصية التي تصلح لارتكاب جريمة من جرائم المعطيات إلى القول أن هذه الجريمة هي جريمة شكلية

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية، مرجع نفسه، ص282.

[2] محمد خليفة، مرجع سابق، ص 203.

يكفي لوقوعها مجرد السلوك الإجرامي ولا يعتد المشرع في قيامها بتحقيق نتيجة معينة، فيكفي أن يقوم الجاني بواحد من تلك الأفعال لتحقيق الركن المادي.

ب) الركن المعنوي: تعتبر هذه الجريمة عمدية[1] تتطلب لقيامها القصد الجنائي القائم على العلم والإرادة وهذا ما يستفاد من عبارات المادة 394 مكرر 02 ".... عمدا وعن طريق الغش...." وعلى ذلك لابد أن يكون الجاني على علم بكافة العناصر المكونة للجرم، سيما علمه بأنه يقوم بالتعامل في معطيات غير مشروعة كونه تعامل فيها دون تصريح من مالكها، وأن يعلم أيضا أن من شأن هذه المعطيات أن تستخدم في ارتكاب جرائم أخرى من جرائم المعطيات، ثم على الرغم من علم الجاني بذلك، فإنه تتجه إرادته لإتيان فعل أو أكثر من أفعال التعامل في المعطيات غير المشروعة.

ورغم أن المشرع لم ينص صراحة على اشتراط القصد الجنائي الخاص ولم يتطلبه لقيام الركن المعنوي لهذه الجريمة، إذ يكفي لقيامها القصد الجنائي على النحو السابق بيانه، لكن بالعودة إلى المادة السادسة من اتفاقية بودابست فإنها اشترطت صراحة للعقاب على التعامل في المعطيات أو البرامج الصالحة لارتكاب جريمة أن يكون هذا التعامل بنية استخدامها لغرض ارتكاب جريمة من الجرائم المشار إليها في المواد 2،5 من هذه الاتفاقية.[2]

ومن ثم يقتضي القصد الجنائي الخاص أن يكون لدى الجاني نية سيئة في ارتكاب أفعال التعامل في معطيات شخصية غير صحيحة، وهو اتجاه القصد من وراء ذلك، عداد والتمهيد لاستعمالها في ارتكاب جريمة من جرائم الإعتداء على نظام المعالجة الآلية للمعطيات.

2-1) العقوبة المقررة قانونا: بقيام أركان الجريمة تقوم المسؤولية الجزائية ومن ثم يستوجب العقاب.

أ) العقوبة الأصلية: تعاقب المادة 394 مكرر2 على جريمة التعامل في معطيات شخصية تكون صالحة لارتكاب إحدى جرائم المعطيات بالحبس من ثلاث أشهر إلى 03 سنوات، وبالغرامة من مليون دج إلى 05 مليون دج.

ب) العقوبة التكميلية: على النحو الذي سبق بيانه فإن المحكوم عليه الذي تم إدانته بهذه الجريمة يخضع للعقوبات التكميلية الإلزامية المصادرة والغلق حسب المادة 394 مكرر6 من قانون العقوبات، خاصة عقوبة المصادرة، حيث تفترض هذه الجريمة ارتكابها بواسطة وسائل تقنية وبرامج وأجهزة تسهل أفعال التعامل مع المعطيات، فضلا عن ذلك فانه يجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة بنص المادة 09 من قانون العقوبات.

---

[1] وقد اعتبرت الإتفاقية الأوروبية للجريمة الإلكترونية (اتفاقية بودابست) في المادة 06 أن هذه الجرائم ترتكب عمدا، وكذلك أشار التقرير التفسيري لهذه الاتفاقية في الفقرة 39 منه، أن جميع الجرائم الواردة في الإتفاقية ترتكب عمدا من أجل تطبيق المسؤولية الجزائية.

[2] تنص الفقرة الثانية 06 من المادة من اتفاقية بودابست أنه لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع، الشراء بغرض الإستخدام، الإستراد، التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها في الفقرة الأولى من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد 2،5 من هذه الاتفاقية ".

2) جريمة التعامل في معطيات شخصية متحصلة من جريمة:

تمثل هذه الجريمة الصورة الثانية من جرائم التعامل في معطيات شخصية وغير مشروعة، نصت عليها المادة 394 مكرر2 في الفقرة الثانية، حيث يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 01 مليون دج إلى 05 مليون دج، كل من يقوم عمدا وعن طريق الغش بحيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

فمن خلال هذا النص يتأكد لنا أن المشرع لم يكتف بتجريم التعامل في المعطيات الصالحة لارتكاب جريمة بل جرم أيضا التعامل في معطيات متحصلة من جريمة، وإذا كان هدفه من الأولى منع حدوث الجريمة، فإن هدفه من الثانية هو الحد قدر الإمكان من آثار هذه الجريمة.[1]

والملاحظ أن المشرع الجزائري قد انفرد بالنص على هذه الجريمة حيث لانجد لها مثيلا في التشريع الفرنسي ولا في الإتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية.

وتتحقق الجريمة في هذه الصورة من خلال مجموعة من الأفعال، وهي حيازة المعطيات الشخصية المتحصلة من جريمة، إفشاؤها، نشرها واستعمالها.

1-2) أركان الجريمة:

أ) الركن المادي: يتحقق الركن المادي لمجرد السلوك الإجرامي الذي يقوم على أي فعل من الأفعال المحددة بنص البند 2 من المادة 394 مكرر2 دون اشتراط اجتماعها كلية، وتتمثل هذه الأفعال فيمايلي:

- **الحيازة** ويعبر هذا الفعل عن السيطرة الإرادية للشخص على الشيء سيطرة تمكنه من الإنتفاع به، أو تعديله أو إتلافه أو نقله، وهي حالة واقعية وليست مركزا قانونيا[2]، وهي أيضا رابطة واقعية بين مال منقول وشخص، تتيح لهذا الأخير السيطرة على هذا المال سيطرة مستقلة مقترنة بنية الإ حتباس.

ومن ثم فإن فعل الحيازة في هذه الجريمة يقتضي سيطرة الجاني على المعطيات الشخصية غير المشروعة سيطرة تمكنه من التأثير عليها أو الانتفاع بها أو إتلافها مع توفر نية إحتباسها لديه بصفة دائمة أو مؤقتة.

غير أن حيازة الجاني للمعطيات الشخصية المتحصلة من جريمة لا يعني خروجها عن سيطرة المجني عليه صاحب هذه المعطيات بصورة كلية، وكل ما يحدث أنه يفقد ميزة الإستئثار بها،[3] كونها ليست منقولا ماديا، وتكون الحيازة لهذه المعطيات في هذه الجريمة دائما غير مشروعة، ذلك أن عدم مشروعيتها مستمد من كونها تم الحصول عليها بطريقة غير مشروعة أي دون علم ورضا صاحبها الشرعي.

- **الإفشاء**: المقصود بفعل الإفشاء في هذه الجريمة هو نقل المعطيات الشخصية المتحصل عليها من إحدى جرائم المعطيات المنصوص عليها في قانون العقوبات، مثل جريمة الدخول غير المرخص به إلى نظام المعالجة إلى أشخاص أو جهات غير مختصة بتلقي هذه المعطيات.

[1] محمد خليفة، مرجع سابق، ص 195.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجرائم ضد الأشخاص والأموال، مرجع سابق، ص 264.

[3] فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص 145.

والملاحظ أن الفرق بين إفشاء المعطيات الشخصية في هذه الجريمة، وإفشاؤها في الجريمة المنصوص عليها في المادة 69 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين اتجاه معالجة المعطيات الشخصية يكمن في طريقة الحصول على هذه المعطيات، فإذا كان الحال في الجريمة الأولى أن تكون المعطيات متحصلة من جريمة وهي بذلك معطيات غير مشروعة، فإنه في الجريمة الثانية يتم الحصول على المعطيات الشخصية التي تم إفشاؤها بطريقة مشروعة، حيث يدلي بها صاحبها طوعا بمناسبة معالجتها، زيادة على أن فعل الإفشاء للمعطيات الشخصية في الجريمة المنصوص عليها في المادة 69 من القانون 07/18 لا يمكن تصور حدوثه إلا من قبل المسيطر عليها بمناسبة معالجتها أو حفظها، وهو لا يخرج عن كونه مسؤولا عن المعالجة أو معالجا من الباطن أو شخص مكلف بالنظر إلى مهامه بمعالجة المعطيات الشخصية، بينما فعل الإفشاء المنصوص عليه في المادة 394 مكرر2 فإنه يرتكب من أي شخص دون تحديد صفته يتحصل على هذه المعطيات بطريقة غير مشروعة، كقيامه باختراق نظام المعالجة الآلية (الدخول غير المصرح به) وأراد المشرع أن يمنعه من إفشائها ونقلها إلى من ليس له الحق في العلم بها، لتضييق انتشارها تقليصا لحجم الضرر الناتج عن ذلك من خلال تقليص انتشار هذه المعطيات لدى الغير، وتجدر الإشارة أن المشر ع الفرنسي لم يفرد نصا خاصا يعاقب على إفشاء المعطيات المتحصلة عن جريمة الدخول أو البقاء غير مصرح بهما، أو من جريمة التلاعب بالمعطيات بغض النظر عن طبيعة المعطيات محل الإفشاء سواء كانت معطيات شخصية أم غير ذلك، في حين أن المشرع الأمريكي من خلال القانون الفدرالي الإتحادي رقم (18) لسنة 1984 الخاص بإساءة استخدام الحاسب الآلي، يجرم في الفقرة "أ" من المادة 1030 عملية الإفشاء لمعطيات توجد في نظام معلوماتي يـ ، ستعمل من طرف الحكومة تم الحصول عليها بطريقة غير شرعية[1].

- النشر: تتحقق الجريمة بهذا الفعل عندما يتم الحصول على المعطيات الشخصية بطريقة غير مشروعة عبر الدخول غير المصرح به إلى نظام المعالجة الآلية المتضمن لهذه المعطيات، ثم بعد ذلك يقوم الجاني بإذاعتها وتمكين الغير من العلم بها والإطلاع عليها بأي وسيلة تحقق هذه الغاية.

- الإستعمال: من بين الأفعال التي يتحقق بها السلوك الإجرامي لجريمة التعامل في معطيات شخصية متحصلة من جريمة هو استعمال هذه المعطيات لأي غرض كان مهما كان هدفه ومهما كان نوعه، وصورة هذا الفعل أن يتم اختراق النظام المعلوماتي والنفاذ إليه بطريقة غير مشروعة والحصول على معطيات شخصية مخزنة به، و يقوم الجاني باستعمالها، أي استغلالها والانتفاع بها بطريقة غير مشروعة، مثل ما قامت به شركة **كامبريدج أناليتكا** (cambridge analytica) التي استخدمت المعطيات الشخصية لأكثر من 50 مليون مستخدم لموقع الفايسبوك تحصلت عليها بطريقة غير شرعية في التأثير على الإنتخابات الرئاسية الامريكية.*

[1] ضرغام جابر عطوش، مرجع سابق، ص 108.

* دخلت شركة فيسبوك في دوامة عاصفة مع الكشف يوم الأحد 18 مارس 2018 عن فضيحة شركة"Cambridge Analytica " التي حصدت بيانات أكثر من 50 مليون مستخدم لموقع فيسبوك، ومن دون موافقتهم، بهدف تطوير برنامج معلوماتي يتيح كشف النوايا الإنتخابية للناخبين وكيفية التلاعب بها، وذلك منذ عام 2014، فهناك اتهامات لهذه الشركة بتوظيف البيانات الشخصية لمستخدمي فايسبوك في التأثير على نتيجة

ويقوم الركن المادي لمجرد ارتكاب الجاني لأي فعل من هذه الأفعال المشكلة للسلوك الإ جرامي، ولا يتطلب لقيامه حدوث نتيجة معينة أو ضرر فعلي يلحق بالمعطيات، ذلك أن سبب التجريم هو خطورة الأفعال ذاتها.

ب) الركن المعنوي: يتخذ الركن المعنوي في هذه الجريمة مثل باقي الجرائم صورة القصد الجنائي العام وعلى ذلك، يجب أن يعلم الجاني أنه يقوم بالتعامل في معطيات غير صحيحة تم الحصول عليها بطريقة غير مشروعة، أي أنها متحصلة من جريمة الدخول غير المصرح به للنظام المعلوماتي أو التلاعب بالمعطيات، ويعلم أيضا أن ارتكابه لأي فعل من الأفعال المكونة للسلوك الإجرامي من حيازة أو إفشاء أو استعمال من شأنه أن يشكل جرما معاقبا عليه، ثم تنصرف إرادته الحرة للتعامل في هذه المعطيات رغم علمه هذا، ويكفي القصد الجنائي العام لوحده لقيام الركن المعنوي ولا يتطلب قصدا جنائيا خاصا.

2-2) العقوبة المقررة قانونا: إنطلاقا من المادتين 394 مكرر2 والمادة 394 مكرر 6 من قانون العقوبات فإن المشرع قرر لهذه الجريمة عقوبات أصلية الحبس والغرامة، وعقوبات تكميلية تشترك فيها مع باقي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أ) العقوبات الأصلية: يعاقب على جريمة التعامل في معطيات شخصية غير صحيحة متحصلة من جريمة بالحبس من شهرين إلى ثلاث سنوات وبالغرامة من 1 مليون دج إلى 05 مليون دج.

وهي عقوبة مشددة من حيث الحد الأقصى لعقوبة الحبس، مقارنة بالجرائم الأخرى تبعا لخطورة فعال.

ب) العقوبات التكميلية: وهي عقوبات تكميلية وجوبية نصت عليها المادة 394 مكرر6 والمتمثلة في المصادرة للأجهزة والبرامج والوسائل المستخدمة، وكذا عقوبة الغلق للمواقع المستعملة في الجريمة وغلق المحل أو المكان المستغل في ارتكابها، بالإضافة إلى عقوبات تكميلية اختيارية منصوص عليها في المادة 09 من قانون العقوبات يمكن أن يضيف القاضي واحدة أو أكثر من هذه العقوبات على حسب ظروف الوقائع.

الفرع الثاني: جرائم الاعتداء على المعطيات الشخصية في قانوني التوقيع الإلكتروني والتجارة الإلكترونية:

تبدو الحاجة إلى التوقيع الإلكتروني لأجل اعتبارات الأمن والخصوصية لاسيما في مجال التعاملات الإلكترونية أمرا يشغل حيزا كبيرا ومثيرا لقلق الكثيرين من المتعاملين عبر شبكة الأنترنت، الأمر الذي يسبب نوعا من انعدام الثقة عبر هذه الشبكة.[1]

الإستفتاء حول خروج بريطانيا من الإتحاد الأوروبين والإتهامات بالتدخل الروسي لتأثير في الإنتخابات الرئاسية الأمريكية في عام 2016 ودعم ترامب مقابل هيلاري كلينتون.

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 72.

فإذا كانت التعاملات الإلكترونية قد شهدت تطورا كبيرا وسريعا، فإن ذلك قد واكب الثورة المعلوماتية التي تطلبت تدخلا سريعا لمواجهة التحديات التي فرضتها في مختلف الدول، والتي يمكن وصفها بالتحديات العامة التي تتعلق بالتجارة الإلكترونية ككل، وأبرزها تحدي خصوصية العلاقة بين المتعاقدين وخصوصية البيانات المتداولة بينهما.[1]

لأجل ذلك فقد تم اللجوء إلى تقنية التوقيع الإلكتروني، حتى يتم رفع مستوى أمن الخصوصية بالنسبة للمتعاملين عبر شبكة الأنترنت، حيث يمكن من خلال هذه التقنية الحفاظ على سرية المعلومات والمعطيات ولا يمكن لأي شخص مهما كانت قدرته معرفة مضمون الرسائل أو الإطلاع عليها أو تحريفها أو تعديل مضمونها، ذلك أن تقنية التوقيع الإلكتروني تضمن تحديد هوية المرسل، والمرسل إليه إلكترونيا والتأكد من مصداقية الأشخاص ومعطياتهم، وأنها نفس المعطيات الأصلية، ولم يتم العبث بها من قبل الأشخاص المخترقين لهذه الشبكات.

أولا: مفهوم التوقيع الإلكتروني:

من خلال ما تم دراسته عن هذا الموضوع يمكن اعتبار أن التوقيع الإلكتروني هو مفهوم فني قادر على إحداث مفعول قانوني يتمثل في ربط اسم الموقع بالرسالة وكذا بيان الموافقة على محتوياتها، فاصطلاح التوقيع عند استخدامه إنما يقصد به معنيان، المعنى الأول ويتعلق بعملية وضع الإمضاء أو أي إشارة أخرى على محرر يحتوي على معلومات معينة، وثانيهما وهو العلامة أو الإشارة التي تسمح بتمييز شخص الموقع، لذلك قيل بأن التوقيع الإلكترونيعتبر أيه علامة مميزة وخاصة بالشخص الموقع تسمح بتحديد شخصيته والتعرف عليها بسهولة.[2]

1) تعريف التوقيع الإلكتروني: لقد صيغت عدة تعريفات فقهية للتوقيع الإلكتروني، حيث اعتبر بأنه عبارة عن بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات.[3]

ويعرف كذلك بأنه ذلك التوقيع الناتج عن اتباع إجراءات محددة، تؤدي في النهاية إلى نتيجة معروفة مقدما يكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي، أو ما يسميه البعض توقيع إجرائي إلكتروني.[4]كما عرف التوقيع الإلكتروني كذلك بأنه ملف رقمي صغير يصدر عن إحدى الهيئات المتخصصة والمستقلة ومعترف بها من الحكومة، يتم التخزين في هذا الملف الإسم وبعض المعلومات الهامة الأخرى مثل الرقم التسلسلي وغير ذلك.[5]

[1] حسام الدين نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الإعتداء على التوقيع الإلكتروني، دار شتات للنشر والبرمجيات دار الكتب القانونية، 2013، ص 21.

[2] محمود إبراهيم غازي، مرجع سابق، ص 343.

[3] حسام الدين نبيل الشنراقي، مرجع سابق، ص 51.

[4] محمد المرسي زهرة، الدليل الكتابي وحجية مخرجات الكمبيوتر في المواد المدنية والتجارية، بحث مقدم لمؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات، ماي 2000 ص 21.

[5] عبد الفاتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 231.

أما من الناحية التشريعية فإن المشرع الجزائري قد عرف التوقيع الإلكتروني في المادة الثانية من القانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1]، بأنه "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق"

وذهب التوجيه الأوروبي رقم 1999/93/CE للبرلمان والمجلس الأوروبي المؤرخ في 13 ديسمبر 1999 المتعلق بالتوقيع الإلكتروني[2] إلى تعريف التوقيع الإلكتروني بأنه "عبارة عن معطيات في شكل إلكتروني ترتبط أو تتصل منطقيا بمعطيات إلكترونية أخرى، تستخدم لإقرارها".[3]

وقد عرفه المشرع الفرنسي في المادة 4/1316 من القانون المدني المعدلة بموجب القانون 2000/230 المتعلق بالتوقيع الإلكترونين[4] بأنه التوقيع الذي يتم باستخدام وسيلة إلكترونية آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه، وإذا قام به موظف عام فإنه يكفل الصفة الرسمية على العمل القانوني".

وحتى تتحقق الحماية الفاعلة للتوقيع الإلكتروني فإنه يجب أن تتوافر فيه مجموعة من الشروط:

- أن يكون ذلك التوقيع خاصا بصاحبه ينفرد به على الآخرين دالا على شخصيته.

- أن يكون لصاحب التوقيع سيطرة على منظومة أو وسيلة التوقيع مثل Token

وحتى يتحقق للتوقيع الإلكتروني الثقة ويتوافر فيه عنصر الأمان يقتضي الأمر وجود سلطة إصدار شهادات التوقيع الإلكتروني والتي تحتفظ بمراقبة المفتاح الخاص بصاحب التوقيع، وهي التي سماها المشرع الجزائري في قانون التوقيع والتصديق الإلكترونيين بمؤدي خدمات التصديق الإلكتروني* ، وهو الشخص الطبيعي أو المعنوي الذي يصدق على التوقيع الإلكتروني لكي يكون لهذا التوقيع قدر من المصداقية والثقة والاعتبار القانوني، وذلك من خلال منح شهادات التصديق التي من خلالها يتم التأكيد على وجود صلة بين بيانات إنشاء التوقيع والموقع، وتعتبر هذه الشهادة بمثابة مستند أو وثيقة إلكترونية

[1] القانون 04/15 المؤرخ في 1 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06 مؤرخة في 10 فيفري 2015.

[2] Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire les signatures électroniques.

[3] Article 02 : définition : aux fins de la présente directive on entend par signature électronique une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ».

[4] Loi n° 2000/230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

* عرف المشرع الجزائري مؤدي خدمات التصديق في المادة 02 من القانون 04/15 في البند 12 بأنه شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني، ويعرف التصديق الإلكتروني بأنه وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر حيث يتم نسبته إلى شخص أو كيان معين عبر جهة موثوق بها أو طرف محايد يسمى مقدم خدمات التصديق الإلكتروني، أنظر محمد حسين منصور، الإثبات التقليدي أو الإلكتروني، دار الفكر الجامعي، 2006 الإسكندرية، ص 289، أنظر كذلك المادة 13/2 من التوجيه الأوروبي 1999/93/CE المؤرخ في 13 ديسمبر 1999.

تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني[1]، وبناء على هذه الشهادة واستنادا عليها يكون الطرف المعول في المعاملة أو الذي يتلقى المراسلة الموقعة إلكترونيا متأكدا من صحة وسلامة التوقيع الإلكتروني للطرف الآخر أو مرسل الرسالة.

حيث أن شهادة التصديق الإلكتروني تؤدي إلى التحقق من هوية الشخص وسلطاته وأهليته وأوصافه المعنية، وتثبت أن الرسالة الموقع عليها صحيحة ولم يطرأ عليها أي تعديل، وتمكن من معرفة المفتاح العام الذي يمكن من خلاله التأكد من المعلومات المرسلة وكذا الإرتباط بينه وبين المفتاح الخاص، وهذا بالنظر إلى البيانات التي تشتملها والتي من أهمها هوية الموقع الفعلي.[2]

وتمنح شهادة التصديق من قبل جهات التوثيق الإلكتروني بعد أن تقوم بالتحقق من صحة البيانات المقدمة لها من طرف الأشخاص المصدر لهم هذه الشهادات، وتوثيق صفاتهم المميزة وهوياتهم وتضمينها في الشهادة ويعد هذا التحقق من بين أهم الإلتزامات القانونية الملقاة على عاتق هذه الجهات، خاصة الحصول على المعطيات الشخصية[3] من الشخص المعني نفسه أو من يمثله بعد الموافقة الكتابية للشخص المعني.[4]

2) صور التوقيع الإلكتروني: للتوقيع الإلكتروني صورتان: إحداهما التوقيع الإلكتروني الرقمي أو الكودي، وهناك التوقيع البيومتري.

أ) التوقيع الكودي أو الرقمي: وهو عبارة عن أرقام مطبوعة لمحتوى المراسلة تسمى HASH والتي يتم التوقيع عليها بالطريقة ذاتها أي باستخدام الأرقام، ويتم الحصول على هذا الكود بتحويل المحرر المكتوب والتوقيع الوارد عليه من نمط الكتابة العادية إلى معادلة رياضية باستخدام مفاتيح سرية (Token) وطرق حسابية معقدة وذلك لتحويل المستند الإلكتروني من صورته المقروءة المفهومة إلى رسالة رقمية غير مقروؤة، أو غير مفهومة، ولا يمكن لأحد إعادة هذه المعادلة إلى صورتها المقروؤة سوى حائز المفتاح[5]، وهو

---

[1] عرف المشرع الجزائري شهادة التصديق في المادة 02 من القانون 04/15 في البند 7 بأنها وثيقة في شكل إلكتروني تثبت الصلة بين التحقق من التوقيع الإلكتروني والموقع، وعرفتها كذلك المادة 90/02 من التوجيه الأوروبي1999/93/CE المتعلق بالتوقيع الإلكتروني بأنها وثيقة تربط بين أداة التوقيع وبين شخص معين اؤكد شخصيته الموقع:

Et aussi l'article 02/90 de la directive 99/93/CE dispose que le certificat une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne. »

[2] حسام محمد نبيل الشنراقي، مرجع سابق، ص 104.

[3] نصت المادة 1/08 من التوجيه الأوروبي 99/93/CE المتعلق بالتوقيع الإلكتروني على أن الدول الاعضاء في الاتحاد الأوروبي تسهر على ضرورة النص في تشريعاتها على إلزام مقدمي خدمة التصديق الإلكتروني باحترام مقتضيات التوجيه الأوروبي رقم 46/95 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي.

[4] علاء حسين مطلق التميمي، الجهة المختصة بإصدار شهادة التصديق الإلكتروني، دار النهضة العربية، القاهرة، 2004، ص 53، أنظر كذلك المادة 2/8 من التوجيه الاوروبي 99/93/CE حيث ألزمت مقدم خدمة التصديق الإلكتروني بأن لا يتلقى المعطيات الشخصية إلا مباشرة من الشخص المعني أو مع رضاه الصريح.

[5] حسام محمد نبيل الشنراقي، مرجع سابق، ص 64.

بذلك عبارة استخدام لمجموعة من الأرقام أو الحروف أو كليهما يختارها صاحب التوقيع لتحديد هويته وشخصيته، ويتم تركيبها أو ترتيبها في شكل كودي لا يعلمها إلا صاحب التوقيع فقط ومن يبلغه بها.[1]

ومن مزايا التوقيع الإلكتروني الرقمي أنه يؤدي إلى إقرار المعلومات التي يتضمنها السند، وهو وسيلة مأمونة لتحديد هوية الشخص الذي قام بالتوقيع، وفي مقابل ذلك من سلبياته احتمال تعرضه للضياع أو للسرقة، فضلا عن ذلك لو كان توقيعه الإلكتروني الصادر بشأنه شهادة موثقة من الجهة المختصة، قد تسرب إلى أشخاص آخرين يكون صاحبه هو المسؤول عن ذلك طالما أنه لم يتخذ إجراءات الحيطة[2]، ويسأل عن خطئه وإهماله في الحفاظ على رقمه السري.

ب) التوقيع البيومتري (التوقيع باستخدام الخواص الذاتية): ويعرف بأنه التحقق من شخصية المتعامل بالاعتماد على الخواص الذاتية والصفات التي تميزه والطبيعة الجسدية والسلوكية له لتمييزه وتحديد هويته.

حيث تتحقق صورة هذا التوقيع بالاعتماد على الصفات والخصائص الفيزيائية للإنسان، وهي التي تختلف من شخص لآخر، وتشمل البصمة الشخصية، مسح قرنية العين البشرية، التحقق من نبرة الصوت، خواص اليد، التعرف على الوجه، درجة ضغط الدم، وغير ذلك من الصفات الجسدية والحيوية للإنسان.[3]

وعمليا يتم تخزين هذه الخواص على جهاز الحاسب الآلي بطريق التشفير في نظام حفظ الذاكرة للحاسب الآلي، ويصادفك هذا التشفير للتحقق من صحة التوقيع وذلك بمطابقة صفات وسمات العميل المستخدم للتوقيع مع الصفات التي تم تخزينها على جهاز الحاسب الآلي.

وقد جاء قانون التوقيع الإلكتروني 04/15 ليقر الحماية للمعطيات الشخصية التي يتم تداولها في نطاق التعاملات الإلكترونية وتجريم بعض الأفعال التي من شأنها المساس بهذه المعطيات.

ثانيا: الجرائم الماسة بالمعطيات ذات الطابع الشخصي في قانون التوقيع الإلكتروني 04/15:

تبين من خلال مواد التجريم الواردة في الأحكام الجزائية لهذا القانون أن الحماية الجزائية للمعطيات الشخصية في ظل القانون 04/15 تكون إما أثناء إنشاء شهادة التصديق من طرف مزود خدمة التصديق وقبل التسجيل لدى هذا الأخير، وتكون كذلك بعد التسجيل لديه (بعد إنشائها).[4]

1) الجرائم الماسة بالمعطيات الشخصية قبل إنشاء شهادة التصديق الإلكتروني: يتعلق الأمر بجريمة الإدلاء بإقرارات كاذبة للحصول على شهادة التصديق الإلكتروني، حيث تنص المادة 66 من القانون 04/15 على أنه "بعاقب بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من 20 عشرين ألف دج إلى

[1] ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، دار الجامعة الجديدة، الإسكندرية 2007 ص50.

[2] عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكومبيوتر والأنترنت، مرجع سابق، ص 240.

[3] محمود إبراهيم غازي، مرجع سابق، ص 358.

[4] ينشأ التوقيع الإلكتروني على أساس شهادة التصديق الإلكتروني، أنظر المادة 07 من القانون 04/15.

مائتي ألف دج (200,000دج) أو بإحدى هاتين العقوبتين كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني".

إن صحة التوقيع الإلكتروني و موثوقيته تتوقف على صحة المعطيات المدلى بها من طرف الشخص المعني بالشهادة الإلكترونية، ذلك أن هذه المعطيات هي معطيات التحقق والتي من خلالها يمكن لجهات التوثيق الإلكتروني إثبات صلة التوقيع الإلكتروني بالموقع، لذلك فإنه يتعين على مزود خدمة المصادقة الإلكترونية عند طلب شهادة جمع المعطيات ذات الطابع الشخصي أن يطلبها مباشرة من الشخص المعني، كما له أن يتحصل عليها من الغير بعد الموافقة الكتابية أو الإلكترونية لهذا الشخص[1]، وعلى هذا الأخير أن يتحرى الإدلاء بهذه المعطيات بصفة صحيحة وغير مغلوطة حتى لا يؤثر سلبا على مصداقية الشهادة الإلكترونية التي يقدمها مزود الخدمة.

1-1) أركان الجريمة: إنطلاقا من نص المادة 66 من القانون 04/15 المذكورة أعلاه فإن أركان هذه الجريمة هي كمايلي:

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة عندما يقوم المستفيد من الشهادة وهو الشخص الموقع الذي يعمل على إنشاء التوقيع بالإدلاء بمعطيات لدى مزود خدمة التصديق الإلكتروني ما يميزها أنها كاذبة وغير صحيحة ومخالفة للحقيقة، مخالفا بذلك قواعد المصداقية.

وترتيبا على ذلك فإن الركن المادي لهذه الجريمة يقوم بتحقق العناصر التالية:

-السلوك الإجرامي: وهو نشاط إيجابي يتمثل في التصريحات المغلوطة والمخالفة للحقيقة سواء تعلق بهوية صاحبها أو نشاطه أو أي معطيات ذات علاقة بإنشاء شهادة التوقيع.

- صفة الجاني: يتعلق الأمر بالشخص الموقع طالب إنشاء التوقيع، والذي عرفه المشرع في المادة 2 من القانون 04/15 بأنه شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله، وهو نفس التعريف الذي ورد في المادة 3/02 من التوجيه الأوروبي CE/99/93 المتعلق بالتوقيع الإلكتروني.[2]

- النتيجة الإجرامية: وهي الغرض من السلوك الإجرامي، حيث يهدف الجاني من وراء سلوكه إلى الحصول على شهادة تصديق إلكترونية.[3]

والملاحظ أن المشرع الجزائري استعمل كلمة "إقرارات" في حين أن التشريعات الأخرى تعتبر أن ما يصرح به الموقع لطلب إنشاء التوقيع هي عبارة عن "معطيات إنشاء التوقيع" [1] ونعتقد أن مصطلح إقرارات أشمل ويستغرق المعطيات الشخصية أو أي معلومات أخرى.

---

[1] أنظر المادة 16 من قانون المبادلات والتجارة الإلكترونية التونسي عدد 83 لسنة 2000 المؤرخ في 09 أوت 2000.

[2] L'article 2/3 de la directive 93/99/CE dispose que... « signataire » : toute personne qui ditient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité personne physique ou morale qu'elle présente.

[3] عرفها الشرع في المادة 2 البند 7 من القانون 04/15 بأنها وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع.

ب) الركن المعنوي: تعتبر جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكترونية جريمة عمدية، يكفي لقيام الركن المعنوي فيها عنصراه العلم والإرادة.

وعلى ذلك يجب أن يعلم الجاني بعدم صحة المعلومات المقدمة، ورغم ذلك تتجه إرادته إلى التصريح والإدلاء بها، بغية الحصول على شهادة تصديق إلكترونية لتوقيعه.

2-1) العقوبة المقررة قانونا: يعاقب الشخص الطبيعي المدان بهذه الجريمة بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من عشرين ألف دج (20,000دج) إلى مائتي ألف دج (200,000دج) أو بإحدى هاتين العقوبتين.

وعن العقوبة التكميليةفإن المشرع لم يحدد في القانون 04/15 لهذه الجريمة عقوبات تكميلية وجوبية وعليه يمكن إخضاع المحكوم عليه لعقوبة أو أكثر من العقوبات التكميلية الإختيارية المنصوص عليها في قانون العقوبات.

2) الجرائم الماسة بالمعطيات الشخصية بعد إنشاء شهادة التصديق:

كما ألزم المشرع الأشخاص الذين يقدمون المعطيات إلى جهات التصديق الإلكتروني بضرورة تقديمها بشكل صحيح وعاقب من يخالف ذلك، فإنه أيضا ألزم هذه الجهات التي تضع المعطيات تحت يدها، بالمحافظة على سريتها وعدم جمعها إلا بعد الموافقة الصريحة من الشخص المعني بها، وعدم استعمالها لأغراض أخرى غير تلك التي جمعت لأجلها.

1-2) جريمة إفشاء المعطيات الشخصية: نصت المادة 70 من القانون 04/15 على أنه "يعاقب بالحبس من ثلاث أشهر إلى سنتين وبغرامة من مائتي ألف دج إلى مليون دج أو بإحدى هاتين العقوبتين، فقط كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون".

وبمطالعة أحكام المادة 42 فإنها تنص على أنه "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة".

كما تنص المادة 74 أنه "يعاقب بالحبس من ثلاث أشهر إلى سنتين وبغرامة من 20 ألف إلى مائتي ألف دج أو بإحدى هاتين العقوبتين كل مكلف بالتدقيق يقوم بكشف معلومات سرية أطلع عليها أثناء قيامه بالتدقيق".

1-1-2) أركان الجريمة:

أ) الركن المادي: من خلال نص المواد المذكورة أعلاه فإن الركن المادي لهذه الجريمة يتحقق بتوفر العناصر التالية:

[1] أنظر المادة 47 من القانون التونسي، حيث تنص على أنه "يعاقب كل من صرح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الإلكترونية لكافة الأطراف".

صفة الجاني: وهو مؤدي خدمات التصديق، و الذي حسب المادة 02 البند 12 من القانون 04/15 يعد كل شخص طبيعي أو معنوي يقوم بمنح شهادات التصديق الإلكتروني أو تقديم خدمات أخرى في مجال التصديق الإلكتروني، وهو نفس التعريف الوارد في المادة 11/2 من التوجيه الأوروبي CE/99/93. [1]

أو يكون حسب نص المادة 74 كل شخص مكلف بالتدقيق، وهي عملية عرفتها المادة 02 البند 16 بأنها التحقق من مدى المطابقة بغرض مراقبة مؤدي خدمة التصديق الإلكتروني من قبل السلطة الإقتصادية.

السلوك الإجرامي: وهو عدم المحافظة على سرية المعطيات الشخصية التي قدمها طالب إنشاء التوقيع وذلك من خلال القيام بإفشائها للغير، ومن ثم يفترض لقيام هذا السلوك الإجرامي أن يكون الجاني قد اطلع أو تحصل على معطيات شخصية بحكم عمله المتمثل في إنشاء شهادات التصديق الإلكترونية بالنسبة لمقدم خدمة التصديق أو أثناء قيامة بالتدقيق بالنسبة للشخص المكلف بعملية التدقيق، ثم يقوم بإذاعتها وإطلاع الغير ممن ليس له الحق في الإطلاع عليها، وإخراجها بسبب ذلك من حيز الكتمان والسرية، بعد أن كان العلم بها قاصرا على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم، دون علم أو رضا صاحبها.[2]

محل الجريمة: وهي المعطيات الشخصية التي يطلع مقدمو خدمة التصديق أو المكلفون بالتدقيق أثناء قيامهم بمهامهم، والممنوحة لهم من طرف أصحابها في سبيل عمليات التصديق الإلكتروني.

وإن كان المشرع الجزائري لم يحدد في المادة 42 طبيعة البيانات التي يتوجب على مزود خدمة التصديق المحافظة على سريتها، مما يمكن أن يندرج ضمنها المعطيات الشخصية التي تستوجبها شهادة التصديق. ويتحقق الركن المادي لهذه الجريمة بمجرد تحقق السلوك الإجرامي، دون اشتراط تحقق نتيجة الضرر لصاحب المعطيات، لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية المعطيات في حد ذاتها.

ب) الركن المعنوي: يتحقق الركن المعنوي في هذه الجريمة كغيرها من الجرائم العمدية بقيام العلم لدى الجاني بعناصر الجريمة، وذلك بانصراف علمه إلى أن المعطيات التي يسيطر عليها قد تحصل عليها بحكم وظيفته وأنه لا يجوز له إطلاع الغير عليها، ورغم ذلك تنصرف أيضا إرادته إلى مخالفة هذا الالتزام والقيام بإفشائها إلى الغير.

2-1-2) العقوبة المقررة قانونا: بتحقق أركان الجريمة تقوم المسؤولية الجزائية ومن ثم استوجب الجاني إنزال العقوبة المقررة قانونا، وانطلاقا من المادة 70 من القانون 04/15 يعاقب مؤدي خدمة التصديق الذي يفشي المعطيات الشخصية بالحبس من 03 أشهر إلى ثلاث سنوات وبالغرامة من 200 ألف دج إلى (01) مليون دج، أو بإحدى هاتين العقوبتين، وهي تقريبا نفس العقوبة المقررة للشخص المكلف بالتدقيق الذي يفشي معطيات شخصية ما عدا في الحد الأقصى للغرامة الذي يحدد بـ 200 مائتي ألف دج.

[1] L'article 2/11 de la directive 93/99/CE « prestataire de service de certification toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques »

[2] رشيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص 130.

2-2) جمع مؤدي خدمة التصديق الإلكتروني للمعطيات الشخصية دون موافقة الشخص المعني:

تنص المادة 71 من القانون 04/15 على أنه "يعاقب بالحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من مائتي ألف دج إلى 01 مليون دج أو إحدى هاتين العقوبتين كل مؤدي خدمات التصديق أخل بأحكام المادة 43 من هذا القانون، وهي التي تنص على أنه لا يمكن لمؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة".

الملاحظ أن المشرع جرم فقط عملية جمع المعطيات الشخصية من قبل مزود خدمة التصديق الإلكتروني[1] وهي إحدى العمليات المكونة لنشاط المعالجة الآلية للمعطيات الشخصية حسب أحكام المادة 02 من القانون 05/18، وهذا خلافا لما ذهب إليه المشرع التونسي الذي تكلم في المادة 38 من قانون المبادلات والتجارة الإلكتروني عن تجريم معالجة المعطيات الشخصية دون موافقة الشخص المعني وليس عملية الجمع فقط[2] ونعتقد أن المشرع قد جانب الصواب في هذه المسألة، ذلك أنه قد تكون عملية الجمع بموافقة الشخص المعني، لكن العمليات الأخرى اللاحقة لها مثل الحفظ، أو النقل أو التسجيل أو الاستخراج... قد تأتي دون موافقته وهو أمر من شأنه الإفلات من المسؤولية الجزائية.

غير أن هذا الأمر جاء متوافقا مع أحكام المادة 42 من القانون 07/18 المتعلق بحماية المعطيات الشخصية التي أوجبت على مؤدي خدمات التصديق الإلكتروني ضرورة الحصول على المعطيات الشخصية لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني عن طريق جمعها من المعني شخصيا، وفي هذا سبيل وسانحة لأن بيدي هذا الأخير موافقته على جمع معطياته الشخصية.

1-2-2) أركان الجريمة

أ) الركن المادي: يتحقق الركن المادي لهذه الجريمة بمجرد السلوك أو النشاط الإجرامي المتمثل في قيام الجاني وهو مزود خدمة التصديق الإلكتروني بجمع معطيات شخصية تخص طالب شهادة التصديق بغير موافقة هذا الاخير، دون الحاجة إلى اشتراط ترتب نتيجة معينة.

والمعطيات الشخصية التي يحظر جمعها من طرف مزود خدمة التصديق الإلكتروني دون موافقة الشخص المعني هي كل معلومة من شأنها أن تجعل هذا الأخير معرفا أو قابلا للتعريف، مثل عناصر هويته.

ب) الركن المعنوي: تعتبر هذه الجريمة أيضا من الجرائم العمدية التي يتطلب لقيامها القصد الجنائي العام وذلك من خلال علم الجاني بأنه يقوم بجمع معطيات ذات طابع شخصي دون أن تكون لديه موافقة مسبقة من صاحب هذه المعطيات إلا أن إرادته تنصرف إلى إتيان هذا الفعل رغم ذلك.

---

[1] حتى بالنص الفرنسي للمادة 43 نجد المشرع استعمل مصطلح أو عبارة التجميع حيث تنص المادة:

Le préstataire de servicess de certification électronique ne peut recueillir des données personnelles qu'après constentement explicite de l'intéréssé

[2] تنص المادة 38 من القانون التونسي عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية على أنه: "لا يمكن لمزود خدمات المصادقة الإلكترونية معالجة المعطيات الشخصية إلا بعد موافقة المعني".

2-2-2) العقوبة المقررة قانونا: يعاقب مزود خدمة التصديق الإلكتروني عن جريمة جمع معطيات شخصية دون موافقة صاحب شهادة التصديق بالحبس من 06 (ستة) أشهر إلى ثلاث سنوات وغرامة من 200 ألف دج إلى 1 مليون دج أو بإحدى هاتين العقوبتين، وتكون عقوبة الشخص المعنوي حسب المادة 75 من نفس القانون هي ما يعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي أي غرامة بـ 05 مليون دج.

هذا ويجوز لجهة الحكم أن تقرر توقيع إحدى العقوبات التكميلية الإختيارية المنصوص عليها في المادة 18 مكرر من قانون العقوبات، تكون متناسبة مع طبيعة الجرم وخطورته وكذا طبيعة الجاني.

3-2) جريمة جمع واستعمال معطيات شخصية بطريقة غير مشروعة:

إضافة إلى التزام مقدم خدمة التصديق الإلكتروني بشرط الموافقة لطالب شهادة التصديق حتى يتمكن من جمع معطياته الشخصية، هاهو المشرع يقيده بالتزام آخر حرصا على حماية المعطيات الشخصية، وذلك بأن لا تنصب عملية الجمع لهذه المعطيات إلا على الضرورية واللازمة بالقدر الكافي للتمكن من إنشاء شهادة التصديق الإلكتروني، وأن يتجنب المبالغة في مطالبة الشخص المعني بمعطيات شخصية إضافية قد لا تكون مفيدة في عملية منح هذه الشهادة، وفي نفس الوقت من شأنها التوغل في خصوصيات الشخص المعني.

إلى جانب ذلك فإن الغرض من جمع المعطيات الشخصية من قبل مزود خدمة التصديق الإلكتروني هو منح الشخص المعني شهادة التصديق الإلكتروني، وفي سبيل ذلك يحظر عليه استعمالها في غير هذا الغرض.

1-3-2) أركان الجريمة: وترتيبا على ما سبق فإن أركان جريمة جمع واستعمال معطيات شخصية من طرف مقدم التصديق الإلكتروني طبقا للمادتين 43،71 من القانون 04/15 تتمثل فيما يلي:

أ) الركن المادي: يقوم الركن المادي لهذه الجريمة بمجرد السلوك الإجرامي الذي يأخذ صورتين:

الصورة الأولى: وهي جمع معطيات شخصية من قبل مزود خدمة التصديق خاصة بطالب شهادة التصديق تكون غير ضرورية لمنح هذه الشهادة، وإن كان المشرع الجزائري لم يحدد معيار تصنيف المعطيات الضرورية من غيرها لمنح شهادة التصديق، فإن المشرع التونسي في قانون المبالات والتجارة الإلكترونية اعتبر في المادة 39 المعطيات الضرورية هي التي تكون لازمة لإبرام العقد وتحديد محتواه وتنفيذ وإعداد وإصدار الفاتورة[1]، وهي مسألة موضوعية تخضع لتقدير القضاء.

الصورة الثانية: وهي تتعلق بفعل الاستعمال للمعطيات الشخصية المجمعة لأغراض أخرى غير الغرض الأساسي الذي وافق الشخص المعني على تجميعها لأجله، حيث أن مورد التصديق الإلكتروني يعلم الكثير

[1] رشيدة بوبكر، مرجع سابق، ص 128. وتنص المادة 39 من قانون المبادلات والتجارة الإلكترونية التونسي على:" باستثناء حالة موافقة صاحب الشهادة لا يمكن لمزود خدمة المصادقة الإلكترونية أو أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة إلا ما كان منها ضروريا لإبرام العقد وتحديد محتواه وتنفيذ وإعداد وإصدار الفاتورة.

عن العملاء الذين يبادرون في الحصول على شهادات التصديق، وعن حجم معاملاتهم وأسرارهم التجارية التي تساوي بالنسبة لهم الكثير ماديا ومعنويا، لذلك فإنه يحظر عليه استخدامها في غير الغرض الذي قدمت له من أجله[1]، وهذا ما أكده المشرع في المادة 42 من القانون 07/18 التي تحظر على مؤدي خدمات التصديق الإلكتروني الذي يجمع معطيات شخصية لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني أن يقوم بمعالجتها لأغراض أخرى غير تلك التي جمعت من أجلها، وهنا نجد أن المشرع استعمل مصطلح "المعالجة" وبذلك يكون قد وسع من دائرة الأنشطة غير المشروعة التي يمكن أن تنصب على المعطيات الشخصية المجمعة، لتشمل كافة الأفعال التي تدخل في إطار المعالجة ولم يقصرها على فعل الاستعمال فقط.

ب) الركن المعنوي: يقوم الركن المعنوي لهذه الجريمة لمجرد القصد الجنائي العام دون القصد الجنائي الخاص، فهي من الجرائم العمدية التي تقتضي أن يكون الجاني عالما بأن ما يقوم بجمعه من معطيات عن الشخص المعني صاحب شهادة التصديق الإلكتروني مبالغ فيها وغير ضرورية لمنح هذه الشهادة، أو علمه بأنه يقوم باستخدام المعطيات التي جمعها عن هذا الاخير في غير غرضها القانوني، وتنصرف إرادته الواعية للقيام بهذه الأفعال.

2-3-2) العقوبة المقررة قانونا: بموجب المادة 71 من القانون 04/15 "يعاقب المشرع على هذه الجريمة بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 200,000(مائتي ألف دج) إلى 01 مليون دج، أو بإحدى هاتين العقوبتين".

وبالنسبة للشخص المعنوي فإن عقوبته الأصلية حسب المادة 75 من نفس القانون هي الغرامة التي تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ومن ثم تكون الغرامة 05 مليون دج بالإضافة إلى العقوبات التكميلية المحددة في نص المادة 18 مكرر من قانون العقوبات.

ثالثا: جرائم الإعتداء على المعطيات الشخصية في قانون التجارة الإلكترونية.

لقد بدأت التجارة الإلكترونية انتشارها في السنوات الأخيرة من القرن الماضي، سيما في أوروبا والولايات المتحدة الأمريكية، حيث يكون لكل من المتعاقدين أن يتخذ له موقعا على شبكة الأنترنت للإعلان عن السلع التي يقوم بإنتاجها، وذلك لتسويقها و التعاقد بشأنها، حيث يتم الإتصال مباشرة بين الطرفين عن طريق الأنترنت وسداد قيمة السلعة أو الخدمة عن طريق التحويلات البنكية، ثم بتسلم المستهلك البضاعة إذا كان المبيع ماديا أو يتسلمها بالطرق الإلكترونية إذا كان محل التعاقد بخدمات أو استشارات قانونية أو طبية.[2]

ونظرا لأهمية موضوع التجارة الإلكترونية فقد صدرت مواثيق وتشريعات تنظم هذا الموضوع، فالأمم المتحدة في لجنة القانون التجاري الدولي – ونيسترال- أصدرت عام 1996 قرار باعتماد القانون النموذجي

[1] عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض، 2012، ص 115.
[2] مدحت عبد الحليم رمضان، مرجع سابق، ص 09.

المتعلق بالتجارة الإلكترونية، وفي أوروبا أصدر المجلس الأوروبي التوجيه رقم CE/2000/31 المتعلق بالتجارة الإلكترونية، وفي فرنسا صدر القانون المتعلق بالمبادلات والتجارة الإلكترونية.[1]

والمشرع الجزائري لم يقف بمعزل عن ذلك التطور الحادث في مجال التنمية التكنولوجية بوجه عام والتجارة الإلكترونية بوجه خاص، حيث كان الحرص على إصدار القانون رقم 05/18 المتعلق بالتجارة الإلكترونية المؤرخ في 2018/05/10.[2]

ولقد اهتم المشرع الجزائري في هذا القانون كغيره من التشريعات المقارنة بتوفير حماية للمعطيات الشخصية التي أصبحت القوة الدافعة لجزء كبير من النشاط التجاري عبر شبكات الأنترنت، ففي هذه البيئة يبرز أمن المعطيات بوصفه مصدر قلق متزايد للحكومات والمشاريع التجارية والمستهلكين على السواء، ومن الممكن أن تتزايد حدة هذه الشواغل نتيجة تحليلات البيانات الضخمة التي تهدف إلى فهم سلوك المستهلكين والتأثير فيه من أجل تحقيق الأرباح التجارية.[3]

وفي هذا الإطار نصت المادة 26 من القانون 05/18 على أنه ينبغي للمورد الإلكتروني[4] الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات للزبائن، وللزبائن المحتملين ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية، كما يحرص على ضرورة حصوله على موافقة المستهلكين قبل جمع معطياتهم، بالإضافة إلى ضمانه أمن نظم المعلومات وسرية البيانات.

وكذلك منعت المادة 31 من نفس القانون استعمال المعطيات الشخصية لأي شخص طبيعي من أجل إرسال رسائل عن طريق الاتصالات الإلكترونية في إطار الاستبيان المباشر دون موافقته المسبقة، ثم رافق هذه المادة بنص تجريمي يعاقب على الإخلال بأحكامها، في حين لم يجرم الإخلال بأحكام المادة 26 المذكورة أعلاه، مما قد يحد من توفير الحماية الجزائية الفعالة للمعطيات الشخصية في إطار التجارة الإلكترونية، وعلى هذا الأساس يمكن القول أن المشرع الجزائري يوفر الحماية الجزائية للمعطيات الشخصية في قانون التجارة الإلكترونية 05/18من خلال تجريم فعل الإستبيان المباشر أو كما يسميه في قانون 07/18 المتعلق بحماية المعطيات الشخصية بالاستكشاف المباشر دون الموافقة المسبقة للشخص المعني.

وقبل الخوض في معرفة الأركان التي تقوم عليها هذه الجريمة لا بأس أن نوضح فكرة الاستبيان أو الاستكشاف المباشر، la prospection directe.

---

[1] عبد الفتاح بيومي حجازي، التجارة الإلكترونية، مرجع سابق، ص 21.

[2] القانون 05/18 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 صادرة بتاريخ 16 ماي 2018.

[3] مذكرة مقدمة من أمانة الأونكتاد في إطار إجتماع للخبراء بشأن قوانين الفضاء الإلكتروني وتنظيمه من أجل تعزيز التجارة الإلكترونية، دراسات الحالات الإفرادية والدروس المستفادة، لجنة الاستثمار والمشاريع والتنمية، جنيف 25، 27 مارس 2015، ص 14. متوفر على الموقع:
https://unctad.org/ar/docs/dom20071_ar.pdf

[4] عرفت المادة 06 من الاقنون 05/18 المتعلق بالتجارة الإلكترونية المورد الإلكتروني بأنه "كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الإلكترونية".

ولضبط مفهوم هذا المصطلح والوصول إلى المعنى الدقيق له وجب التعرض إلى أهم ما جاء من تعاريف له، حيث عرف على أساس أنه الاتصال المباشر مع مستهلكين مستهدفين بعناية، غالبا في شكل فردي وعلى أساس تفاعلي[1]، وكذلك تم تعريفه بأنه مسار تسويقي يحمل الصبغة الشخصية من خلال الاستغلال المنظم للمنظمات الفردية.[2]

ويستخدم هذا الأسلوب في البحث والتفتيش أو التنقيب عن الزبائن المرتقبين من خلال تكوين ملفات معلوماتية لهؤلاء، وهذا بالوصول إلى المعطيات الشخصية لهم، فإضافة إلى أسمائهم وعناوينهم و أرقام هواتفهم، هناك عدة معطيات شخصية أخرى يتم استكشافها والتنقيب عنها من خلال الإتصالات الإلكترونية التي يقومون بها عبر شبكات الأنترنت، كنمط الاستهلاك، آراء الزبون المحتمل وميولاته... وبمعالجة هذه المعطيات يتم تجزئة الزبائن وتصنيفهم، وتوليد عروض تجارية مختلفة تتعلق بخصائص كل صنف منهم لاستهدافهم بها.[3]

1) أركان الجريمة: تنص المادة 40 من قانون التجارة الإلكترونية على أنه يعاقب بالغرامة من 50,000 إلى 500,000 دج كل من يخالف أحكام المادة 31 من هذا القانون، وتنص هذه الأخيرة على أنه يمنع ستبيان المباشر اعتمادا على إرسال الرسائل عن طريق الإتصالات الإلكترونية باستعمال معلومات شخص طبيعي بأي شكل من الأشكال لم يبد موافقته المسبقة لتلقي استبيانات مباشرة عن طريق الإتصال الإلكتروني.

أ) الركن المادي: تقوم جريمة استعمال معطيات شخصية بطريقة غير مشروعة للاستبيان المباشر دون موافقة الشخص المعني بسلوك إجرامي يتمثل في إرسال رسائل إلكترونية عبر شبكات الأنترنت أو أي وسيلة اتصال إلكترونية أخرى وبأي شكل، كإعلانات تجارية مثلا تستهدف أشخاصا طبيعيين معينين عن طريق استعمال معطياتهم الشخصية، دون إبدائهم لموافقتهم المسبقة لتلقي الاستبيانات المباشرة.

ومن ثم يستمد هذا الفعل عدم مشروعيته من عدم أخذ رأي الشخص المعني وإبداء رغبته في تلقي هذه ستبيانات من عدمها، وهذا ما تؤكده المادة 32 من نفس القانون التي تفرض على المورد الإلكتروني أن يضع منظومة إلكترونية يسمح من خلالها لكل شخص بالتعبير عن رغبته في عدم تلقي أي إشهار منه عن طريق الإتصالات الإلكترونية.

والملاحظ أنه خلافا للقواعد العامة التي تلقي عبئه على الشخص المعني الذي يلزمه وفقا لهذه القواعد في حالة النزاع أن يثبت أن المورد الإلكتروني قد قام باستعمال معطياته الشخصية في إرسال استبيانات مباشرة دون موافقته، لكن المشرع في هذه الجريمة نقل عبئ الإثبات على الجاني (المورد الإلكتروني) والذي

[1] Philipe Kotler, Gary Armstrong, principles of marketing, Pearson 14th edition, USA, 2012 P 496, disponible sur le site: www.baixardx.com

[2] Pierre Desmet, Marketing Direct, consepts et méthodes, Dunoet, 3ème édition mars 2005, P 7 disponible sur le site : https://www.livre.fnac.com

[3] أنظر في هذا المعنى خليل وليد، دور التسويق المباشر في تحقيق ولاء الزبون، مذكرة ماجيستار في العلوم التجارية، تخصص دراسات وبحوث تسويقية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة فرحات عباس، سطيف، 2016، ص 8.

عليه أن يثبت أن إرسال الإشهارات الإلكترونية قد خضع لموافقة الشخص المعني، وهذا في اعتقادنا لتعلق المسألة بجوانب تقنية مرتبطة بالمنظومة المعلوماتية التي بحوزته والتي لا يسع الشخص المعني الإطلاع أو الوصول إليها.

ب) الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية القائمة على القصد الجنائي، الذي يتحقق في حالة ما إذا كان المورد الإلكتروني على علم بأنه يقوم بإرسال استبيانات مباشرة إلى أشخاص طبيعيين مستعملا معطياتهم الشخصية دون موافقتهم المسبقة، وتنصرف إرادته إلى إتيان هذا الفعل رغم ذلك.

وهذه الجريمة تقوم لمجرد القصد الجنائي العام ولا عبرة للقصد الجنائي الخاص، الذي نعتقد أنه أمر مفترض يتعلق بتحقيق الجاني للربح والفائدة من خلال كسب عملاء وزبائن محتملين.

2) العقوبة المقررة قانونا: يعاقب على جريمة استعمال المورد الإلكتروني للمعطيات الشخصية بطريقة غير مشروعة في الاستبيان المباشر حسب المادة 40 من القانون 05/18 بالغرامة من 50,000 دج إلى 500 ألف دج

أما بالنسبة للشخص المعنوي، فطالما لم ينص المشرع في هذا القانون على معاقبة هذا الأخير على الجرائم الواردة فيه، فإنه بحسب المادة 51 مكرر من قانون العقوبات، يكون الشخص المعنوي معفى من المسؤولية الجزائية في هذه الجريمة.

الفرع الثالث: أحكام خاصة للمسؤولية الجزائية عن الجرائم الماسة بالمعطيات الشخصية.

تثير المسؤولية الجزائية عن الجرائم التي تشكل اعتداء على المعطيات الشخصية مسألتان تبدوان في غاية همية، تتعلق الأولى بأحكام المعاقبة على الشروع في هذه الجرائم، وأما الثانية فتتعلق بالمسؤولية الجزائية للشخص المعنوي عند ارتكابه لمثل هذه الجرائم.

أولا: أحكام المعاقبة على الشروع في جرائم المساس بالمعطيات ذات الطابع الشخصي.

يحمل الشروع في طياته كل معاني الإعتداء على المصلحة التي يحميها القانون، لكنه إذا أوقف أو خاب أثره فإنه يتحول من صورة الإعتداء الفعلي إلى صورة اعتداء محتمل[1]، وإذا كانت الجريمة لا تكتمل إلا بتوافر الفعل المادي، فهذا لا يعني أنه من الضروري أن يترتب على هذا الفعل نتيجة تلحق الضرر بتلك المصلحة المحمية حتى تكون الجريمة قابلة للجزاء[2]، ومن ثم نخلص إلى أن الشروع يفترض توافر كل عناصر الجريمة التامة ما عدا النتيجة.

وعلى هذا الأساس كيف يمكن تصور الشروع في الجرائم الماسة بالمعطيات الشخصية، وهي فكرة نتطرق إليها من خلال تبيان القواعد العامة للشروع، ثم إسقاط ذلك على هذا النوع من الجرائم.

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول الجريمة، ديوان المطبوعات الجامعية، 2009، ص 94.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر، الطبعة الثامنة، 2009، ص 94.

1) القواعد العامة للشروع:

إن الغاية من التجريم هي الدفاع عن المجتمع من ظاهرة الجريمة، ولتحقيق هذه الغاية اعتنى القانون بحماية المصالح الأساسية في المجتمع، وعلى هذا كانت الجرائم على نوعين: جرائم الضرر وهي الجرائم التي تحدث نتائج ضارة، وجرائم الخطر وهي التي تهدد أمن المجتمع وتحدث فيه اضطرابا، ولما كان من أهم ما يميز الشروع هو عدم تحقق النتيجة التي قصدها الجاني، فيكون إذن من جرائم الخطر.[1]

ومن العادة ما تمر الجريمة قبل تمامها بمراحل ثلاث، هي مرحلة التفكير ثم تليها مرحلة التحضير وأخيرا مرحلة التنفيذ.

فمرحلة التفكير وتسمى أيضا بالمرحلة النفسية، هي المرحلة التي تنبت أثناءها فكرة الجريمة في ذهن الجاني وتنعقد لديه النية على ارتكابها، حيث تكون الجريمة مجرد فكرة قد تدوم لحظات وقد تستمر لأشهر طويلة وأحيانا يعدل عنها صاحبها، وهي في جميع الأحوال لا عقاب عليها طالما أن التفكير في ارتكاب الجريمة لا يتعدى حيز النوايا وما يدور في ذهن الجاني من أفكار دون أن يكون له أي مظهر خارجي يشكل خطرا، بحيث تبقى الفكرة حبيسة في ذهن الجاني ونفسه ولم تخرج إلى العالم الخارجي[2]، لأن القانون لا يعاقب على النوايا وسرائر الأنفس، وإنما يعاقب على الأفعال التي يبرزها صاحبها إلى حيز الوجود بسلوك إيجابي أو بموقف سلبي.[3]

أما مرحلة التحضير فهي المرحلة التي تعقب الإقتناع بالجريمة والتصميم عليها، فمتى تستقر فكرة الجريمة في نفس الفاعل، يبدأ بنشاط ظاهر للإعداد لها، وهي تتخذ ثوبا ماديا يقتضي من الجاني مباشرة الأعمال المادية استعدادا لتنفيذ الجريمة وهي ما يعرف بالأعمال التحضيرية، وهي تلك الأعمال التي يتهيأ بها الجاني لتنفيذ جريمته، وبذلك تكون مرحلة تتوسط التفكير في الجريمة والبدء في تنفيذها، كمن يقوم بشراء البرامج الخبيثة كالفيروسات لاستعمالها في كسر نظام الحماية للتمكن من الولوج إلى النظام المعلوماتي أو تصميم برنامج اختراق، أو برامج اعتراض لكود فك الشيفرة...

وهذه المرحلة لا تنطوي على درجة من الخطورة، طالما أن الجريمة لم تدخل طور التنفيذ، وبالتالي لا تتطلب تدخل المشرع للتجريم والعقاب، وذلك بهدف إفساح المجال أمام الجاني ليتراجع عن فعله ويعدل عن نيته الإجرامية، كما أن هذه الأفعال إذا لم تكن في حد ذاتها جريمة فهي ليست على هذا القدر من الخطورة والأهمية إلى الحد الذي يستدعي تدخل المشرع بالتجريم والعقاب، فهي وإن كانت تمثل مظهرا خارجيا ماديا للتصميم على الجريمة، إلا أنها لا تدخل في تنفيذها، ولا تربطها إلا رابطة فكرية في ذهن الجاني، بالإضافة إلى أنها لا تفيد بصورة قطعية عن اتجاه القصد بذاتها لدى الجاني.[4]

---

[1] خيري أبو العزايم فرجاني، نطاق الشروع في الجريمة بدون دار نشر وتاريخ النشر، ص 12.

[2] خيري أبو العزايم فرجاني، مرجع نفسه، ص 17.

[3] عبود السراج، شرح قانون العقوبات القسم العام، الجزء الأول (نظرية الجريمة)، محاضرات في كلية الحقوق جامعة دمشق، ص 129، متوفر على الموقع https://www.elibrary.mediu.edu.my/books/MAL11484.pdf

[4] أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، قانون العقوبات ونطاق تطبيقه، التجريم والاباحة، الجريمة -المجرم -العقوبة، الطبعة السادسة، دار النهضة العربية، القاهرة 2015، ص 338.

أما إذا أصبحت هذه الأعمال التحضيرية تشكل خطرا على المصالح التي يتوجب حمايتها، فإن المشرع يعتبرها حينئذ جريمة مستقلة بذاتها ويعاقب عليها، كما هو الحال لبعض الأفعال التي نصت عليها المادة 394 مكرر2 كالبحث والتصميم، فهي إن كانت تبدو بطبيعتها أعمالا تحضيرية، إلا أن المشرع قد اعتبرها جرائم قائمة بذاتها،[1] ويعتبرها المشرع كذلك أي جريمة مستقلة بذاتها، حتى ولو لم ترتكب الجريمة التي تقع هذه الأفعال تحضيرا لها.

وأما مرحلة التنفيذ فهي المرحلة التي تنصرف فيها إرادة الجاني إلى البدء في تنفيذ النشاط الإجرامي المكون للركن المادي، فإذا ما أتم الجاني جميع الأفعال المكونة للجريمة وحقق نتيجتها فإنه يكون قد ارتكب جريمة تامة، أما إذا لم يتم الفاعل جميع العناصر اللازمة لارتكاب جريمته، حيث لم تتحقق النتيجة لأسباب لا دخل لإرادته فيها كان الفعل شروعا[2]، فالجاني في هذه المرحلة يكون قد بادر وأقدم بالفعل على تنفيذ الجريمة وصار قاب قوسين أو أدنى من إتمامها، لولا تدخل عامل خارجي لا شأن لإرادته فيه حال دون ذلك، ومن ثم كان الشروع مرحلة تتوسط مراحل الجريمة فهي تالية للتحضير لها وسابقة على تمامها.

وتجريم الشروع هو خروج عن القواعد العامة التي تقتضي اكتمال العناصر المكونة للركن المادي، لكن المشرع تجاوز هذه القواعد وجرمه لأنه سلوك يتضمن عدوانا على حق يحميه القانون، وفيه تهديد لمصالح اجتماعية على درجة من الخطورة يتعذر على المشرع السكوت عنها، فغالبية التشريعات الجزائية لا تتدخل بالعقاب إلا عندما يبدأ الجاني في تنفيذ جريمته، أما الأعمال السابقة على ذلك فإنها تظل بمنأى عن العقاب، ومن ثم كان البدء في التنفيذ هو الحد الفاصل بين الإباحة والتجريم.[3]

لذلك فكر المشرع الجنائي الحديث في تحديد حالة الشروع وبيان أركانها عندما ظهرت له خطورتها، ووجد من اللازم معاقبة صاحبها عنها، فجاءت جميع قوانين العقوبات الحديثة تتضمن تعريفا للشروع يبين الأركان اللازمة لتحققه[4]، وكان هذا مسلك قانون العقوبات الجزائري، حيث جاءت المادة 30 منه معرفة للشروع ومبينة أركانه بقولها أن الشروع هو كل محاولة لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها، تؤدي مباشرة إلى ارتكابها، تعتبر كالجناية نفسها إذا لم تتوقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها، حتى لو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها.

ومن هذا التعريف يظهر لنا أنه لتحقق حالة الشروع لا بد من توافر الأركان الثلاثة التالية:

الركن الأول وهو البدء في التنفيذ: إن التمييز بين الأعمال التحضيرية والأعمال التي تعتبر من قبيل البدء في التنفيذ، إذا كان واضحا في بعض الأحوال، إلا أنه دقيق وملتبس فيه في أخرى، حيث تبقى بعض الأفعال متأرجحة بين مرحلتي التحضير والبدء في التنفيذ، وهي ما تسمى بالحالات الحدية التي تظهر

[1] رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة، مرجع سابق، ص 351.

[2] عبود السراج، مرجع سابق، ص 130.

[3] سمير الشناوي، الشروع، دراسة مقارنة، دار النهضة العربية، القاهرة 1971، ص 153.

[4] علي حسين خلف، سلطان عبد القادر الشناوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية بغداد، 2015، ص 161.

ضرورة وجود ضابط أو معيار يمكن من خلاله التمييز بين الأعمال التحضيرية وتلك التي تحقق البدء في التنفيذ.[1]

لذلك فقد انقسم الفقهاء حول تحديد الضابط أو المعيار الذي بواسطته يمكننا أن نميز الأعمال التحضيرية عن أعمال الشروع إلى مذهبين:

- المذهب الموضوعي: يرى أنصاره أن الشروع يتطلب بدءا في تنفيذ الفعل المادي المكون للجريمة ويصيب به الجاني الركن المادي الذي يشترطه القانون لوقوعها[2]، فالعامل المهم عند هؤلاء هو السلوك الإجرامي الذي يرتكب وما يترتب عليه من ضرر أو ما يمثله من خطر، فهم يعتدون بالسلوك ذاته.

وقد تعرض هذا الرأي إلى الإنتقاد على أساس أنه يتعارض مع مقتضيات الدفاع الإجتماعي ويؤدي في كثير من الحالات إلى إفلات الجاني من المسؤولية رغم كونه شارعا في الجريمة.[3]

- المذهب الشخصي: ويذهب أنصاره إلى القول بأن قيمة الوقائع المادية التي يرتكبها الفاعل إنما تكمن في الدلالة على نفسية فاعلها، فليس الفعل إلا مؤشرا أو قرينة على خطورة الفاعل، فحسبهم أن العقاب على الشروع لا يقصد به مقابلة للسلوك الإجرامي الذي قام به الجاني، لان السلوك عندهم لم يحقق النتيجة، وإنما الغرض من العقاب هو مواجهة خطورة الجاني التي كشف عنها سلوكه[4].

ومن ثم كان الشروع عند أصحاب هذا المذهب هو السلوك الذي يؤدي حالا ومباشرة إلى الجريمة وأصبح عدوله عنها أمرا غير محتمل.

والظاهر أن المشرع الجزائري من خلال نص المادة 30 من قانون العقوبات قد أخذ بالمذهب الشخصي كمعيار لتحديد البدء في التنفيذ، متأثرا في ذلك بالإتجاه الغالب في معظم التشريعات وعلى رأسها المشرع الفرنسي[5].

الركن الثاني وهو قصد ارتكاب الجريمة: ومضمونه انصراف إرادة الجاني إلى ارتكابها وفق السلوك الذي كان احتمال وقوعها به قويا.

الركن الثالث وهو عدم إتمام الجريمة لظروف خارجة عن إرادة الفاعل، ويكون هذا بأحد الأمرين، إما أن يوقف تنفيذ السلوك الذي هدف به الجاني تحقيق الجريمة، أو أن يكمل الجاني سلوكه الإجرامي اللازم لتحقيق الجريمة ولكنها لا تتحقق ويخيب أثرها لسبب خارج عن إرادته، ومن ثم فإن الفيصل في الإهتداء إلى الشروع هو عدم تحقق النتيجة، وتكون هذه الأخيرة أي النتيجة هي أساس الفرق بين الشروع والجريمة التامة، والتي لم تتحقق لظروف خارجية لا يد لإرادة الجاني فيها، وتجعل النشاط الإجرامي

[1] علي حسين الخلف، سلطان عبد القادر الشناوي، مرجع سابق، ص 162.
[2] عبد الله سليمان، مرجع سابق، ص 170.
[3] عبد الله سليمان، نفس المرجع، ص 172.
[4] عبود السراج، مرجع سابق، ص 132.
[5] أحسن بوسقيعة، الوجيز في القانون العام، مرجع سابق، ص 96.

يتوقف عند حد سابق على حد تمام الجريمة[1]،و لذلك فإن الشروع جريمة ناقصة، وهذا النقصان لا يعتري الركن المعنوي، لأن القصد ثابت لدى الفاعل وإنما يعتري الركن المادي.

2) مدى العقاب على الشروع في الجرائم الماسة بالمعطيات ذات الطابع الشخصي:

بعد عرض أحكام الشروع على النحو السابق بيانه ومعرفة موقف المشرع من ذلك، إلا أنه فيما يتعلق بجرائم الإعتداء على المعطيات ذات الطابع الشخصي، يبدو أن الأمر ليس بذات البساطة، حيث أن كل هذه الجرائم ذات وصف جنحي، وبالتالي فما كان ليعاقب على الشروع فيها لولا تدخل المشرع بالعقاب عليه صراحة بنص المادة 73 من القانون 07/18 وكذلك المادة 394 مكرر من قانون العقوبات، ذلك أن الشروع في الجنح لا يعاقب عليه إلا بناء على نص صريح في القانون[2]، وعقاب المشرع على الشروع في هذه الجرائم ينم على رغبته في تغطية أكبر قدر ممكن من العدوان على المعطيات الشخصية.

غير أن ذلك لا يعني تصور الشروع في جميع الجرائم الماسة بالمعطيات الشخصية، لأن أغلبها من الجرائم الشكلية ذات السلوك المجرد، والتي تتميز بانعدام النتيجة فيها، وتكتمل الجريمة فيها لمجرد حصول السلوك أو النشاط الإجرامي[3]، ومن ثم فإعمالا لرواسي القواعد العامة، فانه لا يكون هناك مجال للحديث عن الشروع في هذه الجرائم، فلكي يكون هناك مجال للحديث عن خيبة الأثر، لا بد أن يكون للفعل نتيجة ولا تتحقق لظروف خارجة عن إرادة الفاعل، أما الجرائم الشكلية أو كما يسميها الفقه أيضا بجرائم الخطر، إما أن تقع لمجرد ارتكاب الفعل فتعد جريمة تامة به، وإما ألا تقع،[4]فإسقاطا على جريمة معالجة معطيات شخصية دون ترخيص مسبق من السلطة الوطنية أو دون تصريح لديها، أو جريمة معالجة هذه المعطيات دون موافقة الشخص المعني، أو جريمة إفشاء المعطيات الشخصية وغيرها من الجرائم الماسة بالمعطيات الشخصية التي تتميز بانعدام النتيجة وتتم لمجرد إتيان الفعل، فإنه لا يمكن تصور حدوث الشروع فيها، إذ وهي على هذا النحو لا مجال للتفرقة فيها بين الشروع والجريمة التامة، وذلك لأن ما يكفي لأن يوصف ماديا في ظل القواعد العامة بأنه شروع، يكفي في نفس الوقت قانونا لأن يكون جريمة تامة، بمعنى أن الشروع يبدأ من لحظة انتهاء الأعمال التحضيرية ويرتقي في نفس اللحظة إلى الجريمة التامة،[5] بمعنى أن هذه الجرائم تختلف عن بقية الجرائم بأن لا شروع فيها، لأن نظرية الشروع تتطلب أن يكون للفعل نتيجة لكي لا يخيب أثرها أو عدم تحققها لظروف خارجة عن إرادة الفاعل، ولا يمكن لها أن تكون موقوفة أو خائبة، لأنها تتحقق بمجرد البدء بتنفيذها ولا يشترط حصول النتيجة فيها.

---

[1] خيري أبو العزايم فرجاني، مرجع سابق، ص 45.

[2] تنص المادة 31 من قانون العقوبات أن المحاولة في الجنح لا يعاقب عليها إلا بناء على نص صريح في القانون"

[3] آدم سميان، رباب الغريري، الأوصاف الخاصة بالجرائم مبكرة الإتمام، مقال منشور في مجلة جامعة تكريت كلية الحقوق السنة الثانية المجلد 02، العدد 02 الجزء الأول، 2017، ص 9. متوفر على الموقع:https://iasj.net/iasj?func=fulltext&aId=155801 أطلع عليه في:2020/05/20

[4] رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة الآلية، مرجع سابق، ص 355.

[5] عبد الفتاح مصطفى الصيفي، قانون العقوبات، القسم الخاص- الجرائم الماسة بأمن الدولة، منشأة المعارف، الاسكندرية، 2000، ص 34.

ويسعفنا في هذا الرأي ما أشار إليه التقرير التفسيري لاتفاقية بودابست حول صعوبة تصور الشروع في بعض الجرائم التي تستهدف المعطيات من الناحية النظرية.[1]

كذلك تبقى مسألة التمييز بين أعمال البدء في التنفيذ والأعمال التحضيرية من المسائل الصعبة عندما يتعلق الأمر بهذه الجرائم، حيث جرم المشرع أفعالا تعتبر من قبيل الأعمال التحضيرية بوصفها جرائم مستقلة، كعملية البحث أو التصميم في جرائم التعامل في معطيات شخصية غير مشروعة نظرا لدرجة خطورتها وتأثيرها على المصلحة المراد حمايتها، وفي هذا استثناء على القواعد العامة للشروع التي لا عقاب فيها على الأعمال التحضيرية، إذ يمكن العقاب على هذه الأعمال بوصفها جريمة قائمة بذاتها إذا كانت تنطوي على خطر يهدد بعض المصالح أو الحقوق التي يرغب المشرع في حمايتها على نحو أشمل، أو كانت هذه الأعمال تدل على خطورة خاصة لدى القائم بها، أو كانت تنطوي على أخطار إجتماعية.[2]

أما عن مسألة العقاب على فعل الشروع فإن جميع القوانين العقابية تتفق على عقاب الشروع، غير أنها تختلف في تقدير خطورته وبالتالي مقدار العقوبة المخصصة له.

فمن القوانين ما يحدد للشروع عقوبة أخف من عقوبة الجريمة التامة، على اعتبار أن الضرر لم يتحقق كله، ومنها ما يفرض للشروع عقوبة الجريمة التامة وبالتالي فهي تساوي في العقاب بين الشروع في الجريمة وبين الجريمة التامة نفسها، ومنها المشرع الجزائري، حيث أن المادة 73 من القانون 07/18 تنص على أنه يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القانون بنفس العقوبات المقررة للجريمة التامة، وكذلك فعلت المادة 394 مكرر 7 من قانون العقوبات حيث يعاقب بموجبها على الشروع في ارتكاب الجنح المنصوص عليها في القسم المتعلق بهذه الجرائم بنفس العقوبات المقررة للجنحة ذاتها.

ثانيا: أحكام المسؤولية الجزائية للشخص المعنوي عن جرائم المساس بالمعطيات الشخصية:

يسأل عن الجرائم الماسة بالمعطيات ذات الطابع الشخصي كل من الشخص الطبيعي والشخص المعنوي على حد سواء، ذلك أن الفاعل في هذه الجرائم قد يكون مسؤولا عن المعالجة، أو معالجا من الباطن أو مورد خدمات الأنترنت، أو مزود خدمة التصديق الإلكتروني أو موردا إلكترونيا أو يكون من الغير، وفي كل هذه الأحوال لا يخرج عن كونه إما شخصا طبيعيا أو شخصا معنويا.

وإذا كانت أحكام المسؤولية الجزائية عن هذه الجرائم بالنسبة للشخص الطبيعي لا تثير أي إشكال، فإنها بالنسبة للشخص المعنوي تستوجب الإلتفات إليها بنوع من التوضيح سواء من حيث تحديد نطاق الأشخاص المعنوية المسؤولة جزائيا، أو من حيث شروط هذه المسؤولية.

1) تحديد الأشخاص المعنوية المسؤولة جزائيا عن الجرائم الماسة بالمعطيات الشخصية: إن نجاح مبدأ إقرار المسؤولية الجزائية للشخص المعنوي يقتضي تحديد من هم الأشخاص المعنويين الذين يخضعون لهذه المسؤولية الجزائية، وانطلاقا من النصوص القانونية التي تعرف المسؤول عن المعالجة، أو

[1] أنظر التقرير التفسيري لاتفاقية الجريمة الإلكترونية الموقعة في بودابست بتاريخ 23 نوفمبر 2001 بمناسبة المؤتمر الدولي لحماية الجريمة الإلكترونية، الفقرة 120 ص19.

[2] فتحي سرور، الوسيط في قانون العقوبات، القسم العام، مرجع سابق، ص 338.

المعالج من الباطن أو مزودي الخدمات بأنهم كل شخص طبيعي أو معنوي عام أو خاص، فهذا يعني أن النصوص التجريمية التي تخاطب هؤلاء عن أفعال الإعتداء على المعطيات الشخصية ترتب المسؤولية الجزائية على كل من الشخص المعنوي العمومي أو الخاص على حد سواء.

إلا أنه وفي نفس الوقت نجد أن المشرع الجزائري عندما أقر المسؤولية الجزائية للشخص المعنوي في المادة 51 مكرر من قانون العقوبات فإنه استثنى الأشخاص المعنوية العامة من الخضوع لهذه المسؤولية الجزائية، فما مدى إذن إمكانية مساءلة الأشخاص المعنوية العامة جزائيا عن الجرائم الماسة بالمعطيات الشخصية.

تنص المادة 70 من القانون 07/18 على أن الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون، يعاقب وفقا للقواعد المنصوص عليها في قانون العقوبات.

وبالرجوع إلى المادة 51 مكرر من قانون العقوبات نجدها تنص على أنه باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه، من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

وعليه فإن المشرع استبعد صراحة كل الأشخاص المعنوية العامة من نطاق خضوعها للمسؤولية الجزائية بصفة مطلقة، ولم يترك أي مجال لإمكانية مساءلتها جزائيا، وقصرها فقط على الشخص المعنوي الخاص.*

ومن ثم فإذا كان فعل الإعتداء على المعطيات الشخصية المشكل للجرم صادرا عن أحد الأشخاص المعنوية العامة، فإن المسؤولية الجزائية تقع على الموظف الذي قام بالفعل مباشرة، أو على المسؤول عن الإدارة التابعة للشخص المعنوي العام، خاصة إذا كان هو الآمر بالمعالجة للمعطيات الشخصية[1]، فليس هناك ما يمنع من المساءلة الجزائية لممثلي الشخص المعنوي العام كأشخاص طبيعيين.[2]

أما الأشخاص المعنوية الخاصة* فهي جميعها مسؤولة جزائيا عن الجرائم الماسة بالمعطيات الشخصية دون استثناء مهما كان هدفها أو شكلها.

---

*أما بالنسبة للمشرع الفرنسي حسب المادة 121-1 من قانون العقوبات فقد اعتبر أن الأشخاص المعنوية العامة مسؤولة جزائيا عن الجرائم التي يحدد القانون المسؤولية الجزائية لها، ومنها فئة الجرائم المتعلقة بالمساس بالمعطيات الشخصية، باستثناء الدولة وفروعها، في حين اقتصر المسؤولية الجزائية للجماعات الإقليمية (الولاية والبلدية) فقط على الجرائم التي ترتكب أثناء ممارستها لأنشطة قابلة لأن تكون موضوع اتفاقيات تفويض مرفق عام ،وهي تعني أنشطة الخدمات العامة التي يمكن للجماعات الإقليمية المكلفة بها أساسا ألا تقوم بإدارتها بذاتها وإنما تفوض لإدارتها شخصا آخر، سواء كان خاضعا للقانون العام أو للقانون الخاص، أما باقي الأشخاص المعنوية الأخرى فتكون مسؤولة جزائيا على قدم المساواة مع الأشخاص المعنوية الخاصة، ولا يفرق المشرع الفرنسي بينها .

[1] طباش عز الدين، مرجع سابق، ص 42.

[2] محمود هشام محمد رياض، المسؤولية الجنائية للشخص المعنوي، دراسة مقارنة رسالة دكتوراه كلية الحقوق، جامعة القاهرة، 2000، ص 111

* تعرف الأشخاص المعنوية في القانون الخاص بأنها تلك الأشخاص أو الهيئات التي تقوم بأغراض تهدف إلى تحقيق مصالح أفراد معينين أو مصالح الدولة بصفتها شخصا عاديا لا شخصا صاحب سلطة، تؤسس لغايات خاصة تجارية أو مدنية وتخضع مبدئيا للقانون الخاص،

2) شروط المسؤولية الجزائية للشخص المعنوي: تختلف المسؤولية الجزائية للشخص المعنوي عنها بالنسبة للشخص الطبيعي، ذلك أنها مسؤولية مشروطة بشروط محددة من أجل قيامها، وإذا تخلف شرط من هذه الشروط لا تقوم هذه المسؤولية، وهي أن ترتكب الجريمة من طرف شخص طبيعي يملك حق التعبير عن إرادة الشخص المعنوي، وقد أوضحت المادة 51 مكرر من قانون العقوبات وكذلك المادة 2-221 من قانون العقوبات الفرنسي أن الشخص المعنوي يكون مسؤولا جزائيا عن الجرائم التي ترتكب من طرف أجهزته أو ممثليه الشرعيين، بالإضافة إلى أن ترتكب تلك الأفعال التي تشكل اعتداء على المعطيات الشخصية لحساب هذا الشخص المعنوي، و بالتالي فهما شرطان متلازمان، تقوم المسؤولية الجزائية للشخص المعنوي باجتماعهما معا.[1]

كما تقوم المسؤولية الجزائية للشخص المعنوي على ارتكابه للجرائم الماسة بالمعطيات الشخصية سواء كان مقيما أو غير مقيم على التراب الوطني، ويعد مقيما فوق التراب الوطني الشخص المعنوي المسؤول عن معالجة المعطيات الشخصية الذي يمارس نشاطا بالتراب الجز ائري في إطار منشأة أيا كان شكلها القانوني، أما بالنسبة للشخص المعنوي غير المقيم فوق التراب الوطني فيلزم لقيام المسؤولية الجزائية أن يلجأ من أجل معالجة المعطيات ذات الطابع الشخصي إلى استعمال وسائل آلية أو غير آلية توجد فوق التراب الوطني باستثناء تلك المعالجات التي تستعمل لأغراض العبور فوق التراب الوطني.[2]

3) العقوبات المقررة للشخص المعنوي: وفي الأخير نشير إلى أن العقوبات التي تطبق على الشخص المعنوي الذي يرتكب إحدى الجرائم المتعلقة بالمساس بالمعطيات الشخصية تخضع لأحكام المادة 18 مكرر من قانون العقوبات، وهي إما عقوبات أصلية أو تكميلية.

فأما العقوبات الأصلية فهي الغرامة التي حسب المادة 55 من القانون 07/18 **تساوي** مرة (1) إلى خمس مرات (5) الحد الأقصى للغرامة المقررة للشخص الطبيعي، فتكون جنحة معالجة معطيات شخصية دون موافقة الشخص المعني مثلا، والتي الحد الأقصى فيها للغرامة المقررة للشخص الطبيعي هي 300 ألف دج، فتكون حينئذ عقوبة الشخص المعنوي المرتكب لهذه الجريمة الغرامة من 600 ألف دج إلى 1,500,000 دج.و حسب المادة 394 مكرر4 من قانون العقوبات هي غرامة مالية **تعادل** خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، ومن ثم فهي تتراوح بين 750.000دج كما في جريمة إتلاف معطيات شخصية المنصوص عليها في المادة 394 مكرر/2 الى أن تصل الى 25 مليون دج كما في جريمة التعامل في معطيات شخصية غير صحيحة حسب المادة 394 مكرر2.

وأما العقوبات التكميلية فهي واحدة أو أكثر من العقوبات التالية:

- حل الشخص المعنوي.

كالشركات التجارية مثلا، أنظر توفيق حسن فرج، المدخل للعلوم القانونية، النظرية العامة للحق، مؤسسة الثقافة الجامعية، الإسكندرية، مصر 1983، ص 282.

[1] Jean Paul Antona, Philippe Colin, François Lenglart, la responsabilité pénale des cadres et des dirigents dans le monde des affaires, Dalloz 1996, p26.

[2] انظر المادة 04 من القانون 07/18.

- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 05 سنوات.

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية، بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

- نشر وتعليق حكم الإدانة.

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 05 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

والسؤال المطروح هل يجوز تطبيق الظروف المخففة المنصوص عليها في المادة 53 من قانون العقوبات على الشخص المعنوي أمام استعمال المشرع صراحة لعبارة "غرامة تعادل"في قانون العقوبات وعبارة "غرامة تساوي" في القانون 07/18 وهما العبارتان التي يمكن أن يفهم منهما مباشرة أن المشرع أراد أن تكون الغرامة التي يحكم بها على الشخص المعنوي لا تقل عن خمس أضعاف الغرامة المقررة للشخص الطبيعي، إذا ما تم التمسك بالتفسير الحرفي أو الضيق للنص.

لقد أخذت المحكمة العليا بالتفسير الحرفي للنص في القضايا المتعلقة بجرائم الشيك حيث تنص المادة 374 و375 صراحة على عقوبة الغرامة التي لا تقل عن قيمة الشيك أو قيمة النقص في الرصيد، حيث استقر قضاؤها على عدم جواز تطبيق الظروفة المخففة على هذه العقوبة وألا ينزل القاضي في تطبيق عقوبة الغرامة على مقدار الشيك.[1]

إلا أننا نرى في هذه المسألة أن نص المادة 53 من قانون العقوبات المتعلقة بظروف التخفيف نص عام ورد ضمن المبادئ العامة في الأحكام الإجرائية الجزائية، ومن ثم يجوز تطبيقه في كل الأحوال على العقوبات الأصلية من حبس أو غرامة، ما لم يستبعد تطبيقه بنص خاص، ومن ثم يكون للقاضي كامل الحرية في إعمال سلطته التقديرية في تقدير العقوبة الجزائية، وله بناء على ذلك أن ينزل عن هذا الحد، ويسلط الغرامة التي يقدر توافقها مع وقائع كل قضية وظروفها ودرجة خطورتها.

[1] انظر قرار المحكمة العليا المؤرخ في 1994/12/04 ملف رقم 122110، القرار المؤرخ في 1997/09/07 ملف رقم 149072، القرار المؤرخ في 1999/07/26 ملف رقم ،190606 القرار المؤرخ في 1999/03/12 ملف رقم 193319، القرار المؤرخ في 1999/09/27 ملف رقم 209673 غير منشورة.

المبحث الثالث: الحماية الجزائية الإجرائية للمعطيات ذات الطابع الشخصي وقواعد الاختصاص القضائي:

إضافة إلى إرساء قواعد قانونية موضوعية لحماية المعطيات الشخصية من الإعتداءات الناتجة عن المعالجة غير المشروعة فإن الحماية القانونية الكاملة للمعطيات ذات الطابع الشخصي تقتضي أيضا ضرورة وضع قواعد إجرائية قادرة على كفالة هذه الحماية.

فإذا استطاع المشرع أن يحيط بالقاعدة الموضوعية من خلال تجريم هذه الإعتداءات الناتجة عن المعالجة غير المشروعة للمعطيات الشخصية، فإن نجاحه يبقى مرهونا بمدى فعالية التنظيم الإجرائي الذي يضمن لتلك القواعد الموضوعية الأثر الفعال لمجابهة هذه الجرائم، ومن ثم فإذا لم توجد القاعدة الإجرائية، فإن القاعدة الموضوعية تبقى مجرد قاعدة نظرية لا تجد سبيلا إلى التطبيق.

إن معالجة المعطيات ذات الطابع الشخصي إما أن تكون يدوية عن طريق ملفات وسجلات ورقية، أو تكون آلية عن طريق نظم المعالجة الآلية للمعطيات الشخصية، وعليه فإذا كانت إجراءات البحث والتحري عن الجرائم الناتجة عن المعالجة اليدوية غير المشروعة للمعطيات الشخصية لا تطرح إشكالات مهمة، فإن هذه الإجراءات تطرح العديد من الصعوبات عندما يتعلق الأمر بالمعطيات المعالجة آليا في نظم المعلومات، وذلك راجع إلى الطابع التقني الذي يتسم به ارتكابها وإلى البيئة الإفتراضية التي تقع فيها، والتي تختلف كليا عن النطاق التقليدي.

ويتجلى ذلك بصورة واضحة في كون الحاسبات الآلية التي تعتمد عليها الكثير من المؤسسات والشركات والهيئات حكومية كانت أو خاصة، لا تمثل بالنسبة لها مجرد وسيلة جديدة، لها من القدرات الهائلة التي تجعلها قادرة على عمليات جمع وتخزين ومعالجة واسترجاع ومقارنة ونقل كم هائل ورهيب من المعطيات الشخصية لأفراد المجتمع في قطاعات مختلفة، بل إن هذه الحاسبات تحمل كذلك في ثناياها كمًا من الأخطار التي تهدد الحق في الخصوصية التي عرفتها الإنسانية من خلال الطرق اليدوية المستخدمة في تسجيل وحفظ المعطيات الخاصة بالأفراد.[1]

وعلى هذا فإن جرائم المعالجة الآلية للمعطيات ذات الطابع الشخصي تعد من قبيل جرائم تقنية المعلومات، والتي ترجع صعوبة إثباتها إلى خصائص التقنية ذاتها، وذلك بالنظر إلى السرعة التي ترتكب بها هذه الجرائم، وسهولة طمس معالمها ومحو آثارها قبل اكتشافها.[2]

وبالتالي يقرر هذا الجانب أن هناك خطورة أساسية ناتجة عن نظم المعالجة الآلية تتمثل في تميزها عن الوسائل التقليدية، مما يلقي على عاتق القائمين على مكافحة الجريمة عبئا شديدا ومهاما جساما تفوق

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشأة المعارف، الإسكندرية، دون سنة نشر، ص 249.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2006، ص 15.

القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث والتحري والإثبات الجنائي التقليدية، نظرا لعدم كفاية وعدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم.[1]

وإزاء هذا التصور يبرز إلى الوجود مسألة صعوبة إثبات هذه النوعية من الجرائم التي توجد في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات، بل على نبضات إلكترونية غير مرئية، لا يمكن قراءتها إلا بواسطة الحواسيب الآلية، وينحصر الدور التقليدي للوثائق في الإثبات[2]. وعلى هذا الإعتبار فبقدر ما أثرت تقنية المعلومات وما صاحبها من جرائم جديدة غير مألوفة من قبل على إجراءات البحث والتحري التقليدية التي تضمنتها التشريعات الجزائية الإجرائية، فإنها أثرت كذلك على وسائل الإثبات الجنائي، إذ أصبحت الأدلة الجنائية التقليدية بدورها غير قادرة على إثبات هذا النوع من الجرائم ذات الصبغة الفنية وتحتاج إلى وسائل إثبات جديدة تتناسب مع طبيعتها المستمدة من التقنية ذاتها.

لذلك فإذا ما حدث أن وقعت إحدى الجرائم الماسة بالمعطيات الشخصية المعالجة آليا، فإن العقاب عليها لن يكون إلا بكشفها وتثبيت الدليل عليها، عن طريق تكريس قواعد مناسبة لبيئة النظم المعلوماتية التي تحصل فيها هذه الجرائم، كون الدليل الذي يمكن الإستناد عليه في إثباتها له ذاتيته وخصائصه التي تتناسب مع خصوصية هذه الجرائم حتى يكون صالحا لإثباتها[3]، ويتمثل في الدليل الإلكتروني الذي يتشكل من طبيعة الجريمة التي يولد منها.

المطلب الأول: طرق إثبات الجرائم الماسة بالمعطيات ذات الطابع الشخصي:

إن الإثبات في المواد الجزائية هو إقامة الدليل على وقوع الجريمة أو عدم وقوعها، وعلى إسنادها إلى المتهم أو عدم إسنادها، ومن ثم فإن الركيزة الأولى لعملية الإثبات هذه هو مدى توفر الدليل الذي بمقتضاه يمكن إبراز الإدانة أو البراءة[4]، ونتيجة لكون جرائم الاعتداء على المعطيات الشخصية المعالجة آليا تحصل في بيئة إلكترونية، فإن الدليل الجنائي التقليدي أصبح لا يتفق بشكل كامل مع طبيعة الوسط الذي ترتكب فيه هذه الجرائم، ولهذا ظهرت طائفة جديدة من الأدلة التي تتفق مع طبيعة الوسط الذي ارتكبت فيه وهو الدليل الإلكتروني.[5]

الفرع الأول: الدليل المناسب لإثبات جرائم الإعتداء على معالجة المعطيات الشخصية:

يختلف الوسط الذي ترتكب فيه الجرائم التي تشكل اعتداء على المعطيات الشخصية المعالجة آليا من وسط مادي عندما يتعلق الأمر بالمعالجة اليدوية إلى وسط معنوي أو ما يعرف بالوسط الإفتراضي بالنسبة للمعالجة الآلية، وعلى ضوء ذلك فإن البحث في أدلة الإثبات في إطار مدى اتفاقها مع الطبيعة التقنية

[1] وليد عاكوم، مفهوم ظاهرة الإجرام المعلوماتي، بحوث مؤتمر القانون والكمبيوتر والأنترنت، المنعقد من 1 إلى 03 ماي 2000 بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، الطبعة الثالثة، 2004، ص12.

[2] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2007. ص 92.

[3] أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الطبعة الأولى، 2005، دارالنهضة العربية، القاهرة، ص 187.

[4] محمد فتحي، تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة 2014، ص 312.

[5] خالد عياد الحلبي، إجراءات التحري في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011، ص 229.

لهذه الجرائم يصبح غير ذي معنى إذا لم يكن مدعما بتوفيق من التقنية ذاتها[1]، فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي ينشؤ منها، فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر الذي يقع عليه، ودليل جريمة القتل قد ينشؤ من فحص الأداة التي استخدمت في هذه الجريمة، وتطبيق ذلك على الجرائم المرتبطة بالمعطيات الشخصية المعالجة آليا فإن هذه الأخيرة يمكن إثباتها بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها.[2]

فالتقنية المعلوماتية قد أمدت الجناة بوسائل متطورة تمكنهم من إخفاء أفعالهم غير المشروعة كاستخدام أساليب فك التشفير والتلاعب في المعطيات الشخصية المخزنة أو الولوج بطريقة غير مشروعة للأنظمة المعلوماتية وجمع معطيات شخصية ومعالجتها دون علم أصحابها، أو العبث بها ومحوها وهتك سريتها، أو تحويلها إلى من ليس له الحق في الإطلاع عليها، وذلك عن طريق نبضات رقمية إلكترونية وفي وقت قياسي عبر النظم المعلوماتية أو شبكات الإتصال الإلكترونية، وهذا الوضع لا شك أنه يضعف بكثير من قوة طرق الإثبات التقليدية وعدم كفايتها في إقامة الدليل على مثل هذه الجرائم.

أولا: تعريف الدليل الإلكتروني:

إن التطور المستمر للبيئة الرقمية كان وراء صعوبة الإتفاق الفقهي حول وضع تعريف موحد للدليل الرقمي خاصة وأن العالم الإفتراضي الذي ينشأ فيه هذا الدليل لا يزال في بداية عهده ولم يبلغ ذروته بعد، وأنه عالم رقمي من غير الممكن احتواؤه.

ومن التعاريف التي صاغها الفقه القانوني للدليل الإلكتروني أنه ذلك الدليل الذي يجد أساسا له في العالم الإفتراضي ويقود إلى الجريمة، وهو بذلك كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني، بحيث تمكن الحاسوب من إنجاز مهمة ما.[3]

كما عرف كذلك بأنه معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية، وذلك بترجمة البيانات المخزنة في الحاسوب وملحقاته وشبكات الإتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل شيء أو شخص له علاقة بالجريمة،[4] وهو أيضا الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.[5]

---

[1] فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعلومات المدنية التجارية، دار الفكر والقانون، المنصورة، مصر 2010، ص 581.

[2] رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة الآلية، مرجع سابق، ص 380.

[3] محمد أبو بكربن يونس، الجرائم الناشئة عن الأنترنت، دار النهضة العربية، القاهرة، 2004، ص 969.

[4] محمد الأمين بشري، التحقيق في الجرائم المستحدثة، منشورات جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2004 ص 234.

[5] خالد ممدوح إبراهيم، الدليل الإلكتروني في الجرائم المعلوماتية، بحث منشور على موقع:

وكذلك هو المعطيات الرقمية المشتقة من أو بواسطة النظم المعلوماتية والبرامجية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الإتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا[1]. وهو أيضا مجموعة المعطيات المأخوذة من العالم الإفتراضي التي يمكن إعدادها وتجميعها وتخزينها وتحليلها إلكترونيا باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية[2]، كما نجد تعريفا آخر يعتبر الدليل الإلكتروني أنه طريقة خاصة لإظهار الحقيقة، والذي يتم اللجوء فيه إلى أحد الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب والرسائل الإلكترونية المخزنة والمنقولة رقميا[3].

وقد اقترحت المنظمة الدولية للأدلة والحاسوب IOCE تعريفه بأنه المعلومات المخزنة أو المتنقلة في شكل ثنائي، ويمكن أن يعتمد عليها في المحكمة.[4]

وبالنظر إلى جملة التعريفات السابقة نلاحظ أن منها من ألحق مفهوم الدليل الرقمي بمفهوم البرنامج على الرغم من اختلافهما، فإذا كان كل من المكونين يتفقان في خصوصية الإلتصاق بمفهوم تقنية المعلومات من حيث تكوينهما، إلا أنهما عبارة عن آثار معلوماتية رقمية تستخدم الشبكة المعلوماتية أو الأنترنت ويظهران في الشكل الرقمي، لأن المعطيات داخل نظام المعالجة الآلية سواء كانت نصوص أو حروف أو أرقام أو أصوات أو صور تتحول إلى طبيعة رقمية، حيث ترتكز تكنولوجيا المعلوماتية على تقنية الترقيم التي تقوم بترجمة أي مستند معلوماتي وتحويله إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي، قوامه الرقمان (0)،(1)، إلا أن الفرق بين الدليل الإلكتروني وبرامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فالبرنامج له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية عن طريق مجموعة من الأوامر، وهي قادرة على معالجة الدليل من مرحلة التبليغ عن وقوع الجريمة إلى غاية عرضه أمام المحكمة، مرورا بجمعه وحفظه وتحليله وتوثيقه وإنتاج تقريره، أما الدليل الإلكتروني فله أهمية ودور في معرفة كيفية حدوث جرائم تقنية المعلومات بهدف إثباتها ونسبتها إلى مرتكبيها.[5]

كما أن هناك من التعريفات من حصرت مصادر الدليل الرقمي في الحاسب الآلي، وهذا يعد تضييقا لدائرة التقنية، فإن كانت الحواسيب تعتبر مصدرا غنيا بالأدلة الإلكترونية، خاصة تلك الحواسيب

---

https://www.kenanaonline.com/users/khaledmahmoud/posts/77859

أطلع عليه يوم 2020/04/19 على الساعة 19:06

[1] عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، للفترة من 2 إلى 1428/11/4هـ

[2] طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مقال منشور في مجلة الحقوق، المجلد 12 العدد 01، جامعة بن غازي، ص 43 متوفر عبر الموقع:https://journal.uob.edu.bh/bitstream/handle/123456789/1438/LAW120102.pdf

[3] Clement-Fontaine Mélanie, définition et cadre juridique de la preuve numérique, colloque sur la preuve numérique à l'épreuve du litige, les acteurs de litige à la preuve numérique, organiser par la compagne nationale des experts de justice en informatique et associées le 13/04/2010. Disponible sur le site : https://www.cnejita.org

[4] Eoghan Casey, digital évidence and computer crime, 3rd édition, Academic presse, April 2011 p 261.

[5] ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الحاسوب، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد الرابع المنعقد في دبي في الفترة من 26-2003/04/28 ص 7. متوفر على الموقع: https://www.f-law.net/

الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد، إلا أن هناك من المصادر ما لا تقل أهمية عنها، سواء كانت من نظم التخزين كالهواتف الذكية، أو نظم التراسل كخوادم شبكة الأنترنت ، (les serveurs) والتي تحتوي الكثير من المعطيات الشخصية، مثل معرفة المواقع الإلكترونية التي سبق زيارتها، وغرف الدردشة التي تم الدخول إليها والرسائل الإلكترونية المرسلة والمستقبلة، والهويات المقدمة للمواقع الإلكترونية في سبيل الحصول على خدماتها أو التسجيل والإشتراك فيها...

كما اتجهت بعض التعريفات إلى حصر صفة الدليل وإضفائها فقط على تلك الأدلة المأخوذة والمستخلصة من الوسط الإفتراضي، وبمفهوم المخالفة فإن تلك المعطيات التي لازالت لم يتم فصلها عن الحاسوب وهي في شكل مجالات أو نبضات مغناطيسية أو كهربائية لا تصلح لأن توصف بالدليل الرقمي وهذا اتجاه غير صحيح.[1]

ومن جانب آخر فإن معظم هذه التعريفات التي ساقها الفقه القانوني للدليل الرقمي اعتنقت مبدأ الحياد التقني، ولم تحصر هذا الدليل في هيئة معينة، إذ يمكن أن يكون معطيات غير مقروءة، كما لو كان نتاج مراقبة عبر الشبكات والملقمات والخوادم، وقد يكون مفهوما كما لو كان مستندا إلكترونيا، كما يمكن أن يكون صورة ثابتة أو متحركة.

ويبدو أن الدليل الإلكتروني قد أبدى تجاوبا كبيرا تشير إليه مقدمات التعامل معه من خلال تطوره بسرعة كبيرة، فبعد أن كان هذا الدليل صامتا يشير إلى ما يمكن الحصول عليه من مخرجات الحاسوب مثل الوثائق والصور، فإن التطور التكنولوجي اقتضى أن يكون له مظهر آخر يعبر عنه المنطق التقني المعلوماتي المتسم بالحركة والذكاء.[2]

ووفقا لهذا المدلول الذي تم سرده يظهر جليا أن الدليل الرقمي ينبثق مفهومه من الربط بين الظاهرة الرقمية ذات الطبيعة الإلكترونية وبين الإثبات الجنائي، ليضم استلزاما لتأطيره خليطا من متخصصي القانون وعلوم تقنية الحاسوب، ليصبح بذلك الدليل الرقمي نوعا متميزا من طرق الإثبات، له من المواصفات ما يؤهله ليكون كإضافة جديدة لأنواع الأدلة في المادة الجزائية.

ثانيا: خصائص الدليل الإلكتروني:

إنه وبالنظر إلى الطبيعة الخاصة لجرائم الإعتداء على المعطيات ذات الطابع الشخصي والتي حتما تستمدها من طبيعة البيئة الإفتراضية التي تقع فيها، فإن الدليل الرقمي الذي يصلح لإثبات هذه الجرائم نتيجة لارتباطه بهذه البيئة التي انعكست على طبيعته، أصبح يتصف بعدة خصائص يتميز بها عن الدليل الجنائي التقليدي.

1) الطبيعة التقنية للدليل الرقمي: إن الطبيعة التقنية للدليل الرقمي تقتضي أن يكون هناك توافقا بين الدليل المرصود وبين البيئة التي يعيش فيها، فلا تنتج التقنية سكينا يتم به اكتشاف القاتل، أو

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، مرجع سابق، ص 385.

[2] أنظر في هذا المعنى فتحي محمد أنور عزت، مرجع سابق، ص 635.

اعترافا، أو شاهدا، أو بصمة، وإن ما تنتجه التقنية هو نبضات رقمية، تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها، ومثل هذا الأمر يجعل من المقرر أنه لا وجود للدليل الرقمي خارج بيئته التقنية، ولكي يكون هناك دليل رقمي يجب أن يكون مستوحى أو مستنبطا من البيئة الرقمية أو التقنية نفسها[1]، هذه البيئة التي تتمثل في الأقراص بأنواعها، بالإضافة إلى معالجات حركة البرامج والذاكرة، وكل قطعة يمكن أن تقوم بدور في هذا الشأن، بما في ذلك القطع المرنة التي لا يعمل النظام بدونها، مثل نظام التشغيل والبرمجية التي تعمل على تنفيذ أوامر تشغيل الملفات التي وضعها الإنسان، فضلا عن نظام الحزم التراسلية التي يمكن من خلالها التوصل إلى الدليل الإلكتروني.[2]

وعلى هذا يكون الدليل الرقمي ذو خاصية تقنية لأن بيئته الأصلية هي العالم الإفتراضي ذو الطبيعة التقنية وهو العالم الكامن في الحاسوب والخوادم والمضيفات والشبكات التي يتم تداول الحركة فيه عبرها.

وكنتيجة للطبيعة التقنية للدليل الرقمي فإنه اكتسب مميزات عن الدليل التقليدي المادي من حيث قابليته للنسخ، حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية وهذه الخاصية لا تتوفر في أنواع الأدلة الأخرى، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير[3]، بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث فيه أو تعديله، وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.

2) صعوبة التخلص من الدليل الرقمي: إن القاعدة التي تسري على كافة ما يتعلق بهيكلة تكنولوجيا المعلومات، هي أنه كلما حدث اتصال بتكنولوجيا المعلومات في معنى إدخال بيانات إلى ذلك العالم (Input) فإنه من الصعب التخلص منها، ولو كان ذلك باستعمال أعتى أدوات الإلغاء، فمحاولة التخلص من الدليل الرقمي باستخدام خصائص التخلص من الملفات الحاسوبية كخاصية Erase, Remove, Delete ،لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة، إذ تتوافر برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب، ومن هذه البرمجيات: Foremost, Recoverpeg, Photorec... وهي مصممة خصيصا لهذا الغرض.

ويمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، إذ يمكن بكل سهولة التخلص من الأوراق والأشرطة المسجلة إذا حملت في طياتها دليل الجريمة بتمزيقها أو حرقها، كما يمكن أيضا التخلص من بصمات الأصبع بمسحها من موضعها، أما بالنسبة للدليل الرقمي فإن الحال غير ذلك حيث يمكن استرجاعه بعد محوه وإصلاحه بعد إتلافه وإظهاره بعد إخفائه وإعادته إلى الحياة حتى وإن كان قد تعرض للإزالة، مما يؤدي إلى صعوبة التخلص منه، كما أن نشاط الجاني في محو الدليل

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 181.

[2] عمر محمد يونس، الجرائم الناشئة عن استخدام الأنترنت، مرجع سابق، ص 977.

[3] عمر محمد أبوبكربن يونس، مذكرات في الإثبات الجنائي عبر الأنترنت، ندوة الدليل الرقمي، بمقر جامعة الدول العربية في الفترة من 05-2005/3/8. ص 17.

والتخلص منه يشكل بحد ذاته دليلا ضد الجاني، لأن هذا النشاط يتم تسجيله في الحاسب الآلي ويمكن استخلاصه لاحقا[1].

3) الدليل الرقمي دليل متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع خاص، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، وتعني هذه الخاصية، أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة الرقمية، إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بينات غير مقروءة، من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات والملقمات والخوادم وقد يكون بيانات مفهومة كما لو كان وثيقة (Document) معدة بنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري، أو يكون مخزنا في البريد الإلكتروني، وقد يكون أيضا مرتبطا بالتشفير، وهذا التنوع إنما يعد تعبيرا عن اتساع قاعدة الدليل الرقمي، حيث يمكنه بهذه الصورة أن يشمل أنواعا متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لأن تكون دليلا بالإدانة أو البراءة.

وأما عن كون الدليل الرقمي دليلا متطورا فهي خاصية تكون تلقائية، نظرا لارتباطه بالطبيعة التي تتمتع بها حركة التطور التكنولوجي التي يشهدها العالم الإفتراضي، الذي لا يزال في بدايته ولم يصل بعد إلى منتهاه ولن يكون من السهل حينئذ احتواءه، وهذا التطور في مجال الدليل الرقمي ومع التطور المستمر في مجال التكنولوجيا قد يشكل عائقا في الوصول للأدلة الإلكترونية التي تفيد اكتشاف الجريمة ومرتكبيها، لذا فإنه يكون من الواجب مواكبة التطور التقني، سواء من حيث الأجهزة المستخدمة أو البرامج التشغيلية المستعملة داخل هذه الأجهزة وكذا برامج الحصول على الأدلة الإلكترونية، وذلك ما يساعد على الكشف عن الأدلة الرقمية وإثبات الجريمة بطريقة أسهل وأسرع.[2]

ثالثا: أنواع الدليل الرقمي:

يأخذ الدليل الرقمي نوعين رئيسيين، يتعلق النوع الأول بالأدلة التي أعدت لتكون وسيلة إثبات، والنوع الثاني يتعلق بأدلة لم تعد لتكون كذلك، ويمكن إجمال النوع الأول فيما يلي:

- السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.

- السجلات التي جزء منها تم حفظه بالإدخال، وجزء تم إنشاؤه بواسطة الجهاز، ومن أمثلة ذلك المعطيات التي تم إدخالها إلى الأدلة وتتم معالجتها من خلال برنامج خاص.

[1] عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الأنترنت، مرجع نفسه، ص 982.

[2] مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مقال منشور بمجلة كلية القانون الكويتية العالمية، ملحق خاص، العدد 03، الجزء الثاني، أكتوبر 2018، ص 198، متوفر على الرابط:http://www.journal.kilaw.edu.kw أطلع عليه في 2020/04/19

وأما النوع الثاني فهي تلك الأدلة التي تنشأ دون إرادة الشخص، فهي أي أثر يتركه هذا الأخير دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية الرقمية،[1] وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي القائم بمعالجة المعطيات الشخصية بسبب قيامه بأي نشاط من الأنشطة التي تدخل في إطار المعالجة أو إرسال هذه المعطيات أو استقبالها.

وتبدو أهمية التمييز بين هذين النوعين من الأدلة الرقمية في كون أن النوع الأول قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها، لذلك فإنهادة ما يـ ،عمد إلى حفظه للإحتجاج به لاحقا، وهو ما يقلل من إمكانية فقدانه، كما يكون من السهل الحصول عليه، بينما النوع الثاني، فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه، لهذا فهو في الغالب ما يتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها، ويكون الحصول عليه باتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، وهو على العكس من النوع الأول، كونه لم يـ ،عد ليحفظ مما يجعله عرضة للفقدان بسهولة.[2]

رابعا: صعوبة الإثبات في جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:

نظرا لكون إثبات هذه الجرائم مرتبط بالدليل الرقمي وما يتميز به من خصائص، فإن ذلك يطرح جملة من الصعوبات في إثبات هذه الجرائم أكثر مما يمكن أن يطرحه إثباتها لو تعلقت بالمعالجة اليدوية، ويرجع ذلك لعدة اعتبارات أهمها:

- الطابع الخفي لهذا النوع من الجرائم والذي يعد من بين أهم الصعوبات التي تواجهها عملية إثباتها، ويتجلى ذلك من خلال عدم علم المجني عليه في أحيان كثيرة بها، ويرجع ذلك لقيام الجاني بإخفائها عن طريق التلاعب في النبضات والذبذبات الإلكترونية المكونة للمعطيات الشخصية المخزنة آليا، وبذلك فإنه يكون من غير السهل للبيئة الرقمية التي تستوعب كما هائلا وضخما من المعطيات الشخصية أن تقوم بعملية فرز ذاتية داخلية للملفات البريئة عن تلك المجرمة والتي تعد موضوعا للدليل الجنائي الرقمي، بل وقد يمكن أن يكون الملف البريء ستارا للملف المجرم.[3]

- غياب الدليل المرئي، حيث يشكل هذا الطابع أحد الصعوبات الكبيرة التي تطرح بصدد إثبات الجرائم الماسة بالمعطيات الشخصية المعالجة آليا أو إلكترونيا، فأغلب الأدلة التي يتم اللجوء إليها لإثباتها عبارة عن تسجيلات إلكترونية على دعائم للتخزين ذات طبيعة ضوئية أو ممغنطة، فيكون حينئذ من الصعب الإطلاع المباشر على المعطيات[4] الشخصية المعنية بالبحث، والمستندات المحفوظة في النظم المعلوماتية أو التي يتم تداولها عبرها.

[1] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 22، 38.

[2] طارق محمد الجملي، الدليل الرقمي في الإثبات الجنائي، مرجع سابق، ص 44

[3] عمر محمد بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي (المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية)،دار النهضة العربية للطبع والنشر والتوزيع، 2004، ص 24.

[4] هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين –مجلة الأمن والقانون، السنة السابعة، العدد 02، جويلية 1999، ص 28.

ومن بين الصعوبات كذلك قيام الجاني بإعاقة الوصول إلى الدليل من خلال وسائل الحماية التقنية، مما يطرح عراقيل أمام الحصول على أدلة الإثبات ومنع الوصول إليها من خلال تقنيات التشفير، وما يزيد من صعوبة إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا هو هشاشة الدليل الرقمي في حد ذاته إذ يمكن أن يتعرض لصدمات التعديل فيه أو محوه سواء كان ذلك عن قصد من قبل الجاني أو عن غير قصد من قبل المحققين أثناء جمعه، فيكون بذلك الدليل الرقمي موضع شك من حيث سلامته من العبث والخروج به على نحو يخالف الحقيقة من ناحية، وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى.[1]

الفرع الثاني: إجراءات الحصول على الدليل الرقمي لإثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا.

حتى يتحقق الدليل الرقمي اللازم لإثبات الجرائم الماسة بالمعطيات ذات الطابع الشخصي، فإنه لا بد من جمع عناصر التحقيق والدعوى وتقديم هذه العناصر إلى القضاء للاستناد إليها، إما في إدانة المتهم أو القضاء ببراءته[2]، لذلك كان الهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة، وفي سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات.[3]

ولا شك أن التطور الحاصل في مجال المعلوماتية قد رتب آثارا هامة انعكست على الجرائم من حيث الوسائل التي ترتكب بها والمحل الذي تقع عليه، وعلى الوسائل التي تصلح لتحصيل دليل إثباتها، فالحاصل أنه مع ظهور طائفة الجرائم المعلوماتية والتي تعد الإعتداءات على المعطيات الشخصية المعالجة إلكترونيا جزءا منها وهي ضرب من ضروب الذكاء الإجرامي، أصبح لا يجدي معها اتباع الطرق التقليدية في تحصيل الدليل لإثباتها لما تثيره طبيعتها غير المادية من إشكالات.

فالتطور التقني الذي لحق نظم المعالجة الآلية للمعطيات فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما ودون أي شك إلى تغيير كثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الامر الذي يحتاج بالضرورة إلى إعادة تقييم لمنهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية، فضلا عن استحداث قواعد إجرائية تتلاءم مع طبيعة البيئة التقنية.

---

[1] طارق محمد الجملي، مرجع سابق، ص 45.

[2] محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي والأردني)، رسالة استكمال متطلبات الحصول على درجة الماجيستار في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2015، ص 77.

[3] علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي –دراسة مقارنة-مقال منشور في مجلة مركز الإعلام الأمني، سنة 2009 ص 2، متوفر على الرابط:http://www.policemc.gov.bh/mcms-store/pdf

ومن جانب آخر فإن هذا النوع الجديد من الأدلة قد لا يندرج ضمن أنواع الأدلة الجنائية التي ألفتها الضبطية القضائية، وبالتالي تكون هذه الأخيرة في حاجة إلى مهارات جديدة وتخصصات غير تقليدية للتعامل مع الأدلة الرقمية.[1]

ومن هذا المنطلق فإنه إذا كانت عملية البحث والتحري تعتمد على ذكاء وفطنة ضابط الشرطة القضائية وقوة ملاحظته وسرعة البديهة لديه، فإن هذه العملية في البيئة الإلكترونية تستوجب بالإضافة إلى كل هذا تطويرا لأساليبها وتكليف جهات مختصة لممارستها من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة.

وترتيبا على ذلك سوف نستعرض الجهات المكلفة أو المخول لها قانونا صلاحية جمع الدليل في إثبات جرائم الإعتداء على المعطيات الشخصية، ثم أهم الوسائل أو الإجراءات القانونية التي تمارسها هذه الجهات لتحصيل هذا الدليل.

أولا: الجهات المكلفة بالبحث والتحري عن جرائم الإعتداء على المعطيات الشخصية:

تنص المادة 50 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي أنه إضافة إلى ضباط وأعوان الشرطة القضائية، يؤهل أعوان الرقابة الآخرون الذين تلجأ إليهم السلطة الوطنية للقيام ببحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون تحت إشراف وكيل الجمهورية.

1) ضباط وأعوان الشرطة القضائية: يستمد ضباط الشرطة القضائية اختصاصهم في البحث والتحري عن الجرائم الماسة بالمعطيات الشخصية المعالجة آليا من خلال المادة 50 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي.

ويأتي هذا انسجاما مع الإختصاص الأصيل للشرطة القضائية حسب القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية بشأن البحث والتحري عن الجرائم وجمع الأدلة عنها وضبط مرتكبيها، حيث تنص المادة 12 من ذات القانون أنه يناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها".

وبشكل عام فإن رجال الشرطة القضائية يتمتعون في إطار التحري عن الجرائم المتعلقة بالمعالجة الآلية غير المشروعة للمعطيات ذات الطابع الشخصي بكافة السلطات المخولة لهم بموجب نصوص قانون الإجراءات الجزائية، إلا أنه ولما كان الأمر يتعلق ببحث ٍ وتحر ٍ عن جرائم ذات طبيعة خاصة، فإن الأمر يستلزم إيجاد ضباط شرطة قضائية متخصصين في مجال تكنولوجيا المعلومات، من أجل القدرة على مواجهة مختلف الصعوبات التي تطرح بصدد التحري عن هذه الجرائم.

[1] محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الأنترنت، بحث مقدم في إطار الحلقة العلمية "الأنترنت والإرهاب" خلال الفترة بين 15 – 2008/11/19، جامعة نايف العربية للعلوم الأمنية، بالتعاون مع جامعة عين شمس، ص 23.

فأمام التطور التقني والتكنولوجي الذي يعتمد عليه في ارتكاب جرائم الإعتداء على المعطيات الشخصية المعالجة آليا، يصبح التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية، وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن هذه الجرائم وكشف النقاب عنها.[1]

لذلك يمكن القول أن المشكلة الأساسية التي تواجه المحققين في مثل هذا النوع من الجرائم والجرائم المعلوماتية بصفة عامة، هي خلفية المحقق نفسه، ذلك أن متخصصي الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة وتقديمها للمحكمة. ففي كثير من الحالات نجد أن هؤلاء يعتقدون أن لديهم الدليل الحاسم حول الجريمة، لكن يتبين من الناحية القانونية فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، وكذلك بالنسبةللمحققين ذوي الخلفية القانونية فقط قد تكون لديهم الخبرة الواسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم، فإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه عند مباشرته التحقيق في جرائم ذات الطابع المعلوماتي يلزمه معرفة العديد من الجوانب الفنية، فافتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل الرقمي، على اعتبار أن جهله بأساليب ارتكاب هذا النوع من الجرائم يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها، كإتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها المعطيات.[2]

لذلك يفترض على ضباط الشرطة القضائية المكلفين بالتحري والتحقيق في هذه الجرائم معرفة آلية عمل تشكيلات الحاسوب وشبكات الأنترنت، لكونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الإفتراضي من اعتراض لحزم البيانات أثناء انتقالها عبر الشبكات، واختراق لنظم المعلومات والتلاعب بالمعطيات الشخصية المخزنة بها، كما أنها تعطي لضابط الشرطة القضائية المحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الإعتداء على الشبكة وعلى نظم المعالجة الآلية.[3]

وعلى هذا فغالبا ما توكل مهمة التحقيق في الجرائم التي ترتكب عبر الحاسب الآلي وشبكاته، سواء شكلت اعتداء على المعطيات الشخصية أو غير ذلك إلى نوعين من المتخصصين:

النوع الأول: يمثل الكفاءة المهنية وهم المتخصصون في مجال التحقيق الجنائي، لأن أخذ أقوال الشهود وسماع تصريحات المشتبه فيهم يعتمد على قواعد مهنية وعلى قدرات لا تتوافر في خبراء الحاسب الآلي

[1] سعيداني نعيم، مرجع سابق، ص 114.

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة 2002، ص115.

[3] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، مقال متوفر على الموقع:
https://knowledgemanagements.files.wordpress.com/ ص06.

فطريقة توجيه الأسئلة وترتيب أولوياتها واستنتاج الحقائق منها من الأمور المهنية التي لا يوفيها حقها إلا من لديه خبرة ومعرفة بفنيات التحقيق.[1]

النوع الثاني: يمثل الخبرة الفنية وهم النخبة المتخصصة في مجال الحاسب الآلي وشبكاته، ويتم الاستعانة بهم في جميع مراحل ضبط هذه الجرائم والتحري بشأنها واكتشافها والتحقيق مع المتهمين فيها، وكذلك في تقديم الأدلة الجنائية أمام المحكمة وشرح أبعاد الجريمة.

ولعل هذه الخصوصية التي تتمتع بها جرائم الإعتداء على المعطيات الشخصية وما استتبعه من خصوصية في إجراءات البحث والتحري بشأنها هو ما دفع بالمشرع إلى إسناد مهمة البحث ومعاينة هذه الجرائم إلى فئة أخرى من المتخصصين وهم أعوان السلطة الوطنية لحماية المعطيات الشخصية.

2) أعوان السلطة الوطنية لحماية المعطيات الشخصية: إلى جانب عناصر الضبطية القضائية، فإن المشرع أسند في المادة 55 من القانون 07/18 مهمة القيام بالبحث عن الجرائم المنصوص عليها في هذا القانون ومعاينتها لأعوان السلطة الوطنية لحماية المعطيات الشخصية، ونظرا للطابع التقني الذي تمتاز به هذه الجرائم التي يعاينونها، فإنه يتم اختيار هؤلاء الأعوان وكذا أعضاء السلطة حسب اختصاصهم التقني في مجال معالجة المعطيات ذات الطابع الشخصي، كما يكون للسلطة حسب المادة 23 من القانون 07/18 أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أداء مهامها، ولهم في سبيل ذلك حسب المادة 49 من ذات القانون صلاحية القيام بكل التحريات المطلوبة، وكذا المعاينات اللازمة والأماكن التي تتم فيها معالجة المعطيات الشخصية بالإضافة إلى إمكانية الولوج إلى أنظمة المعالجة الآلية للمعطيات والإطلاع على المعطيات الشخصية المخزنة بها، وإعداد محاضر تثبت فيها معاينتهم لأفعال تشكل جرائم اعتداء على المعطيات الشخصية ترسل فورا إلى وكيل الجمهورية المختص إقليميا*.

وتمارس السلطة الوطنية هذه الصلاحيات إما في إطار التحقيق في الشكاوى والإحتجاجات والطعون المرفوعة إليها في إطار تنفيذ معالجة المعطيات ذات الطابع الشخصي من المعنيين بهذه المعالجات حسب أحكام البند 04 من المادة 25 من القانون 07/18، أو في إطار توقيع العقوبات في حق المسؤول عن المعالجة حال خرقه للإلتزامات التي تفرضها عليه في إطار احترام أحكام هذا القانون.

وبالرجوع إلى التشريع الفرنسي نجد أن هذا الأخير قد مدد من صلاحيات التحقيق les pouvoirs d'enquête للجنة الوطنية للمعلوميات والحريات (CNIL) بموجب القانون 2004/801 المؤرخ في 06 أوت 2004 لتحسين مستوى الحماية للمعطيات الشخصية على ما كان عليه الأمر من قبل وجعله أكثر كفاءة، حيث تنص المادة 2/11-f من هذا القانون أنه يجوز للجنة الوطنية (la CNIL) أن تكلف عضوا أو أكثر من أعضائها أو أعوانها بموجب قرار خاص وفقا للشروط المنصوص عليها في المادة 44 القيام بعمليات المعاينة

[1] محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة 2008، ص254.

* نصت المادة 25 البند 13 من القانون 07/18 أنه في إطار ممارسة مهامها تعلم السلطة الوطنية النائب العام المختص فورا في حالة معاينة وقائع تحتمل وصف جزائي، في حين تنص المادة 51 من نفس القانون على أن الجرائم المنصوص عليها في هذا القانون تعاين بواسطة محاضر توجه فورا إلى وكيل الجمهورية المختص إقليميا،لذلك نرى أنه من باب التنسيق بين النصوص القانونية أي بين المادة 25 البند23 والمادة 51 أن يتم تعديل محتوى البند 13 لتكون كما يلي: في إطار .... تعلم السلطة الوطنية وكيل الجمهورية المختص فورا..." بدل النائب العام.

والمراقبة لجميع المعالجات، وإذا لزم الأمر الحصول على نسخ لجميع الوثائق أو دعامات إلكترونية تراها مفيدة لمهامها، ويلزم المشرع الفرنسي حسب المادة 19 من القانون 17/78 هؤلاء الأعوان للقيام بمهام البحث والمعاينة أن يكونوا مفوضين أو معينين من قبل رئيس اللجنة الوطنية للمعلوماتية والحريات la CNIL، وأنه لا يمكن ممارسة أو تنفيذ مهام التحقيق المحددة في المادة 44 من ذات القانون إلا من طرف الأعوان الذين تم استدعاؤهم للمشاركة في هذه المهام وتأهيلهم من طرف اللجنة الوطنية للمعلوماتية والحريات (la CNIL)*.

وما يمكن ملاحظته بخصوص هذه المسألة أن المشرع الجزائري لم يحدد كيفية ممارسة السلطة الوطنية لحماية المعطيات الشخصية مهام البحث والمعاينة لجرائم الإعتداء على المعطيات الشخصية عن طريق أعوانها أو عن طريق أعوان آخرين يمكن أن تلجأ إليهم هذه السلطة.

وهذا على خلاف ما نجده في التشريع الفرنسي، حيث نظم هذا الأخير الصلاحيات الخاصة باللجنة الوطنية للمعلوماتية والحريات المتعلقة بالبحث والتقصي ومعاينة هذا النوع من الجرائم، وذلك في القانون 17/78 وكذا المرسوم رقم 2005/1309 المؤرخ في 20 أكتوبر 2005 المتعلق بتطبيق أحكام القانون 17/78، وكذلك فعل المشرع المغربي الذي نظم هذه الصلاحيات من خلال المرسوم التطبيقي 2/09/165 المؤرخ في 21 ماي 2009 المتعلق بتطبيق القانون 08/09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

ولذلك فإنه يمكننا الإستناد على التشريع الفرنسي في توضيح هذه المسألة، حيث يمنحهذا الأخير لأعوان اللجنة الوطنية المؤهلين لمعاينة وبحث الجرائم المحددة في القانون 17/78 إمكانية ممارسة هذه المهام من خلال:

- الرقابة في عين المكان (la vérification sur place) أو عن طريق طلب الإتصال بالوثائق (la demande de communication de documents) .

* L'article 19 de la loi 78/17 du 06 janvier 1978 relative à l'informatique aux fichiers et aux libertés dispose que :

« .... Les agents de la commission sont nommés par le président .... Ceux des agents qui peuvent être appelés à participer à la mise en œuvre des missions de vérification mentionnées à l'article 44 doivent y être habilités par la commission ... »

غير أنه ومنذ صدور القانون رقم 2014/344 المتعلق بالإستهلاك (loi n°2014/344 relative à la consommation) المؤرخ في 17 مارس 2014 تم إنشاء المديرية العامة للمنافسة والإستهلاك وقمع الغش (DGCCRE) أين يتمتع الأعوان التابعين لها بنفس السلطات التي يتمتع بها أعوان اللجنة الوطنية للمعلوماتية والحريات في إطار البحث ومعاينة الخروقات والمخالفات للقانون 17/78 والتي من شأنها أن تشكل مساسا بسلامة المعالجة للمعطيات الشخصية، على أن يقوم هؤلاء الأعوان التابعين لهاته المديرية بإعداد محاضر عما قاموا به من معاينات وإرسالها إلى اللجنة الوطنية la CNIL لتقرر هذه الأخيرة ما تتخذه بشأنها.

وبمناسبة هذا الإمتياز الجديد الممنوح لـ DGCCREتم تعيين ما يقارب 300 محقق موزعة على التراب الفرنسي من أجل الزيادة في رفع مستوى حماية الضوابط والقواعد المتعلقة بجمع ومعالجة المعطيات الشخصية المحددة في القانون 17/78.

Voir dans ce cadre la loi n° 2014/344 du 17 mars 2014 relative à la consommation JORF n° 0065 du 18 mars 2014 p 5400 dite : « loi Hamoun » et aussi : Emilie BAILLY, les pouvoirs d'enquête et de sanction de la CNIL, RLDA, numéro 93 mai 2014, p89 disponible sur le site : http://anyline.lamy.fr

أ) الرقابة في عين المكان: وتعد هذه الطريقة من وسائل العمل المفضلة لدى أعوان CNIL يمكن تنفيذها في إطار التحقيق في الشكاوى التي تقدم إلى اللجنة الوطنية أو في إطار إجراءات توقيع العقوبات، مثل التحقيق في مدى التزام المسؤول عن المعالجة وامتثاله للالتزامات التي سبق فرضها عليه، ولا يمكن لأعوان اللجنة الوطنية الخروج والانتقال إلى أماكن المعالجة للقيام بهذه المهمة إلا بموجب قرار صادر عن رئيس اللجنة الوطنية بعد اقتراح من مصلحة الرقابة (service des controles)، وكذلك نصت المادة 16 من المرسوم التطبيقي في التشريع المغربي على أنه للإضطلاع بسلطات التقصي والتحقيق تكلف اللجنة الوطنية أعوانها المفوضين من طرف الرئيس، وفي سياق الأمر ذاته ألزمت المادة 19 من ذات المرسوم التطبيقي هؤلاء الأعوان بضرورة تقديم وثيقة تكليفهم بالمهمة، وأن يثبتوا عند الضرورة أهليتهم لمباشرة تلك المراقبة، وتعد باطلة بناء على ذلك كل عملية مراقبة أو معاينة يقوم بها أعوان اللجنة في غياب قرار يمكن لأعوان اللجنة الوطنية الانتقال إلى المكان وإجراء عدة معاينات بموجب قرار واحد من رئيس اللجنة، ولا يحتاج الأمر إلى إصدار عدة قرارات، وهذا ما أكدته اللجنة الوطنية (la CNIL) في إحدى مداولاتها المتعلقة بتوقيع عقوبات مالية على شركة Google، حيث اعتبرت اللجنة في هذا القرار أنه لا توجد أية أحكام في القانون 17/78 تلزم رئيس اللجنة بإصدار عدة قرارات لتفويض أعوان اللجنة بإنجاز عدة مهام للمراقبة في المكان الواحد.[1]

والمشرع الجزائري أيضا قد منح السلطة الوطنية لحماية المعطيات الشخصية صلاحية الإنتقال إلى الأماكن التابعة لشركات أو مؤسسات أو هيئات تتم فيها عمليات المعالجة، بغرض إجراء التحريات والمعاينات المطلوبة مستثنيا منها المحلات السكنية، غير أن المادة 44 من القانون الفرنسي 17/78 قد وضعت شرطا زمنيا يتعلق بتوقيت الدخول إلى هذه الأماكن، إذ لا يمكن حسبها لأعوان اللجنة الوطنية الدخول إلى الأماكن والمحال والمنشئات أو المؤسسات الموضوعة في الخدمة أو المخصصة للاستعمال المهني التي تتم فيها معالجة المعطيات الشخصية باستثناء تلك المخصصة للسكن لإجراء التحقيقات والمعاينات، إلا من الساعة السادسة صباحا إلى غاية التاسعة ليلا[2]، مع وجوب إعلام وكيل الجمهورية المختص إقليميا الذي تقع الأماكن الخاضعة للمعاينة والرقابة بدائرة اختصاصه، وذلك من طرف الأعوان المكلفين لهذه المراقبة قبل 24 ساعة على الأكثر من التاريخ المحدد للدخول للمكان المراد معاينته أو مراقبته[3]، في حين اكتفى المشرع الجزائري بالنص على أن عمليات المعاينة والبحث التي يقوم بها أعوان السلطة الوطنية تتم تحت إشراف وكيل الجمهورية، ونعتقد أن المشرع الجزائري لم يكن موفقا عندما استهل عبارة تحت إشراف وكيل الجمهورية ذلك أن هذه الصلاحية واسعة وغير محددة المعالم، والمشرع لم يبن

[1] Délibération n° 2011/035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la sociétés(x), disponible sur le site : http://ww.legifrance.gouv.fr/affichcnil

[2] L'article 44 dispose que : « les membres de la commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies… ont accès e 6 heures à 21 heures, pour l'exercice servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé ».

[3] Voir l'article 61 du décret n° 2005/1309 du 20 octobre 2005 pris pour l'application de la loi n° 78/17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

بوضوح كيف يمارس هذا الإشراف، ومن جهة أخرى قد يكون في المسألة تناقضا مع الإطار العام الذي تقوم عليه استقلالية هذه السلطة، حيث نجد أن أغلب التشريعات اعتبرت أن هذه الهيئة في إطار ممارستها لصلاحيتها، لا يتلقى أعضاؤها أي تعليمات من أي جهة.[1]

لذلك فإنه في هذا السياق أقرت اللجنة الوطنية للمعلوماتية والحريات الفرنسية (la CNIL) في إحدى مداولاتها أن هوية المنظمة المقصودة بعمليات المراقبة والبحث ليس لازما أن يتضمنها الإعلام المسبق الموجه إلى وكيل الجمورية المختص إقليميا، فحسب هذه الأخيرة أنه لا المادة 44 من القانون 17/78 ولا المادة 61 من المرسوم 1309/2005 تلزم المراقبين التابعين للجنة الوطنية للمعلوماتية و الحريات بأن يخطروا وكيل الجمهورية المختص بعناصر أخرى غير تلك المتعلقة بتاريخ وساعة ومكان وموضوع المراقبة، وبالنتيجة يستثنى أن يتضمن الإخطار هوية المنظمة[2]، وهذا ما أكده المشرع المغربي من خلال المادة 19 من المرسوم التطبيقي رقم 2.09.165 حينما نصت على أن الإخطار الموجه إلى وكيل الملك يتضمن تاريخ وساعة ومكان وموضوع المراقبة فقط.

وبالإضافة إلى إعلام وكيل الجمهورية بقرار رئيس اللجنة من أجل تنفيذ المعاينات في المكان، يبلغ بها أيضا المسؤول عن الأماكن المقصودة بهذه المراقبة أو من يمثله، وهو في كل الظروف المسؤول عن المعالجة، ويكون تبليغ هذا الأخير على أقصى تقدير عند وصول الأعوان المؤهلين للمراقبة إلى المكان المقصود بها (محل المراقبة)[3]، ومع ذلك فإن اللجنة الوطنية الفرنسية (la CNIL) اعتبرت أنها غير ملزمة بتبليغ المسؤول عن المعالجة مقدما بأنه سوف يتم إجراء هذه المراقبة في المكان، ذلك أن القرار بإجرائها من عدمه يكون حسب الظروف المناسبة التي تستوجبها[4]، كما أن تبليغ المسؤول عن المعالجة بأن اللجنة سوف تفوض من يقوم بالمراقبة بالأماكن التابعة له يمكنه من أن يطلب تحضير الملفات التي من شأنها تسهيل عملية المراقبة.[5]

وأثناء عملية المراقبة يمكن للأعوان التابعين للجنة المكلفين والمؤهلين أن يطلبوا الحصول والإطلاع على أي ملف، غير أنه ليس لهم أن يحجزوا الملفات الأصلية، وقد أشار المشرع الجزائري في المادة 49 من القانون 07/18 أن السلطة الوطنية تستطيع القيام بمهام الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها، وأنه لا يعتد أمامها بالسر المهني، وبهذا المقتضى يكون لأعوانها مكنة الولوج إلى البرامج

[1] Voir l'article 21 de la loi 78L17 : « dans l'exercice de leurs attributions les membres de la commission reçoivent d'instruction d'aucune autorités ».

[2] Délibération de la CNIL n° 2012/176 du 21 juin 2012 portant avertissement à l'encontre de la société x (groupe y) disponible sur le site : http://www.legifrance.gouv.fr

[3] Voir l'article 62 du décret n°2005/1309, op.cit

[4] Emilie Bailly, op.cit, p 89.

[5] Voir l'article 54 du règlement interieur de la CNIL, notification préalable d'un contrôle, version consolidée au 22/01/2015 disponible sur le site : http://www.cnil.fr/fr/règlement-interieur

« Lorsque le responsable de traitement est informé que la commission va diligenter un contrôle dans ses locaux, il peut lui etre demander de prépare tous documents de nature à faciliter le déroulement du contrôle ».

والأنظمة المعلوماتية وكذلك إلى المعطيات الشخصية المخزنة بها، وطلب نسخ عنها بواسطة أي معالجة تقنية مناسبة تجعلها في وثائق تكون قابلة للاستعمال مباشرة من أجل احتياجات المراقبة.

ومن جهة أخرى نجد أن التشريع الفرنسي من خلال المادة 44 من القانون 17/78 يعطي للشخص المسؤول عن الأمكنة المقصودة بالمراقبة الحق في معارضة الأعوان المؤهلين لزيارة الأماكن وفي قيامهم بعملية المراقبة وعلى هؤلاء الأعوان في هذه الحالة تحرير محضر[1] يؤكدون فيه هذه المعارضة من قبل المسؤول عن الأماكن وأسباب هذا الرفض ودوافعه، وقد يكون هذا الإعتراض في أي مرحلة تكون عليها عملية المراقبة، إذ يمكن للمسؤول عن المعالجة بعد مرور ساعتين مثلا من بدء عملية المراقبة أن يعترض على ولوج أعوان اللجنة إلى ملف خاص داخل النظام المعلوماتي، وهنا على هؤلاء الأعوان أن يوقفوا عملية المراقبة وتحرير محضر بهذا الإعتراض، وقد أكد مجلس الدولة الفرنسي في هذا الإطار مستندا إلى نص المادة 08 من الإتفاقية الأوروبية لحقوق الإنسان في النقطة المتعلقة بحرمة المساكن، أن المسؤولين على الأماكن لهم الحق في الاعتراض على عمليات المراقبة التي يقوم بها أعوان اللجنة الوطنية (la CNIL) وأن هؤلاء ملزمون بإبلاغهم بحقهم في الإعتراض.[2]

وفي هذه الحالة أشارت المادة 44 من القانون 17/78 أنه في حالة اعتراض المسؤول عن المعالجة على إجراء المراقبة في الأماكن، فإنه لا يمكن للأعوان المؤهلين تنفيذ هذه المهام إلا بأمر من رئيس المحكمة المختص إقليميا، والذي يتم إخطاره بموجب عريضة طرف رئيس اللجنة، ويفصل فيها بموجب أمر مسبب وفقا لأحكام المادتين 493،498 من قانون الإجراءات المدنية.

وإذا تعلق الأمر بالمراقبة التي يجريها وينفذها الأعوان المؤهلون التابعون للجنة الوطنية (la CNIL) في الأماكن والمنشئات المهنية الخاصة، فإن القانون رقم 344/2011 المتعلق بالمدافع عن الحقوق[3] والذي عدل المادة 44 من القانون 17/78ص صراحة على أنه يجب على أعوان اللجنة أن يـ ُعلموا تلقائيا المسؤول عن هذه الأماكن والمنشئات المهنية الخاصة محل المراقبة بحقه في الإعتراض على الزيارة التي يقومون بها، وإذا مارس هذا الأخير حقه في الإعتراض على الشكل السابق بيانه، فإن المراقبة والمعاينة لهذه الأماكن لا يمكن أن تجرى إلا بإذن قضائي، ولكن هذه المرة ليس من طرف رئيس المحكمة المختصة إقليميا، وإنما من طرف قاضي الحريات والإحتباس للجهة القضائية التي تقع بدائرة اختصاصها الأماكن التي ستتم زيارتها.[4]

[1] Voir l'article 56 du règlement interieur de la CNIL.

[2] Emilie, Bailly, OP.CIT P90.

[3] La loi n°2011/344 du 29 mars 2011 relative au défenseur des droit JORF n° 075 du 30 mars 2011 p 5504.

[4] Article 07 de la loi 2011/344 dispose que :« le responsable de locaux professionnels privés est informé de son droit d'opposition à la visite, lorsqu'il éxerce ce droit, la visite ne peut se dérouler qu'après l'autorisation de juge des libertés et de la détention du tribunal de grande instance dans le ressort du quel sont situés les locaux à visiter … »

ويعتبر حق الإعتراض هذا تقييدا معتبرا وإلى حد كبير من نطاق وفعالية الرقابة التي يقوم بها أعوان اللجنة الوطنية (la CNIL) حيث يمكن للمنظمة محل المراقبة أن تستفيد من الوقت اللازم استغراقه في الحصول على أمر الجهة القضائية المختصة في مسح أو إخفاء المعطيات المعلوماتية التي تكون مخالفة للقانون.

لذلك فإنه يمكن لرئيس اللجنة أن يخطر قاضي الحريات مباشرة للحصول منه على إذن مسبق بالرقابة ثم قيام الأعوان التابعين لها بزيارة الأماكن وإجراء عملية المراقبة قبل أن يكون الشخص المسؤول عن الأماكن قد أبلغ بهذه الزيارة، ودون انتظار أن يبدي هذا الأخير معارضته، وذلك متى توفرت حالة الإستعجال التي تبررها خطورة الوقائع، سبب الرقابة أو خطر تدمير ومحو المعطيات، ولا يجوز للشخص المسؤول عن الأماكن في هذه الحالة أن يعارض الزيارة[1]، ومن ثم يكون المشرع الفرنسي في هذه الحالة قد عزز فعالية وكفاءة اللجنة الوطنية (la CNIL) في القيام بمهام الرقابة والمعاينة دون أن تحمل هذه الرقابة اعتداء على حقوق الشخص المسؤول عن الأماكن التي تتم زيارتها.

ويختتم أعوان اللجنة مهامهم بتحرير محاضر تشير بشكل خاص إلى الغرض من المهمة والأشخاص الذين تم مقابلتهم، وإذا لزم الأمر تسجيل تصريحاتهم وكذلك جرد كل الوثائق والدعامات الإلكترونية التي ترفق بهذه المحاضر.[2]

وتشير المادة 21 من المرسوم التطبيقي 165-09-02 أنه يمكن لأعوان اللجنة الوطنية لحماية المعطيات الشخصية بموجب ترخيص من وكيل الملك حجز المعدات موضوع المخالفة.

وإذا كانت المعاينات التي تم إجراؤها بمناسبة هذه المراقبة لا تدعو إلى ملاحظات هامة، أو كانت الإخلالات لا تبرر اتخاذ إجراءات الخصومة القضائية، فإنه يتم إغلاق هذه الإجراءات، أما إذا تبين وجود خروقات خطيرة فإن الأعوان يقومون بإرسال هذه المحاضر إلى قسم التقاضي على مستوى اللجنة، والتي تقرر إما فرض عقوبة إدارية أو إحالة الملف على وكيل الجمهورية المختص إقليميا في إطار المادة 40 من قانون الإجراءات الجزائية الفرنسي[3]. وكذلك فعل المشرع الجزائري، عندما أشارت المادة 51 من القانون 07/18 على أن السلطة الوطنية عند معاينتها للجرائم في إطار مهامها المرتبطة ببحث ومعاينة الجرائم المنصوص عليها في هذا القانون أن تحرر محاضر توجه فورا إلى وكيل الجمهورية المختص إقليميا.

ب) المراقبة بناء على الوثائق وعن طريق الإستدعاء: وهي طريقة أخرى تجد سندها في القانون الجزائري في المادة 3/44 من القانون 07/18، حيث تنص على أنه يمكن لأعوان اللجنة طلب الإتصال بكل وثيقة ضرورية ولازمة لاستكمال مهمة المراقبة، كما يمكن عن طريق استدعاء المعني تحصيل كل معلومة وتبرير مفيد.

---

[1] L'article 07 de la loi 2011/344, OP.CIT

[2] Voir l'article 64 du décrit 2005/1309, précité

وهو كذلك نصت المادة 20 من المرسوم التطبيقي 02/09/165 لتطبيق القانون المغربي 08/09 المشار إليه سابقا.

[3] Article 40 de la procédure pénale française

ويعتبر القانون الفرنسي أنه لا يمكن تنفيذ هذه الطريقة في مراقبة وبحث المخالفات الماسة بمعالجة المعطيات الشخصية من طرف أعوان اللجنة الوطنية إلا بموجب قرار من رئيس اللجنة مثل ما هو الشأن بالنسبة للمراقبة في المكان، وتأخذ هذه الطريقة في المراقبة شكل إرسال بريدي أو إلكتروني يوجه إلى المنظمة المعينة بالمراقبة، ويمكن من خلاله طلب أي وثيقة أو دعامة إلكترونية تكون مفيدة لإنجاز مهام المراقبة المقصودة.

أما عن المقصود بالوثيقة فإن اللجنة الوطنية (la CNIL) قد كان لها الفرصة للتوضيح بأن يأخذ مفهوم الوثيقة بالمعنى الواسع، حيث أكدت في إحدى مداولاتها أنه يدخل في معنى الوثيقة أرقام التشفير أو الترميز للبرنامج الذي يعتبر المصدر في جمع المعطيات الشخصية.[1]

وبشكل عام يمكن لأعوان اللجنة في سبيل إنجاز مهام المراقبة عن طريق الوثائق أن يطلبوا الإتصال بجميع الوثائق الضرورية واللازمة لإنجاز واستكمال مهامهم، وذلك من خلال الإتصال بالمعطيات الشخصية المستخدمة أو المحتواة في المعالجات المستهدفة آليا أو يدويا للتأكد من مدى موافقتها للقانون، وكذلك كل المعلومات المتعلقة بشروط تنفيذ معالجة المعطيات الشخصية مثل عقود تكنولوجيا المعلومات، اتفاقات استخدام موارد تكنولوجيا المعلومات، استمارات جمع المعطيات الشخصية والمذكرات.[2]

وإذا ما قدرت اللجنة أنه لم يتم إعلامها بجميع الوثائق المطلوبة بالشكل الكافي والمفيد لتحقيق أغراض المراقبة من خلال ما أرسل إليها من طرف المسؤول عن المعالجة المقصود بالمراقبة، فإن لها أن تقرر اتخاذ إجراء المراقبة في المكان، أو استدعاء المسؤول عن المعالجة لسماعه حول جميع المعلومات المفيدة.[3]

وفي هذه الحالة تتم عملية المراقبة من طرف اللجنة وأعوانها عن طريق استدعاء وسماع أي شخص تراه قادرا على إمدادها بالمعلومات والتبريرات المفيدة، مع تحرير محضر بذلك.

ج) المعاينات عن بعد: منح القانون الفرنسي رقم 2014/344 المتعلق بالإستهلاك لأعضاء اللجنة وأعوانها في إطار مهام وصلاحيات التحقيق وبحث الجرائم الماسة بالمعطيات الشخصية إمكانية جديدة وهي المعاينة عن بعد عبر شبكات الأنترنت، حيث تنص المادة 144 من هذا القانون والتي عدلت المادة 44 من القانون 17/78 على أنه يمكن لأعوان اللجنة المؤهلين من خلال شبكة اتصال مفتوحة للجمهور معاينة المعطيات والوصول إليها بكل حرية، أو الولوج داخل نظام المعالجة الآلية للمعطيات خلال الوقت الضروري للمعاينة، ويمكن إعادة نسخ هذه المعطيات بأي معالجة مناسبة في وثائق قابلة للاستعمال في أغراض واحتياجات المراقبة، ومن المسلم به أن المعاينات التي يمكن أن يقوم بها أعوان اللجنة تقتصر فقط على المعطيات الشخصية التي يتم تداولها بكل حرية عبر شبكات الأنترنت، لأنه لا يمكن لأعوان اللجنة الدخول عن بعد إلى المعطيات المخزنة في أنظمة معلوماتية محمية بأي شكل من الأشكال.

---

[1] Voir la délibération de la CNIL n° 2011/035 du 17 mars 2011 ; op.cit

[2] Emilie Bailly, op.cit, p 91.

[3] Voir l'article 66 du décret 2005/1309.

ويكون لهذه الطريقة القدرة على تمكين أعوان اللجنة من الحصول على أدلة رقمية بطريقة مباشرة من الأنترنت دون الحاجة إلى التثبت منها عن طريق المراقبة والبحث عبر الوثائق أو في عين المكان،[1] بالإضافة إلى منح أعوان اللجنة سلطة تحقيق عن بعد عبر شبكات الأنترنت مماثلة لتلك المعترف بها في العالم المادي، بل وتكون أسهل منها لأن هذه التحقيقات الرقمية (investigations numériques) سوف تجرى دون التمكن من ممارسة حق المعارضة من المسؤول عن المعالجة ودون إبلاغه وبالتالي دون إعداد محاضر.[2]

وفي الأخير نشير أنه من خلال السلطات الممنوحة لأعوان السلطة الوطنية المؤهلين لإجراء التحريات ومعاينة المحلات والأماكن للبحث عن جرائم الإعتداء على المعطيات الشخصية وإعداد محاضر بشأنها توجه إلى وكيل الجمهورية المختص، يكون المشرع قد خولهم بعض سلطات الضبط القضائي يمارسونها في حدود مهامهم المنوطة بهم في إطار القانون 07/18، وفقا لأحكام المادة 27 من قانون الإجراءات الجزائية[3]، كما أن المحاضر التي يعدونها في إطار مهامهم هذه تتمتع بقيمة إثباتية إلى غاية قيام الدليل العكسي، حسب ما تقتضيه أحكام المادة 216 من قانون الإجراءات الجزائية.[4]

ثانيا: القواعد الإجرائية في استخلاص الدليل الرقمي:

إن إجراءات التحقيق هي مجموعة الأعمال التي يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة، وهي تنقسم إلى إجراءات تهدف إلى الحصول على الدليل كالتفتيش والمعاينة، وإجراءات تمهد للدليل، كأوامر القبض والضبط. [5]

وسوف تقتصر دراستنا على الطائفة الأولى، لبحث أهم الإجراءات المناسبة في تحصيل الدليل الإلكتروني وتحديدا ما جاء في التعديلات التي قام بها المشرع لمواجهة الجرائم المعلوماتية، من خلال إجرائي التفتيش والضبط وذلك بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

وحتى اللحظة يصعب في غالبية الأنظمة القانونية تحديد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الادلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم المعلوماتية بصفة عامة[1]، والتي تشكل اعتداء على المعطيات الشخصية المعالجة آليا بصفة خاصة.

---

[1] Emilie Baailly, op.cit, p 91.

[2] Yann Padova, la CNIL, nouvel acteur du contrôle dans le cyber espace, un article disponible sur le site : http://www.cio-online.com

[3] تنص المادة 27 من قانون الإجراءات الجزائية على أنه:" يباشر الموظفون وأعوان الإدارات والمصالح العمومية بعض سلطات الضبط الإداري التي تناط بهم بموجب قوانين خاصة وفق الأوضاع وفي الحدود المبينة في تلك القوانين"

[4] تنص المادة 216 من قانون الإجراءات الجزائية على أنه: "في الأحوال التي يخول فيها القانون بنص خاص لضباط الشرطة القضائية أو أعوانهم أو للموظفين وأعوانهم الموكلة إليهم بعض مهام الضبط القضائي سلطة إثبات جنح في محاضر أو تقارير تكون لهذه المحاضر أو التقارير حجيتها ما لم يدحضها دليل عكسي بالكتابة أو شهادة الشهود".

[5] طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، مجلة الشريعة والقانون، العدد الثامن والعشرون المجلد الأول، جامعة الطائف، المملكة العربية السعودية، ص 277.

ومما لا شك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط، بل نظم ذلك عن طريق قواعد إجرائية معينة، تتناسب مع طبيعة هذه الجريمة وطبيعة الدليل الذي يصلح لإثباتها الذي ينمو في رحم البيئة المعلوماتية، ومما لا شك فيه أيضا أن هذه القواعد عامة النطاق، تنظم استخلاص الدليل في جميع الجرائم تقليدية كانت أم معلوماتية، إلا أنها في هذه الأخيرة قد تكون بحاجة إلى تطوير لكي تتناسب مع الطبيعة الخاصة لهذه الجرائم وطبيعة الدليل الذي يصلح لإثباتها، وطبيعة البيئة الإفتراضية التي ينشؤ فيها.

1) التفتيش عن الدليل الرقمي: إذا كان التفتيش هو التنقيب في وعاء السر بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة، وأن جوهره هو كشف نقاب السرية عما تحويه أنظمة الحاسوب من خفايا وأسرار ونوايا إجرامية، وبالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة، فهو بهذا المعنى لا يتقيد بالكيان المادي لوعاء السر.

1-1) التفتيش* في البيئة الرقمية: يعد تفتيش أنظمة المعالجة الآلية من أخطر الإجراءات كونه ينصب على محل غير مادي، لا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي، لذلك فقد ثار التساؤل حول مدى إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب وشبكات الأنترنت، طالما أن هذا الإجراء يهدف إلى جمع الأدلة المادية في حين أن نظم المعلومات هي عبارة عن كيان معنوي.[2]

ومن المعروف أن النظام المعلوماتي يتكون من مكونات مادية (HardWare) ومكونات منطقيه (SoftWare) كما أن له شبكات اتصال بعدية سلكية ولا سلكية على المستوى المحلي والدولي[3]، ومن ثم فإن محل التفتيش في مثل هذا النوع من الجرائم هو هذه المكونات.

غير أنه إذا كان التفتيش الواقع على المكونات المادية للحاسوب فإنه لا توجد أي مشكلة في تنفيذه لإمكانية ذلك وسهولته[4]، مع الأخذ بعين الإعتبار الضمانات الخاصة بهذا الإجراء المنصوص عليها طبقا للقواعد التقليدية للتفتيش[5]، لكن المشكلة التي يستشعرها الفقه تتعلق بمدى إمكانية تفتيش مكونات الحاسوب

---

[1] الرائد عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، مقال منشور على الموقع: www.arablawinfo.com بدون ترقيم.

* تعددت التعريفات الفقهية لإجراء التفتيش ومن أهمها: أنه عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بحرمة، وذلك وفقا لمقتضيات وضمانات وقيود مقررة قانونا، أنظر هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، الطبعة الأولى، دار النهضة العربية 1997، مصر 47، وكذلك على حسن الطوالبة، مرجع سابق، ص ص 10،11.

[2] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة إربد، الأردن 2004، ص 07.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دار الفكر الجامعي، الإسكندرية 2009، ص 195.

[4] علي حسن الطوالبة، مرجع سابق، ص 28.

[5] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت الطبعة الأولى، دار الثقافة للنشر والتوزيع عمان الأردن 2011، ص 151.

المنطقية أو المعنوية، نظرا لغياب الطبيعة المادية للمعطيات في حد ذاتها عندما تكون مجردة من دعامتها المادية،[1] وقد أخذ الفقه في هذه المسألة اتجاهين:

الإتجاه الأول يرى عدم إمكانية انسجام وتطابق أحكام التفتيش المنصوص عليها في القوانين الإجرائية مع ما قد يتطلبه كشف الحقيقة فيما يتعلق بالمعطيات المعلوماتية، من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته، وأن هدف التفتيش يتحدد في البحث عن الأشياء وضبطها وهذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس، ولا يمتد في نطاق شموله إلى الكيانات المنطقية أو المعنوية للحاسب الآلي.[2]

بينما تتمثل فكرة أصحاب الإتجاه الثاني في أن برامج الحاسوب وبياناته ينطبق عليها خصائص وسمات المادة وبالتالي تدخل في نطاق الأشياء[3] التي يصلح تفتيشها وضبطها، لأن الغاية من التفتيش هو الحصول على الأدلة الخاصة بالجريمة وكشف الغموض الذي أحاط بها وتقديم المعطيات المعالجة بطريقة غير مشروعة والمخزنة على الحاسوب الخاص بالجاني كدليل اتهام ضده.[4]

وبالنتيجة تكون هذه المعطيات المخزنة في الحاسوب صالحة لأن تكون محلا للتفتيش، ويمكن ضبطها وتسجيلها على الورق أو على أية دعامة أخرى يصح الإستناد إليها كدليل على ارتكاب الجريمة[5]، وذلك من خلال الدخول إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت.[6]

ومن خلال القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، يتضح موقف المشرع الجزائري حيث أجاز صراحة تفتيش المنظومات المعلوماتية وذلك بموجب المادة 05 منه، والتي نصت على أنه "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية... الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين معلوماتية. والمشرع الفرنسي من جانبه قام بتعديل الأحكام التي تحكم التفتيش مضيفا عبارة المعطيات المعلوماتية لنص المادة 94 من قانون الإجراءات الجزائية بموجب المادة 42 من القانون 2004/575 المتعلق بالثقة في

[1] عبد العظيم وزير، شرح قانون العقوبات، القسم الخاص، جرائم الإعتداء على الأموال الطبعة الأولى، دار النهضة العربية، القاهرة 1993، ص 40.

[2] علي حسن الطوالبة، مرجع سابق، ص 31.

[3] هلالي عبد الله أحمد، تفتيش نظم الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص 75 وما بعدها.

[4] خالد عياد الحلبي، مرجع سابق، ص 160.

[5] خالد عياد الحلبي، نفس المرجع، ص 160.

[6] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 194.

الاقتصاد الرقمي،[1] ليصبح نص هذه المادة على النحو التالي: "يباشر التفتيس في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".[2]

وينص القانون الإنجليزي المتعلق بإساءة استخدام الحاسوب لسنة 1990 «the computer Misuse Act » على جواز تفتيش نظم الحاسوب المادية والمعنوية، حيث اعتبر هذا القانون أن إجراءات تفتيش نظم الحاسوب في جرائم الولوج والتعديل غير المصرح به للمعطيات المخزنة بأنظمة الحاسوب تتم دون إذن طالما كان هدف الولوج ارتكاب أفعال غير مشروعة عن قصد، أما إذا كان الولوج مجردا دون نية ارتكاب أفعال غير مشروعة، فإن التفتيش يكون بموجب إذن قضائي.[3]

وكذلك كان الشأن في الاتفاقية الأوروبية للجريمة الإلكترونية المسماة اتفاقية بودابست، حيث تضمنت في الفصل الرابع الذي جاء تحت عنوان البحث عن بيانات الكمبيوتر المخزنة ومصادرتها، المادة 19 التي نصت على أنه "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من التفتيش والنفاذ إلى:

- أي نظام كمبيوتر أو أي جزء منه، وكذلك المعطيات المعلوماتية المخزنة فيه.

- أي دعامة أو وسائط تخزين بيانات الكمبيوتر المخزنة داخلها على أراضي تلك الدولة الطرف.

وقد أشار التقرير التفسيري لهذه الإتفاقية أنه في إطار البحث عن الأدلة لاسيما المعطيات المعلوماتية، لا تزال العديد من خصائص التفتيش التقليدي قائمة في البيئة المعلوماتية، إلا أنه من الضروري وضع أحكام إجرائية إضافية بغية تأمين الحصول على معطيات الكمبيوتر بنفس الدرجة من الفعالية، كالبحث في سجل مادي للبيانات ومصادرته.[4]

وإذا كان قد انتهى لدينا أن تفتيش الأنظمة المعلوماتية عملية مشروعة قانونا، إلا أنه في نفس الوقت يحمل في طياته عمليات إلكترونية غاية في التعقيد، فقد تكون المنظومة محمية بكلمات السر، أو تكون المعطيات المقصودة مشفرة، أو تكون متواجدة ضمن ملايين الملفات، فيكون بذلك من الصعب تنفيذه عمليا، خاصة أمام عدم جواز إلزام الشخص بالإفصاح عن كلمات السر أو مفتاح التشفير، لأجل ذلك أدرج التقرير التفسيري لاتفاقية بودابست تدبيرا قسريا يرمي إلى تسيير البحث عن بيانات الكمبيوتر عندما يكون من الصعب النفاذ إليها بسبب كمية المعطيات التي يمكن معالجتها وتخزينها، وكذا نشر التدابير الأمنية، وذلك عن طريق إرغام مسؤول النظام المعلوماتي على تقديم المساعدة "بالقدر المعقول" في إجراء

[1] L'article 42 de la loi n° 2004/575 du 21 juin 2004 pour la confiance dans l'économie numérique JORF n° 143/du 22 juin 2004 dispose que :« L'article 94 du code de procédure pénale après les mots : « des objets » sont insérés les mots : « ou de données informatiques » »

[2] L'article 94 du code de procédure pénale dispose que : « les perquisitions sont effectués dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité ou des biens dont la confiscation est prévue à l'article 131-21 du code pénale »

[3] علي حسن الطوالبة، مرجع سابق، ص 34.

[4] التقرير التفسيري لاتفاقية الجرئم الإلكترونية، سلسلة المعاهدات الأوروبية 185، ص 30.

عمليات التفتيش والمصادرة، ويشمل القدر المعقول الإفصاح عن كلمة السر أو أي تدابير أمنية أخرى لسلطات التحقيق مع الإلتزام في كل الأحوال بضرورة عدم تهديد معطيات شخصية لمستخدمين آخرين أو معطيات أخرى غير مرخص بالبحث فيها[1]، وهو الإجراء الذي أخذ به المشرع الجزائري في الفقرة الأخيرة من المادة 05 من القانون 04/09 حيث نصت على أنه "يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تضمنتها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

وقد كان المشرع الفرنسي هو الآخر قد فرض هذا الإجراء القسري بغية تسهيل عملية التفتيش من خلال نص المادة 57-1 من قانون الإجراءات الجزائية[2]، بل أكثر من ذلك فإن المشرع الفرنسي أعطى الجهات المختصة من وكيل الجمهورية أو لقاضي التحقيق أو لضابط الشرطة القضائية بعد ترخيص من وكيل الجمهورية أو لجهة الحكم، سلطة تعيين شخص طبيعي أو معنوي يكون مؤهلا للقيام بفك التشفير عن المعطيات المشفرة اللازمة لتحقيق جنائي إذا كان هذا الإجراء ضروريا.[3]

2-1) التفتيش الإلكتروني عن بعد: Perquisition à distance: مع التطور التكنولوجي لثورة الإتصالات عن بعد لم يعد نطاق الإتصالات محدودا في إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم بعد ظهور شبكة الأنترنت، والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لامركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسيب الموزعة عبر مختلف دول العالم.

لذلك فالسؤال المطروح في هذا الصدد يتعلق بمدى خضوع شبكات نظام المعالجة الآلية للتفتيش، وهي مسألة تتعلق بالتفتيش عن بعد، نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة رقمية عبر شبكات حاسوبية في أماكن مجهولة بعيدا تماما عن الموقع المادي للتفتيش[4]، فقد يكون الموقع الفعلي للشبكات داخل اختصاص قضائي آخر وحتى في بلد آخر، باعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم تقريبا، وبالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة تخضع للقانون الإجرائي الخاص بتلك المنطقة.[5]

---

[1] أنظر التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مرجع سابق، ص 33.

[2] L'article57-1du code de la procedure penale Français dispose que les offissiers de police judiciaire peuvent par tout moyen requérire toute personne susceptible : de leur remettre les informations permettant d'accéder aux données aux quelles il est permis d'accéder dans le cadre de la perquisition.

[3] Voir l'article 230-1 du code de la procédure pénale inséré par l'article 30 de la loi n° 2001/1062 du 15 novembre 2001 relative à la sécurité quotidienne, JORF n° 266 du 16 novembre 2001 p.18215 : « le procureur de la république la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la république, ou du juge d'instruction, ou la juridiction de jugement saisie de l'affaire, peut désigner toute personne physique ou morale qualifier en vue d'effectuer les opérations techniques permettant d'obtenir l'accès à ces informations ... dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de d'échiffrement, si cela apparait nécessaire.

[4] رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، مرجع سابق، ص 401.

[5] علي حسن الطوالبة، مرجع سابق، ص 42.

ويمكن التمييز في هذه الصورة بين احتمالين على النحو التالي:

- اتصال حاسب المشتبه فيه بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل نفس الدولة: والسؤال المطروح هنا حول مدى إمكانية أن يمتد إجراء التفتيش إلى أجهزة الحاسوب الأخرى المتصلة بجهاز المشتبه فيه، وفي هذه الحالة هناك من التشريعات الإجرائية من عمد إلى حل هذه المشكلة من خلال النص على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجرى تفتيشه (أي الشبكة وما يتصل بها) وتسجيل كل المعطيات اللازمة كأدلة إثبات.[1]

ويعتبر المشرع الجزائري من بين هذه التشريعات، حيث نصت الفقرة الثانية من المادة 05 من القانون 04/09 بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها، وكانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، فإنه يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، والمشرع الفرنسي حسم هذه المسألة أيضا بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون 2003/239 المتعلق بالأمن الداخلي[2]، حين أجازت المادة 17 منه والتي أضافت المادة 57-1 لقانون الإجراءات الجزائية لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية في إطار التفتيش المنصوص عليه، الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، بما أن هذه المعطيات يتم الدخول إليها أو تكون متاحة انطلاقا من النظام الرئيسي.[3]

وكذلك تسمح الإتفاقية الأوروبية لجرائم تقنية المعلومات للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله نظام معلوماتي معين إلى غيره من الأنظمة المرتبطة به، في حال الإستعجال إذا كان يتواجد به معطيات يتم الدخول إليها في هذا النظام من خلال النظام محل التفتيش.[4]

- إتصال حاسب المشتبه فيه بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة: وهنا من المتصور طبقا لهذه الحالة أن يقوم مرتكبوا الجرائم بتخزين المعطيات في أنظمة معلوماتية خارج الدولة عن طريق شبكات الإتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة[5]، ولذلك فمن المشاكل

[1] علي حسن الطوالبة، نفس المرجع، ص 43.

[2] L'article 17 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieur, JORF n° 66 du 19 mars 2003, p 4761 modifié par la loi n° 2016-731 du 03 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale dispose que : le code de procédure pénale est modifié, il est inséré un article 57-1 ainsi rédige :

« Les officiers de police judiciaire ou sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique, dés lorsque ces données sont accessibles à partir du système initiale ou disponibles pour les système initial »

[3] Voir plus Myriam Quéméner, Joel Ferry, cybercriminalité défi mondial, 2ème édition, economica, 2009, P2.

[4] أنظر المادة 2/19 من اتفاقية بودابست، مرجع سابق، ص 10

[5] عبد الله حليس علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث منشور على موقع: www.arablawinfo.com

التي تواجه جهات التحقيق في هذه الحالة، هو تطلب امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر عن جهاتها المختصة الإذن بالتفتيش، ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به لتمسك كل دولة بسيادتها وحدودها الإقليمية.[1]

لأجل هذا فإن جانبا من الفقه يرى أن التفتيش الإلكتروني العابر للحدود ينبغي أن يتم في إطار اتفاقيات ثنائية أو دولية تجيز هذا الإمتداد، وأنه لا يجوز القيام به في ظل غياب تلك الإتفاقيات.[2]

ولمواجهة هذا الإحتمال أجاز المشرع الجزائري تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو الأمر الوارد بالفقرة الثالثة من المادة 05 من القانون 04/09 حيث تنص على أنه: "....إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة وفقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل، وهذا ما نجده أيضا في نص الفقرة الثانية من المادة 57-1 من قانون الإجراءات الجزائية الفرنسي.[3]

وفي نفس الإطار تجيز التوصية الأوروبية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات، أن يمتد التفتيش الإلكتروني لنظام معلوماتي إلى الشبكة المتصل بها ولو كانت تلك الشبكة تقع خارج إقليم الدولة.[4]

2) ضبط الدليل الرقمي: إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه، فهو بذلك غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه هذا الإجراء،[5] لذلك فإنه يقصد بالضبط من حيث طبيعته القانونية كإجراء من إجراءات التحري أو التحقيق هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها[6]، بعد استبقائه تحت تصرف المحقق لمصلحة التحقيق.

ولقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال جرائم الإعتداء على المعطيات ذات الطابع

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 205.

[2] محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية الشرطة، مركز البحوث والدراسات، دبي خلال الفترة 26-28 أفريل 2003، ص 10 منشور على الموقع: www.arablawinfo.com

[3] L'article 57-1/2 du code de procédure pénal français dispose que :

« s'il est préalablement avéré que ces données initiales, sont stockées dans un autre système informatique situé en dehors du territoire nationale elle sont recueillies par l'officier de police judiciaires, sous réserve des conditions d'accès par les engagements internationaux en vigueur. »

[4] Voir : alinéa n° 02 de l'annexe à la recommandation n° R (95)13 du comité des ministres aux états membres de conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée par le comité des ministres le 11 septembre 1995 lors de la 543ème réunion des délégués des ministres.

[5] علي حسن الطوالبة، مرجع سابق، ص 135.

[6] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 394.

الشخصي المعالجة آليا ذات الطبيعة المعلوماتية، فإن الضبط ينصب على المكونات المعنوية للحاسب من مختلف البرامج والمعطيات المعالجة آليا والتي تعد عبارة عن نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي الذي يتوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم.

وعلى هذا الأساس فإذا كان ضبط المكونات المادية للحاسوب بشكل كامل لتأكيد الإحتفاظ بالدليل إذا كان مستعمل الجهاز غير متعاون مع جهات التحقيق[1]، فإنه بالنسبة للمكونات المعنوية للحاسب نجد أن التشريعات الإجرائية والاتجاهات الفقهية قد اختلفت حول مسألة صلاحية ضبطها كونها لا تصلح بطبيعتها لأن تكون محلا لوضع اليد وهي مجردة من دعامتها المادية المثبتة عليها، كضبط ملفات إلكترونية تحوي معطيات شخصية تم التلاعب بها.

لقد حسم المشرع الجزائري موقفه عندما شايع الإتجاه الفقهي الذي يرى أنصاره أن المعطيات المخزنة آليا كونها مجردة عن الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط، طالما أن الغاية من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل المعطيات المعلوماتية بمختلف أشكالها، لذلك تدخل بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولجيات الإعلام والإتصال أين استحدث المادة 06 التي تنص على أنه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، فإنه يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية، وأنه يجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، كما يجوز لهذه السلطة استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط ألا يؤدي ذلك إلى المساس بمحتوى المعطيات".

وإلى جانب المشرع الجزائري اعتمد المشرع الفرنسي تعديلا على قانون الإجراءات الجزائية وذلك بموجب قانون الأمن الداخلي عندما استحدث المادة 57-1 والتي نصت بدورها على أن المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة (إجراءات التفتيش) يتعين نسخها على دعامات التخزين المعلوماتية، وهذه الدعامات يتعين تحريزها في أحراز مختومة وفقا للشروط المنصوص عليها في هذا القانون.

وقد جاء هذا التعديل في التشريع الفرنسي التزاما منه باتخاذ التدابير التشريعية التي ألزمت اتفاقية بودابست الأطراف الموقعة باتخاذها، من خلال الفقرة الثالثة من المادة 19 من هذه الاتفاقية، حيث ألزمت كل طرف بمنح سلطاته المختصة صلاحية ضبط أو تأمين معطيات الكمبيوتر التي يتم الدخول إليها طبقا للفقرتين الأولى والثانية وتشمل هذه الإجراءات صلاحية:

- ضبط أو تأمين النظام المعلوماتي أو جزء منه أو وسيط تخزين المعطيات.

[1] عفيفي كامل عفيفي، مرجع سابق، ص 353.

- إجراء نسخة من هذه المعطيات والإحتفاظ بها.

- المحافظة على تجانس معطيات الكمبيوتر المخزنة ذات الصلة.

- جعل هذه المعطيات غير قابلة للدخول عليها أو إزالتها على نظام الكمبيوتر الذي يتم الدخول عليه.

أما عن إجراءات ضبط الدليل الرقمي، فإنه من خلال استقرائنا للمادتين 6 و7 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، نجد أن المشرع وضع طريقتين لضبط الأدلة الرقمية:

- الأولى وتكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز، حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية.[1]

- الطريقة الثانية تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة، أو القيام بنسخها، ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى.

وإذا كان مما تقدم ذكره لا يضير أن يخضع الدليل الرقمي في ضبطه من خلال قواعد تحريز الأدلة الجنائية عموما، إلا أنه ونظرا إلى الطبيعة الخاصة له فإن عملية ضبطه وتحريزه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا والحفاظ عليه وصيانته من إمكانية العبث به، وهذا ما نوه عليه المشرع الجزائري في المادة السادسة الفقرة الثالثة من القانون 04/09 حينما أوجب على السلطات التي تقوم بعملية ضبط الدليل الرقمي أن تحرص على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات.

وفي هذا الإطار بالذات نجد الهيئة الدولية لدليل الحاسب الآلي (international organisation on computer evedence (IOCE))وضعت عدة ضوابط لعملية ضبط الدليل الرقمي، ومنها ألا تكون الإجراءات المتخذة في تحريز الدليل الرقمي سببا في تغيير طبيعة هذا الدليل، وأن تكون جميع الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها أو نقلها موثقة توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة[2].

المطلب الثاني: القيمة القانونية للدليل الرقمي في مجال إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:

لقد توجس الفقه والقضاء خيفة من الدليل الرقمي، وذلك لإمكانية عدم تعبيره عن الحقيقة، نظرا لما يمكن أن تخضع له طرق الحصول عليه من التزييف والتحريف والعبث، مما أثيرت مسألة مشروعية

[1] راجع المادة 84 من قانون الإجراءات الجزائية.

[2] http://www.oas.org/juridico/english/cyber_links_ioce.htm

الأخذ به. حيث يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه.[1]

كما أثيرت أيضا مسألة مصداقية أو حجية الدليل الرقمي في تعبيره عن الحقيقة التي تهدف إليها الدعوى الجزائية، خاصة إذا أخذنا بعين الإعتبار الصعوبات التي تصاحب استخلاص هذا الدليل، فضلا عن التطور في مجال المعلوماتية الذي قد يتيح العبث بهذا النوع من الأدلة مما يجعل مضمونه مخالفا للحقيقة، وعلى ذلك كيف يمكن ضمان مصداقيته ومن ثم تكون له الحجية في الإثبات.

لذلك فإن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يمكن التعويل عليه، إذ يلزم أن تكون لهذا الدليل قيمة قانونية، وقيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين: الأولى تتعلق بمشروعية الدليل والثانية مرتبطة بحجية أو يقينية الدليل على الوقائع المراد إثباتها.[2]

الفرع الأول: مشروعية الدليل الرقمي:

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، والمشروعية بهذا المفهوم تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول على هذه الحريات والحقوق في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الإجتماعي، وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[3]

ومما لا شك فيه أن مبدأ شرعية الجرائم والعقوبات الذي يستقيم عليه بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي، ويفرض خضوعها هي الأخرى لمبدأ الشرعية، والتي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريقة غير مشروعة، لذلك فإن مسألة قبول الدليل الجنائي تعد الخطوة الأولى التي يتخذها القاضي الجنائي تجاهه، وذلك بعد التنقيب عنه وقبل إخضاعه لتقديره.

وقبول الدليل على هذا النحو يقتضي أن يكون مشروعا في وجوده، فيكون من ضمن الأدلة التي يجيز القانون الإستناد إليها ومشروعا في الحصول عليه.

أولا: مشروعية وجود الدليل الرقمي:

يقصد بمشروعية وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه ضمن قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الإستناد إليه في تكوين اقتناعه[4].

[1] رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، مرجع سابق، ص 478.

[2] طارق محمد الجملي، مرجع سابق، ص 51.

[3] هلالي عبد الله أحمد، مرجع سابق، ص 104.

[4] رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية للمعطيات، مرجع سابق، ص 479.

ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي، يتمثل في طبيعة نظام الإثبات المعتمد في المنظومة التشريعية الجزائية، حيث تعرف التشريعات الإجرائية الجزائية نظامين رئيسيين للإثبات هما:

- نظام الإثبات المقيد: يحظر على القاضي بمقتضى هذا النظام أن يقيم حكمه في الدعوى الجزائية إلا بناء على أدلة محددة سلفا من قبل المشرع[1]، حيث يقوم المشرع بتحديد أدلة الإثبات حصرا وكذا القوة الإثباتية لكل دليل من الأدلة[2] ويقدر قيمتها الإقناعية[3]، وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، حيث يحدد للقاضي الأدلة التي يجوز له قبولها واللجوء إليها في الإثبات، ولا سبيل للإستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، وعليه فإنه في ظل هذا النظام لا يمكن الإعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات القانونية، ولا يجوز للقاضي أن يستند عليه لتكوين عقيدته مهما توافرت فيه شروط اليقين، طالما خلا القانون من النص عليه.[4]

ويمكن أن يعاب على هذا النظام أنه من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها القانون فيصبح القاضي كالآلة في إطاعته للنصوص القانونية، لذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اقتناعا به.

فبريطانيا مثلا التي تأخذ بهذا النظام مثل باقي الدول الأنجلوسكسونية بدأت تخفف من غلوائه، حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك، والتي مفادها أن القاضي يستطيع أن يكون قناعته من أي دليل وإن لم يكن ضمن الأدلة المنصوص عليها، متى كان هذا الدليل قاطعا في دلالته، وتطبيقا لهذا الفهم اتجه المشرع البريطاني نحو قبول الدليل الرقمي وتحديد قيمته الإثباتية تجاوبا واتفاقا مع طبيعة النظام القانوني البريطاني، حيث يوجد قانون البوليس والإثبات الجنائي لسنة 1986، الذي يحوي تنظيما محددا لمسألة قبول مخرجات الحاسوب والأنترنت كأدلة إثبات في المواد الجنائية، وكذلك في الولايات المتحدة الأمريكية مثل قانون الحاسوب لسنة 1984 الصادر في ولاية (إيوا) الذي يعتبر أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والمعطيات المخزنة فيه حسب نص المادة (716/أ/16)، وكذا قانون الإثبات الصادر في سنة 1983 في ولاية كاليفورنيا الذي يعتبر أن النسخ المستخرجة من المعطيات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه المعطيات.

- نظام الإثبات الحر: وتأخذ به القوانين ذات الصياغة اللاتينية، ويقتضي هذا النظام عدم القيام سلفا بتحديد أدلة بعينها يتوجب على القاضي أن يستند إليها في إصداره لحكمه، وإنما يكون متمتعا بسلطة

[1] عفيفي كامل عفيفي، مرجع سابق، ص 365.
[2] طارق محمد الجملي، مرجع سابق، ص 52.
[3] علي حسن الطوالبة، مرجع سابق، ص 196.
[4] طارق محمد الجملي، مرجع نفسه، ص 52.

تقديرية واسعة، سواء من حيث قبول الأدلة ذاتها أو من حيث تقديره الشخصي لقيمة كل منها[1]، ففي ظل هذا النظام لا يرسم المشرع طرقا محددة للإثبات يتقيد بها القاضي الجنائي، بل يترك حرية الإثبات لأطراف الخصومة الجزائية في أن يقدموا ما يرون أنه مناسب من أدلة لإقناع القاضي، ولهذا الأخير أن يقدر القيمة الإقناعية لها[2] وليس للقانون أن يلزمه بأدلة معينة يستند إليها في تكوين قناعته.[3]

فمثل هذا النظام لا يحفل بالنص على أدلة محددة للإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية بقبول الدليل أو رفضه إذا لم يطمئن إليه[4]، ويستند هذا النظام إلى عدة مبررات من أهمها أن الإثبات في المسائل الجزائية لا ينصب إلا على الوقائع المادية الخاصة بالواقعة الإجرامية ولا ينصب على تصرفات قانونية يتفق معها قيام المشرع سلفا بتحديد وسائل إثباتها ومدى الحجية التي تتمتع بها بالإضافة إلى أن الجناة غالبا ما يعمدون بقدر ما يستطيعون أن يزيلوا آثار جرمهم، الأمر الذي يحتم تخويل القضاء كافة الوسائل المتاحة والممكنة لتقصي الحقيقة.[5]

والمشرع الجزائري قد أقر بمبدأ حرية الإثبات الجزائي في المادة 212 من قانون الإجراءات الجزائية، حيث نصت على أنه "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي"، وكذلك كان موقف المشرع الفرنسي حينما نصت المادة 427 من قانون الإجراءات الجزائية على أنه "مالم يرد نص مخالف، يجوز إثبات الجرام بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي[6]"

ومن ثمة فإن الدليل الإلكتروني يستمد مشروعية وجوده وقبوله انطلاقا من مبدأ حرية الإثبات، فالمشرع الجزائري كغيره من التشريعات المنتمية إلى هذا النظام لا نجده قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، ومن ثم فلا تثار مسألة مشروعية وجود الدليل الإلكتروني وقبوله، فالقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكذلك القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي لم يتضمنا أية أوضاع خاصة في الإثبات، وتركا الأمر للقواعد العامة التي تقتضي أن الأصل في الأدلة مشروعية وجودها، ومن ثم يكون الدليل الرقمي مشروعا من حيث وجوده اصطحابا للأصل.

---

[1] عفيفي كامل عفيفي، مرجع نفسه، ص 369.

[2] عبد الله موسى مسعود رحومة، حرية القاضي الجنائي في تكوين عقيدته، دراسة مقارنة، الطبعة الأولى، الدار الجماهيرية للنشر والتوزيع والإعلان، مصراتة ليبيا، 1988، ص 25.

[3] طارق الجملي، مرجع سابق، ص 12.

[4] هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، مرجع سابق، ص 91.

[5] عفيفي كامل عفيفي، مرجع سابق، ص 369.

[6] Article 427/1 du code de procédure pénal français dispose que : « hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction »

ثانيا: مشروعية الحصول على الدليل الرقمي:

وإذا كان مبدأ حرية الإثبات يجيز للقاضي الجزائي الإستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل الرقمي لتكوين اقتناعه، إلا أن الإدانة في أي جريمة لابد أن تكون مبنية على أدلة مشروعة، تم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي، فلا يكون مشروعا الدليل الإلكتروني إلا إذا جرى التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء و إقامته أمامه وفقا للطرق والإجراءات التي رسمها القانون[1]، فمتى ما تم الحصول على الدليل الرقمي خارج هذه القواعد القانونية، فلا يعتد بقيمته ولا يقبل كدليل إثبات مهما كانت دلالته الحقيقة، وذلك لعدم مشروعية الحصول عليه، لأن مشروعيته تقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن[2]، وإذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليه، فإنها تكون باطلة وبالتالي بطلان الدليل المستمد منها.[3]

ومشروعية الحصول على الدليل بصفة عامة لا تعن بالضرورة اتفاق الإجراء مع القواعد القانونية التي ينص عليها المشرع فحسب، بل تتعدى ذلك إلى مراعاة إعلانات حقوق الإنسان والمواثيق والإتفاقيات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع[4].

وقد كان الفقه والقضاء الفرنسي بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أو التنقيب في الجرائم المرتبطة بالمعلوماتية، حيث يشير رأي فقهي فرنسي إلى أن القضاء قد قبل باستخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ومن بينها الأدلة الرقمية بطريقة مشروعة ونزيهة[5]، كما تجسد هذا المبدأ من خلال التطبيقات القضائية الفرنسية، حينما أكدت محكمة النقض الفرنسية أن الأدلة المقامة ضد المتهم ليست مشروعة كونها تم الحصول عليها نتيجة تحريض المعني على ارتكاب الجريمة، وهو إجراء غير معترف به في القانون الفرنسي، واعتبرت أن التحريات لم تراع مبدأ المشروعية ويتعين إلغاؤها بالرغم من تحقق إدانة المتهم بالجريمة.[6]

وترتيبا على ذلك فإنه لا يجوز للقاضي القبول بدليل رقمي تم الحصول عليه من إجراء تفتيش إلكتروني جرى القيام به دون مراعاة للشروط الشكلية والموضوعية الخاصة بهذا الإجراء*، والحكمة من تقرير

---

[1] Jen-Raphael Dermachi, la loyauté de la preuve en procédure pénale, outil transational de protection du justiciable, note sous crime 7 févr 2007, Recueil Dalloz n°28. 7301, page 2012-2016.

[2] طارق الجملي، مرجع سابق، ص 59.

[3] رشيدة بوكر، جرائم الا عتداء على نظم المعالجة الآلية، مرجع سابق، ص 490.

[4] هلالي عبد الله أحمد، مرجع سابق، ص 118.

[5] علي حسن محمد الطوالبة، مرجع سابق، ص 186.

[6] Cass.crim, 04 juin 2008 n° de pourvoi 08-81045, bulletin criminel, n° 141, 2008 ; « au motif que la procédure conduite en France serait fondée sur un stratagème des autorités américaines ayant provoqué l'intéressé à la commission d'une infraction, l'arrêt retient que si la provocation à la commission d'une infraction porte atteinte au principe de loyauté des preuves et les poursuites furent annulées, malgré la certitude que la prévenu s'était bien rendu coupable des infractions qui lui était reprochées »

* من الشروط والضمانات التي يجب توافرها في التفتيش الرقمي منها ماهو شكلي ومنها ما هو موضوعي:

مشروعية الحصول على الدليل عموما هو التوفيق بين مصلحة المجتمع في تقريره للعقاب ومصلحة الفرد في احترام حرياته في إطار مبدأ الشرعية الإجرائية، ومن ثم تصبح هذه الضمانات الإجرائية غير ذات قيمة ما لم يتقرر الجزاء على مخالفتها، لذلك فإن قانون الإجراءات الجزائية يرتب البطلان كجزاء إجرائي على الإجراء المخالف للقانون[1]، والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة، وهو الرأي الذي أخذ به المشرع الجزائري بنص المادة191 من قانون الإجراءات الجزائية التي نصت على أنه :"تنظر غرفة الإتهام في صحة الإجراءات المرفوعة إليها، وإذا تكشف لها سبب من أسباب البطلان، قضت ببطلان الإجراء المشوب به وعند الإقتضاء ببطلان الإجراءات التالية له كلها أو بعضها".

الفرع الثاني: حجية الدليل الرقمي في إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:

إن مسالة تقدير الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، لأجل هذا فالسائد في الفقه الجنائي أن القاضي الجزائي له الحرية في تقدير الأدلة الجنائية وتكوين قناعته[2]، وأن يبني حكمه على أي دليل متى اطمأن إليه حتى ولو كان هذا الدليل مستمدا من محاضر جمع الإستدلالات.[3]

وإذا كانت مسألة حرية القاضي في قبول الأدلة مسألة قانونية حسمها المشرع بتحديده للشروط القانونية للدليل القابل للإثبات، ومن ثم لا مجال للقاضي لإعمال سلطته التقديرية بشأنها، فمتى توفرت في هذا الدليل الشروط المحددة طبقا لمبدأ الشرعية الإجرائية، وجب على القاضي قبول الدليل، وإن كان خلاف ذلك كان له طرحه، فإن مسألة حرية القاضي في تقدير الدليل مسألة موضوعية تتعلق بقيمة الدليل لإثبات الحقيقة للقاضي أن يمارس سلطته التقديرية فيها.

أهم الشروط الشكلية للتفتيش في البيئة الرقمية:

- إذن بالتفتيش صادر من الجهة القضائية المختصة.
- إجراء التفتيش بحضور أشخاص معينين بالقانون وهم المشتبه فيه أو المتهم أو من ينوبه.
- احترام الميقات الزمني للتفتيش، وبالنسبة للجرائم ذات الطبيعة المعلوماتية فإنه يجوز التفتيش في كل ساعة من ساعات النهار والليل حسب المادة 47 من قانون الإجراءات الجزائية.
- تحرير محضر التفتيش تدون فيه كل الخطوات والإجراءات المتخذة أثناءه.

ومن أهم الشروط الموضوعية:

- سبب التفتيش ويتحقق بوقوع الجريمة التي يتم توجيه الاتهام بموجبها إلى الشخص المراد تفتيشه.
- محل التفتيش ويقصد به هنا المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الإلكترونية.
- السلطة المختصة بالتفتيش إما جهات التحقيق القضائي أو ضابط الشرطة القضائية.

[1] حسن الطوالبة، مرجع سابق، ص 167.

[2] يعرف الفقه الجنائي الاقتناع الشخصي للقاضي الجزائي بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة، والتي يثيرها الخصوم إما لإثبات أو إنكار اتهام، وعرف أيضا بأنه حالة ذهنية ذاتية تنجم عن إمعان الفكر في وقائع معروضة من أجل بحثها والوصول بعد ذلك إلى حالة تطرد الشك والاحتمال، أنظر زبدة مسعود، الإقتناع الشخصي للقاضي الجزائي، الطبعة الأولى، المؤسسة الوطنية للكتاب، الجزائر 1989، ص 08، وكذلك نصر الدين ماروك، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، الجزء الأول، دار هومة، الجزائر، 2009، ص 620.

[3] محمد عبد الغريب، حرية القاضي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية، دار النهضة العربية، القاهرة 2008، ص 32.

غير أن تطبيق ذلك على الدليل الرقمي قد يثير بعض الصعوبات، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المرتبطة بأصالة الدليل الرقمي، فضلا عن تمتع هذا الدليل من حيث قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين، شأنه في ذلك شأن الأدلة العلمية عموما، ومن جهة أخرى فإن الطبيعة الفنية للدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة، دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث.[1]

ومن ثم فهل يمكن التسليم بأن الدليل الرقمي لا يحظ بقوة حاسمة في الإثبات، وهو مجرد دليل لا تختلف قيمته عن غيره من الأدلة الأخرى، وبالتالي يخضع للمناقشة والبحث في مصداقيته لقبوله أو طرحه لعدم الاقتناع به، ولا يجوز إلزام القاضي بالاقتناع به ولو لم تكن في الدعوى أدلة سواه.

وعلى هدي ما سبق طرحه سوف نناقش ما هي الشروط التي يجب أن يتوفر عليها الدليل الرقمي حتى يعبر عن حقيقة علمية ثابتة الحجية ومدى تأثير ذلك على مبدأ الاقتناع الشخصي للقاضي الجزائي.

أولا: شروط اكتساب الدليل الرقمي للحجية في إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:

مما لاشك فيه أن الدليل الرقمي ما هو إلا تطبيق من تطبيقات الدليل العلمي بل وأكثر منه حجية في الإثبات لما يتميز به من موضوعية وحياد وكفاءة، وهو محكم وفق قواعد علمية حسابية قاطعة لا تقبل التأويل، مما يقوي من يقينيته، ويساعد القاضي في التقليل من الأخطاء القضائية والإقتراب من تحقيق العدالة بخطوات أوسع، والتوصل بدرجة أكبر نحو الحقيقة،[2] ولكن إذا كان صحيحا أن الدليل الرقمي وبحكم طبيعته العلمية يمثل إخبارا صادقا عن الواقع باعتبار علميته وموضوعيته وحياده وكفاءته، إلا أن هذا لا ينفي استبعاد كونه موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى.

وعلى هذا الأساس فإن الشك في الدليل الرقمي لا يتعلق بمضمونه، وإنما بعوامل مستقلة عنه تؤثر في مصداقيته، لذلك فإن الأمر يتطلب وجوب توفر مجموعة من الشروط في الدليل الرقمي من أجل اقترابه نحو الحقيقة.

1) وجوب أن تكون الأدلة الرقمية يقينية وغير قابلة للشك: يشترط في الأدلة الرقمية المستخرجة من المنظومة المعلوماتية والأنترنت أن تكون غير قابلة للشك، حتى يمكن الحكم بموجبها بالإدانة.

ويتحقق اليقين للأدلة الرقمية من خلال إخضاعها للتقييم الفني بوسائل فنية، من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وكذا صحة الإجراءات المتبعة في الحصول عليه من أجل تفادي تلك العيوب التي قد تشوبه، فمثلما يخضع الدليل الرقمي لقواعد وإجراءات معينة تحكم طرق الحصول

[1] طارق الجملي، مرجع سابق، ص 66

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، مرجع سابق، ص 497.

عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية من الناحية العلمية وذلك راجع إلى الطبيعة الفنية لهذا الدليل[1]، ومن أهم وسائل تقييم الدليل الرقمي:

أ) وسائل تقييم الدليل الرقمي للتحقق من سلامته من العبث: ويمكن التأكد من سلامة الدليل الرقمي من وقوع العبث به بعدة طرق منها:

- فكرة التحليل التناظري: والتي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم يتم التأكد من مدى حصول عبث بالنسخة المستخرجة أم لا.[2]

- إستعمال الدليل المحايد وهو نوع من الأدلة الرقمية المخزون في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في النظام الكمبيوتري.[3]

- استخدام عمليات حسابية خاصة تسمى الخوارزميات، ولجوء إلى هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي، أو في حالة حصول عبث بها، إذ بالإمكان التأكد من سلامة الدليل الرقمي من التبديل والتحريف والتغيير باستعمال هذه العمليات الحسابية.[4]

ولا شك أن الخبرة التقنية تحتل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي، فإذا كانت للخبرة التقنية أهمية كبرى في مجال استخلاص الدليل الرقمي، فإن لها ذات الدور في بحث مصداقيته وتقييمه.

ب) وسائل تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه: للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الرقمي من حيث سلامة إنتاجها لدليل رقمي تتوافر فيه المصداقية، يمكن إخضاعها لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك باتباع اختبارين رئيسيين هما:[5]

- اختبار السلبيات الزائفة: ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لم يتم إغفال معطيات مهمة عنه.

- اختبار الإيجابيات الزائفة: ومفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار يمكن التأكد من خلاله أن هذه الأداة لا تعرض معطيات إضافية جديدة.

---

[1] خالد عياد الحلبي، مرجع سابق، ص ص، 248، 249.

[2] طارق الجملي، مرجع سابق، ص 66

[3] ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مقال منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، الفترة من 10-2003/05/12، المجلد الخامس، ص، 2247.

[4] طارق الجملي، مرجع سابق، ص 66.

[5] طارق الجملي، مرجع نفسه، ص 67. وكذلك خالد عياد الحلبي، مرجع سابق، ص 251.

2) وجوب إخضاع الدليل الرقمي للمناقشة: إن حرية الإثبات الجنائي مشروطة بأن يكون الدليل الذي يستند إليه القاضي قد طرحت مناقشته في الجلسة، ويكون كذلك متى كان له أصل ثابت في أوراق القضية المطروحة على القاضي.[1]

فمن القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، ولم تتح لهم فرصة الإطلاع عليها ومناقشتها، وغاية ذلك أن يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وأن تتاح لهم إمكانية مناقشتها والرد عليها، ومن ثم فتحقق شرط سلامة الدليل الرقمي من العبث وسلامته من الخطأ في إجراءات الحصول عليه وحده لا يكف لاكتسابه حجية دامغة في الإثبات بل لابد من ماقشة هذا الدليل بصفة علانية في جلسة المحاكمة.[2]

وهذا يعني أن مخرجات الحاسوب كأدلة رقمية متحصلة لإثبات الجرائم الماسة بالمعطيات الشخصية المعالجة آليا حتى وإن استمدت من إجراءات مشروعة احترمت فيها الحريات وأمنت فيها الضمانات التي رسمها القانون، وتمتعت بقوة استدلالية في كشف الحقيقة، فإنها تكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة.

ثانيا: سلطة القاضي الجزائي في تقدير الدليل الرقمي:

يذهب في هذا الصدد اتجاه من الفقه الجنائي إلى القول أن الأدلة الرقمية تتمتع بحجية قاطعة في الدلالة على الوقائع التي تتضمنها، وأنه يمكن التغلب على مشكلة التشكيك في مصداقيتها من خلال إخضاعها لاختبارات تمكن من التأكد من صحتها وسلامتها، وأنه لا يجب الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به، أو لوجود خطأ في الحصول عليه، وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية، والقول فيها هو قول أهل الخبرة، ولا يملك القاضي أن يقطع فيها برأي حاسم وإن لم يقطع به أهل الإختصاص. فإن سلم الدليل الرقمي وتوافرت فيه شروط الكفاءة والمصداقية والموثوقية العلمية، فإنه لن يكون القاضي سوى القبول به ولا يمكنه رده أو التشكيك في قيمته التدليلية، لكونه وبحكم طبيعته الفنية يمثل إخبارا صادقا عن الوقائع.[3]

لذلك فهذا الإتجاه يرى أن الدليل الرقمي أصبح يقيد حرية القاضي في تقديره ويجبره على الحكم بمقتضاه ولو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه، على اعتبار أن الدليل الرقمي من تطبيقات الدليل العلمي، بما يتميز به من حياد وموضوعية وكفاءة في إقناع القاضي، وهو أمر يدفع إلى القول بأنه بمقدار اتساع مساحة الأدلة العلمية بمقدار ما يكون انكماش وتضاؤل دور القاضي في تقدير الدليل.[4]

---

[1] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 392.

[2] تنص المادة 2/212 من قانون الإجراءات الجزائية أنه "لا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

[3] هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية، مرجع سابق، ص 95.

[4] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، مرجع سابق ص 498.

إلا أن هذا التصور يذهب اتجاه فقهي آخر إلى مخالفته، ويدعو أنصاره إلى ضرورة التمييز بين القيمة العلمية القاطعة للدليل الرقمي وبين الظروف والملابسات التي وجد فيها هذا الدليل، فتقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل، والتي تقوم على أسس علمية، خاصة بعد ظهور وإنشاء المعامل والمخابر الجنائية لفحص هذه الأدلة وتقييمها.

أما ما يتعلق بالظروف والملابسات التي وجد فيها هذا الدليل، فإنها ما يدخل في نطاق تقديره الشخصي، وله في هذه الحالة أن يطرح الدليل الرقمي إذا تبين له أنه لا يتفق منطقيا مع ظروف الواقعة وملابساتها[1]، فمجرد توفر الدليل العلمي ومنه الدليل الرقمي لا يعني أن يحكم القاضي مباشرة بموجبه بالإدانة أو البراءة دون البحث في الظروف والملابسات للواقعة المراد إثباتها به، فالدليل العلمي ليس آلية أعدت لتقرير اقتناع القاضي نحو مسألة غير مؤكدة[2]، ومن جانبنا نميل إلى رأي الإتجاه الأخير، فمهما علا شأن الأدلة العلمية ومنها الدليل الرقمي في مسألة الإثبات الجنائي، فإنه يجب أن نبقي على سلطة القاضي التقديرية في تكوين اقتناعه من هذه الأدلة، وذلك من أجل ضمان تنقيتها من شوائب الحقيقة العلمية، ومن جهة أخرى يظل القاضي هو المسيطر على هذه الحقيقة، لأنه من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم، وأن يستبعد الأدلة التي يتم الحصول عليها بطرق غير مشروعة، و تكون هذه السلطة ضرورية أكثر من أجل جعل هذه الحقيقة العلمية، حقيقة قضائية.

المطلب الثالث: قواعد الاختصاص في جرائم الإ عتداء على المعطيات الشخصية المعالجة آليا:

إن المشكلة التي تشترك فيها جرائم الإعتداء على المعطيات ذات الطابع الشخصي أثناء معالجتها آليا مع غيرها من الجرائم الواقعة في العالم الرقمي، هو أن السلوك أو النشاط الإجرامي فيها لا يعترف بالحدود، فالطبيعة التقنية العالية لنظم المعلوماتية المرتبطة بشبكات الإتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة،[3] الأمر الذي قد ينجم عنه تنازع في الاختصاص القضائي بين هذه الدول فقد يحدث أن ترتكب جريمة من الجرائم التي تشكل اعتداء على المعطيات الشخصية المعالجة الكترونيا في إقليم دولة وتتحقق النتيجة الجرمية في دولة أخرى، ومن ثم تتعدد القوانين التي يمكن أن تحكم هذه الجرائم وينعقد بذلك الاختصاص لأكثر من دولة لتعدد الدول المرتبطة بها.

وإذا كان الاختصاص المحلي على المستوى الداخلي أو الوطني لا يثير أي إشكال، إذ يتم الرجوع في تحديده إلى المعايير المحددة سلفا في قانون الإجراءات الجزائية وهو مكان وقوع الجريمة، محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل القبض لسبب آخر،[4] فإن مشكلة الإختصاص المحلي تثار بحدة بالنسبة للاختصاص على المستوى الدولي حيث يكون لهذه الجرائم في هذه الحالة طابعا دوليا كونها تتم في عالم افتراضي يلغي

[1] رشيدة بوكر، مرجع نفسه، ص 508.

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 22.

[3] عادل عزام سقف الحيط، مرجع سابق، ص 349.

[4] أنظر المادة 37، 329 من قانون الإجراءات الجزائية.

جميع الحواجز الإقليمية والدولية باعتبارها جرائم عابرة للحدود،[1] وبالتالي اختلاف التشريعات والنظم القانونية وتباينها، وهو أمر قد ينجم عنه تنازع في الاختصاص بين الدول بالنسبة لجرائم الاعتداء على المعطيات الشخصية في نظم معلوماتية مرتبطة بشبكات اتصال الكترونية عالمية.

والمعروف أن تحديد القانون الواجب التطبيق، يترتب عليه تحديد المحكمة المختصة للفصل في النزاع، لذلك فإن المسألة تقتضي منا معرفة المبادئ أو المعايير التي يعتمد عليها في تحديد القانون الواجب التطبيق على هذا النوع من الجرائم، و بالتبعية تحديد الولاية القضائية أو الاختصاص القضائي.

واستنادا على القواعد العامة المتعلقة بتطبيق القانون الجزائي من حيث المكان نجد أن مسألة انعقاد الاختصاص العالمي للمحاكم الوطنية في هذا الإطار تحكمها ثلاث مبادئ وهي: مبدأ الإقليمية، مبدأ الشخصية و مبدأ العينية. فإلى أي مدى يمكن تطبيق هذه المبادئ على جرائم الإعتداء على المعطيات الشخصية المعالجة آليا في النظم المعلوماتية المرتبطة بشبكات الإتصال الإلكترونية العالمية.

الفرع الأول: قواعد تحديد الاختصاص القضائي وفق مبدأ الإقليمية

إن قواعد القانون الجنائي بشقيه الموضوعي أو الجزائي تعد مظهرا من مظاهر سيادة الدولة، لذلك فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر ألا وهو مبدأ الإقليمية، والذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها، ولا تخضع لسلطان أي قانون أجنبي، وفي المقابل فلا مجال لأن يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها، حيث يصطدم بسيادة غيرها من الدول إلا في أحوال استثنائية تقتضيها حماية المصالح الجوهرية للدولة، أو متطلبات الدول في مكافحة الإجرام[2]، ويستند هذا المبدأ إلى أن من حقوق الدولة الأساسية حقها في سيادتها على أرضها وحقها في صيانة أمنها ونظامها والدفاع عن سلامة الأشخاص والأموال والأشياء الموجودة ضمن نطاق حدودها الإقليمية، ومن أولى مظاهر استعمال هذه الحقوق تطبيق القانون الجزائي للدولة على الجرائم التي تقع في إقليمها، ومن ثم افتراض أن محاكمها هي صاحبة الإ ختصاص بمحاكمة مقترفي هذه الجرائم هو مبدأ معمول به في جميع قوانين دول العالم كونه مظهر من مظاهر سيادة الدولة على إقليمها ويترتب على ذلك عدة نتائج أهمها:

1. أن الحيز الطبيعي لتطبيق القانون الجزائي لدولة ما إنما هو إقليمها الوطني، حيث تخضع كل الجرائم المرتكبة فيه لقانونها مهما كانت جنسية مرتكبيها سواء مواطنا أم أجنبيا، وبالضرورة عدم تطبيق القوانين الجزائية الأجنبية على هذه الجرائم.

[1] أيمن بن ناصر بن حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي دراسة مقارنة، الطبعة الأولى، 2015، مكتبة القانون والاقتصاد، الرياض، ص 20.

[2] أمال فكيري، إشكالات الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، عدد 17 جانفي 2018، جامعة لونيسي علي البليدة 2، الجزائر، ص 640.

2. أن القانون الجزائي الوطني هو وحده المختص في قمع الجرائم التي تقع في الإقليم الوطني، فلا يشاركه أو ينوب عنه قانون آخر، فعلى خلاف القاضي المدني، لا يملك القاضي الجزائي أن يطبق غير القواعد والأحكام المنصوص عليها في قانونه الجزائي الوطني، ومرد ذلك أن هذه القواعد القانونية الجزائية تتعلق بالنظام العام، وتعبر عن سيادة الدولة.[1] بالإضافة إلى عدم تطبيق القانون الجزائي على أية جريمة ترتكب خارج حدود الدولة[2].

والمشرع الجزائري اعتمد هذا المبدأ كحل أولي ومعيار أساسي عند تطبيق القانون الجزائي من حيث المكان عندما نصت المادة الثالثة من قانون العقوبات على أنه "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية". معتبرا أنه تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر،[3] وهو نفس المبدأ الذي سبق للمشرع الفرنسي أن كرسه من خلال المادة 113-2 من قانون العقوبات الفرنسي.[4]

ويستفاد من هاته النصوص أن تطبيق مبدأ الإقليمية على جرائم الإعتداء على المعطيات ذات الطابع الشخصي، لا يثير أي صعوبة إذا كانت جميع العناصر المكونة للجريمة قد وقعت بإقليم الدولة الواحدة[5] بغض النظر عن جنسية مرتكبها سواء كان وطنيا أم أجنبيا، وسواء كان وقوع الجريمة على إقليم التراب الوطني كاملا أو جزء منها، وهو ما أكدته المادة 22 من مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والإتصالات، عندما نصت على أنه تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها وفقا لمبدأ الإقليمية، مع الإشارة إلى أن مفهوم هذا المبدأ قد شهد تطورا ملحوظا فيما يتعلق بتحديد مكان وقوع الجريمة المعلوماتية والتي يندرج ضمنها تلك المتعلقة بالاعتداء على المعطيات الشخصية المعالجة آليا، حيث لم يعد مبدأ الإقليمية في الاختصاص القضائي يلازم وقوع فعل مادي أو أحد العناصر المكونة له، بل بلغ الأمر إلى حد نزع الصفة المادية كلية عن هذا الفعل.[6]

ولفهم المقصود بإقليم الدولة يمكن الرجوع إلى قواعد القانون الدولي العام، والذي في إطاره يمكن اعتبار إقليم الدولة بأنه الإقليم البري المعين ضمن حدود سياسية بموجب اتفاقيات دولية، وكذلك الإقليم

[1] محمد عدنان الخطيب، موجز القانون الجزائي، المبادئ العامة في قانون العقوبات، الكتاب الأول، مطبعة جامعة دمشق، 1963، ص 79.

[2] عبد الله سليمان، مرجع سابق، ص 102.

[3] تنص المادة 586 من قانون الإجراءات الجزائية على أنه "تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر".

[4] L'article 113-2 du code pénal français dispose que : (la loi pénale française est applicable aux infractions commises sur le territoire de la république, l'infraction est réputée commise sur le territoire de la république dés lors qu'un de ses faits constitutifs a eu lieu sur ce territoire.).

[5] محمد طارق عبد الرؤوف الحن، مرجع سابق، ص 212.

[6] مفتاح بوبكر المطردي، الجريمة الإلكترونية، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25- 09-2014، دون ترقيم، متوفر على موقع:www.swideg-gegraphy.blogspot.com

البحري ويشمل المياه الإقليمية للدولة، وأخيرا الإقليم الجوي وهو ما يعلو الإقليمين البري والبحري،[1] زيادة على الإقليم الاعتباري والمتمثل في السفن والطائرات التابعة للدولة أينما وجدت.

وهناك من ذهب إلى اعتبار أن مساحة الأنترنت الخاضعة لإدارة الدولة تعتبر جزءا من الإقليم الإعتباري لها فالنطاق العلوي الجزائري على الأنترنت الذي يخضع للحكومة الجزائرية والذي ينتهي بـ (dz.) هو نطاق يحمل الجنسية الجزائرية، وبالتالي فإنه على اعتباره امتدادا افتراضيا للإقليم الوطني في بيئة الأنترنت الرقمية ومن ثم فإن الجرائم التي ترتكب عبر هذا النطاق يمكن أن تطولها قواعد الاختصاص الجزائي.*

وتطبيقا لذلك، فقد ذهب المشرع الفرنسي في المادة 113-2-1 من قانون العقوبات إلى القول بأن أي جناية أو جنحة ترتكب أو يحاول ارتكابها إضرارا بشخص طبيعي مقيم على الإقليم الفرنسي أو إضرارا بشخص معنوي له مقر على الإقليم الفرنسي، وذلك بواسطة شبكة اتصالات الكترونية تعتبر وكأنها مرتكبة على الإقليم الفرنسي.[2]

ومن الاتجاهات القضائية المقارنة التي تتجه إلى التوسع في مفهوم الإقليمية نجد أن القضاء الأمريكي يعطي الاختصاص لمحاكمه الجنائية بمجرد حدوث آثار الجريمة على إقليمها، فقد قضي في أمريكا بأنه إذا تم إدخال معطيات من مكان معين، وكانت تتضمن ما يشكل جريمة معلوماتية، وكانت هذه المعطيات مقروءة وممكن الاطلاع عليها في دولة أخرى، فإن الإختصاص ينعقد لمحاكم الدولة التي يمكن الاطلاع على تلك البيانات في إقليمها ، ومن ثم فإذا كان الجاني قد وضع صورا مؤتمة على جهاز الخادم (serveur) المتواجد في إيطاليا وكانت هذه الصور متاح الاطلاع عليها في الولايات المتحدة الأمريكية، فإن القضاء الأمريكي يحكم اختصاصه.

لذلك وعلى الرغم من اختلاف القوانين المقارنة في تحديد المحكمة المختصة، عندما تمر الرسالة الإلكترونية المعاقب عليها في إقليم أكثر من دولة وكان القانون الجزائي في كل دولة منها يعاقب عليها، فإن الحل الأنسب عند بعض الفقه الجنائي هو أن يؤول الاختصاص لجميع هذه الدول، وذلك مادامت النتيجة تتحقق في بلد آخر غير بلد تحميل الرسالة وإدخالها في الشبكة المعلوماتية،[3] ومن ذلك أن يرسل شخص ما برنامجا من شأنه التقاط معطيات شخصية أو اتلافها من جهاز يقع في دولة معينة إلى جهاز آخر يقع في دولة ثانية، مرورا بأجهزة أخرى في دول أخرى، وبالتالي استنادا إلى هذا المذهب ينعقد الاختصاص لمحاكم الدولة التي حدث منها البث والدولة التي انتهى إليها ذلك البرنامج، وكذا الدول التي مر بها من خلال أي جهاز فيها.

---

[1] عبود السراج، مرجع سابق، ص 66.

* نصت المادة 590 من قانون الإجراءات الجزائية على أنه تختص الجهات القضائية الجزائرية بالنظر في الجنايات والجنح التي ترتكب في عرض البحر على بواخر تحمل الراية الجزائرية أيا كانت جنسية مرتكبيها، ونصت المادة 591 على أنه تختص الجهات القضائية الجزائرية بنظر الجنايات والجنح التي ترتكب على متن طائرات جزائرية أيا كانت جنسية مرتكب الجريمة، وبهذا اعتبرت البواخر والطائرات امتدادا للإقليم الجزائري ويختص القضاء الجزائري بالنظر في الجرائم التي ترتكب على متنها في أي إقليم وقعت وأيا كانت جنسية مرتكبها".

[2] محمد عبد الرؤوف الحن، مرجع سابق، ص 217.

[3] شيماء عبد الغني، محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، مصر 2007، ص 376.

وقد تصدت في تحديد الاختصاص القضائي اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة الوطنية لتكون أساسا لاتخاذ التدابير اللازمة للحصول على الولاية القضائية على الجرائم المرتبطة بالتقنية المعلوماتية، حيث نصت المادة 15 من هذه الاتفاقية على أنه يتعين على كل دولة طرف أن تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية في مجموعة من الحالات، منها عندما يرتكب الجرم في إقليم تلك الدولة.

وكذلك تضمنت اتفاقية بودابست التي لم تخرج عن هذا المعيار حينما أوردت في الباب الثالث منها بالمادة 22 مسألة الاختصاص بنصها أنه يعتمد كل طرف ما قد يلزم من تدابير تشريعية، وذلك لإقرار الاختصاص بشأن أي جريمة معلوماتية عندما ترتكب في إقليمه.

وهنا تثار مسألة أخرى تتعلق بتحديد مفهوم مكان ارتكاب الجريمة الواقعة في العالم الافتراضي، والثابت أن موضوع الاختصاص المحلي التقليدي يطرح جملة من الصعوبات ذلك أن مكان ارتكاب الجريمة المعلوماتية والذي يكون دائما البيئة الافتراضية غير الملموسة، يختلف عن مكان ارتكاب باقي الجرائم التقليدية الأخرى في العلم المادي الملموس، حيث أن قواعد الاختصاص القضائي المنصوص عليها في قانون الإجراءات الجزائية دائما صيغت لكي تحدد الاختصاص القضائي المتعلق بجرائم قابلة للتحديد المكاني، ومن ثم يصبح إعمالها بشأن الجريمة المعلوماتية والتي ترتكب في فضاء افتراضي تنعدم فيه الحدود الجغرافية أمرا في غاية الصعوبة، حيث يصعب تحديد مكان وقوع الفعل الجرمي في هذا النوع من الجرائم ومن ثم ينبغي تجاوز المعايير التقليدية،[1] لذلك فقد اعتبر القضاء الفرنسي أن مكان ارتكاب الجريمة الذي يعقد به الإ ختصاص القضائي في هذه الطائفة من الجرائم قد يأخذ معايير أخرى، تتناسب مع الطبيعة الإفتراضية لها ومنها:

إما المكان الذي يعاين المستخدم فيه وجود الموقع المشروع، أو الذي تتم فيه مشاهدة الصور والنصوص ذات الطبيعة غير المشروعة.

وإما المكان الذي يوجد فيه خادم إيواء الموقع إذا ظهر انطلاقا من المراقبات الأولى أن هذا الموقع قد تم تحديده أو معاينته على التراب الوطني.[2]

غير أنه إذا كان مبدأ الإقليمية، يعتبر المبدأ المهيمن على تطبيق القانون الجزائي من حيث المكان ومن خلاله ينعقد الاختصاص لقضاء الدولة التي وقع بإقليمها الجرم، إلا أن تطبيقه ليس دوما بهذه السهولة، ويفقد صلاحية التطبيق بالنسبة لجرائم الإعتداء على المعطيات الشخصية المعالجة آليا عبر وسائل الإتصال الإلكترونية المعالجة والتي تتجاوز حدود المكان، لذلك فإنه وبالإضافة إلى مبدأ الإقليمية في تحديد القانون الواجب التطبيق والإ ختصاص القضائي، يمكن أن يتحدد أيضا وفقا لمعايير أو مبادئ أخرى غالبا ما تأخذ بها التشريعات الجزائية كمبادئ احتياطية أو مكملة لمبدأ الإقليمية وهي مبدأ الشخصية، مبدأ العينة ومبدأ العالمية.

[1] يوسف قجاج، إشكالية الا ختصاص في الجريمة الإلكترونية، مقال متوفر على الموقع .www.hespres.com/opinions/256777

[2] Mgriam Quéméner, yves chrpenel, op, cit, p.p 161.162.

الفرع الثاني: المبادئ الاحتياطية في تحديد قواعد الاختصاص القضائي

يصطدم تطبيق مبدأ الإقليمية على الجرائم محل الدراسة بالعديد من العقبات، سيما كونها جرائم يصعب تحديد مكان وقوع الفعل الجرمي فيها لأن طبيعتها الخاصة تتجاوز المكان الواحد، كما أن من أهم خصائصها إثارة أنها متعدية الحدود، إذ يتجاوز نطاق ارتكابها والنتائج المترتبة عنها حصر معيار الاختصاص القضائي بشأنها على مبدأ الإقليمية فقط.

فلقد أثبتت الضرورات العملية في مكافحة الإجرام أن مبدأ الإقليمية على أهميته ليس قادرا وحده على ضبط جميع أنواع الجرائم التي يتعدى نطاقها إقليم الدولة، مما حدى بالمشرع للأخذ ببعض المبادئ الأخرى لتكملة المبدأ الأصلي، حرصا منه على تأكيد المحاربة الفعالة ضد الجريمة. ولكيلا يفلت من العقاب الجناة الذين يستغلون قصور هذا المبدأ عن التطبيق في مواجهتهم.[1]

فقد يحدث أن ترتكب جريمة من جرائم الإ عتداء على المعطيات الشخصية المعالجة آليا في إقليم دولة ما مثل الولوج إلى قاعدة بيانات تابعة لهيأة حكومية في الجزائر والعمل على التلاعب والعبث في المعطيات الشخصية المسجلة فيها، وهنا تكون هذه الجريمة خاضعة للاختصاص القضائي الجزائي للدولة التي ارتكبت الجريمة في إقليمها استنادا على مبدأ الإقليمية، وكذلك لاختصاص قضاء الدولة التي ينتمي إليها الجاني انطلاقا من مبدأ الشخصية، وهي كذلك تلحق تهديدا لأمن وسلامة المعطيات بدولة أخرى فتدخل أيضا في اختصاصها استنادا إلى مبدأ العينة، وهو أمر يؤدي إلى تنازع إيجابي في الاختصاص بين أكثر من قانون، ومن ثم أكثر من اختصاص قضائي.[2]

لذلك وفي هذا الإطار يمكن استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، لذلك فإن القضاء يستعين إلى جانب المبدأ الأصلي أو الأساسي (مبدأ الإقليمية) لإحكام طوق القانون الجزائي حول الجريمة بمبادئ أخرى تكون مكملة له وهي مبدأ شخصية النص الجزائي، مبدأ العينة ومبدأ عالمية النص الجزائي.

أولا: مبدأ الشخصية في إقامة الاختصاص القضائي الجزائي:

يقصد بهذا المبدأ إمكانية خضوع الشخص الذي يرتكب جريمة خارج إقليم بلده إلى قانونها أينما وجد، فإذا ارتكب شخص جريمة إفشاء معطيات شخصية أو الولوج إلى قواعد بيانات تابعة لدولة أجنبية والتلاعب بالمعطيات الشخصية المخزنة بها أو حذفها وتخريبها في الخارج، ثم عاد إلى (أرض الوطن) إقليم بلاده قبل أن يحاكم عن هذه الأفعال أو قبل تنفيذ العقوبة التي حكم بها عليه، فإنه يجوز أن يتابع ويحكم عليه في بلاده عن هذه الجرائم استنادا إلى مبدأ الشخصية، وهو ما أكدته المادة 53 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي عندما نصت على أن الجهات القضائية الجزائرية تختص بمتابعة الجرائم المنصوص عليها في هذا القانون إذا كانت مرتكبة خارج إقليم الجمهورية من طرف جزائري، وهو تكريس لقاعدة الإختصاص الشخصي التي فصل في شرحها المشرع في قانون الإجراءات الجزائية من خلال المادتين 582و583.

[1] عبد الله سليمان، مرجع سابق، ص 102.

[2] جميل عبد الباقي الصغير، مرجع سابق، ص 73.

حيث يتم إعمال المادة 582 من قانون الإجراءات الجزائية عندما تكون الجريمة المرتكبة في الخارج من طرف جزائري ذات وصف جنائي، والمادة 583 إذا كانت ذات وصف جنحي*، والذي يسعفنا في دراسته هو حالة الجنحة، كون أغلب الجرائم التي تشكل اعتداء على المعطيات ذات الطابع الشخصي المعالجة آليا ذات وصف جنحي، ويتبين من هذه النصوص القانونية أنه لإعمال مبدأ الشخصية لعقد الإ ختصاص القضائي الجزائي للمحاكم الجزائرية:

- أن تكون الواقعة مكيفة بوصف جنحة في القانون الجزائري والأجنبي الذي ارتكبت بدائرته الواقعة وتكون من الجنح التي تشكل اعتداء على المعطيات ذات الطابع الشخصي محل المعالجة الإلكترونية.

-أن ترتكب الجريمة خارج الإقليم الجزائري، لأن ارتكابها في نطاق الإقليم الجزائري يجعلها خاضعة لمبدأ الإقليمية وليس لمبدأ الشخصية.

- لا يحاكم الشخص إلا بعد عودته إلى إقليم بلاده سواء باختياره أو بعد تسليمه، فلا يحاكم عنها غيابيا.

- ألا يكون الشخص قد حوكم نهائيا من أجل هذه الجريمة في الخارج ونفذت عليه العقوبة، أو لم يثبت أنها سقطت عنه بالتقادم أو العفو.

ويضيف المشرع شرطا آخر وهو أنه لا يجوز أن تجري المتابعة الجزائية ضد مرتكبي الجنحة إلا إذا أخطرت النيابة من قبل الشخص المضرور، أو ببلاغ من سلطات القطر الذ ارتكبت الجريمة فيه.

-يجب أن يكون الفاعل جزائريا وقت ارتكابه للجنحة، ويسري النص أيضا على من ارتكب الجنحة ثم اكتسب الجنسية الجزائرية بعد اقترافه لها *، وذلك حتى لا يكون اكتساب الجنسية سبيلا للتهرب من المسؤولية.

و يبدو واضحا من هذه النصوص القانونية أن المشرع الجزائري أراد ملاحقة الجزائريين الذين يرتكبون خارج الإقليم الجزائري جريمة يعاقب عليها القانون الجزائري، وعلة ذلك أن أي جزائري يقترف جريمة على أرض أجنبية فإنه يسيء إلى سمعة بلده وينال من اعتبار مواطنيها، وهو في نفس الوقت يكون قد ارتكب فعلا معاقبا عليه في الجزائر ويمنع على أي جزائري ارتكابه، ومن ثم فإنه لا يجوز أن يكون الوطن

* تنص المادة 383 من قانون الإجراءات الجزائية على أنه كل واقعة موصوفة أنها جنحة سواء في نظر القانون الجزائري أم في نظر تشريع القطر الذي ارتكبت فيه يجوز المتابعة من أجلها والحكم فيها في الجزائر إذا كان مرتكبها جزائريا، ولا يجوز أن تجري المحاكمة أو يصدر الحكم إلا بالشروط المنصوص عليها في الفقرة الثانية من المادة 582.

وعلاوة على ذلك لا يجوز أن تجري المتابعة في حالة ما إذا كانت الجنحة مرتكبة ضد أحد الأفراد، إلا بناء على طلب النيابة العامة بعد إخطارها بشكوى من الشخص المضرور أو ببلاغ من سلطات القطر الذي ارتكبت الجريمة فيه. وتنص الفقرة الثانية من المادة 582 "على أنه لا يجوز أن تجري المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر ولم يثبت أنه حكم عليه نهائيا في الخارج، وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو عنها ".

* تنص المادة 584 على أنه "يجوز أن تجري المتابعة أو بصدور الحكم في الحالات المنصوص عليها آنفا في المادتين 582.583. حتى ولو لم يكن المستلم قد اكتسب الجنسية الجزائرية إلا بعد ارتكابه الجناية أو الجنحة.

موئلا للخارجين عن القانون الذين يسيئون لوطنهم بارتكاب الجرائم في الخارج، فيكون لهم في العودة إلى بلادهم ملجأ يحميهم من تحمل نتائج أعمالهم الإجرامية.[1]

لذلك كان لمبدأ الشخصية جانبان يطبق لأجلهما، جانب إيجابي ويقصد به تطبيق الدولة لقانونها الجزائي على مرتكب الجريمة الذي يحمل جنسيتها ولو ارتكبها خارج إقليمها، وأما الجانب السلبي فيقصد به تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملا لجنسية الدولة ولو ارتكبت الجريمة خارج إقليمها وأيا كانت جنسية مرتكب هذه الجريمة.[2]

لذلك نعتقد أن المشرع الجزائري كان محقا عندما وسع من نطاق اختصاص القضاء الجزائري لينعقد على متابعة الجرائم المنصوص عليها في القانون المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي حتى عندما ترتكب خارج إقليم الجمهورية من طرف شخصي أجنبي[3]، لكن من العقبات التي يصطدم بها تطبيق مبدأ شخصية النص الجزائي هو اعتماده على تحديد جنسية مرتكب الفعل، وهو من أحد أهم المشاكل التي يطرحها الإجرام المعلوماتي الذي يكون فيه من الصعوبة تحديد فاعل الجريمة، ففي غالب الأحيان تتوقف إجراءات البحث والتحري عند الكشف على عنوان بروتوكول الأنترنت، أو الخادم المضيف، وتبقى في ظروف كثيرة هوية الفاعل مجهولة.

ثانيا: مبدأ العينية في إقامة الاختصاص القضائي الجزائي:

يقصد بمبدأ العينية تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة المرتكبة خارج إقليمها أيا كانت جنسية مرتكبها، فقد يرتكب الأجنبي وفي بلد أجنبي جريمة تهدد المصالح الجوهرية للدولة فلا يسعفها الإختصاص الإقليمي لمواجهة هذه الحالة بالإضافة إلى الخشية من ألا تعير الدولة الأجنبية الإهتمام الكافي لمواجهة هذه الجرائم باعتبارها جرائم لا تمس مصالحها، لذلك كان مبدأ العينة من أجل صلاحية تطبيق الدولة لقانونها الجزائي على الجرائم التي تشكل إخلالا بمصالحها الأساسية بصرف النظر عن مكان وقوع الجريمة وأيا كانت جنسية فاعلها.

لذلك تدخل المشرع الجزائري بالنص في المادة 53 الفقرة الثانية من القانون المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي على أن الجهات القضائية الجزائرية تختص بمتابعة الجرائم المنصوص عليها في هذا القانون، وفقا لقواعد الإ ختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية[4] ، حيث يكون وفقا لهذا النص القانوني إمكانية متابعة ومحاكمة كل أجنبي

[1] عبد الله سلمان، مرجع سابق، ص 111.

[2] محمود نجيب حسني، شرح قانون العقوبات اللبناني، القسم العام، مرجع سابق، ص 201.

وقد نص المشرع الفرنسي على مبدأ الشخصية السلبية بمقتضى المادة 113-7 من قانون العقوبات الفرنسي عندما نصت على أنه يطبق القانون الفرنسي على كل جريمة يرتكبها فرنسي أو أجنبي خارج فرنسا إذا كان المجني عليه فرنسيا لحظة وقوع الجريمة.

" la loi pénale française est applicable a tout crime ainsi qui à tout délit puni d'emprisonnement, commis par un français ou par un étranger hor territoire de la république lorseque la victime est de nationalité française au moment de l'infraction ".

[3] تنص المادة 53 من القانون 07/18 على أنه تختص الجهات القضائية الجزائرية بمتابعة الجرائم المنصوص عليها في هذا القانون، التي ترتكب في خارج إقليم الجمهورية، من طرف جزائري أو شخص أجنبي مقيم في الجزائر، أو شخص معنوي خاضع للقانون الجزائري.

[4] يقابل نص المادة 588 من قانون الاجراءات الجزائية المادة 113-10 من قانون العقوبات الفرنسي التي تنص على:

وفقا للقانون الجزائري ارتكب خارج الإقليم الجزائري بصفته فاعلا أو شريكا جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا لنقود أو اوراق مصرفية وطنية متداولة قانونا بالجزائر، وإذا ألقي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه له.

وعليه فإنه يستفاد من هذا أنه لإعمال مبدأ عينية النص الجزائي ينبغي:

- أن يكون الفاعل أجنبيا فلا يسري هذا النص على من كان ذو جنسية جزائرية، لأن ذلك مداعاة لإعمال مبدأ الشخصية، ويستوي أن يكون فاعلا أصليا أم شريكا في ارتكاب الجريمة.

- أن ترتكب الجريمة خارج الإقليم الوطني أي في بلد أجنبي، لأن وقوعها في الجزائر معناه الخضوع لمبدأ الإقليمية.

- أن يقع الفاعل في يد العدالة الوطنية بعد إلقاء القبض عليه من قبل السلطات المختصة أو أن يسلم إليها في إطار تسليم المجرمين، ومفاد ذلك أنه لا يجوز محاكمة الأجنبي غيابيا حتى ولو ثبت أنه قام بالفعل حقيقة.

فضلا عن ذلك نلاحظ أن المشرع قد حصر الجرائم التي يؤول فيها الاختصاص للقضاء الجزائري فقط في تلك التي ترتكب ضد أمن الدولة أو المتعلقة بتزييف النقود الوطنية أو الأوراق المصرفية.

وعلى هدي ذلك فإن الجرائم التي تشكل اعتداء على المعطيات ذات الطابع الشخصي التي نص عليها القانون المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي لم تكن لتخضع لاختصاص القضاء الجزائري وفقا لمبدأ العينية لو لم يتدخل المشرع بالنص صراحة على ذلك في نص المادة 53 من هذا القانون، ليضيف هذه الطائفة من الجرائم إلى اختصاص القضاء الجزائري عندما ترتكب من طرف أجنبي في الخارج إعمالا لمبدأ العينية إلا إذا ترتب على ارتكاب هذه الجرائم مساس بأمن الدولة، حسب مقتضيات المادة 558 من قانون الإجراءات الجزائية، كالقيام باختراق النظام المعلوماتي لوزارة الدفاع الوطني عبر الشبكة والحصول على معطيات شخصية أو إتلافها، وهو الأ مر المؤكد أيضا في المادة 15 من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 04/09 حيث اعتبر المشرع أنه بالإضافة إلى قواعد الاختصاص القضائي المنصوص عليها في قانون الإجراءات الجزائية، فإن الجرائم المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، يتوسع اختصاص المحاكم الجزائرية للنظر في جرائم ترتكب خارج الإقليم الوطني من طرف أجنبي استنادا إلى مبدأ عينية النص الجزائي.

وتطبيقا لذلك فإن بعض الجرائم المحددة في هذه النصوص يمكن أن ترتكب عبر شبكات الإتصال الإلكترونية، كقيام شخص أجنبي في الخارج باختراق النظم المعلوماتية لشركات وطنية كبرى مثل شركة

" la loi pénale française est s'applique aux crime et délits que lifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés «par le titre 1er du livre IV. A la falsification et à la contrefaçon du sceau de l'état, de pièces de monnaie, de billets de banque ou de ffets publics réprimés par les articles 4... et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires commis hors du territoire de la république ».

سوناطراك مثلا ليتلف معطيات شخصية أو يتلاعب بها أو يكشفها للغير بمقابل أو بدونه، وبهذا يكون خاضعا لأحكام المادة 394 مكرر من قانون العقوبات.

ثالثا: مبدأ عالمية النص الجزائي في إقامة الاختصاص القضائي:

يطلق على هذا المبدأ في كتابات أخرى مبدأ التعاون الدولي في مكافحة الإجرام، فالأصل أن الجريمة مهما كانت طبيعتها فهي تهدد الأمن البشري، وتمس مصالح الناس أينما وقعت، ولذا وجبت مقاومتها حيثما ارتكبت وضد أي مصلحة كانت بغض النظر عن جنسية مرتكبها، فلا يجوز أن يفلت مجرم من العقاب، لذلك يكون لأي دولة تضبط المجرم أن تعاقبه بحسب قانونها الوطني إذا تعذر محاسبته أمام قاضيه الطبيعي، وذلك فيه عمل على حماية المصالح البشرية وتأكيد لتظافر الجهود في محاربة الإجرام،[1] فالغاية من هذا المبدأ إذن هي عدم إفلات أي إنسان من العقاب، ضمن نطاق التعاون الدولي في مكافحة الإجرام، لأن كثيرا من المجرمين يمكنهم أن يقترفوا جرائمهم ثم يهربون إلى دولة أخرى لا تعلم بها دولتهم ليعيشوا في طمأنينة تحت حماية الدولة المضيفة ورعايتها.[2]

ويعتبر مبدأ عالمية النص الجزائي مبدأ تكميليا يضاف إلى المبادئ التكميلية الأخرى في تطبيق النص الجزائي وهي مبدأ الشخصية ومبدأ العينة، ومن ثم يعد الاختصاص القضائي المترتب عن إعماله اختصاصا احتياطيا، فلا يعاقب قضاء الدولة من يقيمون على أرضها إلا إذا لم يوجد من يعاقبهم من الدول الأجنبية من أجل ضمان عدم إفلات المجرمين الذين تسول لهم أنفسهم ارتكاب جرائم في دولة ثم الفرار إلى دولة أخرى تملصا من المسؤولية.[3]

لذلك فإنه يقصد بهذا المبدأ أنه ذلك النظام الذي يعطي المحاكم الجزائية الوطنية حق ممارسة ولايتها القضائية في متابعة ومحاكمة المتهم بارتكاب جريمة تكيف على أنها خطيرة دوليا، بغض النظر عن جنسية ومكان ارتكابها، ومن ثم يكون مضمون هذا المبدأ هو تطبيق القوانين الجزائية الوطنية على جرائم ارتكبت في الخارج من قبل أشخاص أجانب دون اشتراط مساس هذه الجرائم بالمصلحة الخاصة للدولة.[4]

وبالرجوع إلى القواعد العامة المقررة لاختصاص القضاء الجزائري بالنسبة للجرائم، سواء القواعد التي أوردها قانون العقوبات أو قانون الإجراءات الجزائية نجدها جاءت قاصرة على مبدأ الإقليمية كمبدأ أصلي، ومبدئي الشخصية والعينية كمبدئين احتياطين فقط، ولا توجد أي إشارة إلى مبدأ العالمية في إعمال الإ ختصاص القضائي الجزائي الجزائري على الجرائم ذات الصبغة العالمية، لكننا نعتقد أن المشرع الجزائري قد طبق مبدأ العالمية عندما يتعلق الأمر بالجرائم التي تشكل اعتداء على المعطيات الشخصية المعالجة آليا، وذلك عندما نصت المادة 53 من القانون المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي أنه "تختص الجهات القضائية الجزائرية بمتابعة الجرائم المنصوص عليها

[1] عبد الله سليمان، مرجع سابق، ص 115.

[2] عبود السراج، مرجع سابق، ص 71.

[3] محمد طارق عبد الرؤوف الحن، مرجع سابق، ص 225.

[4] عبد المؤمن بن صغير، تطبيق النص الجنائي بين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة. مجلة العلوم القانونية والسياسية المجلد 10 العدد 03. ديسمبر 2019، جامعة الواد، ص 71.

في هذا القانون التي ترتكب في الخارج من طرف شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري"، وهذا النص القانوني نراه الأول الذيجلب الإ ختصاص القضائي للمحاكم الجزائرية استنادا على مبدأ العالمية، والذي بموجبه يكون القانون الجزائري له صلاحية الإنطباق، وأن القضاء الجزائري له إمكانية الإنعقاد على كافة الجرائم التي تشكل اعتداء على المعطيات الشخصية بمفهوم القانون 18-07 والتي تقع في أي مكان في العالم، أيا ما كانت جنسية مرتكب هذه الجرائم، ودونما اعتبار أو اشتراط لمسألة الإضرار بمصالح جوهرية للجزائر في الخارج، طالما أن مرتكب الفعل الأجنبي مقيم في التراب الجزائري بالنسبة للشخص الطبيعي، أو كان خاضعا للقانون الجزائري إذا كان شخصا معنويا.

ومن ثم فوفقا لهذا النص يستوجب الأمر توفر مجموعة من الشروط لأجل تطبيق مبدأ عالمية النص الجزائي لإقامة اختصاص القضاء الجزائري في مواجهة الجرائم الماسة بالمعطيات ذات الطابع الشخصي.

- أن ترتكب هذه الجرائم خارج إقليم الجمهورية أي في بلد آخر.

- أن يكون مرتكب الجريمة شخصا أجنبيا.

- أن يكون الفاعل مقيما في الجزائر سواء التواجد الاختياري في الإقليم الجزائري أو الإقامة بمعناها القانوني.

- أن تكون طبيعة الجريمة تنتمي إلى فئة الجرائم التي تشكل اعتداء على المعطيات ذات الطابع الشخصي المعالجة آليا المنصوص عليها في القانون 18/ 07.

- أن تمس الجريمة المرتكبة بمصالح دولة أخرى، ولا يتعلق الأمر بالمصالح الوطنية.

وتطبيقا لذلك فإذا قام فرنسي موجود في الخارج مثلا باختراق نظام معلوماتي لهيأة حكومية مغربية أو مصرف مغربي واطلع على معطيات ذات طابع شخصي وقام بإتلافها أو التلاعب بها، ثم عند حضوره إلى الجزائر ألقي القبض عليه فيها، فإنه يمكن أن ينعقد الإ ختصاص للمحاكم الجزائرية لمحاكمته وفقا للقانون الجزائري.

وعليه يمكن القول أن جرائم الإعتداء على المعطيات ذات الطابع الشخصي التي تكون محل معالجة آلية هي بهذه الصفة تعد من الجرائم المعلوماتية، وهو ما يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني، ومن ثم فإن الطبيعة الخاصة لهذا الصنف من الجرائم تتطلب تجاوز المعايير التقليدية، قصد التغلب على مشكلة تعدد الإ ختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها والتخلص من آثارها، وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لهذه الجرائم، وتجعل من التعاون الدولي آلية مهمة لا مجال لغض الطرف عنها، ونعتقد أن هذا ما حذا بالمشرع الجزائري إلى الأخذ بمبدأ عالمية النص الجزائي عندما يتعلق الأمر بطائفة جرائم الاعتداء على المعطيات الشخصية المعالجة آليا.

ملخص الفصل الثالث

نخلص في هذا الفصل إلى القول بأن الإطار القانوني وحده لا يعد فاعلا إلا متى تأمنت آليات وإمكانات الإنفاذ الفاعل والتطبيق السليم للقانون، سواء عن طريق إيجاد جهة مستقلة ذات طابع إداري تكون لها سلطات واسعة بما يكفل لها ممارسة دورها الإشرافي والرقابي بشكل يمكنها من التطبيق الدقيق لأحكام القانون المتعلق بحماية المعطيات الشخصية، أو عن طريق آلية الردع الجزائي لتوفير مستويات من الحماية الجزائية، والوقوف على صور الإعتداء والإنتهاكات التي تطال الحق في الخصوصية المعلوماتية وصونه وردع هذه الاعتداءات، وبالتالي اتباع حماية جزائية فاعلة على هذا الحق.

لذلك تكون حماية الحق في الخصوصية المعلوماتية إما حماية إدارية تجسدها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وهي جهة مستقلة بصلاحيات واسعة ومضبوطة بما يكفل لها ممارسة دور رقابي وإشرافي بشكل يسمح بالتطبيق الصارم لقانون حماية المعطيات الشخصية، حيث يكون لها القدرة على التوفيق بين ضرورة وجود الأنظمة المعلوماتية وتطورها وضمان الحق في الخصوصية للأفراد.

والمشرع الجزائري استلهم حاجته في إنشاء هذه الهيأة الإشرافية المستقلة من تجربة معظم الدول التي لديها تشريعات في مجال حماية البيانات الشخصية، حيث استحدث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب نص المادة 22 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أين كلفها بالسهر على مطابقة عمليات معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيا الإعلام والإتصال على أية أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، كما تتولى هذه السلطة إعلام الأشخاص المعنيين بالمعالجة والمسؤولين عنها بحقوقهم وواجباتهم، وتقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، وإعلام أصحابها بمآلها والترخيص بنقلها إلى الخارج، ومنح تراخيص وتلقي التصريحات المتعلقة بمعالجة هذه المعطيات . وفي سبيل ذلك أضفى المشرع على هذه السلطة مجموعة من الخصائص تؤهلها لهذا الدور، أهمها أنها سلطة مستقلة، بالإضافة إلى منحها مجموعة من المهام والصلاحيات سواء في الإشراف والرقابة السابقة أو اللاحقة أو في سلطة توقيع عقوبات الغرامة دارية.

ثم عرفنا أن تعزيز الحماية القانونية للمعطيات الشخصية استدعى تدخل المشرع لتحديد قواعد ومبادئ الحماية الجزائية لهذا النوع من المعطيات، وكان ذلك إما من خلال الحماية الجزائية الموضوعية التي تتصل بتكريس هذا الحق وصونه وردع الإعتداءات التي تطاله، وعلى هذا الأساس عمل المشرع على إصدار نصوص جزائية تعاقب على الجرائم الماسة بالحق في الخصوصية المعلوماتية في إطار القانون 07/18، ولم يقتصر الأمر فقط على هذا النص القانوني الإطار، فمن أجل تحقيق حماية جزائية فعالة وناجحة للحق في الخصوصية المعلوماتية، نجد بعض النصوص القانونية الأخرى التي تحمل في طياتها أحكاما جزائية تضمن توفير الحماية الجزائية للمعطيات الشخصية في مجالها، من خلال القسم السابع مكرر في قانون العقوبات بعنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في 10

نوفمبر 2004 والتي تحمي أنظمة المعالجة الآلية بشكل عام كيفما كان محتواها والذي يكون في كثير من الحالات معطيات شخصية.

ثم تناولنا أحكاما خاصة تثيرها المسؤولية الجزائية عن الجرائم التي تشكل اعتداء على المعطيات الشخصية ويتعلق الأمر بمسألتان تبدوان في غاية الأهمية، الأولى مرتبطة بأحكام المعاقبة على الشروع في هذه جرائم، وأما الثانية فتتعلق بالمسؤولية الجزائية للشخص المعنوي عند ارتكابه لمثل هذه الجرائم.

إضافة إلى إرساء قواعد قانونية موضوعية لحماية المعطيات الشخصية من الإعتداءات الناتجة عن المعالجة غير المشروعة، فإن الحماية القانونية الكاملة للمعطيات ذات الطابع الشخصي تقتضي أيضا ضرورة وضع قواعد إجرائية قادرة على كفالة هذه الحماية، فإذا استطاع المشرع أن يحيط بالقاعدة الموضوعية من خلال تجريم هذه الإعتداءات الناتجة عن المعالجة غير المشروعة للمعطيات الشخصية، فإن نجاحه يبقى مرهونا بمدى فعالية التنظيم الإجرائي الذي يضمن لتلك القواعد الموضوعية الأثر الفعال لمجابهة هذه الجرائم، لذلك فإذا ما حدث أن وقعت إحدى الجرائم الماسة بالمعطيات الشخصية المعالجة آليا، فإن العقاب عليها لن يكون إلا بكشفها وتثبيت الدليل عليها، عن طريق تكريس قواعد مناسبة لبيئة النظم المعلوماتية التي تحصل فيها هذه الجرائم، كون الدليل الذي يمكن الإستناد عليه في إثباتها له ذاتيته وخصائصه التي تتناسب مع خصوصية هذه الجرائم حتى يكون صالحا لإثباتها، ويتمثل في الدليل الإلكتروني الذي يتشكل من طبيعة الجريمة التي يولد منها، وعرفنا أنه هو الدليل المناسب لإثبات هذا النوع من الجرائم بعد تفحص خصائصه التي تؤهله لذلك ، ثم تناولنا موضوع إجراءات الحصول على الدليل الرقمي من خلال معرفة الجهات المكلفة بالبحث والتحري عن جرائم الإعتداء على المعطيات الشخصية والقواعد الإجرائية في استخلاص الدليل الرقمي، وأخيرا القيمة القانونية للدليل الرقمي في مجال إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا.

خاتمة

خاتمة

قليلون هم من ينكرون الفوائد الكبرى لتطبيقات المعالجة الإلكترونية للمعطيات ذات الطابع الشخصي، لكن الكثيرين منهم من يتزايد قلقهم بشأن احتمالات الإستخدام غير المشروع لمعطياتهم الشخصية، بالنظر إلى القدرات العالية التي توفرها التقنية المعلوماتية على أداء عمليات الجمع والتخزين والمعالجة لهذه المعطيات، وأصبح نتيجة لذلك يبدو صعبا على الأفراد اتخاذ وسائل وإجراءات لحماية بياناتهم الشخصية من مخاطر المعلوماتية، قياسا بما يتطلبه الأمر لحماية خصوصيتهم من أنشطة الجمع والمعالجة التقليدية اليدوية.

لذلك كانت نقطة الإنطلاق الصحيحة هو الإتجاه نحو نظام قانوني يحاكي تحديات العصر ويدرؤ مخاطر الآثار السلبية لهذه التقنية المعلوماتية في مواجهة معالجة المعطيات ذات الطابع الشخصي.

وعلى ضوء ذلك، تحددت إشكالية هذه الدراسة في بحث مدى نجاعة وفعالية التدابير القانونية التي كرسها المشرع الجزائري في القانون 07/18 لتوفير الحماية للخصوصية المعلوماتية من خلال حماية المعطيات ذات الطابع الشخصي.

ووفاء لهذه الغاية وترتيبا على هذه الدراسة فقد تم التوصل في نهايتها إلى جملة من النتائج نذكر أهمها كما يلي:

1- تبين معنا من خلال هذه الدراسة أن هناك معطيات يمكن عن طريقها الإستدلال على هوية شخص ما ويمكنها التعريف به بصورة صريحة وبصفة مباشرة، كالإسم مثلا أو أن تكون هذه المعطيات في مجموعها قادرة عن طريق معالجتها بالربط بينها ودمجها على الوصول إلى تحديد هوية ذلك الشخص، وهي ما يعرف بالمعطيات ذات الطابع الشخصي.

2- تبين لنا أن المعطيات ذات الطابع الشخصي المتعلقة بالأفراد تكون متفرقة ومشتتة بين مختلف قواعد البيانات، وهي على هذه الحالة تكون لوحدها وبذاتها غير ضارة، لكن بفعل ما تتيحه التقنية المعلوماتية من إمكانية جمع هذه المعطيات ومعالجتها، فإنها تتحول إلى معطيات قد تشكل تهديدا حقيقيا لخصوصية الأفراد، حيث تصبح نوعا من البيان التفصيلي عن حياة الفرد وأنشطته وكشفا لخبايا أسراره.

3- لقد كرس المشرع مجموعة من الضوابط القانونية التي تحكم المعالجة السليمة والمشروعة للمعطيات ذات الطابع الشخصي، حيث تكون هذه الضوابط موضوعية ترتبط أساسا بحقوق المعني بالمعالجة وهو صاحب المعطيات الشخصية محل المعالجة، يهدف المشرع من وراء إقرارها له ، هو إعطاؤه إمكانية السيطرة على معطياته الشخصية، وتتمثل هذه الحقوق أساسا في الحق في الإعلام، الحق في الولوج، الحق في التصحيح والحق في الإعتراض، بالإضافة إلى تكريس المشرع لمجموعة من المبادئ التي يتوجب احترامها عند كل معالجة للمعطيات ذات الطابع الشخصي، كي لا ينتج عن ذلك أي إساءة إلى أصحابها، وذلك من خلال مبدأ مشروعية المعالجة الذي يقتضي أن تكون العمليات التي تتم آليا بهدف استغلال

المعطيات الشخصية عن طريق الربط ودمج معطيات شخصية مع معطيات أخرى، وتحليلها للحصول على معلومات ذات دلالة خاصة، قائم على عدم الإعتماد على بيانات شخصية غير صحيحة أو غير دقيقة.

4- وقد تكون ضوابط المعالجة إجرائية تندرج ضمن مجموعة الإجراءات المسبقة على معالجة المعطيات ذات الطابع الشخصي والتي ينبغي على كل شخص طبيعي أو معنوي ينتمي إلى القطاع العام أو الخاص يقوم بمعالجة معطيات ذات طابع شخصي يعتبر معنيا باحترام هذه الإجراءات قبل البدء في إنشاء معالجة معلوماتية لمعطيات شخصية، وتنحصر أساسا في التصريح لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الترخيص منها قبل القيام بهذه المعالجات، مالم تكن المعالجة تنصب على حالة من الحالا ت التي استثنى فيها المشرع الخضوع لهذه الإجراءات.

5- تتعرض المعطيات ذات الطابع الشخصي لجملة من المخاطر والتهديدات خلال عمليات معالجتها بواسطة أجهزة الكومبيوتر، حيث يعد تجميعها وتخزينها في هذه الأجهزة مدعاة لأن يجعل من فرص الوصول إليها على وجه غير مأذون به وبطرق التحايل أكثر من ذي قبل، ومن ثم يفتح المجال واسعا لإساءة استخدامها أو توجيهها توجيها منحرفا أو استخدامها في غير الغرض المشروع الذي جمعت لأجله، وهو أمر من شأنه المساس بخصوصية الأفراد أصحاب هذه المعطيات.

6- ولا يتوقف تهديد الخصوصية المعلوماتية للأفراد عند حد بنوك المعطيات فقط، بل كان لشبكات الإتصالات الإلكترونية دور في كشف وتعرية خصوصية الأفراد، كونها لا تتوافر على سبل الأمان لما ينقل عبرها من بيانات شخصية، مما يسهل من إمكان الحصول عليها بطريقة غير مشروعة والعبث بها.

7- وانطلاقا من هذه المخاطر أورد المشرع آليات الحماية القانونية لمواجهة التحديات والمشكلات الجديدة الناشئة عن أثر التقنية المعلوماتية على خصوصية الأفراد في مجال معالجة معطياتهم الشخصية، وذلك عن طريق آلية الحماية الإدارية المجسدة في إيجاد جهة إدارية مستقلة يكون لها دور الإشراف والرقابة على عمليات معالجة المعطيات ذات الطابع الشخصي بشكل يكفل التطبيق السليم للقانون، أو عن طريق آلية الردع الجزائي من خلال العقاب على كل صور الإنتهاكات والإعتداءات التي تطال الحق في الخصوصية المعلوماتية.

الإقتراحات:

1) تضمن القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي النص على تمكين المعني بالمعالجة مجموعة من الحقوق، كحق الإعلام والتصحيح وغيرها متأسيا بباقي التشريعات المقارنة، مثل المشرع الفرنسي في القانون 2004/801 والمشرع المغربي في القانون 09/08 ، غير أن هذه القوانين رافقتها مراسيم تنفيذية تبين بشكل واضح كيفية ممارسة هذه القوانين لرفع أي لبس أو غموض يمكن أن يلتبس بهذه الحقوق في الواقع العملي، مثل ما فعل المشرع الفرنسي من خلال المرسوم 1309/2005 المؤرخ في2005/10/20 ، والمشرع الغربي بموجب المرسوم165.09.2 المؤرخ في 2009/05/29. لذلك نأمل أن يصدر مرسوم تنظيمي في هذا الشأن يكون تطبيقا لأحكام القانون 07/18 في

العديد من المسائل، سواء في توضيح كيفية ممارسة الشخص المعني بالمعالجة لحقوقه، أو بخصوص كيفية ممارسة السلطة الوطنية لصلاحياتها وسلطاتها.

2) بشأن الضمان الحقيقي لاستقلال السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، فإننا نعيب على المشرع الجزائري إدراجه في تشكيلة هذه الهيئات 07 أعضاء تابعين لوزارات مختلفة، وهذا من شأنه إضعاف الإستقلال العضوي للسلطة الوطنية، لذلك نقترح أن يعاد النظر في تشكيلة هذه السلطة على ألا يكون أي عضو فيها يجمع بين عضويته في السلطة الوطنية وعضويته في الحكومة لعدم التوافق بين المنصبين، وتكريسا للاستقلالية الحقيقية لهذه السلطة.

3) نقترح تعديل الفقرة الأخيرة من المادة 23 من القانون 07/18 التي تتحدث عن تعيين رئيس وأعضاء السلطة الوطنية بموجب مرسوم رئاسي لعهدة مدتها 05 سنوات قابلة للتجديد، دون تحديد لعدد المرات، وهو من شأنه أن يفتح باب التأويل عن إمكانية التجديد لأكثر من مرة، لذلك ينبغي أن يكون النص كما يلي: "لعهدة مدتها 05 سنوات قابلة للتجديد مرة واحدة".

4) نقترح تعديل نص المادة 23 أيضا فيما يتعلق بمدة العضوية بالنسبة للعضوين المقترحين من طرف المجلس الشعبي الوطني ومجلس الأمة، بالنص صراحة في هذه المادة أن تكون مدة عضويتهم في السلطة الوطنية مرتبطة بمدة عضويتهم بمناصبهم الأصلية، لأنه في حالة انتهاء صفتهم الأصلية فإنه يترتب عليه وجودهم كأعضاء في السلطة الوطنية غير مبرر قانونا، وبالتالي يجب أن يعوضوا بأعضاء آخرين بنفس الشروط للمدة المتبقية.

5) نقرح أن يحذو المشرع الجزائري حذو المشرع الفرنسي ويدرج صور التجريم الناتجة عن أفعال الإعتداء على المعطيات ذات الطابع الشخصي التي جاء بها القانون 07/18 ضمن أحكام القسم الخاص من قانون العقوبات وفي ذلك إقرار بانطباق الأحكام العامة عليها.

6) ولكون قوانين حماية المعطيات ذات الطابع الشخصي من شأنها أن تعزز إمكانية الإستغلال الأفضل لهذه المعطيات سواء من خلال استخدامها في ربط الخدمات الإدارية الرسمية تسهيلا لأمور المواطنين، أو في تطوير خدمات القطاع الخاص، أو تعزيز الثقة في الإقتصاد الرقمي والتجارة الإلكترونية، ندعو المشرع الجزائري إلى استكمال الأسس التشريعية والتنظيمية للتعاملات الإلكترونية التي تستوجب التعامل مع المعطيات ذات الطابع الشخصي بما يتوافق مع أحكام القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي سيما في مجال الصحة أو مجال الصحافة وغيرها.

7) وما يمكن ملاحظته أن المشرع الجزائري لم يحدد كيفية ممارسة السلطة الوطنية لحماية المعطيات الشخصية مهام البحث والمعاينة لجرائم الإعتداء على المعطيات الشخصية عن طريق أعوانها أو عن طريق أعوان آخرين يمكن أن تلجأ إليهم هذه السلطة، حيث جاءت نصوص القانون 07/18 في هذا الخصوص مقتضبة وغير كافية لتوضيحها بشكل دقيق، وهذا على خلاف ما نجده في التشريع الفرنسي، الذي نظم الصلاحيات الخاصة باللجنة الوطنية للمعلوماتية والحريات المتعلقة بالبحث والتقصي ومعاينة هذا النوع

من الجرائم، لذلك ندعو في هذا الصدد إلى إصدار مرسوم تنظيمي تحدد من خلاله صلاحيات السلطة الوطنية في إطار مهامها المتعلقة بالبحث والتقصي ومعاينة جرائم الإعتداء على المعطيات ذات الطابع الشخصي المعالجة آليا، وهذا من أجل تحسين مستوى الحماية الجزائية الإجرائية لهذه المعطيات الشخصية.

8) نهيب بالمشرع الجزائري أن يجتهد في اعتماد المعايير اللازمة في حماية المعطيات ذات الطابع الشخصي على غرار ما هو معمول به على المستوى الدولي، لتحقيق التنسيق الذي يؤمن الإنسجام مع القوانين المقارنة في مجال حماية المعطيات الشخصية، وذلك لضمان التدفق الحر للمعطيات الشخصية عبر الحدود ورفع مستوى الثقة في إمكانية تحويل ونقل المعطيات نحو الجزائر في إطار الإستثمارات الإقتصادية الأجنبية وغيرها.

تم بحمد الله، والله ولي التوفيق

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر

القوانين:

1) دستور سنة 63 الجريدة الرسمية رقم 64 الصادر بتاريخ 1963/09/10.
2) دستور سنة 76 الصادر بموجب الأمر 97/76 مؤرخ في 1979/11/22 الجريدة الرسمية عدد94.
3) دستور سنة 89 المنشور بموجب المرسوم الرئاسي رقم 18/89 المؤرخ في 1989/02/28 الجريدة الرسمية عدد 09.
4) دستور سنة 96 الصادر في الجريدة الرسمية رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل سنة 2016.
5) القانون 19/04 مؤرخ في 25 ديسمبر 2004 يتعلق بتنصيب العمال ومراقبة التشغيل الجريدة الرسمية عدد 83 مؤرخ في 26 ديسمبر 2004.
6) القانون رقم 23/06 المؤرخ في 2006/12/20 المعدل والمتمم للأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات.
7) قانون 04/09 مؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر عدد 47.
8) القانون رقم 04/15 مؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني ج ر عدد 06 مؤرخة في 2015/02/10.
9) القانون رقم 12/15 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل، جريدة رسمية عدد 39 الصادرة بتاريخ 19 جويلية 2015.
10) القانون 03/16 المؤرخ في 2016/06/19 متعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، ج ر عدد 37 صادرة في 19 جوان 2016.
11) القانون 04/18 المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، المؤرخ في 10 ماي 2018 جريدة رسمية عدد 27.
12) قانون رقم 05/18 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الالكترونية، الجريدة الرسمية عدد 28 مؤرخة في 16 ماي 2018.
13) القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي
14) قانون 11/18 المؤرخ في 02 جويلية، المتعلق بالصحة وترقيتها. جريدة رسمية عدد 46.

المراسيم:

1) المرسوم التشريعي رقم 01/94 المؤرخ في 15 جانفي 1997، يتعلق بالمنظومة الإحصائية، جريدة رسمية عدد 03 بتاريخ 16 جانفي 1994.

2) المرسوم التنفيذي رقم 313/14 المؤرخ في 10نوفمبر 2013 المتضمن الموافقة على رخصة لإقامة شبكة عمومية للمواصلات السلكية الخلوية، جريدة رسمية عدد37.

الإتفاقيات:

1) علان العالمي لحقوق الإنسان، منشور بموجب قرار الجمعية العامة للأمم المتحدة 217 (ألف-د-3) بتاريخ 1948/12/10.

2) إتفاقية مجلس أوروبا رقم 108 المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي الموقعة في ستراسبورغ في 28 جانفي 1981.

3) الاتفاقية الأوروبية المتعلقة بالإجرام المعلوماتي رقم 185، موقعة في بودابست بتاريخ 2001/11/23.

4) الإتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديموقراطية الشعبية وحكومة الجمهورية الفرنسية، الموقعة بباريس بتاريخ 05 أكتوبر 2016 والمصادق عليها بالمرسوم الرئاسي رقم 73/18 المؤرخ في 2018/02/25 ج ر عدد 13.

5) التقرير التفسيري لإتفاقية الجريمة الإلكترونية الموقعة في بودابست بتاريخ 23 نوفمبر 2001 بمناسبة المؤتمر الدولي لحماية الجريمة الإلكترونية.

ثانيا: المراجع باللغة العربية:

الكتب العامة:

1) أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص (الجرائم ضد الأشخاص والجرائم ضد الأموال وبعض الجرائم الخاصة)، الجزء الأول، دار هومة، الجز ائر، 2009.

2) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر، الطبعة الثامنة، 2009.

3) أحمد عبد الظاهر، الحماية الجنائية لحق الشخص المعنوي في الشرف والاعتبار دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2005.

4) أحمد فتحي سرور، أصول قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1999.

5) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الأول الطبعة السادسة، دار النهضة العربية، القاهرة1996.

6) أحمد كامل سلامة، الحماية الجنائية للأسرار المهنية، دار النهضة العربية للنشر والتوزيع، القاهرة.

7) خيري أبو العزايم فرجاني، نطاق الشروع في الجريمة، بدون دار نشر وتاريخ النشر.

8) رامز محمد عمار، نعمت عبد الله مكي، حقوق الإنسان والحريات العامة، الطبعة الأولى 2010، بدون دار النشر.

9) سعيد أمجد الزهاوي، التعسف في استعمال حق الملكية في الشريعة والقانون، دار الإتحاد العربي للطباعة الطبعة الأولى، القاهرة، 1975.

10) سمير الشناوي، الشروع، دراسة مقارنة، دار النهضة العربية، القاهرة 1971.

11) ضاري خليل محمود، أثر رضا المجني عليه في المسؤولية الجزائية، دار القادسية للطباعة، الطبعة الأولى، 1982.

12) عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، الجزء الأول، مطبعة المعارف بغداد، الطبعة الأولى 1974.
13) عبد السميع أسامة السيد، التعويض عن الضرر الأدبي، دراسة تطبيقية في الفقه الإسلامي والقانون، دار الجامعة الجديدة الإسكندرية، 2007.
14) عبد العزيز محمد سرحان، الإتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، دار النهضة العربية، القاهرة، 1966.
15) عبد الفتاح مصطفى الصيفي، قانون العقوبات، القسم الخاص- الجرائم الماسة بأمن الدولة، منشأة المعارف، الاسكندرية، 2000.
16) عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول الجريمة، ديوان المطبوعات الجامعية، 2009.
17) عبد المهيمن بكر سالم، القسم الخاص في قانون العقوبات جرائم الإعتداء على الأشخاص والأموال، دار النهضة العربية القاهرة 1976.
18) علي حسين خلف، سلطان عبد القادر الشناوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد 2015.
19) محمد أبو العلا عقيدة، الإتجاهات الحديثة في قانون العقوبات الفرنسي الجديد الصادر في 1992/07/22، دار النهضة العربية، القاهرة 2004.
20) محمد زكي أبو عامر. "قانون العقوبات القسم الخاص" دار المطبوعات الجامعية، الإسكندرية، مصر 1977.
21) محمد صبحي نجم، شرح قانون العقوبات الجزائري –القسم الخاص- ديوان المطبوعات الجامعية، الطبعة الخامسة، الجزائر، 2005.
22) محمد طه البشير، غني حسون طه، الحقوق العينية القسم والأول والثاني الحقوق العينية الأصلية والحقوق العينية التبعية، الدار الجامعية للطباعة والنشر، بغداد 2017.
23) محمد عدنان الخطيب، موجز القانون الجزائي، المبادئ العامة في قانون العقوبات، الكتاب الأول، مطبعة جامعة دمشق، 1963.
24) محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص، الطبعة الأولى، دل النهضة العربية للنشر والتوزيع، القاهرة 1988.
25) محمود شريف بسيوني، محمد سعيد الدقاق، عبد العظيم وزير، حقوق الإنسان. الوثائق العالمية والإقليمية، المجلد الأول، الطبعة الأولى، دار العلم للملايين، بيروت، 1998.
26) مصطفى الجمال، إبراهيم سعد، النظرية العامة للقانون –الحق- منشورات الحلبي الحقوقية، بيروت بدون تاريخ نشر.
27) هاني سليمان الطعيمات، حقوق الإنسان وحرياته الأساسية الطبعة الثانية، دار الشروق للنشر والتوزيع 2003.

الكتب الخاصة:

1) أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة دار النهضة العربية، الطبعة الأولى 2000.
2) أحمد درويش، حرية تداول المعلومات في مصر، مكتبة الإسكندرية للنشر، مصر 2009.

3) أحمد عمر حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، الطبعة الأولى 2000.

4) آدم عبد البديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي. القاهرة، دار النهضة العربية للنشر والتوزيع، 2000.

5) أسامة أحمد بدر، الوسائط المتعددة بين واقع الدمج الإلكتروني للمصنفات وقانون حماية حق المؤلف، دار الجامعة الجديدة للنشر الإسكندرية، 2004.

6) أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة، الطبعة الثالثة، دار النهضة العربية القاهرة، 1994.

7) أسامة عبد الله قايد، المسؤولية الجنائية للطبيب عن إفشاء سر المهنة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة 1986.

8) أسامة عبد الله قايد، حقوق وضمانات المشتبه فيه في مرحلة الاستدلالات دراسة مقارنة، دار النهضة العربية 1992.

9) أشرف صابر سيد، مسؤولية مقدمي خدمات الأنترنت عن المضمون الإلكتروني غير المشروع، دار النهضة العربية، القاهرة، 2010.

10) أشرف فتحي الراعي، حق الحصول على المعلومات دراسة مقارنة، الطبعة الأولى، دار الثقافة للطباعة والنشر والتوزيع، عمان 2010.

11) أندريه برتران نيكولا فتوش، الحق في الحياة الخاصة والحق في الصورة، المنشورات الحقوقية صادر، الطبعة الأولى، دون سنة النشر.

12) أيمن بن ناصر بن حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، دراسة مقارنة، مكتبة القانون والاقتصاد الرياض، الطبعة الأولى، 2015.

13) أيمن عبد الله فكري، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد للنشر والتوزيع، الطبعة الأولى، 2014، الرياض العربية السعودية.

14) بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2009، بيروت لبنان.

15) بولين أنطونيوس أيوب، تحديات شبكة الأنترنت على صعيد القانون الدولي الخاص، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت 2006.

16) توفيق حسن فرج، المدخل للعلوم القانونية، النظرية العامة للحق، مؤسسة الثقافة الجامعية، الإسكندرية مصر 1983.

17) جلال علي العدوي، رمضان أبو السعود، الحقوق وغيرها من المراكز القانونية، منشاة المعارف، الإسكندرية 1996.

18) جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001.

19) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار الفكر العربي، القاهرة، 2001.

20) جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، مكتبة دار النهضة العربية، القاهرة، 1992.

21) حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة الطبعة الثانية، دار النهضة العربية، 2002.

22) حسام شوقي، حماية وأمن المعلومات على الانترنت، دار الكتب العلمية، القاهرة، 2003.

23) حسان أحمد محمد، نحو نظرية عامة لحماية الحق في الحياة الخاصة، دار النهضة العربية، القاهرة، 2001.

24) حسين الغافري، محمد الألفي، جرائم الانترنت بين بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، 2008.

25) حسين فاروق، الأنترنت، الشبكة الدولية للمعلومات، دار الراتب الجامعية، بيروت، 1995.

26) حسين محمد عبد الظاهر، المسؤولية المدينة للمحامي تجاه العميل، دار النهضة العربية للنشر والتوزيع، القاهرة، طبعة 1993.

27) خضر مصباح، إسماعيل الطيطي، أساسيات إدارة المشاريع وتكنولوجيا المعلومات، دار حامد للنشر والتوزيع الطبعة الأولىعمان ـ 2002.

28) رأفت رضوان، عالم التجارة الإكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، الطبعة الأولى، 1999.

29) ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنت والمعلوماتية، دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، مصر، الطبعة الأولى، 2017.

30) رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الأنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2013.

31) رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية الطبعة الأولى، 2012.

32) سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتبكة عبر الأنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

33) سليمان علي حمادي الحلبوسي، المسؤولية المدينة الناشئة عن إفشاء السر المهني، دراسة قانونية، منشورات الحلبي الحقوقية، بيروت2012.

34) شريف بدوي، أسباب بطلان الضبط والتفتيش، دار الثقافة للطباعة والنشر، القاهرة 1989.

35) شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لحق الاطلاع على البيانات الشخصية دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، المنصورة، الطبعة الأولى، 2015.

36) شمس الدين أشرف توفيق، الصحافة والحماية الجنائية لحرمة الحياة الخاصة، دراسة مقارنة، دار النهضة القاهرة، العربية 1999.

37) شيماء عبد الغني، محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر 2007.

38) صلاح محمد أحمد دياب، الحماية القانونية للحياة الخاصة للعامل وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب الحديثة وشتات للنشر والبرمجيات، الطبعة الأولى، مصر 2010.

39) ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي –دراسة مقارنة- مكتبة دار السلام القانونية، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، القاهرة 2017.

40) طارق جمعة السيد راشد، المسؤولية المدنية للناشر الإلكتروني – دراسة مقارنة- المركز العربي للدراسات والبحوث العلمية، القاهرة 2017.

41) طارق صديق رشيد كه ردى، حماية الحرية الشخصية في القانون الجنائي، (دراسة تحليلية مقارنة) منشورات الحلبي بيروت، الطبعة الأولى 2011.

42) طوني مشال عيسى، التنظيم القانوني لشبكة الأنترنت، دراسة مقارنة في ضوء القوانين الوضعية والإتفاقات الدولية، المنشورات الحقوقية، بيروت 2001.

43) عادل جبري محمد حبيب، مدى المسؤولية عن الأفعال بالالتزام بالسر المهني أو الوظيفي مع عرض لأهم الحالات التي يرتفع فيها الالتزام بالسر المهني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2003.

44) عادل عبد الصادق، البيانات الشخصية، الصراع على نفط القرن الحادي والعشرين، مركز الأهرام للدراسات السياسية والاستراتيجية، كراسات استراتيجية، العدد 287، المجلد السابع والعشرون، أفريل 2018.

45) عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية (شبكة الانترنت، وشبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات). دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، ردن2011.

46) عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والأنترنت، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الاردن 2009.

47) عبد الحميد بيسوني، الحماية من أخطار الأنترنت، أخطار الأنترنت ومصادر التهديد، دار الكتب العلمية القاهرة، 2003.

48) عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والإقتصاد، الرياض 2012.

49) عبد الفتاح بيومي حجازي، الأحداث والأنترنت: دراسة معمقة على أثر الانترنت في انحراف الأحداث، دار الفكر الجامعي، الطبعة الأولى، 2002.

50) عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، دراسة متعمقة ومقارنة، الطبعة الأولى، منشاة المعارف، القاهرة.2009.

51) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، الطبعة الأولى 2002 الإسكندرية.

52) عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الإلكترونية، دار الفكر الجامعي، الاسكندرية 2003.

53) عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والأنترنت في القانون العربي النموذجي، دراسة معمقة في مكافحة جرائم التقنية الحديثة، دار النهصة العربية، الطبعة الأولى، 2009 القاهرة.

54) عبد الهادي فوزي العوضي- الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة 2005.

55) العربي جنان، معالجة المعطيات ذات الطابع الشخصي، الحماية القانونية في التشريع المغربي والمقارن، المطبعة والوراقة الوطنية، الداوديات، الطبعة الأولى، 2010.

56) عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة الإسكندرية 2005.

57) عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية 2003.

58) علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس لبنان،2006.

59) علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة – دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى 2013.

60) علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدارالجامعية للطباعة والنشر، بيروت لبنان 1999.

61) علي عبود جعفر. جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة منشورات زين الحقوقية، الطبعة الأولى، 2013.

62) علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية (دراسة مقارنة)، المؤسسة الحديثة للكتاب، لبنان، الطبعة الأولى، 2011.

63) عمار عباس الحسيني، التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجنائي، دراسة مقارنة في التشريعات واجتهادات الفقه والقضاء، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع القاهر ة2017.

64) عمار عباس الحسيني، جرائم الحاسوب والانترنت الجرائم المعلوماتية، منشورات زين الحقوقية، الطبعة الأولى، 2017.

65) عمر فاروق الحسيني، المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الثانية، 1995.

66) عوض منصور، محمد أبو النور، مقدمة في علم الحاسب الإلكتروني وبرمجة البيسك، دار الأمل للنشرو التوزيع، الطبعة الخامسة، 1996.

67) عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان الأردن 2007.

68) غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكومبيوتر والأنترنت وجرائم الإ حتيال المنظم باستعمال شبكة الأنترنت، دار الفكر والقانون، المنصورة مصر 2017.

69) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الثانية، 2007.

70) فتوح عبد الله الشاذلي، جرائم الإ عتداء على الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية 2002.

71) قدري علي عبد المجيد، الإعلام وحقوق الإنسان قضايا فكرية ودراسة تحليلية وميدانية، دار الجامعة الجديدة الإسكندرية مصر العربية 2010.

72) محسن عبد الحميد البيه، نظرة حديثة إلى خطأ الطبيب الموجب للمسؤولية المدنية في ظل القواعد القانونية التقليدية، مكتبة الجلاء الجديدة، المنصورة 1993.

73) محمد أمين الرومي، التعاقد الإلكتروني عبر الأنترنت، دار المطبوعات الجامعية، الطبعة الأولى، الإسكندرية 2004.

74) محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثالث، 2009 عمان الأردن.

75) محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، 2003.

76) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الاسكندرية 2007.

77) محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الأنترنت، الأحكام الموضوعية والأحكام الإجرائية منشورات الحلبي الحقوقية، الطبعة الأولى، 2011.

78) محمد عبد الكريم حسين الداوودي، المسؤولية الجنائية لمورد خدمة الأنترنت، منشورات الحلبي الحقوقية الطبعة الأولى، بيروت2017.

79) محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية، جرائم الكومبيوتر والانترنت، منشاة المعارف الإسكندرية 2006.

80) محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي، مطبوعات جامعة الكويت، أفريل 1992.

81) محمد عبد الودود عبد الحفيظ أبو عمر، المسؤولية الجزائية عن إفشاء السر المصرفي، دار وائل للطباعة والنشر، عمان الأردن، 1999.

82) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت – دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، القاهرة،2009.

83) محمدعلي السالم عياد الحلبي، ضمانات الحرية الشخصية أثناء التحري والإستدلال في القانون المقارن. الطبعة الأولى، الكويت، منشورات ذات السلاسل، 1986.

84) محمد كمال محمد الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دراسة مقارنة دار الفكر والقانون، المنصورة مصر، 2017.

85) محمد لطفي عبد الفتاح، القانون الجنائي واستخدامات التكنولوجيا الحيوية، دراسة مقارنة، دار الفكر والقانون، الطبعة الأولى، المنصورة، 2012.

86) محمد محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، الطبعة الأولى 2005 القاهرة مصر.

87) محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر 2012.

88) محمد نصر محمد، حق الإنسان في حماية حياته الخاصة في القانون الدولي والتشريعات الداخلية، مكتبة القانون والاقتصاد الرياض 2013.

89) محمد يوسف علوان، محمد خليل الموسى، القانون الدولي لحقوق الإنسان، الحقوق المحمية، الجزء الثاني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثالث 2011.

90) محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الطبعة الأولى 2014، الإسكندرية مصر.

91) محمود أحمد طه، التنصت والتلصص على سرية الاتصالات الشخصية بين التجريم والمشروعية، دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر 2017-2018.

92) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع عمان الأردن، الطبعة الأولى، الإصدار الثاني 209.

93) محمود صالح العدلي، الحماية الجنائية لالتزام المحامي بالمحافظة على أسرار موكليه –دراسة مقارنة- دار الفكر الجامعي، الإسكندرية، 2005.

94) محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة أو الخصوصية دراسة مقارنة، دار النهضة العربية، القاهرة.

95) مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، 2001.

96) مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الإتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، 2016.

97) مصطفى أحمد عبد الجواد حجازي، الحياة الخاصة ومسؤولية الصحفي، دراسة فقهية قضائية مقارنة في القانونين الفرنسي والمصري، دار الفكر العربي، القاهرة 2001.

98) مصطفى مجدي هرجة، جرائم السب القذف والبلاغ الكاذب المكتبة القانونية للنشر والتوزيع، الطبعة الثالثة دون بلد النشر، دون تاريخ النشر.

99) مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها ومكافحتها) دراسة مقارنة، دار الكتب القانونية، 2005.

100) ممدوح خليل العاني، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة، 1983.

101) ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة 1996.

102) منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، بيروت لبنان، 2018.

103) منير محمد الجنبي وممدوح محمد الجنبي، أمن المعلوماتالإلكتروني، دار الفكر الجامعي، الإسكندرية 2005.

104) موفق علي عبيد، المسؤولية الجزائية للأطباء عن إفشاء السر المهني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 1998.

105) ناصر وسام خليل، التجارة والتسويق الإلكتروني، دار أسامة للنشر والتوزيع، الطبعة الأولى، عمان، 2008.

106) نايل إبراهيم عيد، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي، دار النهضة العربية 2000 القاهرة.

107) نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الاولى، بيروت 2005.

108) نعيم مغبغب، حماية برامج الكومبيوتر، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية بيروت، 2009.

109) نعيم مغبغب، مخاطر المعلومات والأنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية2008.
110) نهلا عبد القادر المومني، الجرائم المعلوماتية، دارالثقافة للنشر والتوزيع، الطبعة الثانية، الأردن،2010.
111) هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، الطبعة الأولى، 1992.
112) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992.
113) هلالي عبد الله أحمد،الجوانب الموضوعية والإ جرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة.2003
114) وسيم شفيق الحجار. النظام القانوني لوسائل الإتصال الإجتماعي- دراسة قانونية مقارنة حول الخصوصية والحرية الشخصية والمسؤولية والإ ختصاص، المركز العربي للبحوث القانونية والقضائية لجامعة الدول العربية – بيروت، الطبعة الأولى 2017.
115) يحيى شقير، قانون ضمان حق الوصول إلى المعلومات دراسة مقارنة مع المعايير الدولية، مركز القدس للدراسات السياسية، الطبعة الأولى، 2013، عمان الأردن.
116) يوسف الشيخ يوسف، حماية الحق في حرمة الأحاديث الخاصة- دراسة مقارنة في تشريعات التنصت والحياة الخاصة، دار الفكر العربي، الطبعة الأولى، القاهرة، مصر، 1998.
117) يونس عرب، موسوعة القانون وتقنية المعلومات والخصوصية، الجزء الثاني، الخصوصية وحماية البيانات في العصر الرقمي، إتحاد المصارف العربية، الطبعة الأولى 2002.

الرسائل العلمية

أطروحات الدكتوراه:

1) بشاتن صفية، الحماية الجزائية للحياة الخاصة دراسة مقارنة، رسالة لنيل شهادة دكتوراه علوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2012.
2) بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا (الاعلام والإتصال) أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر باتنة، السنة الجامعية 2015/2014.
3) حامد راشد، الحماية الجنائية للحق في حرمة السكن، دراسة مقارنة، رسالة دكتوراه كليه الحقوق جامعة القاهرة 1987.
4) حبيبة سيف سالم الراشدي، النظام القانوني لحماية جسم الانسان، رسالة لنيل درجة الدكتوراه، كلية الحقوق جامعة عين شمس، قسم القانون المدني، سنة 2005.
5) حسن علي حسن السمني، شرعية الأدلة المستمدة من الوسائل العلمية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة 1983.
6) حليمي ربيعة، الغير في العقد-دراسة في القانون المدني وبعض القوانين الخاصة- أطروحة دكتوراه علوم في الحقوق، قسم القانون الخاص، كلية الحقوق، جامعة الجزائر، 2016-2017.

7) خرشي إلهام السلطات الإدارية المستقلة في ظل الدولة الضابطة، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون العام، كلية الحقوق والعلوم السياسية جامعة سطيف 2 2015/2014.

8) رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2017-2018.

9) رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم، تخصص جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس،2017.

10) شيبوتي راضية، الهيئات الإدارية المستقلة في الجزائر-دراسة مقارنة- رسالة مقدمة لنيل شهادة الدكتوراه علوم في القانون العام، تخصص المؤسسات الإدارية، كلية الحقوق والعلوم الإدارية قسم القانون العام، جامعة الإخوة منتوري قسنطينة، 2014،2015.

11) عبد المجيد كوزي، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، فاس. السنة الجامعية 2014-2015.

12) نبيلة اسماعيل رسلان، النظرية العامة للعلاقات الثلاثية، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 1986.

رسائل الماجيستير:

1) أسامة بن عمر محمد عسيلان، الحماية الجنائية لسر المهنة في الشريعة الإسلامية والقوانين الوضعية وتطبيقاتها في بعض الدول العربية، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، كلية الدراسات العليا- قسم السياسة الجنائية- جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2004.

2) أسامة مصطفى ابراهيم الخضر، العهد الدولي للحقوق المدنية والسياسية، دراسة مقارنة، رسالة ماجيستير مقدمة إلى كلية الدراسات الفقهية والقانونية في جامعة آل البيت الأردن 1997.

3) أمنار إبراهيم، الحماية الجنائية للمعطيات ذات الطابع الشخصي على ضوء القانون المغربي والقانون المقارن، رسالة لنيل دبلوم الدراسات العليا المعمقة، جامعة الحسن الأول، منشورة في مجلة القانون والأعمال، عبر الموقع الالكتروني www.droitetentreprise.org .

4) بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، (دراسة مقارنة) رسالة مقدمة لاستكمال متطلبات الحصول على شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2017.

5) بومدان عبد القادر، المسؤولية الجزائية للطبيب عن إفشاء السر المهني، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة مولود معمري تيزي وزو الجزائر، السنة الجامعية 2010-2011.

6) الحاسي مريم، إلتزام البنك بالمحافظة على السر المهني، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان،2012.

7) خالد بن محمد عبد الله الشهري، رضا المجني عليه وأثره على المسؤولية الجنائية –دراسة مقارنة بين الشريعة والقانون مع التطبيق بين أحكام القضاء الشرعي والوضعي، مذكرة لنيل شهادة ماجيستار، قسم العدالة الجنائية، معهد الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السنة الجامعية 2000-2001.

8) دحماني سمير، التوثيق في المعاملات الإلكترونية، دراسة مقارنة، مذكرة لشهادة ماجيستير كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2017.

9) رافع خضر صالح، الحق في الحياة الخاصة وضماناته في مواجهات استخدامات الكومبيوتر، رسالة ماجستير جامعة بغداد 1993.

10) سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، مذكرة لنيل شهادة الماجيستار، جامعة نايف العربية للعلوم الأمنية السعودية، كلية الدراسات العليا، قسم العدالة الجنائية، 2005.

11) طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الأنترنت، دراسة مقارنة مذكرة ماجستير، قانون جنائي، كلية الحقوق جامعة بسكرة 2007/2006.

12) عنان داود، التزام الطبيب بالحفاظ على السر الطبي، رسالة لنيل شهادة الماجتسر، كلية الحقوق، بن عكنون جامعة الجزائر، 2000-2001.

13) محمد رشيد حامد أبو حجيلة، الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار البنوك المعلومات، دراسة مقارنة، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة الماجستير، كلية الدراسات الفقهية والقانونية، قسم الدراسات القانونية، جامعة آل البيت الأردن 2007.

14) منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلومات السعودي، دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في العدالة الجنائية، الرياض، جامعة نايف العربية للعلوم الأمنية، 2010.

15) مها شبانة أحمد، تأثير توظيف الإعلام الجديد على الجوانب الإدارية في المؤسسات الصحفية، رسالة ماجستير، جامعة المنوفية كلية الآداب، 2016.

16) نبيل فزيع فرج، الحماية الجنائية للحق في الصورة في القانون المصري، رسالة للحصول على درجة ماجستير في الحقوق، جامعة القاهرة، الدراسات العليا 2015-2016.

17) نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي 2012-2013، كلية الحقوق جامعة باتنة.

18) حسن الحافظي، الحماية القانونية للمعطيات ذات الطابع الشخصي بين التشريع الوطني والإتفاقيات الدولية مذكرة ماستر القانون الجنائي والتعاون الجنائي الدولي، كلية العلوم القانونية والاقتصادية والاجتماعية. جامعة مولاي اسماعيل 2017 2018.

المراجع باللغة الفرنسية:

Textes de lois :

1) DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002
2) Directive 97/66/CE du parlement européen et du conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications. Journal officiel n° L024 du 30/01/1998
3) Directive 95/46/CE du parlement européen et de conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Journal officiel n° L281 du 31/11/1995.
4) Directive (UE) 2016/680 du parlement européen et du conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du conseil, journal officiel de l'union européen L119/89.
5) Directive 2000/31/CE du parlement Européen et de conseil du 08 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique) journal officiel des communautés européennes L178/1 du 17/07/2000.
6) Résolution du Parlement européen sur les compétences exécutives de la Commission (comitologie) et le rôle de la Commission dans les relations extérieures de la Communauté (13 décembre 1990) (JOCE). 28.01.1991,
7) RÈGLEMENT (UE) 2018/1725 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE Journal officiel de l'Union européenne L 295/39.
8) Règlement (CE) n°45/2001 du parlement européen et du conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions organes communautaires et à la libre circulation de ces données.
9) Règlement (CE) n°2016/679 du parlement européen et du conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant le dirictives 95/46/CE (règlement général sur la protection des données).

10) Recommandation n° R (87) 15 du comité des ministre aux états membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée par le comité des ministres le 17 septembre 1987 lors de la 410ème réunion des délégués des ministres.
11) Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française.
12) Loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain.
13) LOI no 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes
14) la loi n 91-1382 du 2 décembre 1991 relative a la sécurité des chèques et cartes de paiement, JORF n1 du 1janvier 1992
15) Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications Jorf n° 162 du 13 juillet 1991.
16) Loi n°70-643 du 17 juillet 1970 TENDANT A RENFORCER LA GARANTIE DES DROITS INDIVIDUELS DES CITOYENS JORF du 19 juillet 1970
17) LOI n° 2002-304 du 4 mars 2002 relative au nom de famille JORF du 5 mars2002.
18) Loi n2004/575 du 21 juin 2004, pour la confiance dans l'économie numérique JORGE n 143 du 22 juin
19) LOI no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978
20) Décret n°95-240 du 3 mars 1995 pris pour l'application de la loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française
21) Décret n° 95/682 du 09 mai 1995 modifié le décret n° 78/78 du 17 juillet 1978. Relatif à la recherche sur la santé publique.
22) Décret n° 2005/1309 du 20 octobre 2005 pris pour l'application de la loi n° 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés JORF n° 247 du 22 octobre 2005.
23) Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne JORF n°0050 du 1 mars 2011

Ouvrages et revue

1) Malaurie Philippe et Laurent Aynés, Droit des personnes La protection des mineurs et des majeurs L.G.D.J 10e édition 08/2018.
2) Antoine latreille, La protection juridique des bases de données éléctronique. Petites affiches n 51 du 28 avril 1995 disponible sur le site : http://www.labase.lextenso.fr/revue.
A. Michael Froomkin, The death of privacy. Stanford law review; vol 52 may 2000. http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf
3) Alain Marc Benssoussan, internet, aspects juridiques. Hermés. 2e édition 1998.
4) Alessandro Mantelero, intelligence artificielle et protection des données : enjeux et solutions possibles, direction générale droits de l'homme et état de droit, conseil de l'europe, T-PD (2018) 09 Rev disponible sur le site : http://www.rm.coe.int/intelligence-artificielle

5) André LUCAS, Jean DEVEZE et Jean FRAYSSINET, droit de l'informatique et de l'internet presses universitaires de France, économies, paris 2001.
6) André Lucas, Jeans Deveze et Jean Frayssinet, l'informatique et le secret des fichiers, Revue. Admi 1977.
7) Aoun charbel, l'indépendance de l'autorité de régulation des communication électroniques et des postes, ARCEP thèse pour obtenir le doctorat en droit, université de Gergy Pontoise, Paris 2006.
8) Christiane féral – schuhl, cyber droit, le droit à l'épreuve de l'internet, Dalloz dunod, 3eme édition, Janvier 2002.
9) Christophe VERDURE, les hébergeurs de sites web, victimes ou régulateurs de la société de l'information ? publier sur le site : http://droit-technologie.org DCCR,2005 n°68, doctrine.
10) Eric A. Caprioli, le correspondant à la protection des données à caractère personnel : un nouvel arbitre pour l'entreprise, disponible sur le site : http://www.caprioli-avocts.com
11) Eric meillan, les menaces à la sécurité des systèmes d'information la réponse des institution française, Revue internationale de police criminelle. Mai-juin 1991.
12) Etien-GNOAN N'Da brigitte, l'encadrement juridique de la gestion électronique des données médicales, Thèse pour obtenir le grade de docteur en droit, l'Université Lille 2- droit et santé, décembre 2014.
13) Farid Bouguettaya, la protection des données personnelles en droit communautaire, Mémoire master 02 recherche droit européen des droits de l'homme, mémoire FACULTE DE DROIT – IDEDH Université de montpellier1, 2006.
14) Francois Rigaux « la loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel. Rev.cr.dr.int.pr n°7 1980.
15) Gassin Raymond, informatique et liberté, Encyclopédie juridique, Dalloz, répertoire de droit pénal et procédure pénal, tome 3 paris, 2003.
16) George Kellens, Nouvelles fraudes, permanence et évolutions de droit pénal au regard du renouveau de la fraude, Revue internationale de criminologie et de police technique et scientifique, orange officiel de l'association internationale des criminologues de la langue française 1991 n°2.
17) Guy braibant, données personnelles et société de l'information, Rapport au premier ministre sur la transposition en droit français de la directive 95/46 , la documentation française 3 mars 1998, disponible sur le site https://www.vie-publique.fr/sites/default/files/rapport/pdf/984000836.pdf
18) Hala kassem, « l'internaute et son droit à être laissé tranquille » Formation doctorale : Informatique et Droit mémoire D.E.A informatique et droit, Section CNU : Droit privé et sciences criminelles. 71 Sciences de l'information et de la communication. E.R.I.D. Université de Montpellier1 Année, 2003. Disponible sur le site www.droit-tic.com
19) Hubert delzangles, l'indépendance des autorités de régulation sectorielles communications électroniques, énergie et postes, thèse pour obtenir doctorat en droit, école doctorale de droit (E.D école doctorale n.41) université Montesquieu – Bordeaux 4, 2008.
20) Ibrahim Coulibaly, la protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse doctorat université de Grenoble Spécialité : DROIT PRIVE 2011.
21) Irma ARNOUX, les droits de l'être humain sur son corps et les droits de la personnalité, Presse universitaire de Bordeaux. Pessac 2003.

22) Jacques Francillon, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, revue internationale de droit pénale 64eme année 1993.

23) Jacques Ravanas, la protection des personnes contre la réalisation et la publication de leurs images, Revue internationale de droit comparé. Vol. 31 N°1, Janvier-mars 1979.

24) Jacques robert, Jean duffar, droit de Lhomme et libertés fondamentale, Domat droit public Montchrestien textenso edition, 8 eme edition 2009.

25) Jean frayssinet, conditions du droit d'accès et de communication aux données figurant dans les fichiers des services des renseignements généraux, a.j.d.a (Actualité Juridique Droit Administratif), revue Dalloz, 1994.

26) Jean Paul Antona, Philippe Colin, François Lenglart, la responsabilité pénale des cadres et des dirigeants dans le monde des affaires, Dalloz 1996.

27) Jean Pierre Moussy, des autorités de régulation financières et de concurrence, pourquoi, comment, Rapport du C.E.S.F note D EINA information du conseil économique et social n 124 10janvier les éditions des journaux officiels, 2003.

28) Jean pradel, les infractions à l'informatique, revue internationale de droit comparé, vol 42 n°2, Avril – Juin 1990.

29) Jonathon Michael, privacy and human rights: an international and comparative study with special reference to developments in information technology. Dart mouth 1994.

30) Lothar Deitrmann, Social Media Privacy: A Dozen Myths and Facts Stanford Technology, Law Review volume 7 2012.

31) Malabat Valérie, droit pénale spécial, 4ème édition, dalloz, paris, 2009.

32) Marie- Christine Piatti, les libertés individuelles à l'épreuve des nouvelles technologies de l'information, Presses universitaires de Lyon- pul .2001.

33) Meulders-Klein et Marie-Thérèse, Vie privée, vie familiale et droits de l'homme, In : Revue internationale de droit comparé. Vol. 44 N°4, Octobre-décembre 1992. https://www.persee.fr/doc/ridc_0035-3337_1992_num_44_4_4572.

34) Michel Gentot, Les autorités administratives indépendantes, L.G.D.J ,*La* Librairie générale de droit et de jurisprudence (*L*.G.DJ.) 2ème édition, septembre 1994 .

35) Michel montazeau, les enjeux juridiques de l'anonymat sur internet, mémoire master 2, droit du numérique administration entreprise. Université Paris 1- Panthéon-Sorbonne.

36) Myriam Quéméner, Yves Charpenel, cybercriminalité, droit pénal appliqué, collection pratique du droit, Economisa, Septembre 2010.

37) Nathalie MALLET-POUJOL Protection de la vie privée et des données personnelles Pôle Droit de la Communication Université Montpellier I- UMR 5815 LEGAMEDIA Février 2004 disponible sur le site https://eduscol.education.fr/chrgt/guideViePrivee.pdf

38) Naut Pol, Chevallier Jean-Yves. II - Procédure pénale. In: Revue juridique de l'Ouest, 1994- https://www.persee.fr/doc/juro_0990-1027_1994_num_7_3_2168.

39) Nerson Roger, La protection de la vie privée en droit positif français. In: Revue internationale de droit comparé. Vol. 23 N°4, Octobre-décembre 1971.

40) Olivier barrat, Informatique en nuage. Mettez de côté le patriote act. Penchez-vous sur FISAA Article revue « Sécurité & Stratégie 2013. Disponible en ligne à l'adresse http://www.securite-strategie.fr/international-informatique-en.html-

41) Olivier GRAF, La personne morale : un non-professionnel ? THÈSE Pour obtenir le grade de DOCTEUR EN DROIT DE L'UNIVERSITÉ D'AIX-MARSEILLE, Discipline : Droit Privé UNIVERSITÉ D'AIX-MARSEILLE – ÉCOLE DOCTORALE DES SCIENCES JURIDIQUES ET POLITIQUES.

42) Pascal arrigo et Alain Benssoussan, la cyber criminalité vers une régulation internationale de l'internet, la gazette du palais, n°289 du 16 octobre 2001, Disponible sur le site : http://www.labase-lextenso.fr/revue/GPL/2001L289 .

43) Pascal Gourdon ,L'EXCLUSIVISME AMBIVALENT DU DROIT A L'IMAGE. disponible sur le site https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/nzacl-yearbooks/yearbook-5,-1999/Gourden.pdf

44) Pierre Kayser, la protection de la vie privée par le droit, protection du secret de la vie privée, Préface de Henri MAZEAUD, 3 eme édition, Presses Universitaires D aix- Marseille, economica 1995.

45) Pierre trudel, Quel droit et quelle régulation dans le cyberespace ? Centre de recherche en droit public Faculté de droit, Université de Montréal, Revue sociologie et sociétés vol. xxxii.2 Les Presses de l'Université de Montréal. 2000 disponible sur le site https://www.erudit.org/fr/revues/socsoc/2000-v32-n2-socsoc72/001806ar.pdf

46) Rachid Khalloufi, les institutions de régulation en droit Algérien, Revue IDARA, (numéro spécial) n°2, 2004.

47) Raymond Gassin, informatiques et libertés, Répertoire pénal et procédure pénale, Dalloz, Janvier 1987 n°288.

48) Richard montbeyre, le transfert de données bancaires à caractère personnel vers les Etats-Unis : aspects juridiques de l'affaires SWIFT, master2 professionnel droit de l'internet public administration entreprises, université paris 1, Pantheon-Sorbonne février 2008. Site web : http://www.droit-tic.com

49) Roymond lindon, Dictionnaire juridique, Les droits de la personnalité, dalloz. Paris, 2003.

50) Yves mayaud, code penal 14 eme edition, dallaz 2009.

51) Raymond. Lindon, La création prétorienne en matière de droits de la personnalité et son incidence sur la notion de famille. In: Revue internationale de droit comparé. Vol. 27 N°1, Janvier-mars 1975. https://www.persee.fr/doc/ridc.

52) Rachid Zouaimia, les autorités adminstratives indipendentes et la régulation économique, revue Idara n°28, 2004.

المواقع الالكترونية:

1) https://www.persee.fr/doc/ridc_0035-3337_1971_num_23_4_16099.

2) http://www.droit-technologie.org

3) http://cnil.fr

4) http://epic.org/privacy/ social net/

5) http://lawcenter.birzeit.edu/lawcenter/attachments/article/1517/Dalel.pdf.

6) http://www.almajlis.gov.ae

7) http://www.céprisca.fr

8) http://www.doctrine.fr/d/CEDH

9) http://www.hrlibrary.umn.edu

10) http://www.tvtc.gov.sa/arabic/departements/faculty/

11) https://ahmedazimelgamel.blogspot.com/p/blog-page_26.html

12) https://crsreports.congress.gov/product/pdf/R/R45631.

13) https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf

14) https://www.courdecassation.fr/publications_26/bulletin_arrets_chambres_civiles_2711/

15) https://www.village-justice.com/articles/droit-oubli-numerique-juridique,7614.html

فهرس الموضوعات:

شكر وتقدير 2
إهداء 3
LES ABREVIATIONS 4
الفصل الأول :الإطار المفاهيمي للحق في الخصوصية المعلوماتية 12
المبحث الأول :ماهية الحق في الخصوصية: 12
المطلب الأول: مفهوم الحق في الخصوصية 13
الفرع الأول :التعريف الفقهي والقضائي للحق في الخصوصية 14
أولا-التعريف الفقهي للحق في الخصوصية: 14
ثانيا: دور القضاء في تعريف الحق في الخصوصية: 17
الفرع الثاني :موقف التشريعات المقارنة من الحق في الخصوصية 20
أولا :الإتجاه المعارض للاعتراف بالحق في الخصوصية: 20
ثانيا: الاتجاه الذي يعترف بالحق في الخصوصية: 21
الفرع الثالث :موقف المشرع الجزائري من الحق في الخصوصية: 26
الفرع الثالث :موقف الإعلانات العالمية من الحق في الخصوصية: 28
أولا: الاتفـاقيات الـدولية 29
ثانيا: الاتفاقيات الدولية ذات الطابع الإقـليمي 30
ثالثا: دور المؤتمرات الدولية في تعريف الحق في الخصوصية 32
المطلب الثالث: الطبيعة القانونية للحق في الخصوصية 35
الفرع الأول :الحق في الخصوصية من حقوق الملكية: 36
الفرع الثاني :الحق في الخصوصية من حقوق الشخصية 37
المطلب الرابع: نطاق الحق في الخصوصية 39
الفرع الأول: الأشخاص الذين يتمتعون بالحق في الخصوصية 39
أولا :تمتع الشخص الطبيعي بالحق في الخصوصية 39
ثانيا: مدى تمتع الشخص المعنوي بالحق في الخصوصية. 41
ثالثا :مدى انتقال الحق في الخصوصية إلى الورثة 44
الفرع الثاني: نطاق الحق في الخصوصية من حيث المضمون: 47
أولا: عناصر الخصوصية المتعلقة بالكيان المادي للإنسان 49
ثانيا: الكـيان المـعنوي للإنـسان: 54
الفرع الثالث :إتسـاع نطاق الحق في الخصوصية 77
المبحث الثاني: التطور الحديث لمفهوم الحق في الخصوصية 78
المطلب الأول: نشأة فكرة الحق في الخصوصية المعلوماتية 79
الفرع الثاني: الإعتراف التشريعي بالحق في الخصوصية المعلوماتية 83
أولا: دور المنظمات الدولية في حماية الخصوصية في مجال المعلوماتية 92
ثانيا: دور الهيئات الإقليمية في الإعتراف بالحق في الخصوصية المعلوماتية 96

فهرس الموضوعات

المطلب الثاني: مفهوم الخصوصية المعلوماتية.....106
الفرع الأول: تعريف الخصوصية المعلوماتية.....107
الفرع الثاني: طبيعة البيانات الشخصية المتعلقة بالخصوصية المعلوماتية.....110
أولا: تعريف المعطيات ذات الطابع الشخصي.....112
ثانيا :الفرق بين المعلومات والبيانات.....119
الفرع الرابع: أنواع المعطيات ذات الطابع الشخصي.....122
أولا: المعطيات الشخصية العادية.....122
ثانيا: المعطيات الشخصية الحساسة.....124
أولا: الأهمية الاقتصادية للمعطيات ذات الطابع الشخصي.....126
ثانيا: الأهمية الإجتماعية والأمنية للمعطيات ذات الطابع الشخصي.....127
المطلب الثالث: آثار الإعتراف بالخصوصية المعلوماتية.....128
الفرع الأول: أثر الحق في الخصوصية المعلوماتية على الحق في الوصول إلى المعلومات.....128
أولا: المقصود بالحق في الوصول إلى المعلومات.....128
ثانيا: الأساس القانوني للحق في الوصول إلى المعلومات.....129
ثالثا: الحق في الخصوصية المعلوماتية قيد على الحق في الحصول على المعلومات.....133
الفرع الثاني: أثر الحق في الخصوصية المعلوماتية على حق الدولة في الإطلاع.....134
أولا: المقصود بحق الدولة في الإطلاع.....134
ثانيا: حدود حق الدولة في الإطلاع.....135
المبحث الثالث: المخاطر التي تهدد الخصوصية المعلوماتية.....136
المطلب الأول: مخاطر قواعد البيانات على الخصوصية المعلوماتية.....138
الفرع الأول: مفهـوم قـواعد البيانات.....138
أولا: تعريف قواعد البيانات.....139
ثانيا: خصائص قواعـد البيانات.....140
الفرع الثاني: مفهوم المعالجة الآلية للمعطيات ذات الطابع الشخصي.....141
أولا: تعريف نظام المعالجة الآلية للمعطيات.....142
ثانيا: المقصود بمعالجة المعطيات ذات الطابع الشخصي.....143
أولا: المخاطر التي تهدد المعطيات الشخصية خلال عملية التجميع.....147
ثانيا: المخاطر التي تهدد المعطيات الشخصية خلال عملية التخزين.....150
ثالثا: المخاطر التي تهدد المعطيات الشخصية خلال عملية المعالجة.....152
رابعا: المخاطر التي تهدد الخصوصية المعلوماتية عند عملية إيصال المعلومات.....154
المطلب الثاني: مخاطر الأنترنت على الخصوصية المعلوماتية.....156
أولا مفهوم الانترنت.....157
أولا: أهـم استخدامات شبكة الانترنت:.....161
ثانيا: مخاطر فضاء الانترنت على المعطيات ذات الطابع الشخصي.....164
المطلب الثالث: مخاطر وسائل التواصل الاجتماعي على الخصوصية المعلوماتية.....173

فهرس الموضوعات

أولا: مفهوم مواقع التواصل الاجتماعي.....175
أولا :تداول البيانات الشخصية على مواقع التواصل الاجتماعي وأثره على الخصوصية المعلوماتية:.....177
ثانيا: أهم المخاطر التي تشكلها مواقع التواصل الإجتماعي على الخصوصية المعلوماتية:.....179
ملخص الفصل الأول:.....183
الفصل الثاني.....186
القواعد القانونية لحماية الخصوصية المعلوماتية.....186
الفصل الثاني: القواعد القانونية لحماية الخصوصية المعلوماتية:.....187
المبحث الأول: الضوابط القانونية الموضوعية لمعالجة المعطيات ذات الطابع الشخصي:.....188
المطلب الأول: مبادئ معالجة البيانات ذات الطابع الشخصي.....188
الفرع الأول: مبدأ مشروعية المعالجة الآلية للمعطيات الشخصية:.....189
أولا: مشروعية معالجة المعطيات الشخصية:.....189
ثانيا: مشروعية الهدف المعلن من معالجة المعطيات الشخصية.....193
الفرع الثاني: مبدأ الموافقة المسبقة للمعني بالمعالجة:.....196
أولا: المقصود برضا المعني بالمعالجة:.....196
ثانيا :أثر الرضا المسبق على صحة معالجة المعطيات الشخصية 199
المطلب الثاني :حقوق الشخص المعني بالمعالجة:.....207
الفرع الاول: الحقوق المتعلقة بالإعلام والولوج.....207
أولا: الحـق في الإعـلام (الإخبار droit d'information).....207
ثانيا :الحق في الولوج:droit d'acces 212
أولا :الحق في التصحيحdroit de rectification 218
ثانيا :الحق في الإعتـراضdroit doppsition : 223
ثالثا :حق منع الإستكشاف المباشر Interdiction de la prospection directe :.....225
المبحث الثاني: الضوابط القانونية الإجرائية لحماية المعطيات ذات الطابع الشخصي.....227
المطلب الأول :إحترام الإجراءات المسبقة على معالجة المعطيات ذات الطابع الشخصي:.....228
الفرع الأول: التصريح المسبق:.....228
الفرع الثاني: الترخيص المسبق من طرف السلطة الوطنية لحماية المعطيات الشخصية.....233
أولا :معالجة المعطيات الحساسة.....233
ثانيا :الربط البيني لملفات إلكترونية.....235
ثالثا:حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية.....236
المطلب الثاني :إلتزامات المسؤول عن المعالجة.....238
الفرع الأول: التدابير التقنية لضمان سلامة وسرية المعطيات ذات الطابع الشخصي.....240
أولا: أهداف البرامج التقنية الحمائية 241
ثانيا: أهم أنواع البرامج التقنية الحمائية للبيانات الشخصية.....243
الفرع الثاني :التدابير التنظيمية لحماية البيانات الشخصية.....252
أولا :التنظـيم الـذاتي:.....252

ثانيا :عقود سياسة الخصوصية.....255
الفرع الثالث: الإلتزام القانوني بالسر المهني لضمان سرية البيانات الشخصية.....260
أولا: مفهوم مبدأ الإلتزام بالسر المهني.....260
ثانيا: موقف المشرع الجزائري من الإلتزام بالسر المهني في إطار حماية المعطيات الشخصية.....267
أولا: الطبيعة القانونية لخدمات الأنترنت وصفة مقدميها:.....274
أولا: تحديد التزامات الوسيط الفني في تقديم خدمة الأنترنت:.....282
ثانيا :أساس مسؤولية الوسيط الفني في تقديم خدمات الأنترنت:.....290
ملخص الفصل الثاني.....293
الفصل الثالث.....296
آليات الحماية القانونية للحق في الخصوصية المعلوماتية.....296
الفصل الثالث :آليات الحماية القانونية للحق في الخصوصية المعلوماتية:.....297
المبحث الأول: الحماية الإدارية للحق في الخصوصية المعلوماتية.....297
المطلب الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:.....298
الفرع الأول: الطبيعة القانونية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:.....299
أولا :النظام القانوني للسلطة الوطنية ذات الطابع الشخصي:.....299
ثانيا: خصائص السلطة الوطنية لحماية المعطيات الشخصية:.....303
الفرع الثاني: صلاحيات السلطة الوطنية لحماية المعطيات الشخصية.....315
أولا: مهام السلطة الوطنية لحماية المعطيات الشخصية في الإشراف والرقابة السابقة:.....315
ثانيا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في الإشراف والرقابة اللاحقة:.....318
الفرع الثالث: هيئات حماية المعطيات الشخصية في القوانين المقارنة:.....323
أولا: على مستوى الإتحاد الأوروبي:.....323
ثانيا: على مستوى التشريع الفرنسي:.....333
المبحث الثاني: الحماية الجزائية الموضوعية للحق في الخصوصية المعلوماتية:.....335
المطلب الأول: الجرائم الماسة بالحق في الخصوصية المعلوماتية في إطار القانون 07/18.....338
الفرع الأول: الجرائم الماسة بالقواعد الموضوعية لمعالجة المعطيات الشخصية.....339
أولا: الجرائم الماسة بالمعطيات الشخصية ذاتها:.....339
1) الجرائم المرتبطة بالمعالجة غير المشروعة :يدخل ضمن هذه الفئة من الجرائم:.....339
2) الجرائم المرتبطة بخرق أحكام المادة 02 من القانون 07/18:.....357
3) الجرائم المرتبطة بصاحب المعطيات الشخصية:.....360
الفرع الثاني :الجرائم المرتبطة بمخالفة القواعدالإجر ائية.....371
أولا :الجرائم المرتبطة بالإجراءات المسبقة للمعالجة:.....371
1) معالجة المعطيات الشخصية دون تصريح مسبق أو ترخيص:.....371
2) جريمة الإستمرار في معالجة المعطيات رغم سحب وصل التصريح أو الترخيص:.....375
ثانيا :الجرائم المرتبطة بإجراءات الحماية والتعاون مع السلطة الوطنية:.....378
1)جريمة عدم اتخاذ التدابير التنظيمية والتقنية اللازمة لسلامة المعطيات الشخصية.....379

فهرس الموضوعات

2)جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية:.....382
3)جريمة عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية:.....383
4)جريمة الولوج إلى السجل الوطني:.....385
المطلب الثاني: الجرائم الماسة بالمعطيات الشخصية خارج إطار قانون 07/18:.....386
الفرع الأول: جرائم الإعتداء على المعطيات الشخصية في قانون العقوبات:.....388
أولا :جرائم الإعتداء على معطيات شخصية صحيحة داخل نظام المعالجة الآلية:.....388
1)جريمة إتلاف المعطيات الشخصية:.....389
2)جريمة التلاعب بالمعطيات الشخصية:.....395
ثانيا: جريمة التعامل في المعطيات الشخصية غير صحيحة.....400
1)جريمة التعامل في معطيات شخصية صالحة لارتكاب جريمة:.....401
2)جريمة التعامل في معطيات شخصية متحصلة من جريمة:.....405
الفرع الثاني: جرائم الاعتداء على المعطيات الشخصية في قانوني التوقيع الإلكتروني والتجارة الإلكترونية:
.....407
أولا: مفهوم التوقيع الإلكتروني:.....408
1)تعريف التوقيع الإلكتروني:.....408
2)صور التوقيع الإلكتروني:.....410
ثانيا: الجرائم الماسة بالمعطيات ذات الطابع الشخصي في قانون التوقيع الإلكتروني 04/15:.....411
1)الجرائم الماسة بالمعطيات الشخصية قبل إنشاء شهادة التصديق الإلكتروني.....411
2)الجرائم الماسة بالمعطيات الشخصية بعد إنشاء شهادة التصديق:.....413
ثالثا: جرائم الإعتداء على المعطيات الشخصية في قانون التجارة الإلكترونية.....417
الفرع الثالث: أحكام خاصة للمسؤولية الجزائية عن الجرائم الماسة بالمعطيات الشخصية.....420
أولا: أحكام المعاقبة على الشروع في جرائم المساس بالمعطيات ذات الطابع الشخصي.....420
ثانيا: أحكام المسؤولية الجزائية للشخص المعنوي عن جرائم المساس بالمعطيات الشخصية:.....425
المبحث الثالث: الحماية الجزائية الإجرائية للمعطيات ذات الطابع الشخصي وقواعد الاختصاص القضائي: 429
المطلب الأول: طرق إثبات الجرائم الماسة بالمعطيات ذات الطابع الشخصي:.....430
الفرع الأول: الدليل المناسب لإثبات جرائم الإعتداء على معالجة المعطيات الشخصية:.....430
أولا: تعريف الدليل الإلكتروني:.....431
ثانيا: خصائص الدليل الإلكتروني:.....433
ثالثا: أنواع الدليل الرقمي:.....435
رابعا: صعوبة الإثبات في جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:.....436
الفرع الثاني: إجراءات الحصول على الدليل الرقمي لإثبات جرائم الإعتداء على المعطيات الشخصية
المعالجة آليا.....437
أولا: الجهات المكلفة بالبحث والتحري عن جرائم الإعتداء على المعطيات الشخصية:.....438
ثانيا: القواعد الإجرائية في استخلاص الدليل الرقمي:.....447
أولا: مشروعية وجود الدليل الرقمي:.....456

ثانيا: مشروعية الحصول على الدليل الرقمي:.....459
أولا: شروط اكتساب الدليل الرقمي للحجية في إثبات جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:.....461
ثانيا: سلطة القاضي الجزائي في تقدير الدليل الرقمي:.....463
المطلب الثالث: قواعد الاختصاص في جرائم الإعتداء على المعطيات الشخصية المعالجة آليا:.....464
أولا: مبدأ الشخصية في إقامة الاختصاص القضائي الجزائي:.....469
ثانيا: مبدأ العينة في إقامة الاختصاص القضائي الجزائي:.....471
ثالثا: مبدأ عالمية النص الجزائي في إقامة الاختصاص القضائي:.....473
ملخص الفصل الثالث.....475

ملخص

لقد أصبح التقدم العلمي والتقني الهائل الذي أدى إلى تطور العقول الإلكترونية يضع تحت تصرف الدولة وأجهزتها الأمنية والهيئات العامة والخاصة حجما كبيرا من المعطيات الشخصية المتعلقة بالأفراد، تعجز الوسائل العادية والأساليب التقليدية من الوصول إليها، ومن ثم بات من السهل الحصول على هذه المعطيات المخزنة في أجهزة الكومبيوتر في ثوان وبالطريقة المطلوبة للاستعمال في أي مكان من العالم بشكل لم يكن متاحا من قبل.

ولما بدأت الأنظمة المعلوماتية الضخمة التي تملكها الدولة والمؤسسات تتطور، أصبح يخشى من الإستعمال التعسفي للبيانات المعلوماتية ذات الطابع الشخصي المخزنة في الملفات الإلكترونية والذي يشكل بدوره خطرا على الحق في الخصوصية للأشخاص الطبيعيين.

وهذا ما يدعونا إلى القول بأن الحواسيب الإلكترونية وإن كانت أحد المظاهر الفذة للتقدم العلمي التي وفرت على الإنسان جهدا خارقا، وقدمت للبشرية خدمات جليلة، فإنه لا يمكن التغاضي عن مخاطرها الجمة على الحياة الخاصة للإنسان، حيث أصبح ميسورا بواسطتها جمع كل المعلومات الشخصية عن شخص معين مثل هويته، سنه، وضعه العائلي، حالته الصحية، مركزه العائلي أو المالي، وآرائه السياسية وغيرها من المعطيات ذات الطابع الشخصي، واستخدامها لأغراض مختلفة تماما عن الأغراض التي جمعت لأجلها أو جمعها بطرق غير مشروعة ودون علم صاحبها بذلك، وهو الأمر الذي أبرز الكثير من المشكلات التي تهدد الحق في الخصوصية في المجال المعلوماتي.

وإلى جانب بنوك المعلومات فإن التطورات السريعة والثورات التكنولوجية المتلاحقة كان لها آثارها وتداعياتها الهائلة على وسائل الإتصال الإلكتروني سيما شبكات الأنترنت ومواقع التواصل الإجتماعي، وهي الوسائل التي فرضت واقعا جديدا فتح آفاق التواصل والإتصال بين الناس، وبدأ نتيجة لذلك الكثير منهم بوضع بياناته الشخصية عبر مواقع الأنترنت والشبكات الإجتماعية، وهي المعطيات التي يمكن من خلال استقرائها الوصول إلى مؤشرات معلوماتية هائلة عن الشخص صاحب هذه المعطيات

وبالتالي بدت الحاجة ماسة إلى صياغة نصوص قانونية لوضع وتكريس المبادئ الأساسية لحماية الخصوصية المعلوماتية من خلال التنبيه إلى ضرورة الإلتزام بالاستقامة في جمع البيانات الشخصية، التصريح عن غايات معالجتها، ملائمة البيانات الشخصية المجمعة لغاية المعالجة وكذا إعطاء أصحاب هذه المعطيات بصفتهم معنيين بالمعالجة مجموعة من الحقوق المرتبطة ارتباطا وثيقا بجوهر الحق في الخصوصية.

وقدكان المشرع الجزائري واحدا من هذه التشريعات عندما تدخل بتعديل دستوري سنة 2016 بموجب القانون 01/16 المؤرخ في 2016/03/06 في المادة 16 الفقرة الأخيرة التي أشارت في نصها "على أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه". ثم استحدث القانون 07/18 المؤرخ في10يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخصي

Abstract

The tremendous scientific and technical progress that led to the development of electronic minds has placed at the disposal of the state and its security services and public and private bodies a large volume of personal data related to individuals, the regular means and traditional methods are unable to reach them, and then it is easy to obtain these data stored in computers In seconds and in the manner required to use anywhere in the world in a way that was not available before.

And when the huge information systems owned by the state and institutions began to develop, he became afraid of the arbitrary use of information data of a personal nature stored in electronic files, which in turn constitutes a threat to the right to privacy of natural persons.

This is what calls us to say that electronic computers, even if it is one of the unique manifestations of scientific progress that have provided an extraordinary effort for man, and provided humankind with great services, it is not possible to overlook the great dangers to the private life of the person, as it became easy through which to collect all personal information about a particular person Such as his identity, age, marital status, health status, family or financial status, political opinions and other data of a personal nature, and their use for purposes that are completely different from the purposes for which they were collected or illegally collected without the owner's knowledge of it.

Which highlighted many of the problems that threaten the right to privacy in the information field. In addition to information banks, the rapid developments and successive technological revolutions have had tremendous effects and repercussions on electronic means of communication, especially the Internet and social networking sites, which are the means that imposed a new reality opening the horizons of communication and communication between people, and as a result many of them started to put their personal data through the Internet And social networks, which are data that can be used by extrapolating them to reach huge informational indicators about the person who has these data

Consequently, there was an urgent need to formulate legal texts to develop and devote the basic principles of protecting information privacy by alerting to the necessity of a commitment to integrity in the collection of personal data, declaring the purposes of processing it, the suitability of personal data collected for processing, as well as giving the owners of these data as concerned with processing a set of related rights Closely related to the essence of the right to privacy.

The Algerian legislator was one of these legislations when it entered into a constitutional amendment in 2016 according to Law 01/16 of 06/03/2016 in Article 16 the last paragraph which stated in its text that "the protection of natural persons in the field of processing data of a personal nature is a fundamental right It is guaranteed by law and punished for its violation. " Then he introduced Law 18/07 of June 10, 2018 related to the protection of natural persons towards the treatment of data of a personal nature.