جامعة باتنة1- الحاج لخضر
كلية الحقوق والعلوم السياسية
قســـم الحقـــوق

الحماية الجزائية للأمن الشخصي المعلوماتي

مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق
التخصص: قانون جنائي وعلوم جنائية

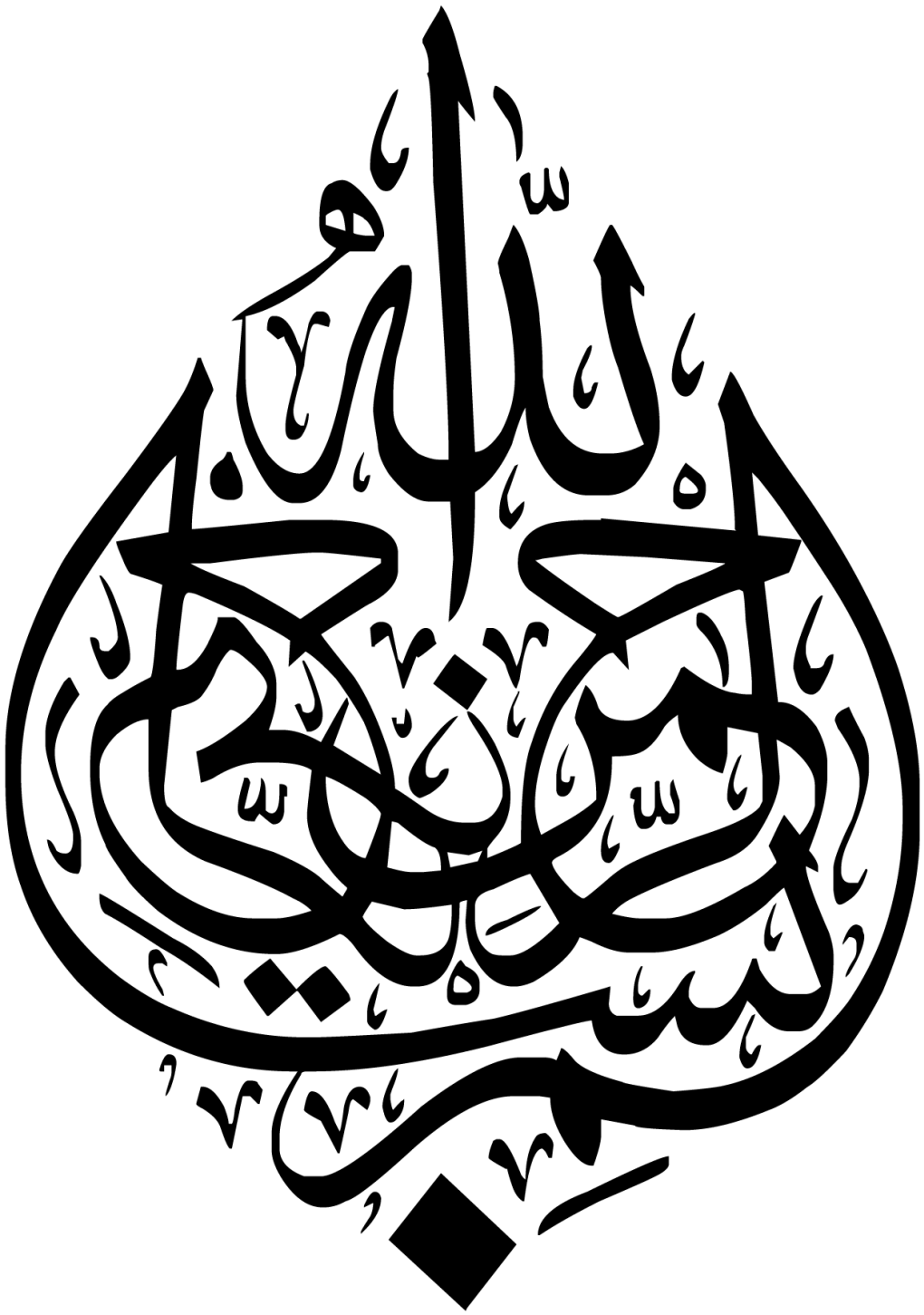
إعـــداد الطـــالبتين:
غبـــغوب نسرين
مـــــزوز هديـــل

إشراف الأستاذة الدكتورة:
بـن بوعبـــد الله وردة

لجنـــــة المنـــــاقشة:

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
دريـــــدي وفـــــاء	أستاذ التعليم العالي	جامعة باتنة1	رئيسا
بن بوعبـد الله وردة	أستاذ التعليم العالي	جامعة باتنة1	مشرفا ومقررا
بن دعـــــاس لميـــاء	أستاذ محاضـــــر- أ	جامعة باتنة1	مناقشا

دورة جوان
السنة الجامعية: **2023-2024**



إهـــداء

الحمد لله الذي بفضله تتم الصالحات، وما توفيقنا إلا بالله.

من القلب إلى القلب

الى كل من تمنى لي النجاح والتوفيق يوما شكركم واجب مني، فشكرا لكل من ساندني في رحلتي التعليمية.

إلى الرجل الأول في حياتي والدي العزيز رحمة الله عليه "غبغوب عبد العالي المدعو "جمال "، أهديه هذه المذكرة بكل حب الذي لطالما تمنى رؤيتي حاملة للشهادة الماستر، وها هي الآن قد اينعت شكرا لك لأنك علمتني حب التطلع

وكان يدعمني دائما بالمعلومات والنقاشات الثرية والبناءة، ولن أنسى أبدا الجهد الذي بذله من أجلي كنت ولازلت مصدر قوتي وإلهامي.

إلى "أمي صديقتي الغالية" التي بفضل مساندتها لي طوال مسيرتي التعليمية، وبفضل دعائها وصلت لما أنا عليه، اهديك هذه المذكرة عرفانا لك بالتضحيات التي قدمتها لأجلي، وأتمنى أن تكون راضية علي وأن تكون فخورة بي.

إلى كل الأساتذة الذين وقفوا بجانبي كل باسمه ومركزه شكرا كثيرا للتوجيهاتكم الدكتورة:

مناني فرح، الدكتور: جداي علي، الكوتش والدكتورة: ميرهان فرج.

إلى كل من سيقرأ المذكرة أتنمى منكم الدعاء لأبي بالرحمة الواسعة.

غبـــــــغوب نســـــــرين

إهـــداء

استمرارية السعي تعني حتمية الوصول
أهدي ثمرة جهدي وفرحتي إلى أمي وأبي حفظهم الله ورعاهم، وإلى كل أفراد عائلتي واحبتي جميعا، كما
أشكر كل من دعمني في مسيرتي الدراسية، وترك بصمة إيجابية لتحفيزي.

هديـــــل مـــزوز

شكر وتقدير

نخص بأسمى عبارات التقدير والعرفان والشكر الجزيل لأستاذتنا الفاضلة والراقية
الأستاذة الدكتورة: "وردة بن بوعبد الله"
التي كانت لنا خير سند لتوجيهنا بإرشاداتها والاشراف على هذا العمل،
ما شكل إضافة كبيرة للعمل البحثي، فكلمات الثناء لا توفيك حقك،
شكرا على عطائك المستمر إلى آخر لحظة وتعاملك الراقي،
وأسأل الله أن يجازيك خير الجزاء.
كما نخص بأسمى عبارات التقدير والاحترام إلى السادة أعضاء لجنة المناقشة كل باسمه ومركزه،
الدكتورة: بن دعاس لمياء والأستاذة الدكتورة: دريدي وفاء،
على تفضلهم لمناقشة هذه المذكرة.

قائمة المختصرات

ق.ع : قانون العقوبات.

ق.إ.ج: قانون الإجراءات الجزائية.

ج.ر: الجريدة الرسمية.

ط: الطبعة

CNIL : Commission National de l'informatique et de Liberté.

ANPDP : Autorité National de Protection Des Caractère Personnel.

مقدمـــة

تعتبر الخصوصية من الحقوق اللازمة للشخص الطبيعي بصفته الإنسانية، ومظهر من مظاهر حق الإنسان في احترام حياته وشخصه، نصت على هذا الحق أغلب الدساتير الوطنية والنظم القانونية، وكذا الاتفاقيات الدولية كالإعلان العالمي للحقوق الإنسان، والذي يشكل إطار قويا وشاملا لتعزيز وحماية الحق في الخصوصية، وهو نفس ما تضمنته الاتفاقية الأوروبية لحماية البيانات، بالإضافة إلى العديد من القواعد التشريعية للاتحاد الأوروبي، وكل الدول الأعضاء في هذه المنظمات التي تبنت مبادئ قانونية تخص حماية الحق في الخصوصية من مخاطر المعالجة الآلية للبيانات.

في ظل التطورات التكنولوجية والتقنية السريعة في شتى مجالات الحياة، وما صاحبه من استخدام متزايد للأنظمة التكنولوجية أدى الى الكثير من المشاكل والمخاطر وبالرغم من أن التحول الرقمي سهل علينا الوصول والحصول على البيانات، إلا أنه جعل خصوصيتنا وأمننا أكثر عرضة للخطر، مما قد يؤدي إلى إساءة استخدامها حيث أصبحت حماية الخصوصية والبيانات الشخصية مصدر قلق كبير لمجتمعاتنا الحديثة، نظرا للاعتداءات الإجرامية التي تستهدف المساس بحقوق وحريات الأخرين ويتخذ المساس بهذه الحقوق احد الاشكال التي نذكر منها قيام الجاني بالاستحواذ على المعلومات أو صور شخصية ومن خلال هذا القلق نشأت الحاجة إلى ضرورة حماية البيانات الشخصية.

لهذا الموضوع **أهمية عملية وعلمية** كبيرة حيث أنه مرتبط بتطبيق الإجراءات الجزائية للحفاظ على الامن الشخصي المعلوماتي، حيث تتمثل **الأهمية العملية** في تبني المشرع الجزائري آليات لحماية حق الشخص في أمن معلوماته، وذلك من خلال إدارة مخاطر معالجة البيانات الشخصية بشكل بناء وتفعيل الضوابط الضرورية وتعزيز الالتزام بمعايير نظام حماية البيانات الشخصية مما يعزز ثقة الأفراد في الجهات المعنية، فيما تتمثل **الأهمية العلمية** فقد شهدت الحماية الجزائية للبيانات الشخصية تطورا في مجالها، باعتبارها مجموعة من الوسائل القانونية التي تنفذها الدولة من أجل ضمان أمن وسلامة البيانات، وذلك من خلال حماية الأشخاص من صور الاعتداء التي تطال حياتهم الشخصية، ولسن التدابير القمعية من أجل معاقبة أي شخص يقوم بالتعدي على البيانات الشخصية.

نسعى من خلال هذه الدراسة لموضوع الحماية الجزائية للأمن الشخصي المعلوماتي تحقيق **الأهداف التالية:**

- ✓ تسليط الضوء على اهم المبادئ والتدابير التقنية والتنظيمية لحماية البيانات الشخصية.
- ✓ الإحاطة بأهم صور الاعتداءات التي تستهدف الحياة الشخصية المعلوماتية.
- ✓ تبيان تقنيات وإجراءات ذو كفاءة بما يتلاءم مع البيئة الرقمية، للوقاية قبل الاعتداء على الأمن الشخصي المعلوماتي للشخص، وللمتابعة مرتكبي جرائم المساس بالأمن الشخصي المعلوماتي وتحقيق الحماية الفعالة.
- ✓ توضيح مسار السياسة الاجرائية والمؤسساتية، التي تبنتها الدولة الجزائرية بشأن حماية بيانات مواطنيها والتصدي لمثل هذا البعد الجديد من الإجرام.

لقد دفعنا إلى اختيار موضوع الحماية الجزائية للأمن الشخصي المعلوماتي عدة **أسباب** منها الذاتية والموضوعية.

الأسباب الموضوعية: تتمثل في:

- ✓ الصلة الوثيقة بين هذه الجرائم والتطور التقني.
- ✓ الاعتداءات والمخاطر التي تطال الحياة الشخصية المعلوماتية.
- ✓ من المواضيع الرائجة على أكبر مواقع البحث مثل SCIVAL.
- ✓ كون الموضوع مهم جدا الا انه لا يوجد دراسات ميدانية وتوعوية بشأن الخصوصية المعلوماتية.

الأسباب الذاتية: تتمثل في:

- ✓ الرغبة والميل والشغف بدراسة كل ما يتعلق بالرقمنة المعلوماتية.
- ✓ للتميز الموضوع بالصياغة الجيدة التي تتسم بالوضوح والشمول والتشويق إضافة الى الحداثة.
- ✓ التساؤلات العديدة التي تطرأ في ذهني وفي ذهن أي شخص بخصوص الموضوع.
- ✓ للزيادة احتمالية قبوله للنشر في الدوريات العلمية.

- ✓ لاكتســـاب قدر من الثقافة العامة بخصـــوص مجال أمن المعلومات وكيفية حماية البيانات الشخصية.

لمواجهة مختلف الهجمات التي يتم على إثرها الاســـتحواذ على المعطيات الرقمية ولاسيما الحساسة منها التابعة للأشخاص أو المؤسسات يستدعى الأمر اتخاذ الإجراءات اللازمة لتعزيز أمن نظام المعلومات، ما يطرح **الإشكالية التالية**:

ما هي الاستراتيجية الوطنية التي اتبعها المشرع الجزائري في سبيل مواجهة الاعتداء على الأمن الشخصي المعلوماتي؟

ويتفرع عن هذه الاشكالية التساؤلات الفرعية التالية:

- فيما تتمثل تقنيات الحماية من أنشطة الاعتداء على الحياة الشخصية في البيئة الرقمية؟
- ماهي أهم القوانين الجزائرية التي تحمي البيانات الشخصية للأفراد من الاستعمال والاستغلال الغير قانوني؟
- هل الجهات المكلفة بالتحقيق تتلاءم مع طبيعة هذا النوع من الاجرام؟
- هل الآليات المؤسساتية الموجودة حاليا كافية للحماية ومطبقة فعليا ام مجرد حبر على ورق؟

تم الاعتماد على **المنهج الوصـــفي بآلية التحليل**، المنهج الوصـــفي من خلال تعداد صـــور الاعتداءات التي تطال خصـــوصـــية الأشـــخاص المعلوماتية والتطرق إلى الآليات القانونية التي تساهم في الحد من هذا النوع من الإجرام، واستخدام آلية التحليل لازمة لتحليل النصـوص القانونية واسـتنتاج موقف المشـرع الجزائري لرسـم سـياسـته في مواجهة المسـاس بالأمن الرقمي المعلوماتي.

إن موضـوع الحماية الجزائية للأمن الشـخصـي المعلوماتي من المواضـيع التي تتسـم بالحداثة، إذ تنحصر في بعض اطروحات الدكتوراه التي نذكر منها:

– رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، قانون خاص، جامعة أبو بكر بلقايد تلمسان، 2017–2018.

حيث اعتمدت في دراســـتها على بابين الباب الأول الذي يتمحور حول الأحكام العامة للأسـرار المعلوماتية أما الباب الثاني الذي يتمثل في الجرائم الواقعة على السـرية المعلوماتية

في إطار القانون حيث ركزت في دراستها على جهاز الكومبيوتر لارتباطه بالشبكة العنكبوتية أما بخصـــوص الجانب الذي تطرقنا له خلال دراســتنا حرمة الحياة الشــخصــية في مجال المعلوماتية.

– راضـية زرقيني، الحماية الجزائية للمعطيات الشـخصـية، أطروحة دكتوراه، تخصـص قانون عام، الوادي، الجزائر، جامعة الشهيد حمه لخضر، السنة 2021–2022.

حيث قســمت دراســتها إلى بابين الباب الأول يتمثل في الأحكام الموضــوعية للحماية الجزائية للمعطيات ذات الطابع الشــخصــي أما الباب الثاني يتمحور حول الأحكام الإجرائية للحماية الجزائية للمعطيات الشـخصـية في حين لم يتطرق للجانب العملي أما خلال دراسـتنا ركزنا على الجانب الموضـــوعي من خلال التدابير الوقائية والردعية أما من ناحية الجانب العملي من خلال الأليات الإجرائية والمؤسساتية.

من **<u>الصعوبات</u>** التي واجهتنا في اعداد هذه المذكرة:

- ✓ الوقت الذي شكل أكبر عائق امامي بسبب عملي كموظفة في الإدارة.
- ✓ عدم وجود دراســات ميدانية للتخصــص الحقوق مع أنه تخصــص حيوي وتطبيقي أكثر من نظري، إضـــافة إلى أنه الموضـــوع يجب ان يكون فيه دراســـات ميدانية للحداثته وللأهمية البالغة.

لقد تم **<u>تقســيم الدراســة</u>** والموضــوع إلى فصــلين وكل فصــل إلى مبحثين على النحو التالي:

الفصل الأول: الآليات الموضوعية لحماية الحياة الشخصية المعلوماتية.

المبحث الأول: صور الحماية الموضوعية الوقائية للحياة الخاصة المعلوماتية.

المبحث الثاني: الحماية الجزائية الردعية للحياة الشخصية في مجال المعلوماتية.

الفصل لثاني: الآليات العملية لحماية الحياة الشخصية المعلوماتية.

المبحث الأول: الآليات الإجرائية لحماية الامن الشخصي المعلوماتي.

المبحث الثاني: الآليات المؤسساتية لحماية الامن الشخصي المعلوماتي.

الفصل الأول:
الآليات الموضوعية لحماية الحياة الشخصية المعلوماتية

تعد الجرائم الإلكترونية من أخطر الجرائم المستحدثة التي تواجه عصر التحول الرقمي، مما جعلها التحدي الحقيقي أمام امتحان لقدرة القواعد القانونية والتنظيمية التي تضعها الدول في سبيل تحقيق مواجهة فعلية للأنشطة الجرمية الإلكترونية، ومكافحة أنماطها المختلفة والمتطورة، التي تمس بحرمة الحياة الخاصة للأفراد، إذ أن من حق أي مستخدم لوسائل الاتصال الحفاظ على سرية معلوماته وبياناته وسرية الاتصالات، التي يجريها باعتبارها من حقوق الإنسان الدولية، وذلك تأسيسا على حرمة الحياة الخاصة للأفراد، التي تعتبر في ذات الوقت من الحقوق المكرسة والمكفولة دستوريا حسب المادة 47 الفقرة الرابعة من الدستور الجزائري المعدل بموجب المرسوم الرئاسي رقم 20-442 [1]، والتي تنص في محتواها أن حماية الأشخاص عند معالجة البيانات الشخصية من الحقوق الجوهرية في عصر المعلوماتية.

ولهذا أصبحت الحاجة ملحة لحماية المعطيات الشخصية للأفراد من كل أشكل الإجرام التي قد تلحق هذه البيانات، ويتم ذلك عن طريق الحماية الجزائية الموضوعية وتمثل النصوص القانونية التي تتناول التجريم والعقاب جرائم المعلومات ومدى كفايتها لبسط الحماية الكافية ضد هذه الجرائم، بحيث بات من الضروري أن يواكب تطور الجريمة وأساليبها تطورا في مجال السياسة التشريعية عموما والسياسة الجزائية على وجه الخصوص للحد من هذه الجرائم، وذلك من خلال التوعية والوسائل الوقائية والردعية للحماية الحياة الشخصية المعلوماتية.

وهذا ما سنتناوله في هذا الفصل من خلال المبحثين التاليين:

-المبحث الأول: صور الحماية الموضوعية الوقائية للحياة الخاصة المعلوماتية.

-المبحث الثاني: الحماية الجزائية الردعية للحياة الشخصية في مجال المعلوماتية.

[1]– المادة 47 الفقرة الرابعة من المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، (ج ر) رقم 82 الصادرة لسنة 2020.

المبحث الأول: صور الحماية الموضوعية الوقائية للحياة الخاصة المعلوماتية

في ظل التطور التكنولوجي الحديث وما صـــاحبه من تعرض للحياة الخاصـــة للأفراد لمخاطر لم تكن ماثلة من قبل، عمد المشـــرع الجزائي إلى توفير أكبر قدر من الحماية الخاصـة وذلك من خلال فرض جزاءات مشددة في هذا الشأن، نظرا للخطورة القصوى التي تشـكلها الجرائم المسـتحدثة فإن التشـريعات الجزائية تدخلت بإفراد قوانين خاصـــة أو تعديل قوانينها العقابية بما يتماشـــى والمواجهة الفعالة لهذه الجرائم، بحيث يتبين من هذه القوانين إفراد ســـياســـات جزائية خاصـــة لمكافحتها تختلف عن تلك المقررة للجرائم العادية، تتنوع مناهجها بين الوقاية والتجريم، هذا ما سنتناوله في هذا المبحث من خلال المطالب التالية:

- المطلب الأول: القواعد الوقائية لحماية الحياة الشخصية المعلوماتية.
- المطلب الثاني: وسائل حماية الحياة الشخصية في مجال المعلوماتية.

المطلب الأول: القواعد الوقائية لحماية الحياة الشخصية المعلوماتية

مع تزايد اسـتخدام التكنولوجيا في الجرائم تظهر تحديات جديدة، في تحقيق العدالة مما دفع العديد من الدول لسـن تشـريعات وتضـمنت قواعد إدارية ومدنية وجزائية من أجل حماية الخصوصية، وذلك من خلال تبنيها مجموعة من السياسات والتدابير والقيود بشأن حق الفرد، وتكون بمثابة ضمانات وقائية لحرمة الحياة الخاصة، ويمكن استخلاص ثلاث مبادئ رئيسية يمكن من خلاله ان نحقق التوازن الملائم للأفراد في الخصـــوصـــية والتحكم في بياناتهم الشخصية والتي تتمثل في: مبدأ الشرعية، مبدأ الموافقة ومبدأ الشفافية.

الفرع الأول: مبدأ الشرعية

إن ضـــمان حماية الحق في الحياة الشـــخصـــية للأفراد في مواجهة نظم المعلومات الإسمية، يقتضـي أن يكون مبدأ الشرعية هو الأساس الذي يقوم عليه نشاط هذه النظم، أي أن تكون كل مرحلة من مراحل المعالجة الالية للبيانات وانتهاء بإيصـــال معلومات المعالجة إلى الغير.

وهذا ما نصـــت عليه صـــراحة المادة 9 الفقرة أ من القانون 18-07 [1]حيث يجب معالجة البيانات الشخصية بشكل قانوني وبطريقة امنة وهذا المبدأ يستحسن أن يكون ضابطا لجميع مراحل هذه العملية والتي تتمثل في:

أولا- شرعية جمع وتسجيل البيانات الشخصية

بموجب المادة 09 الفقرة ب من القانون 18-07 [2] يعد جمع وتســـجيل البيانات الشـخصـية قانونياً وبطريقة امنة ولأغراض محددة، إذا كانت البيانات متاحة للجهة المسؤولة عن نظام المعلومات، ومن ثم يتم إدخالها إلى جهاز الحاسوب بموافقة الشـخص الذي تتعلق به البيانات، أو دون الحاجة للحصـول على البيانات الخاصـة، وتسـتند الظروف التي يوافق عليها الشـخص إلى النصـوص القانونية، وتعتبر المعطيات الشـخصـية مرتبطة بشـخص صاحبها، مثل اسمه، أو حالته الاجتماعية، أو محل إقامته، أو صحته، أو معتقداته السياسية أو الفلسفية أو الدينية أو انتمائه النقابي، أو سجلاته الجزائية، أو أرقام حساباته المصرفية، أو معلوماته الإلكترونية، عناوين البريد الإلكتروني والمعلومات الأخرى الموصـــوفة بأنها حسـاسـة، ويمكن التعرف عليها بشـكل مباشـر على أنها الشـخص الذي تتم معالجته، حيث يتطلب جمع المعلومات حول الشـخص المعني موافقة كتابية صـريحة من الشـخص المعني قبل جمعها، باستثناء الحالات التي تكون فيها الموافقة مطلوبة بموجب القانون[3].

ثانيا- شرعية تخزين البيانات الشخصية:

شـرعية تخزين البيانات الشـخصـية يقتضـي أن يكون التخزين يتناسـب مع الهدف من إقامة نظام المعلومات، وأن يكون لمدة محددة وأخيرا العمل على عدم وصـــول الغير الى البيانات والمعلومات المختزنة، وسوف يتم إيضاح ذلك فيما يلي:

---

[1]- المادة 09 الفقرة أ من قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشـخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج ر)رقم 34، الصادرة بتاريخ 10يونيو 2018.

[2]- المادة09 الفقرة ب من قانون رقم 18-07.

[3]- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية – دراسة مقارنة –، منشورات الحلبي الحقوقية، لبنان، ط1، السنة 2009، ص 459-460.

1-**التناســـب بين التخزين والهدف من إقامة النظام:** يســـتلزم هذا المبدأ أن تكون المعطيات ذات الطابع الشـخصـي مناسـبة وملائمة وغير مفرطة، بالنظر إلى الغاية التي تم على أســاســها تجميع هذه المعطيات ذلك حســب ما نصــت عليه المادة 09 الفقرة ج من القانون سالف الذكر[1]، بحيث ينبغي أن تتم هذه العملية إلا للأغراض التي جمعت من أجلها وعدم المبالغة والاسـراف في عملية الجمع والمعالجة ومن هذا المنطلق يتضـح لنا، أن شـرط التناسب يؤدى منع الاستخدام الغير مبرر الذي يؤدي إلى الاستعمال الغير متوافق مع الغاية التي جمعت البيانات من اجلها.[2]

2- **تخزين البيانات لمدة محددة:** يستلزم أن تكون المعطيات الشخصية مخزنة بطريقة يمكن من خلالها التعرف على الأشخاص المعنيين طوال مدة التي لا تتجاوز المدة الضرورية لتحقيق الغايات التي جمعت من أجلها ولذلك ينبغي على مســـؤول المعالجة بعدم حفظ البيانات لمدة تتجاوز الغرض الذي جمعت من اجله، تحت أي ظرف من الظروف [3]، وهذا وفقا للمادة 09 الفقرة هـ، حيث يجب أن يكون هذا الاحتفاظ متلائما مع الغرض من المعالجة ومع ذلك استثنى المشرع الجزائري في نفس المادة والفقرة، فيما يتعلق بفترة الاحتفاظ المحدودة بالبيانات الشخصية عند معالجتها لأغراض تاريخية أو إحصائية أو علمية [4].

نستنتج أن، مبدأ الشرعية يجب أن يسري في جميع مراحل معالجة البيانات الشخصية، مما يتطلب أن يكون جمع البيانات الشخصية وتخزينها واستخدامها قانونيًا، ودقيقًا بناءً على موافقة الأطراف المعنية، لتجنب الإضـرار بصـاحبها ونقل البيانات المذكورة للأخرين ضـمن الحدود اللازمة لتحقيق الغرض الذي جمعت من اجله.

---

[1]– المادة 09 الفقرة ج من القانون 18-07.

[2]– راضية زرقيني، الحماية الجزائية للمعطيات الشخصية، أطروحة دكتوراه، تخصص قانون عام، الوادي، الجزائر، جامعة الشهيد حمه لخضر، السنة 2021-2022، ص 57-58.

[3]– رضا هميسي، الضمانات القانونية لحماية البيانات الشخصية في الفضاء الرقمي، جامعة قاصدي مرباح ورقلة، السنة 2019، ص 62، متوفر على الموقع الإلكتروني: http://www.researchgate.net، تاريخ الاطلاع2024/05/11، ساعة الاطلاع 13:45.

[4]– المادة 09 الفقرة هـ من القانون 18-07.

الفرع الثاني: مبدأ الموافقة

تعرف الموافقة بأنها ابداء الرأي يعبر من خلاله الشـــخص المعني أو ممثله الشـــرعي بقبول معالجة البيانات الشخصية المتضمنة بوسيلة يدوية أو الكترونية وهذا ما نصت عليه المادة 03 من نفس القانون[1]، حيث يشكل هذا المبدأ مدى سلطة الشخص المعني على بياناته الشخصية بشكل ملحوظ ومهم [2]و بطبيعة الحال لا يمكن معالجة البيانات الشخصية إلا بالموافقة الصـــريحة من الشـــخص المعني وعلاوة على ذلك يســـمح له أن يســـحب هذه الموافقة في أي وقت ولكن لا يفوتنا أن ننوه، اذا كان قاصـــرا او ناقص الأهلية تخضـــع الموافقة في هذه الحالة إلى القواعد القانونية العامة وهذا اســـتنادا لما تم ذكره في المادة 07 من نفس القانون[3].

حيث لا يجوز معالجة بياناتهم الشـــخصـــية بمطلق الحرية إلا بعد موافقة ممثليهم القانونيين أو عند الاقتضـــاء، إذن من القاضـــي المختص ولذلك ينبغي على طاقم المسـؤول على معالجة البيانات التحقق من أن الموافقة تأتي من الشخص المسمى في النص المعني[4] وفي نفس الصدد، يرد على هذا المبدأ استثناءات نصت عليها المادة 07 الفقرة الخامسة من نفس القانون، حيث تعد الموافقة غير واجبة لأي معالجة ضرورية ومحتملة وتتمثل في:

- ✓الامتثال لالتزام قانوني يقع على عاتق الشخص المعني أو المسؤول عن المعالجة.
- ✓التنفيذ، لإنجاز مهمة من مهام الســـلطة العمومية او لتنفيذ عقد أو تدابير ما قبل التعاقد يكون الشخص المعني طرفا فيه.
- ✓الحماية، حماية حياة الشخص المعني والمصالح الحيوية لموضوع البيانات إذا كان غير قادر على التعبير عن رضاه من الجانب الجسدي أو القانوني.

---

[1]– المادة 03 من القانون 18-07.

[2]– نعيم ســعيداني، الحماية الجنائية للحق في الخصـــوصـــية في مجال المعلوماتية، أطروحة دكتوراه، تخصـــص قانون جنائي، باتنة، جامعة باتنة 1، السنة 2020-2021، ص 196.

[3]– المادة07 من القانون 18-07.

[4]– Riad Aradji ,Loi N° 18-07: Protection des données personnelles , https://www.gaan.dz/، متوفر على الرابط، تاريخ الاطلاع 11/05/2024، الساعة 18 :18.

✓تحقيق مصلحة مشروعة[1].

وانطلاقا مما سلف، يعد مبدأ الموافقة كأساس قانوني ووقائي للمعالجة البيانات الشخصية، من خلال السماح للأشخاص المعنيين لهم بتحديد كيفية معالجة بياناتهم الشخصية كتصريح بالموافقة الصريحة بصورة واضحة، لا لبس فيها وإرادة حرة دون وجود ضغوط أو قيود.

الفرع الثالث: الشفافية

يتعين على كل من يدير معالجة البيانات الشخصية، أن يتوفر على نوع من الشفافية في عملية جمع وتخزين المعطيات الشخصية المعلوماتية وأن تكون بطريقة قانونية وأخلاقية وأمنة دون التلاعب بها وتحريفها أو السماح للغير المرخص لهم بالاطلاع عليها [2]و لكي تكون المعالجة عادلة وشفافة، يجب ابلاغ الأشخاص المعنيين بالفترة التي سيتم فيها تخزين البيانات الشخصية، والحق في الوصول إلى المعلومات والتدقيق في البيانات ومحوها وسحب الموافقة في أي وقت حيث يجب تقديم جميع المعلومات في شكل شفاف وذكي ويمكن الوصول إليه بسهولة باستخدام لغة واضحة، حيث تهدف الشفافية إلى تمكين الأفراد من اتخاذ قرارات أكثر استنارة ووعيا بالخصوصية فيما يتعلق بالكشف عن المعلومات الشخصية.[3]

وتحقيقا للمبدأ الشفافية، الذي يعد من المبادئ الأساسية لحماية خصوصية الحياة الشخصية المعلوماتية حيث تكفل للشخص نوعا من الاطمئنان على صحة معلوماته، وبالمقابل أقر المشرع الجزائري في المواد 32 الى 37 من القانون 18-07، تحت عنوان حقوق الشخص المعني بالمعالجة والتي تعبر وتؤكد على أن مبدأ الشفافية يعزز الثقة والاطمئنان في استعمال الأشخاص المعنيين للحقوقهم بما يقره القانون[4].

---

[1]– المادة 07 الفقرة 05 من القانون 18-07.

[2]– بولين أنطونيوس أيوب، المرجع السابق، ص 460-461.

[3]-Jean Hendrik Betzing and others، The impact of transparence on mobile privacy decision making، http://doi.org/10.1007./s12525.019.00332.3,p 609, تاريخ الاطلاع 11/05/2024, الساعة 22: 15.

[4]– نعيم سعيداني، المرجع السابق، ص 206.

وضع هذا المبدأ للتأمين الطمأنينة للأفراد فيما يخص صحة ودقة البيانات المعالجة اليا في كل مراحل المعالجة، جمع وتخزين وتشغيل، وان لا يسمح للغير المأذون بالاطلاع عليها كما تعني تمكين الشخص المعني من الاطلاع على بياناته الشخصية والتأكد من صحتها وسريتها كما يقتضي الحفاظ على سرية هذه البيانات، ومنع الاعتداء عليها، ويتحقق هذا المبدأ من خلال تعزيز شعور الافراد بالأمان والطمأنينة بشأن خصوصياتهم.

المطلب الثاني: وسائل حماية الحياة الشخصية في مجال المعلوماتية

لقد أفرز تزايد استخدام شبكات الاتصال الحديثة والأنظمة المعلوماتية وخاصة على ضوء المستجدات والتوجهات التكنولوجية في قطاع الاتصالات والتحول الرقمي إشكالات قانونية هامة، لاسيما ما يتعلق منها بمسألة حماية الحقوق والبيانات المختلفة المتداولة عبر الوسائط الإلكترونية أو التي تنشأ من خلالها من أي اعتداءات إجرامية تستهدف المساس بحقوق وحريات الأخرين، وعليه تعد الوسائل التقنية والتنظيمية لحماية الحياة الشخصية في عصر المعلوماتية، مسألة أساسية وعنصر جوهري لنمو الأعمال الإلكترونية والتصدي للهجمات السيبرانية، وتوفير الحماية الشاملة للخصوصية المعطيات الشخصية للأفراد.

الفرع الأول: الوسائل التقنية لحماية البيانات الشخصية

من خلال الآليات التقنية يتم التأكد من عدم تعرض المعلومات للأخطار المتمثلة في إمكانية الكشف عنها أو الاطلاع عليها من قبل أشخاص غير مسموح لهم بذلك وبهذه التقنيات يتم حفظ وسرية المعلومات الحساسة وضمان التوصل إلى المعطيات، وهذا ما تحققه هذه الوسائل المتمثلة في التشفير والغفلية، وتقنية الجدار الناري والمراقبة الإلكترونية في مجال توفير أمن وسلامة وسرية المعلومات والمعاملات.

أولا: التشفير المعلوماتي

يقصد به " تلك الطريقة التي تعتمد على الخوارزميات الرياضية الذكية التي تسمح بمن لمن يمتلك مفتاحا سريا أن يحول رسالة مقروءة لرسالة غير مقروءة أو العكس"[1]و في مقابل

[1]– فتيحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية – قراءة في أحكام المرسوم الرئاسي 20/05، مجلة الحقوق والعلوم الإنسانية، العدد03، جامعة بومرداس، الجزائر، السنة 2020، ص 175.

ذلك، لم يعرف المشـــرع الجزائري تقنية التشـــفير ولكنه تطرق من خلال نص المادة الثانية الفقرتين الثامنة والتاسعة من القانون 15-04 المتعلق بالتوقيع والمصادقة الإلكترونية[1]

ولابد من التأكيد على أن التشــفير أداة حاســمة في مجال أمن المعلومات، حيث يوفر طريقة لحماية المعلومات الحساسة من الوصول أو العبث غير المصرح به في عالم اليوم، حيث تتزايد كمية البيانات التي يتم نقلها وتخزينها عبر الأنترنت بشــكل كبير حيث أصــبح التشفير أكثر أهمية من أي وقت مضى، ونتيجة لذلك يسمح لنا بنقل المعلومات الحساسة بأمان مثل كلمات المرور وتفاصيل بطاقة الائتمان والبيانات الخاصة الأخرى، عبر الشبكات العامة مثل الأنترنت [2]، وفي نفس الصــدد يوجد نوعان من التشــفير: التشــفير التناظري، والذي يتم استخدامه باستخدام مفاتيح خاصة لفك تشفير النص من شكله المكتوب الأصلي ويستخدم المشفر المفتاح السري أثناء عمليات فك التشفير، ويكون المفتاح السري متطابقًا للمرسل والمستقبل أما بالنسبة للنوع الثاني، فهو يعتمد على قوة الخوارزمية التي تستخدم في تشــفير المعلومة، ويســتخدم فيه زوج فريد من المفاتيح ويشــتمل على مفتاح عمومي ومفتاح خصوصي فيرسل المرسل بالمفتاح العمومي ويفك المستقبل بالمفتاح الخصوصي ويمتاز هذا التشفير برصانة عالية ويبلغ طول الشفرة 2048 بت[3].

وتستخدم هذه الوسيلة في قطاعات الاتصالات الالكترونية وبصفة خاصة شبكات الانترنت لوقاية الرســائل الالكترونية والمعطيات الضــخمة المنقولة الكترونيا، وبذلك يكون التشفير سلاحا ذو حدين يحمي فحوى البيانات ولكن بضياع ذلك المفتاح السري أو البرنامج الذي شفر المضمون فلا فائدة ترجى من وراء المحتوى المشفر وبذلك هو علم تحويل الكتابة

---

[1]– المادة 02 الفقرتين الثامنة والتاسعة من القانون 15-04، المؤرخ في اول فبراير 2015، المتضمن تحديد القواعد العامة المتعلقة بتوقيع والتصديق الالكترونيين، (ج ر) رقم06، الصادرة بتاريخ فبراير سنة 2015.

[2]–Ruma Yadav, Analysis of Cryptography in information Technology 03, WWW.IJSREM.COM , تاريخ الاطلاع 12/05/2024, الساعة 12: 39 .

[3]– أوس مجيد غالب العوادي، الأمن المعلوماتي الســيبراني، مركز البيان للدراســات والتخطيط، بغداد، الســنة 2016، ص26.

الى اسرار من نسبة لغير المصرح لهم للاطلاع عليها ويأتي مصدر قوة إخفاء المعلومة من عدم إمكانية اكتشاف المعلومات السرية من قبل غير المصرح لهم بذلك[1].

واستخلاصا لما تم ذكره أن التشفير المعلوماتي هو تقنية أمنية حيوية لحماية البيانات الحساسة من الوصول الغير مصرح به فهو يقوم بالتصدي لأي هجوم يعتري هذه المعطيات، وتعد هذه العملية ضرورية جدا للمساعدة في حماية البيانات الشخصية للأفراد وذلك لتعزيز الأمن السيبراني، فهو من أهم الوسائل والتقنيات للتأمين على المعلومات السرية الالكترونية.

ثانيا: تقنية الغفلية

إن جدية هذه المخاطر دفعت إلى ابتكار تقنيات متطورة تؤمن لمستخدمي هذه الشبكة اتصالهم بها بصورة مغفلة ومستترة، وذلك من خلال استخدام معدات يطلق عليها تسمية أجهزة معاودة الإرسال بشكل مغفل، وتسمى بالإنجليزية Anonymous Remaileras، وبالفرنسية Réexpéditeurs anonymes.

وغالبا ما تتوفر هذه الأداة لدى مورد خدمات الاتصال بالإنترنت، ويعرضونها بمثابة خدمة إضافية للمشتركين. وهي تقوم بمحي جميع العناصر المعرفة بأصحاب الرسائل الحقيقيين، ومن ثم ترسلها إلى مقصدها بعناوين مجهولة أو مغفلة[2].

تكون للغفلية ميزات وإيجابيات عديدة، تصب مباشرة في خانة حفظ الحياة الشخصية للفرد، لاسيما حقه بان لا تجمع او تحلل أو تنتهز المعطيات المتعلقة بشخصه أو عائلته أو بمسكنه، وسائر البيانات التي ترخص بالتعرف عليه، بدون رضاه وموافقته الصريحة. في هذا المجال، يعتبر الكثيرون بأن الغفلية، هنا أيضا أداة فعالة في متناول مستخدمي شبكة الإنترنت، لمجابهة مثل هذه الممارسات[3].

من هذا المنطلق يتبين، أن تقنية الغفلية هي تقنية تشفيريه، تستخدم في بروتكولات التبادل الأمن للمعلومات بين طرفين وتهدف هذه التقنية إلى حماية خصوصية البيانات

---

[1]– رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، قانون خاص، جامعة أبو بكر بلقايد تلمسان، 2017-2018 ص 127.

[2]– بولين أنطونيوس أيوب، المرجع السابق، ص 250.

[3]– بولين أنطونيوس أيوب، المرجع نفسه، ص 251.

وســـريتها خلال عملية التبادل وعليه فهي تعتبر وســـيلة وأداة فعالة لحماية البيانات وتوفير اعلى مستويات الأمن الشخصي المعلوماتي.

ثالثا: تقنية الجدران والمراقبة الإلكترونية

تعد هذه الأليات من التقنيات الحديثة الأكثر فعالية التي يمكن الاعتماد عليها، اعتبارا للخصوصية الجرائم الماسة بالأمن الشخصي المعلوماتي.

1: تقنية الجدران

"يعرف أنه مجموعة أنظمة توفر أســاليب امنية بين الإنترنت وشــبكة المؤســســات أو الشركات أو غيرها، لكي تجبر جميع عمليات الدخول إلى الشبكة، الخروج منها أن تمر من خلال الجدار الناري الذي يقوم بصــد اختراقات المســتخدمين المتطفلين، وهو يوفر في ذات الوقت حواجز أمنية قبل الدخول إلى الموقع المعني، مثل التحقق من المســتخدمين المحليين والخارجيين نظام الدخول والخروج".[1]

وتنحصــر المهمة الأســاســية في فحص المعلومات الواردة من الإنترنت واكتشــاف أي عناصــر مشــبوهة ضــمن هذه البيانات الواردة والتي يمكن أن تقوم باختراق المعطيات، فيقوم جدار الحماية بالإصــلاح المؤقت للتجاوزات وهذا ما يمنعها من الوصــول إلى الشــبكة، إذا كانت المعلومات آمنة ومشروعة، فإن حماية الجدار تمنحها إذنًا بالمتابعة والدخول إلى أجهزة الكمبيوتر الموجودة داخل الشبكة[2].

2: المراقبة الإلكترونية

"لم يقم المشرع الجزائري بوضع تعريف للمراقبة الإلكترونية، وبالتالي يجب علينا الرجوع إلى الفقه حيث نجد أن المراقبة هي وضع شخص أو وسائل نقل أو أماكن، أو مواد بصورة سرية تحت رقابة سرية أو دورية، بهدف الحصول على معلومات خاصة بالنشاط، أو كشف

[1]– وليد الزيدي، القرصــنة على الأنترنت والحاســوب، دار أســامة للنشــر والتوزيع، ط1، عمان، الســنة 2003، ص 101،المرجع المشار إليه.

[2]– رابحي عزيزة، المرجع السابق، ص 131.

شـــخصـــية الأفراد، وهي تفيد منع إقحام الجريمة، وجمع الأدلة عنها والتأكيد من صـــحة المعلومات ثم الحصول عليها بالفعل"[1].

من القواعد الفنية الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها نظام المراقبة الإلكترونية، إذ يعد هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية ويسمح القانون بهذا الإجراء في مجال التحقيق الجنائي[2].

واسـتخلاصـا لما سـبق، تعد هذه التقنيات من الأسـاليب الحديثة المنتهجة من طرف العديد من المؤســســات كونها من الأنظمة الأمنية التي تحمي شــبكات المعلومات ضــد المقتحمين والمخربين وذلك لحماية أجهزة الكمبيوتر من الاسـتخدام غير المصـرح به، وعليه تعد هذه التقنيات جزء لا يتجزأ من الأمن السيبراني.

الفرع الثاني: الوسائل التنظيمية لحماية البيانات الشخصية

من القواعد التنظيمية التي تشمل مجموعة من السياسات والإجراءات التي توفر الإطار القانوني والتنظيمي اللازم لضـمان حماية البيانات الشـخصـية، والتي تتمثل في تقنية التنظيم الذاتي والعقد وكل من هاتين الوسيلتين تنتهج سياسة الخصوصية والأمان، حيث تلعب هذه الوسـائل دورا اسـتراتيجيا هاما في حماية المعطيات الشـخصـية أو ما يطلق عليها – عقود توريد البيانات –وذلك للتعزيز الثقة لدى المستخدمين.

أولا: التنظيم الذاتي

التنظيم الذاتي هو وسـيلة لتنظيم المعلومات وحمايتها وقد اعتمد النموذج الأمريكي هذه الوســيلة مما اســتدعى العديد للتبنيها وخاصــة في ميدان التجارة الإلكترونية[3] وهذا للبروز الحاجة إلى تخطي الأليات التقليدية و اكتساب تقنيات قانونية و تنظيمية تتلاءم مع طبيعة

[1] راضية زرقيني، المرجع السابق، ص256.

[2]– رابحي عزيزة، المرجع السابق، ص 133.

[3]– عبد الصـبور عبد القوي على مصـري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصـاد، الرياض، ط1، السنة 2012، ص 313.

شـــبكة الأنترنت و تواكب التطورات التكنولوجيا من خلال هذه التقنية التي تســـمع بالمعالجة الإلكترونية للمعطيات الشخصية و حمايتها [1].

في هذا السـياق نخلص، أن التنظيم الذاتي هو وسـيلة قانونية فعالة للتنظيم المعلومات والمحتوى الرقمي، وتقليل مخاطر فقدان المعطيات أو الوصـول غير المصـرح به إليها نظرا للمخاطر التي تطال هذه البيانات وهذا ما يجعلها طريقة فعالة وأكثر كفاءة.

ثانيا: العقد

تمثل عقود نقل البيانات في الحقيقية تشـريعا في صـيغة عقد، ان الأداة العقدية لحماية البيانات الشخصية، أداة خاصة بين أطراف خاصة غالبا ما تكون هيئات ومؤسسات القطاع الخاص التي تسـتثمر خارج الحدود أو عبر الشـبكات التي تتجاوز الحدود الجغرافية، فيكون من مقتضـيات نشـاطها إما نقل البيانات بعينها أو نقل عمليات المعالجة ذاتها، ولا يوجد ما يمنع من اســتخدامها وســيلة للتعاقد بين جهات القطاع الخاص وجهات القطاع العام لكن الغالب أن لا تحظى جهات القطاع العام في مثل هذه الحالة بامتيازات الســلطة فتكون طرفا متعاقدا عاديا [2] كما تجدر بنا الإشـارة إلى أن العقد يتمثل في وجود وثيقة العقد على الموقع الإلكتروني متضـــمن الحقوق والالتزامات لكلا الطرفين موجود للطباعة بعبارة القبول أو الرفض[3].

اســـتنادا لما تم قوله، نســـتنتج أن تقنية العقد من الوســـائل المبتكرة لتنظيم وتخزين المعطيات بشكل أمن وسري لما تعتمده هذه التقنية من اللامركزية التي تعمل بشكل ألي دون الحاجة لوسيط مما يزيد من الفعالية والشفافية، والتوثيق الزمني الآلي مما يسهل نقل البيانات دون تعرضها للمخاطر من المقتحمين.

---

(1) John Borking : Privacy Protecting Measure IN IT Environment Necessary , In formation Management ,10,1998,P 6-11, Reference indicated.

(2)– بولين أنطونيوس أيوب، المرجع السابق، ص 268.

(3)– مروة زين العابدين صـالح، الحماية القانونية الدولية للبيانات الشـخصـية عبر الأنترنت بين القانون الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، ط1، السنة 2016، ص 271.

المبحث الثاني: الحماية الجزائية الردعية للحياة الشخصية في مجال المعلوماتية

إن من أهم أهداف حماية خصوصية الأفراد المعلوماتية هو تمكينهم من إدارة بياناتهم الشخصية وتحديد حقوقهم، وذلك من خلال تحريك الجهود الوطنية لإيجاد قواعد ردعية من شأنها حماية حق الأشخاص في الوصول والاطلاع والتعديل على بياناتهم الخاصة، وكان لابد من حماية الأفراد من كل صور الاعتداءات التي تطال حياتهم الشخصية من خلال إجراءات عقابية ردعية، تحمي خصوصية الأمن الشخص المعلوماتي وتهدف إلى منع الوصول غير المصرح به وضمان أمن بياناتهم، وما يهمنا في هذه الدراسة هي الجرائم المنصوص عليه في قانون العقوبات وخارج قانون العقوبات والمتعلقة بالتوقيع الإلكتروني.

المطلب الأول: نماذج عن الجرائم المنصوص عليها في قانون العقوبات

من خلال قانون العقوبات، تتمثل صور الاعتداءات على خصوصية الأشخاص المعلوماتية في الاعتداء على المراسلات والمحادثات إضافة إلى الاعتداء على الصورة وانتحال الشخصية.

الفرع الأول: الاعتداء على المراسلات والمحادثات

إن الحق في سرية المراسلات والاتصالات الإلكترونية يعد جوهر الحق، باعتباره من الحقوق الأساسية للإنسان في حرمة حياته الخاصة حيث، تعد هذه الرسائل والمكالمات ترجمة مادية للأفكار شخصية وأراء خاصة، ولكن لا يفوتنا أن ننوه انه لا يسمح للغير الاطلاع عليها[1]، وبالتالي تتحقق جريمة الاعتداء على سرية الاتصالات والمراسلات الالكترونية إما باطلاع الشخص على الرسائل الالكترونية أو سماع المحادثات الالكترونية بصورة غير قانونية، وإذا كان من غير الإلزام ان تتضمن الرسائل أو المحادثات اسرار تتعلق بطرفي الرسالة بالمرسل أو المرسل اليه[2]، ولابد من الإشارة أن الحماية الجنائية تشمل سرية الاتصالات والمراسلات جميع وسائل الاتصال المعاصرة التي تتم من خلال نظم المعلومات،

---

[1]–علي أحمد الزعبي، حق الخصوصية في القانون الجنائي –دراسة مقارنة–، المؤسسة الحديثة للكتاب، لبنان، ط1، السنة 2006، ص 180.

[2]– يوسف سليمان بن عودة، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل التقنية المعلومات الحديثة، كلية الرافدين الجامعة، قسم قانون، المجلد 16، العدد 29–30، السنة 2018. ص11.

ويتضـــمن ذلك حماية المحادثات الخاصـــة التي تتم عبر الإنترنت من التنصـــت، وهذا يعد ضمان للخصوصية الرسائل الإلكترونية المتبادلة عبر الإنترنت سواء اتم ذلك بالحصول على كلمة الســر (Password) أو باعتراض هذه الرســائل والاطلاع على محتواها[1]، فإن هذه التجاوزات تمس بخصوصية الأفراد مما ينبغي العقاب والمساءلة القانونية[2].

1. الأساس القانوني لجريمة الاعتداء على المراسلات والمحادثات الإلكترونية:

لوقوع جريمة الاعتداء على المراســـلات والمحادثات الإلكترونية لابد من توفر ثلاثة اركان تتمثل في:

أ. الركن الشـرعي: نص المشـرع الجزائري على حماية خصـوصـية الأفراد المعلوماتية ضد كل وسائل التجسس كما نص عليها الدستور في المادة 46 بحيث لا يجوز الاعتداء على حرمة الحياة الخاصة [3] فسن نصوصا خاصة للتجريم فعل المساس بحرمة المراسلات والمحادثات وذلك بموجب نص المادة 303 مكرر ق ع والتي تنص في محتواها على أنه يتم معاقبة كل شـخص يقوم بالاعتداء أو المسـاس بحرمة الحياة الخاصـة للأفراد عن طريق أحد الـــأفعال المادية التي تم ذكرها في المادة من (التقاط، تسجيل، نقل مكالمات، حديث خاص أو سـري) بأي وسـيلة كانت دون ترخيص من صـاحبها[4] ومن ناحية أخرى نص المشـرع الجزائري في المادة 137 ق ع في حالة كون الموظف بمصلحة البريد وشدد العقوبة[5].

ولابد من الإشـــارة إلى المادة 164 من القانون 18-04 المتضـــمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية والتي جرمت أيضا هذا الفعل حيث تنص في مجملها على أنه يتم معاقبة كل شـخص يقوم باعتراض أو افشـاء سـرية المراسـلات أو الاتصـالات

---

(1)– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط1، السنة 2008، ص 179.

(2)– وردة بن بو عبدالله، نورة بن بوعبد الله، الجرائم الإلكترونية الماسـة بالأمن الشـخصـي المعلوماتي عبر مواقع التواصـل الاجتماعي، جامعة باتنة 1، ص 7.

(3)–المادة 46 من المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، (ج ر) رقم 82 الصادرة سنة 2020..

(4)– المادة 303 مكرر من قانون 21-14، المؤرخ في 28 ديســـمبر 2021، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن ق.ع.

(5)– المادة 137 من ق.ع.

الإلكترونية دون إذن من صـاحبها[1] ولكن لا يفوتنا أن ننوه، إلى التعديل الأخير للقانون رقم 24-06 المتضـمن قانون العقوبات المعدل والمتمم للأمر رقم 66-156 الذي مس جريمة الاعتداء على المراسلات الإلكترونية من خلال المادة 333 مكرر 04 [2].

ب. **الركن المادي:** من خلال استقراء المادة 303 مكرر ق ع يتمثل الركن المادي في جريمة الاعتداء على المراسـلات والمحادثات بأي فعل من الأفعال المادية التقاط، تسـجيل، نقل من شـأنها أن تؤدي إلى الاطلاع على المراسـلات الإلكترونية عمدا بدون مبرر قانوني[3]، وفي نفس الصـدد من خلال مضـمون المادة 164 من القانون 18-04 يتمثل الركن المادي في الإفشاء، النشر، الاستعمال الغير القانوني وبدون رضا المرسل أو المرسل إليه [4] وعليه تتحقق النتيجة الإجرامية بالأفعال المادية المذكورة في المادة السـالف ذكرها بشرط أن تكون سببا في تعدي على المراسلة ووجود علاقة سببية بين فعل الانتهاك والنتيجة ولكن لا يفوتنا أن ننوه، أن فعل تجريم انتهاك سرية المراسلات الإلكترونية يشمل الأشخاص الطبيعية والمعنوية معا[5]، وبالنسـبة للاعتداء على المحادثات الإلكترونية فإن الركن المادي يتحقق باستراق السمع بغير رضا أطراف المحادثة وحتى وان كان مضمون المحادثة لا يتسم بالسـرية ولكن يجب التمييز حول ما إذا كانت الحوارات مفتوحة ام لا، فعلى سـبيل المثال الحوارات المتداولة على شبكة الأنترنت في هذه الحالة لا تقع الجريمة فهي قرينة على رضى سماع المحادثة[6].

ت. الركن المعنوي: جريمة الاعتداء على المراسـلات والمحادثات الإلكترونية من الجرائم العمدية التي تتطلب توافر القصـد الجنائي بعنصـريه العلم والإرادة، وذلك من خلال علم الجاني بأنه يخالف قواعد قانونية معاقب عليها جزائيا حينما يقوم بهذه الوقائع المادية

---

(1)– المادة 164 من القانون رقم 18-04، المؤرخ في 10 مايو 2018، المتعلق بتحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر (27)، الصادرة بتاريخ 13 ماي2018.

(2)– المادة 333 مكرر 04 من قانون رقم 24-06، المؤرخ في 28 ابريل 2024، المعدل والمتمم للقانون العقوبات.

(3)– يوسف سليمان بن عودة، المرجع السابق، ص12.

(4)– المادة 164 من القانون 18-04.

(5)– رشـيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، منشـورات الحلبي الحقوقية، بيروت، السـنة 2020، ص 05، المرجع المشار اليه.

(6)– وردة بن بوعبد الله، نورة بن بوعبد الله، المرجع السابق، ص 08.

والنشـــاطات الإجرامية ففعل الاطلاع والالتقاط والنقل تشـــكل قرائن على علم الفاعل بعدم مشـــروعيتها، كما يجب أن تنصـــرف إرادة الجاني إلى تحقيق الجريمة بأركانها الكاملة كما حددها القانون أما بالنسبة لاستراق السمع في المحادثات الإلكترونية فيتحقق القصد الجنائي بقيام الجاني بفعل التنصـــت مع علمه بأنه مخالف للقانون واتجاه ارادته لارتكابه ويجب أن يكون قد وقع بغير رضا المجني عليه[1].

2.العقوبة المقررة لجريمة الاعتداء على المراسلات والمحادثات: أكد المشرع الجزائري على ضـرورة حماية الحياة الخاصـة المعلوماتية من أي اعتداء أو انتهاك لهذه الخصـوصـية حيث نص على عقوبات لكل من يخالف الضـوابط القانونية، بالرجوع إلى المادة 303 مكرر ق ع، نجد المشـــرع الجزائري أولى الحماية القانونية لســـرية المراســـلات والاعتداء على المحادثات حيث يعاقب بالحبس من ستة اشهر إلى ثلاث سنوات وبغرامة من 50.000 دج الى 300.000 دج [2]كما يجدر بنا الإشـــارة الى العقوبات المنصـــوص عليها في التعديل الأخير ق.ع 24-06 في المادة 333 مكرر 04 يعاقب بالحبس من ســـنة إلى 5 ســـنوات وبغرامة 100.000 دج إلى 500.000 دج، لكل من اسـتعمل الأفعال المادية المنصـوص عليها في المادة بغير إذن ورضـا المجني عليه حيث شـدد العقوبة بالحبس من ثلاث سـنوات الى سـبع سـنوات في حال قصـد الإضـرار بصـاحبها حيث نلاحظ انه شـدد العقوبة في هذا التعديل[3].

مما لا شـك فيه، إن الاعتداء على سـرية المحادثات والمراسـلات يمثل جريمة قانونية تتعارض مع حقوق الخصوصية والبيانات الشخصية، فهذه الاتصالات والمراسلات قد تشمل اســرار وخفايا يحرص الفرد على ان لا يطلع عليها أحد، خصــوصــا التي تتم عبر شــبكة الانترنت سواء كان ذلك بالحصـول على كلمة السـر او اعتراض المراسـلات يعد تعدي على خصوصية الافراد مما يستوجب المساءلة القانونية.

---

[1]– وردة بن بوعبدالله، نورة بن بوعبد الله، المرجع نفسه، ص 8.

[2]– المادة 303 مكرر من ق.ع.

[3]– المادة 333 مكرر 04 من ق.ع المعدل والمتمم بالقانون رقم 24-06.

الفرع الثاني: الاعتداء على الحق في الصورة وانتحال الشخصية

ضمن المشرع الجزائري عدم المساس بخصوصية الأشخاص بموجب العديد من النصوص القانونية في قانون العقوبات، ومن بين أهم صور الاعتداء على الحق في الخصوصية نجد الاعتداء على الحق في الصورة وانتحال الشخصية.

أولا: الاعتداء على الحق في الصورة

تعد الصورة إحدى الحقوق الشخصية اللصيقة بالإنسان، فهي تعد تجسيدا للشخصيته ليس في مظهرها المادي فحسب بل أيضا في مظهرها المعنوي، فالتشريع الجزائي يؤيد بوجود حق الإنسان على صورته وبناء على ذلك وجب حماية الصورة من كل اعتداء غير قانوني ولاسيما، أمام التطور الرقمي لعالم التكنولوجيا الحاصل في ميدان التصوير مما أدى إلى ازدياد هذا النوع من الجرائم التي أصبح من السهل التقاط الصور وتسجيلها ونقلها بكبسة زر[1].

1.الأساس القانوني لجريمة الاعتداء على الحق في الصورة:

تقوم هذه الجريمة على ثلاثة أركان وهي:

أ. الركن الشرعي: جرم المشرع الجزائري الاعتداء على الحق في الصورة باعتبارها تمس خصوصية الأشخاص وذلك بموجب المادة 303 مكرر ق ع الفقرة 02 الذي تمم وعدل بموجب المادة 333 مكرر 04 من ق ع 24-06، ويتضح انطلاقا من نص هذه المادة على أنه المشرع الجزائري عاقب وشدد العقوبة على كل من يقوم بالتقاط والحصول غير المشروع للصورة الشخص بغير رضاه، والقيام بنشرها وتهديد صاحبها للغاية الإضرار به والحصول على مصلحة ما، كما أشار أيضا وشدد بالعقوبة على كل زوج أو خاطب أو مخطوبة قام بهذه الجريمة سواء أثناء قيام الرابطة الزوجية أو بعد انتهائها وذلك استنادا للمادة 333 مكرر 05 من ق ع المعدل والمتمم[2].

---

[1]– نورة هارون، وهيبة برازة، حق الفرد على صورته بين مقتضيات الحق في حرمة الحياة الخاصة وضرورات الكشف عن الجريمة، المجلد 35، العدد 03، بجاية (الجزائر)، السنة 2021، ص 311.

[2]– المادة 333 مكرر 04 و 05 من ق.ع المعدل والمتمم 24-06 .

ب. الركن المادي: يتكون الركن المادي من ثلاث عناصر، النشاط الإجرامي، النتيجة، والعلاقة السببية حيث حدد المشرع الجزائري السلوك الإجرامي من خلال المادة 333 مكرر 04 ق ع المعدل والمتمم في مجموعة من الصور التي تشكل الاعتداء غير المشروع على صورة الشخص والتي تتحقق من خلالها الجريمة والتي تتمثل في الالتقاط، التحصل والنشر ومن ناحية محل الجريمة يتمثل في الصورة، حيث لم يحدد المشرع الجزائري أي وسيلة للقيام بها واكتفى بعبارة أي تقنية كانت [1]، كما أوجب المشرع الجزائري للقيام بهذه الجريمة أن تتم بدون رضا صاحب الصورة وهو ما يوضح لنا أن انعدام رضا صاحب الصورة يشكل عنصرا رئيسيا وقانونيا لهذه الجريمة ويعد سببا لانتفائها[2].

ت. الركن المعنوي: يجب لتحقق الركن المعنوي ضرورة توافر القصد الجنائي بعنصريه العلم والإرادة، فيجب على الجاني أن يكون عالما بأنه يستخدم وسيلة تمكنه من التقاط الصور وتحويلها الى شخص اخر وأن تتجه إرادته إلى ارتكاب هذا السلوك ويجب أن تكون الإرادة حرة وواعية نحو تحقيق الغاية وخالية من العيوب، كما يجدر بنا الإشارة الا ان مسؤولية الشخص لا تقوم في حالة قام بهذا الفعل عن طريق الخطأ كما أن هذه الجريمة لا تقع إلا بتوافر القصد الجنائي[3].

2.العقوبة المقررة لجريمة الاعتداء على الحق في الصورة: أقر المشرع الجزائري لهذه الجريمة عقوبات أصلية وتكميلية.

أ. العقوبات الأصلية: تحمل هذه الجريمة وصف الجنحة ويعاقب عليها القانون بعقوبات سالبة للحرية وعقوبات مالية، حيث تتمثل العقوبة السالبة للحرية في معاقبة الجاني الذي يقوم بهذه الجريمة بدون إذن ورضا صاحبها بالحبس لمدة سنة إلى خمس سنوات، كما شدد العقوبة في حال كان القصد الإضرار بصاحبها والتي تتمثل في الحبس من ثلاث

[1]– وردة بن بوعبدالله، نورة بن بوعبد الله، المرجع السابق، ص 10.

[2]– عبد القادر رحال، البناء القانوني لجريمة التقاط الصورة ونشرها في التشريع الجزائري والفرنسي – دراسة موضوعية إجرائية مقارنة–، المجلد 15، العدد 01، الجزائر، السنة 2022، ص 355.

[3]– نورة هارون، وهيبة برازة، المرجع السابق، ص 315.

سنوات إلى سبع سنوات حيث تضاعف العقوبة إذا كان تحت الضغط والتهديد بموجب المادة 333 مكرر 04 من ق ع24- 06كما عاقب بالحبس من خمس سنوات إلى عشرة سنوات[1]

إذا كان الجاني خاطب أو مخطوبة أو زوج بموجب المادة 333 مكرر05 من القانون السالف الذكر أما العقوبة المالية والتي تتمثل في الغرامة المالية التي نص عليها بموجب المادة 333 مكرر 04 والتي تتروح بين 100.000 دج إلى 500.000 دج، والمادة 333 مكرر 05 والتي تتروح بين 500.000دج على 1000.000 دج[2].

كما أقر المشرع المسؤولية الجزائية للشخص المعنوي عن هذه الجريمة بموجب المادة 303 مكرر 03 من ق ع كما تطبق عليه عقوبة المالية حسب المادة 18 مكرر والمادة 18 مكرر 02 عند الحاجة[3].

ب. العقوبات التكميلية: تنقسم إلى عقوبات وجوبية وجوازيه حيث تتمثل الوجوبية انطلاقا من المادة 303 مكرر 02 ق ع والتي تنص في مضمونها على مصادرة الأشياء التي استعملت في ارتكاب الجريمة كألة التصوير أما الجوازية استنادا للمادة 09 مكرر 01 من ق ع منع المحكوم عليه من ممارسة حقوقه لمدة لا تتجاوز 5 سنوات، كما يتعرض الشخص المعنوي للعقوبات تكميلية وفقا للمادة 18 مكرر ق ع.[4]

يتضح أن الاعتداء على الحق في الصورة يشكل جريمة في قانون العقوبات الجزائري، مما دفع المشرع الجزائري إلى الاهتمام بحق الشخص في صورته من خلال التعديل الأخير للقانون العقوبات حيث وسع نطاق الحماية وشدد العقوبة.

ثانيا: انتحال الشخصية

انتحال الشخصية أو الهوية هو المكان الذي ينشئ فيه المستخدمون حسابات على وسائل التواصل الاجتماعي تحاكي حسابا شرعيا، على سبيل المثال قد يتظاهر المنتحلون بأنهم اشخاص مشهورين أو ممثلين لعلامة تجارية أو شركة معروفة الخ، حيث يوجد هؤلاء

(1)- المادة 333 مكرر 04 من ق.ع المعدل والمتمم.

(2)- المادة 333 مكرر 04 من ق.ع المعدل والمتمم.

(3)- المادة 303 مكرر 03 والمادة 18 مكرر ومكرر 02 من ق.ع.

(4)- المادة303 مكرر02 والمادة09 مكرر01 والمادة 18 مكرر من ق.ع.

المنتحلون على جميع منصات التواصل الاجتماعي الرئيسية وعلى الرغم من عدد المنتحلين قد يكونون غير ضارين إلا أن هناك حسابات مزيفة وخبيثة ولذلك تعد انتحال الشخصية جريمة لكونها تنطوي على انتحال هوية مزيفة بقصد الاحتيال على شخص اخر أو التظاهر بأنه ممثل للشخص أخر أو منظمة أخرى[1].

1. **البنيان القانوني لجريمة انتحال الشخصية:** تقوم هذه الجريمة على ثلاثة اركان:

أ. الركن الشرعي: جرم المشرع الجزائري فعل انتحال الصفة أو الشخصية بموجب المادتين 248 و249 ق ع، ويتضح من خلال المادتين على أن تتم هذه الجريمة بانتحال اسما كاذب أو صفة كاذبة من شأنها أن تؤدي إلى خدع الضحية[2].

ب. الركن المادي: يتكون من ثلاث عناصر النشاط الإجرامي والنتيجة الإجرامية والعلاقة السببية.

- **النشاط الإجرامي:** هو ذلك السلوك الخارجي المكون للجريمة حيث أن جريمة انتحال الصفة هي جريمة إيجابية تتمثل في عدة صور التزوير الاحتيال، الادعاء[3].
- **النتيجة الإجرامية:** هي الغاية المخطط لها من قبل المنتحل وتتحقق هذه النتيجة الإجرامية ربما بإلحاق الأذى بتشويه السمعة أو الصاق التهمة أو تحقيق مصلحة أو بالتزوير[4].
- **السلوك الإجرامي:** هي تلك العلاقة التي تربط السلوك الإجرامي بالنتيجة الضارة، حيث السلوك الإجرامي هو المؤدي إلى النتيجة الإجرامية، وهذا استنادا لما تم ذكره في المادتين الساف ذكرهما [5]

---

[1]- Koosha Zarei and others , Impersonation on social media –Adeep Neural Approach to Identify Imgenuine Content ,Institut Polytechnique de paris , http://2010.08438 (arxiv.org).

[2]– المادتين 248 و249 من ق.ع الجزائري.

[3]– وردة بن بوعبدالله، نورة بن بوعبد الله، المرجع السابق، ص 12.

[4]– علي حسين الخلف، سلطان عبد القادر الشاوي، المبادئ العامة في ق.ع، بغداد (العراق)، المكتبة القانونية للنشر والتوزيع، السنة 2011، ص44.

[5]– المادتين 248 و249 من ق.ع الجزائري.

ت. **الركن المعنوي:** يتحقق بتوافر القصـــد الجنائي العام بنوعيه العلم والإرادة، حيث يتمثل في "قيام الشـخص بإرادته بانتحال شـخصـية الغير، مع وجود نية في الأذى والخداع للأشخاص وأن يكون المتهم قد مارس الانتحال بالفعل وليس مجرد تهديد أو ادعاء"[1]

2.**العقوبة المقررة لجريمة انتحال الشـــخصـــية:** نص المشـــرع الجزائري على عقوبة منتحل اسم الغير في المادتين 248، 249 ق ع والتي تتضـمن في محتواها بعقوبات سـالبة الحرية حيث يعاقب كل من قام بانتحال صفة كاذبة يعاقب بالحبس من ستة أشهر إلى ثلاث سـنوات وبعقوبة مالية تتروح بين 50.000 دج إلى 300.000 دج بموجب المادة 248 ق ع وفي نفس الصـــدد يعاقب كل من قام بانتحال اســـم الغير بالحبس من ســـنة إلى خمس سنوات وبعقوبة مالية من 100.000 دج إلى 500.000 دج استنادا للمادة 249 ق ع.[2]

وتأسيسا على ما تم ذكره، تعد جريمة انتحال الشخصية من الأفعال المنبوذة في جميع التشـريعات، حيث تتمثل في اسـتعمال هوية شـخص أخر وذلك لغاية الاحتيال أو التلاعب للحصـول على منافع أخرى، ولذلك اهتم المشـرع الجزائري بردع هذه الجريمة مما شـكل له تحديات جنائية وأمنية.

المطلب الثاني: الجرائم المنصوص خارج قانون العقوبات

صـور الاعتداء التي تقع على خصـوصـية الأشـخاص التي تضـمنها القانون 18-07، والتي تتمثل في جريمة المعالجة والاســـتعمال غير المشـــروع والجرائم المرتبطة بالإجراءات المسبقة عن المعالجة أما من ناحية الجرائم المتعلقة بالتوقيع الإلكتروني والتي تتضـمن جرائم قبل إنشاء التصديق الإلكتروني وجرائم بعد إنشاء التصديق الإلكتروني.

الفرع الأول: الجرائم المنصوص عليها في قانون 18-07

تتمثل فيما يلي:

[1]- https://LEGAL. ADVICE. ONLINE/ تاريخ الاطلاع 18/05/2024, الساعة 09: 15.

[2]– المادتين 248 و 249 من ق.ع المعدل والمتمم.

أولا: جريمة المعالجة والاستعمال الغير مشروع

تعتبر هذه الجريمة من أخطر صور الجرائم الماسة بخصوصية الأشخاص المعلوماتية، لذا يستلزم الحماية الجزائية لمثل هذا الاعتداء ويمثل أيضا في الحقيقة اعتداء على حق الدولة في الرقابة على تداول البيانات.

أ. **جريمة المعالجة غير المشروعة:** تعد الجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية من أهم الجرائم التي تناولها المشرع الجزائري في قانون حماية البيانات الشخصية، وذلك لخطورتها على شتى المعاملات الإلكترونية التي يقوم بها الفرد والمجتمع والدولة.

1. البنيان القانوني لجريمة المعالجة الغير مشـــروعة: للقيام هذه الجريمة ينبغي أن تتوفر ثلاثة أركان تتمثل في:

- **الركن الشـرعي:** نص المشـرع الجزائري على هذه الجريمة في المادة 59 من القانون 18-07 على أنه يعاقب كل من يقوم بعملية الجمع خارج الحالات المســـموح بها قانونا ودون ترخيص[1].
- **الركن المادي:** من مراحل معالجة المعطيات عملية الجمع التي من خلالها يتم الحصـــول على بيانات الأشـــخاص كما تعتبر هذه العملية من أبســط أصـــناف الاعتداء على البيانات الشخصية [2].

حيث عرفت المادة 03 من القانون 18-07 المعالجة بأنها تجميع، تســـجيل تنظيم، استعمال وإطلاع وغيره، تتحقق بواسطة عملية واحدة أو عدة عمليات[3].

وتقوم هذه الجريمة سواء تمت العملية يدويا أو بطريقة ألية وذلك استنادا للمادة 04 من القانون 18-07، كما يسـتوجب لقيامها أن تسـتعمل وسـائل احتيالية وغير قانونية كما جاء في المـادة 59 من نفس القـانون وفي مقابـل ذلـك يجـب أن تتم هذه المعـالجـة دون احترام

---

[1]– المادة 59 من قانون رقم 18-07.

[2]– عزالدين طباش، الحماية الجزائية للمعطيات الشـخصـية في التشـريع الجزائري–دراسـة في ظل قانون 18-07 المتعلق بحماية الأشـخاص الطبيعيين في مجال معالجة المعطيات الشـخصـية ذات الطابع الشـخصـي، المجلة الأكاديمية للبحث القانوني، العدد 02، بجاية، السنة 2018، ص30.

[3]– المادة 03 من القانون 18-07.

للخصوصية وكرامة الحياة الخاصة طبقا للمادة 02 من القانون السالف الذكر[1]، كما تتحقق هذه الجريمة أيضـــا في حال تمت المعالجة للغايات أخرى غير المســـموح بها أو المرخص لها[2].

- **الركن المعنوي:** جريمة المعالجة غير المشـروعة من الجرائم العمدية وبالتالي تتحقق بتوافر القصد الجنائي العام من علم وإرادة وذلك من خلال علم الجاني بأن الأفعال التي يقوم بها مخالفة للقانون واتجاه إرادته الحرة لارتكاب هذا الفعل [3]و يتضح ذلك من خلال استعمال المشــرع مصــطلحات " طرق تدليســيه"، "غير نزيهة"، " غير مشــروعة" في المادة 59 من القانون السالف الذكر[4].

2.عقوبة جريمة المعالجة الغير مشــروعة: أقر المشــرع الجزائري عقوبة جزائية على كل من قام في غير الحالات المنصـــوص عليها قانونا بعملية الجمع بطرق احتيالية وغير قانونية وبعقوبات ســالبة للحرية تتمثل في الحبس من ســنة إلى ثلاث ســنوات وبغرامة مالية تتراوح ما بين 100.000 دج إلى 300.000 دج كما نصت المادة 59 من القانون السالف الذكر[5].

ب. : جريمة الاستعمال غير المشروع: جرم المشرع الجزائري هذه الجريمة من خلال الأفعال التي تسبب الاستعمال غير المشروع، من ضمنها التسبب أو الإسهال للاستعمال التعسفي والتدليسي للمعطيات الشخصية حيث حدد ارتكابها من قبل المسؤول عن المعالجة أو المعالج من الباطن أو أي شخص مكلف بالمهمة.

1.البنيان القانوني لجريمة الاســتعمال الغير مشــروع: تقوم هذه الجريمة بتوفر ثلاثة أركان تتمثل في:

---

[1]– المادة 02 والمادة 04 والمادة 59 من القانون رقم 18-07.

[2]-http://revues.imist.ma/ ?journal=REGS، N 24 AOUT 2020 ,P 11. تاريخ الاطلاع: 19/05/2024 , الساعة 12: 15.

[3]– نسـرين مشـتة، اخلاص بن عبيد، الحماية القانونية للمعطيات الشـخصـية، في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، مجلد 06، العدد 01، باتنة، السنة 2021، ص 09.

[4]– المادة 59من القانون رقم 18-07.

[5]– نفس المادة من نفس القانون.

▪ **الركن الشرعي:** نص المشرع الجزائري على جريمة الاستخدام غير المشروع طبقا للمادة 69 من القانون 18-07 حيث يتضح من خلال نص المادة أن المشرع الجزائري نص بشكل صريح على أن هذه الجريمة تتم من طرف المسؤول عن المعالجة أو المعالج الباطن أو الشخص المكلف بمهام المعالجة وذلك للخطورة هذا الفعل وحماية الشخص من استخدام بياناته الشخصية واستغلالها[1].

▪ **الركن المادي:** يتحقق الركن المادي بارتكاب هذه الجريمة بأحد الأفعال التالية:

في حال ارتكبت الجريمة من قبل المسؤول عن المعالجة أو المعالج عن الباطن أو الشخص المكلف بالمهمة، وتم التسبب أو تسهيل في الاستخدام التعسفي أو الاحتيالي للبيانات المعالجة أو المستعملة كما نصت المادة 69 من القانون 18-07، وفي نفس الصدد لكل من سمح لأشخاص غير مؤهلين بالدخول للمعطيات الشخصية بموجب المادة 60 من نفس القانون أو من قام بإفشاء معلومات محمية بموجب المادة 62 من نفس القانون، كما نصت المادة 67 من نفس القانون، على كل من يقوم بنقل البيانات الشخصية إلى دولة أجنبية دون احترام النصوص القانونية الموجودة في المادة 44 من هذا القانون، إضافة إلى ما تم ذكره، فأن أي شخص غير مؤهل للولوج في هذا السجل يعاقب بالعقوبات المنصوص عليها في المادة 63 من هذا القانون[2]، كما أن المشرع كان واضحا حين اعتبر التسبب في الاستخدام التعسفي أو التدليسي غير قانوني وغير نزيه عاملا رئيسيا للتحقق جريمة الاستخدام غير المشروع [3].

▪ **الركن المعنوي:** يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام المتمثل في العلم والإرادة لأنها جريمة عمدية[4].

2.**العقوبة لجريمة الاستعمال غير المشروع:** قرر المشرع الجزائري الجزاء الجنائي لهذه الجريمة لمدى خطورتها وذلك بالحبس لمدة سنة إلى خمس سنوات وعقوبة مالية تتراوح

---

[1]– المادة 69 من القانون رقم 18-07.

[2]– المواد 44، 60، 63، 67، 69 من نفس القانون.

[3]-http://revues.imist.ma/ ?journal=RE، N 24 AOUT 2020 ,P 11. تاريخ الاطلاع: 19/05/2024 , الساعة 15: 23.

[4]– نسرين مشتة، اخلاص بن عبيد، المرجع السابق، ص 10.

ما بين 100.000 دج إلى 500.000 دج حسب ما جاءت به المادة 69 من القانون 07-18 [1].

ومن هذا المنطلق يتضح أن كل جمع أو معالجة أو استعمال مخالف للقانون يشكل جريمة معاقب عليها، وتجدر الإشارة بالرغم من أن تجميع المعطيات قد يتم بطريقة مشروعة، إلا أن ايصالها إلى أشخاص غير مختصين يشكل فعلا غير مشروع ويعد اعتداء على خصوصية الفرد وأسراره الخاصة.

ثانيا: الجرائم المرتبطة بالإجراءات المسبقة للمعالجة:

تتمثل فيما يلي:

أ. جريمة المعالجة دون تصريح أو ترخيص من السلطة الوطنية:

يجب أن تخضع كل عملية معالجة البيانات الشخصية لتصريح مسبق أو ترخيص يودع لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ANPDP حسب ما جاءت به المادة 56 من القانون 18-07 [2].

- **المقصود بالتصريح أو الترخيص:**

من ناحية التصريح: يقدم طلب يتضمن إعلام السلطة الوطنية للإنجاز عملية المعالجة ويقدم هذا التصريح من قبل المسؤول عن المعالجة أو ممثله القانوني في أجل 48 ساعة بالطريق الإلكتروني بموجب المادة 13 من القانون 18-07 [3].

من ناحية الترخيص: استنادا للمادة 17 من نفس القانون يعد الترخيص قرار يصدر من السلطة الوطنية يتضمن الموافقة أو الرفض بخصوص المعالجة.[4]

[1]– المادة 69 من القانون رقم 18-07.

[2]– المادة 56 من القانون رقم 18-07.

[3]– المادة 13 من القانون رقم 18-07.

[4]– المادة 17 من القانون رقم 18-07.

1.البنيان القانوني لجريمة المعالجة دون تصريح أو ترخيص من السلطة الوطنية:

للقيام هذه الجريمة لابد أن تتوفر ثلاثة أركان تتمثل في:

- **الركن الشرعي:** عدم الحصول على التصريح أو الترخيص يعد اعتداء على خصوصية الشخص المعلوماتية وعلى حق الدولة في رقابة البيانات الشخصية، مما يسهل ارتكاب جرائم الاعتداء على المعطيات الشخصية[1] وللحماية خصوصية الفرد ومساعدة جهات الرقابة نص المشرع الجزائري على هذه الجريمة بموجب المادة 56 من نفس القانون على معاقبة كل من يقوم أو يأمر بمعالجة البيانات الشخصية دون مراعاة الإجراءات التي يتطلبها القانون ونصت عليها المادة 12 من نفس القانون[2].
- **الركن المادي:** يتحقق الركن المادي بتوافر عنصرين:

✓ **السلوك الإجرامي:** حيث يتمثل في معالجة البيانات التي تتخذ شكل الإدخال، الحفظ، التسجيل، التوزيع فإذا تمت المعالجة فإن النتيجة تحققت[3].

✓ **عدم مراعاة الإجراءات الأولية الواردة بنص القانون:** أي ان يتم إجراء هذه المعالجة دون إذن من السلطة الوطنية في غياب التصريح أو الترخيص منها[4] حيث تقع المسؤولية على مسؤول المعالجة[5].

- **الركن المعنوي:** تعد هذه الجريمة من الجرائم العمدية حيث تقوم على القصد الجنائي العام بنوعيه العلم والإرادة، فالعلم يعني علم الجاني بقيامه بإجراء معالجة البيانات دون ترخيص من السلطة الوطنية أما الإرادة أن تتجه إلى إجراء هذه البيانات بأي طريقة كانت[6].

---

(1)– بولين أنطونيوس أيوب، المرجع السابق، ص 414.

(2)– المادة 56 و 12 من القانون رقم 18-07.

(3)– محمد أمين الشوابكة، جرائم الحاسوب والأنترنت – الجريمة المعلوماتية–، دار الثقافة للنشر والتوزيع، عمان، ط1، السنة 2007، ص87.

(4)– محمد أمين الشوابكة، المرجع نفسه، ص 88.

(5)– نسرين مشتة، اخلاص بن عبيد، المرجع السابق، ص12.

(6)– علي أحمد الزعبي، المرجع السابق، ص350.

2.العقوبة المقررة لجريمة المعالجة دون تصريح أو ترخيص من السلطة الوطنية:

عاقب المشرع الجزائري كل من يجري أو يقوم بإجراء معالجة البيانات الشخصية دون ترخيص من السلطة الوطنية بعقوبة سالبة للحرية بالحبس من سنتين إلى خمس سنوات وبغرامة مالية تتراوح بين 20.000دج إلى 500.000 دج حسب ما ورد في المادة 56 من القانون 18-07 [1].

ب. جريمة الاستمرار في معالجة رغم سحب وصل التصريح أو الترخيص:

الجهة القانونية التي تملك صلاحيات سحب وصل التصريح للسلطة الوطنية وذلك وفقا للمادة 46 من القانون 18-07 حيث أن هذا القرار قد يكون مؤقتا للمدة لا تتجاوز سنة أو يكون نهائيا[2].

1.**البنيان القانوني لجريمة الاستمرار في معالجة رغم سحب وصل التصريح أو الترخيص:** للقيام هذه الجريمة ينبغي أن تتوفر ثلاثة أركان تتمثل في:

- **الركن الشرعي:** نص المشرع الجزائري على هذه الجريمة بموجب المادة 56 الفقرة 02 من القانون 18-07 حيث تقوم هذه الجريمة في حالتين، في حالة كل من قام بمواصلة نشاط المعالجة رغم سحب وصل التصريح أو الترخيص المسموح له أومن قام بتصريحات كاذبة[3].
- **الركن المادي:** يتحقق السلوك الاجرامي ونتيجة الجريمة بالشروط المتمثلة في القيام بالتصريحات الكاذبة، اصدار السلطة الوطنية قرار يتضمن سحب وصل التصريح أو الترخيص، مواصلة مسؤول عن المعالجة إجراءات المعالجة وهذا استنادا لما تم ذكره في المادة 56 الفقرة 02 من القانون السالف الذكر[4].
- **الركن المعنوي:** يكمن الركن المعنوي لهذه الجريمة في القصد الجنائي العام بنوعيه العلم والإرادة، العلم يقتضي علم مسؤول عن المعالجة بقرار السلطة بسحب وصل التصريح

---

[1]– المادة 56 من القانون رقم 18-07.

[2]– نعيم سعيداني، المرجع السابق، ص 375.

[3]– المادة 56 الفقرة 02 من القانون رقم 18-07.

[4]– نعيم سعيداني، المرجع السابق، ص 375.

أو الترخيص بمعالجة البيانات الشخصية أما إرادته تتجه إلى فعل الاستمرار ومواصلة المعالجة[1].

2.العقوبة المقررة لجريمة الاستمرار في معالجة رغم سحب وصل التصريح أو الترخيص:

ساوى المشرع الجزائري في العقوبة بين جريمة الاستمرار في المعالجة بعد سحب وصل التصريح أو الترخيص وبين جريمة المعالجة بدون تصريح أو ترخيص حيث عاقب بالحبس من سنتين إلى خمس سنوات وبغرامة مالية من 200.000 دج إلى 500.000 دج حسب ما نصت عليه المادة 56 الفقرة 02 من القانون 18-07 [2].

استنادا لما سبق، تخضع كل عملية معالجة البيانات الشخصية لتصريح مسبق أمام السلطة الوطنية أو لترخيص منها في الحالات التي نص عليها القانون، حيث تقتضي المعالجة الصائبة للبيانات الشخصية الزامية احترام القواعد الشكلية والإجرائية التي كرسها المشرع الجزائري بهدف ضمان حماية خصوصية الأمن الشخصي المعلوماتي وهذا ما يجعل المسؤولون عن المعالجة ملزمون بتطبيقها للتجنب المخاطر الناتجة عن هذه المعالجة.

الفرع الثاني: الجرائم المنصوص عليها في قانون 15-04

من أهم الضمانات القانونية للحماية والمحافظة على سلامة التوقيع الإلكتروني هو انشاء شهادة التصديق الإلكتروني، والتأكد من هوية الشخص الموقع بموجب القانون المتعلق بالتوقيع والتصديق الإلكتروني وذلك نظرا للكثرة الاعتداءات على هذا النوع من الجرائم.

[1]– المادة 56 الفقرة 02من القانون رقم 18-07.

[2]–المادة 56 الفقرة 02 من القانون18-07 .

أولا: الجرائم قبل إنشاء شهادة التصديق الإلكتروني

نص المشـــرع الجزائري على هذه الجريمة في المادة 66 من القانون 15-04 حيث تضمنت أن كل من قدم تصريحات كاذبة للتملك شهادة التصديق الإلكتروني موصوفة على أنه يعاقب[1].

1.البنيان القانوني للجرائم قبل إنشاء شهادة التصديق الإلكتروني: للقيام هذه الجريمة يتعين أن تتوفر ثلاثة أركان تتمثل في:

- **الركن الشـرعي:** جرم المشرع الجزائري هذه الجريمة في نص المادة 66 من القانون 15-04 والذي يتضـــمن في فحواها على أنه كل من يقوم بإدلاء قرار كاذب للنيل شـــهادة التصـــديق الإلكتروني فصـــحة التوقيع الإلكتروني مرتبط بصـــحة المعطيات المدلى بها من طرف الشخص المعني[2].
- **الركن المادي:** يتحقق الركن المادي لهذه الجريمة بتحقق النشـــاط الإجرامي والنتيجة الإجرامية من ناحية الســـلوك الإجرامي، الذي يتمثل في القرارات الكاذبة حول المعطيات الشخصية (الهوية، النشاط، البريد الإلكتروني.....) التي لها علاقة بإنشاء شهادة التوقيع[3] في نفس الصـــدد تتمثل صـــفة الجاني بالشـــخص الموقع طالب إنشـــاء التوقيع والتي عرفه المشرع الجزائري في المادة 02 من القانون 15-04 هو ذلك الشخص الطبيعي الذي يمتلك بيانات انشـاء التوقيع الإلكتروني ويعمل لحسـابه الخاص أو لحسـاب الشـخص الطبيعي أو المعنوي في مقابل ذلك تتحقق النتيجة الإجرامية من خلال حصـــول الجاني على شـــهادة التصديق الإلكتروني[4].
- **الركن المعنوي:** تعتبر هذه الجريمة من الجرائم العمدية ويكفي لقيامها عنصـــر العلم والإرادة، العلم يجب أن يعلم الجاني بعدم صـحة المعطيات المعطاة له وبالرغم من ذلك تتجه إرادته إلى التصريح الكاذب للحصول على غايته شهادة التصديق الإلكتروني[5].

---

[1]– المادة 66 من القانون رقم 15-04.

[2]– نفس المادة ونفس القانون.

[3]– نعيم سعيداني، المرجع السابق، ص 412.

[4]– المادة 02 من القانون رقم 15-04.

[5]– نعيم سعيداني، المرجع السابق، ص 413.

2.العقوبة المقررة للجرائم قبل إنشاء شهادة التصديق الإلكتروني:

نص المشرع الجزائري على عقوبة جزائية تتمثل في الحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة مالية تتراوح بين 20.000 دج إلى 200.000 دج على كل من قام بتصريحات كاذبة للحصول على شهادة التصديق الإلكتروني حسب ما نصت عليه المادة 66 من القانون 15-04 [1].

ثانيا: الجرائم بعد إنشاء شهادة التصديق الإلكتروني:

تتمثل الجرائم بعد إنشاء شهادة التصديق الإلكتروني في كل من جريمة الإفشاء وجمع واستعمال معطيات شخصية بطريقة غير شرعية.

أ. جريمة إفشاء المعطيات الشخصية:

1.البنيان القانوني للجرائم بعد إنشاء شهادة التصديق الإلكتروني:

- **الركن الشرعي:** طبقا للمادة 70 من القانون 15-04 تتضمن في محتواها أن كل مؤدي خدمات التصديق الإلكتروني، يجب عليه أن يقوم بالحفاظ على سرية المعطيات المتعلقة بشهادة التصديق الإلكتروني[2].
- **الركن المادي:** من خلال المادة 70 من القانون السالف الذكر يتضح ان الركن المادي لهذه الجريمة يتحقق من خلال العناصر التي تتمثل في النشاط الإجرامي الذي يتجلى في عدم المحافظة على خصوصية البيانات الشخصية، التي قدمها المعني بإنشاء التوقيع وذلك من خلال الاطلاع عليها وإفشائها للغير أما محل الجريمة الذي يتمثل في المعطيات الشخصية في مقابل ذلك[3]، تتحقق النتيجة الإجرامية بمجرد تحقق السلوك الإجرامي دون تحقق الضرر لصاحبها.
- **الركن المعنوي:** تعد من الجرائم العمدية حيث يتحقق ركنها المعنوي بتوافر العلم والإرادة، وذلك من خلال علمه بالمعطيات الشخصية التي يمتلكها نتيجة ووظيفته فلا يجوز

[1]– المادة 66 من القانون رقم 15-04.

[2]– المادة 70 من القانون رقم 15-04.

[3]– نعيم سعيداني، المرجع السابق، ص414.

له الاطلاع عليها ورغم ذلك تنصرف إرادته إلى مخالفة هذه الإجراءات القانونية المنصوص عليها والقيام بإفشائها[1].

2.العقوبة المقررة للجرائم بعد إنشاء شهادة التصديق الإلكتروني:

أقر المشرع الجزائري بعقوبة سالبة للحرية بالحبس من ثلاثة أشهر إلى سنتين وبغرامة مالية تتراوح بين 200.000 دج إلى 1000.000 دج على كل مؤدي خدمات التصديق الإلكتروني وأخل بأحكام المادة 42 من هذا القانون، بموجب المادة 70 من القانون السالف الذكر[2].

ب. جريمة مؤدى خدمة التصديق الإلكتروني للمعطيات الشخصية دون موافقة الشخص:

1.البنيان القانوني للجرائم قبل إنشاء شهادة التصديق الإلكتروني: للقيام هذه الجريمة يتعين أن تتواجد ثلاثة أركان تتمثل في:

- **الركن الشرعي:** جرم المشرع الجزائري هذه العملية بموجب المادة 71 من القانون 15-04 حيث نصت في مضمونها عل أنه لا يجوز للمؤدي خدمات التصديق الإلكتروني جمع المعطيات الشخصية للمعني إلى بعد الحصول على الموافقة [3].
- **الركن المادي:** يتحقق الركن المادي لهذه الجريمة بمجرد السلوك الإجرامي المتجلي في مؤدي خدمة التصديق الإلكتروني الذي يقوم بجمع المعطيات الشخصية بغير موافقة المعني ،ومحل الجريمة تتمثل في المعطيات الشخصية دون الحاجة إلى تحقق النتيجة الإجرامية بل يكفي النشاط الإجرامي [4].
- **الركن المعنوي:** تعتبر هذه الجريمة أيضا من الجرائم العمدية التي يتطلب لتحققها القصد الجنائي العام بنوعيه العلم والإرادة، كعلم الجاني بأن يقوم بعملية جمع البيانات

---

[1]– نعيم سعيداني، المرجع نفسه، ص 414.

[2]– المادة 70 من القانون رقم 15-04.

[3]– المادة 71 من القانون رقم 15-04.

[4]– نعيم سعيداني، المرجع السابق، ص 415.

الشخصية دون الحصول على الموافقة الشخصية من الشخص المعني إلا أن إرادته تتجه إلى القيام بهذا الفعل وذلك استنادا للمادة 71 من القانون 15-04[1].

2.العقوبة المقررة للجرائم بعد إنشاء شهادة التصديق الإلكتروني:

نص المشرع الجزائري على عقوبة جزائية لكل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية تتراوح بين 200.000 دج إلى 1000.000 دج بموجب المادة 71 من نفس القانون[2].

ت. جريمة جمع واستعمال معطيات شخصية بطريقة غير شرعية:

1.البنيان القانوني للجرائم بعد إنشاء شهادة التصديق الإلكتروني: للقيام هذه الجريمة ينبغي أن تتوفر ثلاثة أركان تتمثل في:

- **الركن الشرعي:** يتمثل الركن الشرعي في هذه الجريمة في المادتين 43 و71 من القانون السالف الذكر حيث تنص كلتا المادتين أنه لا يجوز للمؤدي خدمات التصديق الإلكتروني أن يقوم بعملية الجمع إلا بعد الموافقة الصريحة من الشخص المعني، كما يجب عليه ان يقوم بجمع المعطيات الشخصية الضرورية فقط إضافة إلى ذلك لا يمكن أن يستخدمها لغايات أخرى[3].
- **الركن المادي:** يتحقق الركن المادي لهذه الجريمة بتوافر السلوك الإجرامي الذي يأخذ صورتين حيث تتمثل الصورة الأولى في جمع البيانات الشخصية من قبل مؤدي خدمات التصديق الإلكتروني، وأما الصورة الثانية والتي تتعلق بفعل الاستخدام للبيانات الشخصية المجمعة لأغراض أخرى[4].
- **الركن المعنوي:** يتمثل الركن المعنوي للجريمة في القصد الجنائي العام بنوعيه العلم والإرادة كونها من الجرائم العمدية، والتي تقتضي أن يكون عالما بأن ما تم جمعه من بيانات

---

[1]– المادة 71 من القانون رقم 15-04.

[2]– نفس المادة و نفس القانون.

[3]– المادتين 43 و71 من القانون 15-04.

[4]– نعيم سعيداني، المرجع السابق، ص 416.

عن الشخص المعني غير لازمة ومبالغ فيه والاستخدام الذي تم جمعه في غير الغرض الذي تم من أجله [1].

2.العقوبة المقررة للجرائم قبل إنشاء شهادة التصديق الإلكتروني:

عاقب المشـرع على هذه الجريمة بالحبس من سـتة أشـهر إلى ثلاثة سـنوات وبغرامة تتراوح بين 200.000 دج الى 1000.000 دج بموجب المادة 71من القانون 15-04 [2] وبالنسـبة للشـخص المعنوي بغرامة تعادل 5 مرات الحد الأقصـى للغرامة المنصـوص عليها للشخص الطبيعي إضافة إلى عقوبات تكميلية المحددة 18 مكرر ق ع [3]

يرتبط التوقيع والتصـديق الإلكتروني بمجموعة من البيانات والمعلومات الشـخصـية التي يشكل الاعتداء عليها جريمة يعاقب مرتكبيها بعقوبات جزائية، ولهذا أصـدر المشرع الجزائري قانون متعلق بالتوقيع والتصديق الإلكتروني للحماية خصوصية الأمن المعلوماتي.

[1]– نعيم سعيداني، المرجع نفسه، ص 417.

[2]– المادة 71 من القانون 15-04.

[3]– المادة 18 مكرر من ق.ع.

خلاصة الفصل الأول:

يسعى المشرع الجزائري من أجل حماية الحياة الشخصية المعلوماتية، باعتبار أن لكل شـــخص الحق في حماية معطياته الخاصـــة، حيث لا يمكن أن يقع معالجتها إلا في إطار احترام المبادئ، التي نص عليها القانون والتي تكمن في الشـرعية والموافقة والشـفافية، وذلك إدراكا منه للاعتداءات المحتملة في ظل التحول الرقمي.

و لضـــمان المحافظة على خصـــوصـــية الأشـــخاص المعلوماتية أوجد آليات للحماية الجزائية من خلال ق.ع، الذي وضـــع عقوبات ردعية لكل من يخالف القانون ويتعدى على الغير إضافة إلى التعديل الأخير 24-06، الذي وسع نطاق الحماية وشدد العقوبة الجزائية، كما أصـدر قانون 18-07 المتعلق بحماية الأشـخاص الطبيعيين في مجال المعطيات ذات الطابع الشـخصـي، وذلك للسد الفراغ في هذا المجال لا سيما مع التقدم التكنولوجي، إضـافة إلى إصـداره للقانون المتعلق بالتوقيع والتصـديق الإلكتروني لإلزام مؤدي خدمات التصـديق الإلكتروني بواجب حماية جل البيانات الشـخصـية، التي تتضـمن شـهادات التصـديق والتوقيع الإلكتروني.

فيما يخص الوســائل التقنية والتنظيمية لحماية البيانات الشـــخصـــية تعد من التدابير الفعالة والعناصـر الأساسـية للحماية الخصـوصـية المعلوماتية وتشـمل التدابير التقنية ضـوابط وتقنيات الأمن السـيبراني منها التشـفير والغفلية والجدران والمراقبة الإلكترونية، كما تتضـمن التدابير التنظيم كل من التنظيم الذاتي والعقد، لكن هذه الحلول التقنية والقانونية والتنظيمية وحدها غير كافية، فلابد من ارتباطها بالوعي اللازم للأفراد وثقافة التعامل مع البيئة الرقمية، لضمان مستوى أمن وسري فيما يتصل بإدارة البيانات الشخصية وتجاوز مخاطر المعلوماتية.

الفصل الثاني:
الآليات العملية لحماية الأمن الشخصي المعلوماتي

من خلال هذا الفصل سيتم تسليط الضوء على الآليات العملية التي انتهجها المشرع الجزائري لحماية الأمن الشخصي المعلوماتي، وذلك نتيجة للتزايد استخدام التكنولوجيا وتطور تقنيات الاتصال نشأ خطر يهدد البيانات الشخصية للأفراد من حيث الحصول عليها وتداولها ومعالجتها مما استلزم وضع معايير قانونية، تنظيمية وتقنية لحماية حق الشخص في الخصوصية.

ولذلك سارع المشرع الجزائري لإحداث آليات إجرائية ومؤسساتية من أجل السهر على احترام وحماية المعطيات الشخصية، فعلى المستوى الوطني في الجزائر نجد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني، كما استحدث منظومة الأمن للأنظمة المعلوماتية والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، التي تحدد قواعد وإجراءات الحماية في إطار احترام الكرامة الإنسانية، وحقوق الأشخاص وشرفهم وسمعتهم.

حيث تساهم هذه الآليات المؤسساتية في المحافظة على خصوصية الأفراد المعلوماتية، وزيادة قدرة الدولة على مراقبة كل الانتهاكات التي تطال الحياة الشخصية المعلوماتية، ومتابعة الإجراءات بدقة ووضوح.

وهذا ما سنتناوله في هذا الفصل من خلال المبحثين التاليين:

-المبحث الأول: الآليات الإجرائية لحماية الأمن الشخصي المعلوماتي.

-المبحث الثاني: الآليات المؤسساتية لحماية الأمن الشخصي المعلوماتي.

المبحث الأول: الآليات الإجرائية لحماية الأمن الشخصي المعلوماتي

وضع المشرع الجزائري تدابير إجرائية لحماية الحريات وصون الحقوق وذلك من خلال السماح للجهات المختصة بالتفتيش ولو عن بعد في المنظومة المعلوماتية أو جزء منها للمتابعة مرتكبي جرائم المساس بالأمن الشخصي المعلوماتي، وذلك للحفاظ على الأمن والنظام العام، ولذلك سنحاول من خلال هذا المبحث التطرق إلى الآليات التي كرسها المشرع الجزائري للمكافحة الجريمة المعلوماتية، هذا ما سنتناوله في هذا المبحث من خلال المطالب التالية:

- المطلب الأول: جهات البحث والتحقيق عن جرائم المساس بالأمن الشخصي المعلوماتي.
- المطلب الثاني: خصوصية القواعد القانونية الإجرائية لحماية الحياة الشخصية.

المطلب الأول: جهات البحث والتحقيق عن جرائم المساس بالأمن الشخصي المعلوماتي

إن وحدات الأمن الوطني المتخصصة في مكافحة الجرائم الإلكترونية تستعد للتصدي لهذا النوع من الإجرام، وذلك من خلال وحدات متخصصة في مكافحة هذه الجريمة والتي تتمثل في جهازين الشرطة الجزائرية والدرك الوطني.

الفرع الأول: دور الشرطة القضائية في متابعة مرتكبي جرائم المساس بالأمن الشخصي المعلومات

تلعب الشرطة القضائية دورا مهما في المجتمع الرقمي نتيجة انتشار استخدام التكنولوجيا الحديثة، ونظرا للاعتداءات التي تطال الحياة الخاصة المعلوماتية وما ترتب على ذلك من قضايا ومنازعات في هذا الشأن.

أولا: الشرطة الجزائرية

تلعب الشرطة دورا هاما في ملاحقة مرتكبي جرائم المساس بالأمن الشخصي المعلوماتي والقبض على مقترفيها، والحد منها حفظا لكرامة حقوق وحريات الأفراد وذلك

بالتصـــدي لهذه الجرائم بكفاءة من أجل الضـــبط الجيد للأمن[1]"و حفظ النظام العام، وأداء جميع المهام المسندة للأمن الوطني كما حددها التشريع والتنظيم المعمول بهما"[2].

ولأجل التصـــدي لكل أنواع الجرائم الإلكترونية، والتي تعد نتاج العجز الحاصـــل على المســـتوى الدولي والوطني في مجال تكنولوجيا الاعلام والاتصـــال، وضـــعت مديرية الأمن الوطني اسـتراتيجية أمنية ذو كفاءة عالية، بتوفير كل الإمكانيات البشـرية والوسـائل المتاحة لها لحماية المصلحة العامة والخاصة [3].

فتتمثل آليات مكافحة الجريمة المعلوماتية التي اعتمدتها الشرطة الجزائرية فيما يلي:

- ✓إنشاء تشكيل عملياتي متخصص في محاربة الجريمة المعلوماتية.
- ✓التكوين المتخصص لإنجاز متطلبات الاحترافية في الأداة.
- ✓تكوين متخصص في الجرائم المعلوماتية.
- ✓تكوين إطارات متخصص على المستوى الدولي.
- ✓القيام بحملات التوعية والتحسيس[4].

كما خصصت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة، ومخابر جهوية في كل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، إضـافة الى ذلك يوجد على مسـتوى مراكز الأمن الولائي فرق

---

[1]– نعيمة براردي، الاتصـــال بين الشـرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراســة تحليلية اسـتطلاعية بالجزائر العاصمة)، أطروحة دكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر03، السنة الجامعية 2012-2013، ص117.

[2]– المادة 2 من المرســـوم التنفيذي رقم 10-322 المؤرخ في 16 محرم عام 1432 الموافق 22 ديســـمبر ســـنة 2010، المتضـمن القانون الأسـاسـي الخاص بالموظفين المنتمين للأسـلاك الخاصـة بالأمن الوطني، الصـادر بال ج ر، العدد 78، بتاريخ 26 ديسمبر سنة 2010، ص 04.

[3]– حســين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شــهادة الدكتوراه، جامعة باتنة 1، كلية الحقوق والعلوم السياسية، السنة الجامعية 2015-2016، ص 175.

[4]– كمال عمتوت، دور الشـــرطة الجزائرية في الوقاية من الجريمة المعلوماتية ومكافحتها، مجلة القراءة القانونية الدولية، جامعة طاهري محمد ، العدد 02، بشار، السنة 2020، ص 54-55-56.

متخصصة، تتولى أعمال البحث والتحري في الجرائم الإلكترونية حيث تعمل بالتنسيق مع تلك المخابر [1].

من خلال ما وصلت إليه الشرطة الجزائرية من نتائج ونمو في التصدي للجريمة الإلكترونية، كان ذلك محط إشادة من بعض الشخصيات ومنها ما ورد ذلك في تصريح للسيد " مانغ هانغواي" رئيس منظمة الانتربول، خلال زيارة العمل التي قام بها الجزائر في شهر ماي سنة 2018، ودعا من خلال هذا التطور الملحوظ إلى تعزيز التعاون وتفعيل آليات تبادل الخبرات المعلوماتية من أجل ضمان الكفاءة العالية والتطور المستمر للمواجهة مختلف اشكال الجرائم المستحدثة وخاصة التي تمس بسلامة وسرية الامن الشخصي المعلوماتي[2].

ثانيا: الدرك الوطني

تعد الجريمة الإلكترونية من التحديات الكبرى في هذا العصر وذلك نتيجة التطورات السريعة والتحولات الرقمية التي يشهدها العالم بشكل عام والمجتمع الجزائري بشكل خاص، حيث يكمن دور الدرك الوطني في رصد جميع الهجمات الإلكترونية القادمة من الداخل ومن جميع أنحاء العالم على الشبكات الوطنية والأنظمة المعلوماتية[3]، حيث تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني، وذلك حسب الاختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث مستويات مركزية، جهوية، محلية وذلك للتسيير مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على رقابة مختلف الشبكات، والتعرف على جل الجرائم المرتكبة على شبكة الأنترنت[4].

---

[1]– نوال معزوزي، " الطبيعة الخاصة للجريمة المعلوماتية "، ملتقى القيت في الملتقى الوطني الموسوم ب " الجرائم المستحدثة وآليات مكافحتها "المنظم من قبل مخبر بحث نظام الحالة المدنية بالتعاون مع كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة، يومي 06-05 ماي 2019، ص 50.

[2]– خضرة شنتيرة، الآليات القانونية لمكافحة الجريمة الإلكترونية – دراسة مقارنة–، مؤسسة الكتاب القانوني، ط1، السنة 2022، ص207.

[3]– https://radioalgerie.dz/ الساعة 2023/05/03، تاريخ الاطلاع 20 :30.

[4]– حسين ربيعي، المرجع السابق، ص 183.

يقوم جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل، وذلك من خلال إنشاء مدارس ومعاهد لهذا الغرض كمدرسة الشرطة القضائية التابعة للدرك الوطني [1]، والمعهد الوطني للشرطة القضائية والذي تم إنشاؤه سنة 1990 ليقوم بتكوين متخصصين في الشرطة القضائية وإجراء بحوث متعلقة بالظواهر الاجتماعية ذات الصلة بالجريمة، للمواكبة المستجدات الحديثة المتعلقة بالجرائم الإلكترونية وذلك في سبيل تعزيز ثقة الأفراد في جهاز الدرك الوطني[2] "إلا نه تمت عصرنة الدرك الوطني وإنشاء مصلحة مكافحة الإجرام السيبراني"[3].

من خلال ما سبق، نخلص إلى أن كل من جهازي الشرطة الجزائرية والدرك الوطني يسعان جاهدين للمواكبة هذا التطور للتحول الرقمي وذلك من خلال تطوير تقنيات التحقيق واستحداث وحدات خاصة نذكر منها: المصلحة المركزية لمكافحة الجرائم السيبرانية للدرك الوطني بالجزائر والمخبر المركزي للشرطة العلمية، والقيام بحملات التوعية للتذكير بمدى خطورة الجريمة الإلكترونية من خلال وسائل الإعلام، وتعد هذه الاستراتيجية عامل أساسي للنجاح في مكافحة والحد من الجرائم الماسة بالأمن الشخصي المعلوماتي.

الفرع الثاني: انعقاد الاختصاص القضائي في جرائم المساس بالأمن الشخصي المعلوماتي

يقصد بالاختصاص القضائي في مجال الجرائم المعلوماتية هو تحديد الأجهزة المخول لها قانونا التحقيق فيها ومتابعة مرتكبيها، حيث استحدث المشرع الجزائري جهات قضائية متخصصة في مجموعة من الجرائم على سبيل الحصر والتي تمثل أهم صور الجرائم المستحدثة بموجب المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق والعدل [4]و هذا لتسهيل متابعة مرتكبي الجرائم المعلوماتية، حيث يساعد الاختصاص القضائي على

---

[1]– المادة 04 من مرسوم رئاسي رقم 08-151 المؤرخ في 26 ماي 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، المنشور (ج ر)، العدد 27، الصدر بتاريخ 28 ماي2008، ، ص04.

[2]– خضرة شنتيرة، المرجع السابق، ص 214-213.

[3] - https://elmawkie.dz/، تاريخ الاطلاع 03/05/2024 , الساعة 21: 15.

[4]– المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجهورية وقضاة التحقيق معدل، المنشور (ج ر)، العدد 63، الصادرة بتاريخ 8 أكتوبر 2006.

تحقيق السرعة في حسم القضايا الجزائية المتعلقة بالأمن الشخصي المعلوماتي وعدم تراكمها مع تزايد العديد مثل هذه القضايا في الوقت الراهن، وهذا يعد ضمان للتصدي والحد من هذه الجرائم[1].

وفي مقابل ذلك للممارسة الضبطية القضائية اختصاصاتها ينبغي أن تلتزم بالضابط الإقليمي والنوعي حيث يتحدد الاختصاص المحلي في نطاق الدائرة التي يمارس فيها مهامها المعتادة إلا انه يسمح لهم في حالة الاستعجال أو طلب من السلطة القضائية أن يمارسوا مهامهم في كافة الإقليم الوطني كما أن تمديد الاختصاص المحلي فيها يختص بالجرائم الستة إلى كافة التراب الوطني استنادا للمادة 16 من ق ا ج [2].

إضافة إلى الاختصاص النوعي الذي يختص بالنظر إلى نوعية الجرائم التي يكون مختصين بها حيث حددت المادة 12 فقرة 03 من ق ا ج الاختصاصات التي تضمنت البحث والتحري، تلقي التبليغات والشكاوى إضافة إلى جمع الأدلة[3]، وفي مقابل ذلك استحدث المشرع الجزائري قطبا وطنيا متخصص لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب الأمر 21-11 المؤرخ في 25/08/2021 المتمم ق.إ.ج، و ذلك لمعالجة هذه الجرائم و منحه الاختصاص النوعي وذلك بموجب المادة 211 مكرر22 [4] و الاختصاص الإقليمي بموجب المادة 211 مكر23 [5].

استناد الى ما سبق، نخلص أن المشرع الجزائري وسع من نطاق الاختصاص القضاء الجزائري عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للبيانات الشخصية.

---

[1]–امنة بن طاهر، الأمن القضائي ودوره في مواجهة الجرائم المستحدثة " الجريمة المعلوماتية نموذجا "، مجلة البحوث القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، جامعة ام البواقي، المجلد 06، العدد 02، السنة 2023، ص 202، 203.

[2]– المادة 16 من الأمر 66-155، المؤرخ في 8 يونيو سنة 1966، المتضمن ق.إ.ج معدل ومتمم حسب أخر تعديل له الأمر 21-11، المؤرخ في 25 غشت 2021.

[3]–المادة 12 الفقرة 03 من ق.إ.ج.

[4]–المادة 211 مكرر 22 من ق.إ.ج.

[5]–المادة 211 مكرر23 من ق.إ.ج.

المطلب الثاني: خصوصية القواعد القانونية الإجرائية لحماية الحياة الشخصية

استحدث المشرع الجزائري إجراءات أخرى للمساعدة جهات التحقيق في الكشف عن الجريمة المعلوماتية التي تتلاءم مع طبيعة البيئة الرقمية، والتي تتمثل في الإجراءات التقليدية حيث تتجلى في الدليل الإلكتروني، المعاينة والتفتيش الإلكتروني أما الحديثة التي تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، التسرب الإلكتروني.

الفرع الأول: الآليات الإجرائية التقنية

تمثل هذه الآليات جزء لا يتجزأ من التحقيق في القضايا ومتابعة مرتكبي الجرائم، حيث كرس المشرع الجزائري جملة من الإجراءات التي من خلالها يتم مساعدة جهات التحقيق في الكشف عن الجريمة المعلوماتية وفقا للقانون والتي تتمثل في:

أولا: الدليل الإلكتروني

تعد الأدلة الالكترونية من أبرز تطورات العصر الحديث وجاءت لتواكب الثورة العلمية والتكنولوجية والتقنية، فالجرائم الالكترونية قد يتعذر اثباتها دون البحث والتحري عن الدليل الالكتروني لكونه ذو طبيعة خاصة علمية وفنية [1]، وعرفت الأدلة الإلكترونية كذلك بأنها الأدلة التي تتضمن كل البيانات الرقمية التي يمكن أن تؤكد أن هناك جريمة قد ارتكبت أو توجد صلة بين الجريمة والمتضرر منها، والمعطيات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها (النصوص المكتوبة، الرسومات، الخرائط، الصوت، الصورة)[2]

إن شرعية الدليل الإلكتروني تعد ضمانة أساسية للحماية وحفظ حقوق وحرية الأفراد، ضد تعسف السلطة في الحدود التي أقرها القانون ولأجل تمام وصحة إجراءات التحقيق لأنها تعد عامل أساسي في الكشف عن الجرائم والقبض على مرتكبيها كي ينتج عنها أدلة صحيحة وسليمة يعول عليها القضاء في إصدار أحكامه[3].

---

[1]– طاهر ياكر، الجرائم الإلكترونية – الأحكام الموضوعية والإجرائية–، دار بلقيس للنشر، الجزائر، 2024، ص 128.

[2]– عدنان، راضية سلام، شرعية الدليل الإلكتروني، جامعة النهرين، العراق، 2014، ص7، المرجع مشار إليه.

[3]– محمد المنصوري سلامة، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجيستر في القانون العام، كلية الحقوق –قسم القانون العام–، جامعة الإمارات العربية المتحدة، السنة 2018، ص 60-61.

ثانيا: المعاينة والتفتيش الالكتروني

تعتبر هذه التقنيات من أهم الإجراءات المتبعة في مكافحة الجرائم الماسة بالأمن الشخصي المعلوماتي.

1-المعاينة: " هي مناضـــرة ووصـــف وفحص للمكان الذي ارتكبت فيه الجريمة، أو لشـــيء أو لشـــخص له علاقة بالجريمة، كونها إجراء جائز في كافة الجرائم إلا في غالبية التشـــريعات تقتصـــرها على الجنايات والجنح الهامة دون المخالفات، وتعتبر وجوبية في الجنايات وجوازيه في الجنح والمخالفات."[1]، أما من ناحية موقع الجريمة تتمثل في تلك البصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية وذلك من خلال تفحص المواقع الإلكترونية التي زارها أو الملفات التي حملها، أو الرسائل المرسلة منه والواردة إليه وبالتالي فمسرح الجريمة تقع داخل الحاسوب والبيئة الرقمية[2]، ولأجل القيام بعملية المعاينة بشكل لصحيح لابد من مراعاة عدة ضوابط نذكر منها على سبيل المثال يجب الحرص على عدم إتلاف أي معطيات تم الحصـــول عليها من الجهاز، والتحقق من وجود نســـخة منها داخل الجهاز بنفسه، مع فحص جميع الملفات بعناية من أجل التعرف على الجهاز كافة العمليات التي قام بها المستخدم بالإضافة إلى المواقع الإلكترونية التي تم زيارتها[3].

2-التفتيش الإلكتروني: لقد ورد التفتيش الإلكتروني في القانون الجزائري في المادة 05 من قانون 09-04 [4]، ويقصـــد به تفتيش النظم المعلوماتية ولو عن بعد من خلال تجميع الأدلة المخزنة أو المســـجلة بشـــكل الكتروني مثل الملفات والبرامج المخزنة في الحواسيب والمعطيات والاتصالات الإلكترونية سواء كانت ذات طبيعة مادية أو معنوية تفيد

---

[1]- خضرة شنتيرة، المرجع السابق، ص 75.

[2]- خضرة شنتيرة، المرجع نفسه، ص71.

[3]-أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2015، ص134-135، المرجع المشار إليه.

[4]- المادة 05 من القانون 09- 04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، الصادرة في 16غشت سنة 2009.

في الكشـــف عن الحقيقة[1]، وعلى الجهات المخولة بالتفتيش مراعاة جملة من القواعد الموضوعية والشكلية وإلا كان التفتيش خالي من أي اثر قانوني.

و تتمثل القيود الموضـــوعية في ســـبب التفتيش، محل التفتيش، غاية التفتيش، الجهة المختصـــة بالتفتيش في الجرائم الإلكترونية أما القيود الشـــكلية تتمحور حول إجراء التفتيش بحضور أشخاص يحددهم القانون وتحرير محضر التفتيش ووقت تنفيذ التفتيش [2].

وانطلاقا مما سبق، لما تتميز به خصوصية الجرائم المعلوماتية الماسة بخصوصية الأشخاص أجاز المشرع الجزائري استعمال هذه الإجراءات لأنها تدخل ضمن أعمال التحقيق ولكن لا يفوتنا أن ننوه أن القائم بهذه الإجراءات يجب أن يكون ملما بتقنيات المعلوماتية المستحدثة.

الفرع الثاني: اجراءات التحري الخاصة

تعد هذه الإجراءات الحديثة تقنيات خاصة، تستخدمها الضبطية القضائية تحت المراقبة والإشراف المباشر للسلطة القضائية بقصد التحري والتحقيق عن الجرائم الخطيرة، وجمع الأدلة عنها والكشف عن مرتكبيها دون علم ورضا الأشخاص المعنيين، حيث حصرها المشرع الجزائري في أربعة أساليب تتمثل فيمايلي:

أولا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تعد هذه التقنيات التي وضعها المشرع الجزائري، ضمانا لحرمة الحياة الخاصة المعلوماتية وذلك للوصول إلى الحقيقة ويتم عن طريق سلطة ورقابة القضاء.

1-اعتراض المراســـلات: هي نوع من أنواع المراقبة الإلكترونية كونها رقابة مشـــروعة حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب الجريمة وهذا الاعتراض إما أحاديث أو مراســـلات مكتوبة أو مرئية أو أماكن اســـتنادا للمادة 65 مكرر 05 ق إ ج [3]،

---

[1]- ليندة مخلوفي علمي بومحراث، ضـــوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، مجلد 28، العدد01، ص392.

[2]-ليندة مخلوفي علمي بومحراث، المرجع نفسه، ص 393.

[3]-المادة 65 مكرر05 من ق.إ.ج.

بطريقة لا يحس بها الغير نظرا لما تمتاز به من خصوصية [1]، ويشترط في هذه العملية من الناحية الشكلية قيود تتمثل في الخصوصية والسرية أما من الناحية الموضوعية تتمثل في إذن مكتوب من الجهات القضائية المختصة، والتسبيب إضافة الى تحديد الجرائم محل الاعتراض والمراقبة في إطار ما نص عليه القانون[2].

2-تسجيل الأصوات والتقاط الصور:

يتم تسجيل الأصوات عن طريق وسائل الاتصال السلكية واللاسلكية ويتم بواسطتها مراقبة المحادثات بين الأشخاص والتنصت من خلال هذه الأجهزة، وتسجيلها بصفة سرية أما التقاط الصور فيقصد بها التقاط الصور للشخص أو عدة أشخاص يعتمدون في تثبيتها على تقنيات التصوير الفوتوغرافي أو الكاميرات الخفية مما يساعد على نسخها والاطلاع عليها[3].

ثانيا: التسرب الإلكتروني أو الاختراق:

تعد الجرائم الماسة بأنظمة المعالجة الالية للمعطيات واحدة من الجرائم التي أجاز المشرع أن يتم الاعتماد فيها على إجراء التسرب من أجل التحري وذلك بموجب المادة 65 مكرر05 ق ا ج، حيث عرف المشرع إجراء التسرب خلال المادة 65 مكرر 12 التي تتضمن في محتواها أنه إجراء مراقبة للأشخاص المشتبه في ارتكابهم الجريمة [4]، في ما يخص الحماية القانونية للمتسرب، فقد أولى القانون مجموعة الإجراءات التي تضمن له حياته وحياة عائلته وتيسر وتساعده على نجاح مهمته [5]وهذا ما نصت عليه المادة 65 مكرر 16ق ا ج [6].

---

(1)- خضرة شنتيرة، المرجع السابق، ص 133.

(2)- نوال مجدوب، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي مغنية، الجزائر، المجلد 06، العدد 03، السنة 2023، ص 203-202.

(3)- خضرة شنتيرة، المرجع نفسه، ص 140.

(4)- المادة 65 مكرر 05و12من ق.إ.ج .

(5)- خضرة شنتيرة، المرجع نفسه، ص 146.

6 - المادة 65 مكرر16 ق.إ.ج.

في واقع الأمر، نتيجة للتطور التكنولوجي والتحول الرقمي فقد ظهرت وسائل علمية للمساعدة في الكشف عن الجريمة، ومعرفة الحقيقة ويندرج فيها كل من اعتراض المراسلات والمراقبة الإلكترونية وإجراء التسرب وذلك لفعاليتها في الكشف عن الجريمة المعلوماتية.

المبحث الثاني: الآليات المؤسساتية لحماية الأمن الشخصي المعلوماتي

أمام مواجهة الاعتداءات التي تهدد خصوصية الأفراد سارع المشرع الجزائري إلى وضع آليات مؤسساتية للمواجهة هذه الانتهاكات، ومواكبة التطورات التكنولوجيا التي أسفرت على ضرورة وجود ترسانة قانونية للحماية الحياة الخاصة المعلوماتية من خلال هذه الآليات للمراقبة وحماية كل ما قد يهدد سلامتها.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

نظرا للخطورة الجرائم الإلكترونية، سارع المشرع الجزائري إلى تبني آليات مستحدثة في سبيل التصدي لها، وذلك بإصدار قانون خاص بالوقاية من الجرائم المعلوماتية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث يتكون من ستة فصول سعيا منه للسد الثغرات القانونية، حيث تسمح هذه القواعد بمتابعة مرتكبي الجرائم وتهدف للحماية المعطيات ذات الطابع الشخصي للأفراد والمؤسسات، نظرا للمدى أهميتها.

الفرع الأول: تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

تلعب الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها دور كبير في حماية الأمن الشخصي المعلوماتي، وبالرجوع إلى القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته[1]، نص المشرع الجزائري على إنشاء هذه الهيئة بموجب المادة13 بفقرتيها من القانون السالف الذكر [2]، وللتمكن من معرفة تشكيلة هذه الهيئة وكيفية سيرها جاء المرسوم الرئاسي رقم 20-183 ليعيد تنظيم هذه الهيئة وبمقتضى المادتين 02 و03 من ذات المرسوم تتمتع هذه الهيئة بالاستقلال المالي والإداري إضافة إلى الشخصية المعنوية التي توضع تحت سلطة رئيس الجمهورية، حيث يكمن مقرها بالجزائر وفي مقابل ذلك من ذات المرسوم الرئاسي السالف الذكر بموجب المادتين 05 و06 من

---

[1]- القانون 09- 04.

[2]- المادة 13 من القانون 09-04.

الفصـــل الثاني الذي يتضـــمن تنظيم وتشـــكيل الهيئة حيث أنها تتكون من مجلس التوجيه ومديرية عامة[1].

الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في التصدي للجرائم الماسة بالأمن الشخصي المعلوماتي

بالنسـبة لمهام الهيئة فقد تنصـت عليها في المادة 14 من القانون 09-04 المتضـمن القواعد الخاصـة للوقاية من الجرائم المتصـلة بتكنولوجيا الإعلام والاتصـال ومكافحتها، والتي تتضمن :

✓تنشـيط وتنسـيق عمليات الوقاية من الجرائم المتصـلة بتكنولوجيا الاعلام والاتصـال ومكافحته.

✓مسـاعدة السـلطات القضـائية ومصـالح الشـرطة القضـائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز خبرات القضائية.

✓تبادل المعلومات مع نظيرتها في الخارج قصـــد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتحديد مكان تواجدهم[2].

وبالعودة للمرسـوم الرئاسـي رقم 20-183، والذي يتضـمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيا الإعلام والاتصـال ومكافحتها، نجد المشـرع الجزائري قد نص في المادة الرابعة04 من ذات المرسوم نذكر منها:

✓اقتراح عناصـر الاسـتراتيجية الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[1]- المرسـوم الرئاسـي 20-183، المؤرخ في 13 يوليو 2020، المتضـمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الصادرة ب (ج ر رقم 40)، الصادرة في 18 يوليو 2020.

[2]- المادة 14 من القانون 09-04.

✓تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية[1].

وانطلاقا مما سلف، في سبيل مكافحة الجرائم الماسة بالأمن الشخصي المعلوماتي وضع المشرع الجزائري آليات مؤسساتية منظمة لهذا المجال، التي من بينها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، التي يكمن دورها في متابعة العمليات الوقائية لهذه الجرائم مما يدعم السلطات الأمنية والقضائية في البحث والتحري.

المطلب الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

أنشئ القانون ألية مؤسساتية مستقلة تتضمن 76 مادة بها، قواعد قانونية تتعلق بحماية المعطيات الشخصية من الانتهاكات التي قد تطال الحياة الشخصية المعلوماتية وذلك تكريسا للمنظومة الحقوقية واحترام كرامة وخصوصية الأفراد.

الفرع الأول: النظام القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي والمهام المسندة اليها

أقر المشرع الجزائري للسلطة الوطنية للحماية المعطيات الشخصية التنظيم القانوني الخاص بها، إضافة إلى جملة من المهام الواجب إتباعها.

أولا: التنظيم القانوني للسلطة الوطنية

أنشئ القانون ألية مؤسساتية من أجل حماية حقوق الإنسان وحفاظا على كرامة خصوصية المعطيات الشخصية وذلك من خلال القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي في احداث السلطة الوطنية لحماية المعطيات والغرض منها وضع قواعد وقيود لحماية البيانات الشخصية وترسيخ للمبادئ

[1]- المادة 04 من المرسوم الرئاسي 20-183.

جديدة بمقتضـــى هذا القانون[1] وبموجب المادة 22 من نفس القانون يتبين من خلالها أن السـلطة الوطنية تتمتع بالطابع المسـتقل لها سـواء من الناحية الإدارية فهي لا تخضـع لأي رقابة هرمية أو من الناحية المالية فهي تؤمن المصـــادر المالية اللازمة لمزاولة نشـــاطها والاستقلالية في استخدام تلك المصادر بما يخدمها[2].

وفي نفس السياق تتكون السلطة الوطنية من 16 عضو، من بينهم رئيسها حسب نص المادة 23 من نفس القانون معينون بالمرسوم الرئاسـي22-187 الذي يتضـمن تعيين رئيس وأعضـاء السـلطة الوطنية لحماية المعطيات ذات الطابع الشـخصـي[3] كما يتم انتقائهم بناءً على قدراتهم في الميادين القانونية والتقنية في مجال البيانات الشخصية، كما يمكن الاستعانة بأي شـــخص يتميز بمؤهلات ومهارات تقنية وعلمية في المجالات للإفادة الســـلطة الوطنية بخبراته ومسـاعدتها في أعمالها[4]، حيث يقوم أعضـاء هذه السـلطة بتأدية اليمين الذي يعد التزام وشـرف تقوم عليه الأخلاقيات وتفرضـه القوانين وحفاظهم على الطابع السـري للبيانات الشخصية وهذا ما تبينه المادتين 24 و25 من نفس القانون[5].

كما أوجبت المادة 27 على الأمين التنفيذي ومستخدمو الأمانة التنفيذية الالتزام بسرية المعلومات التي يقوموا بالاطلاع عليها حتى بعد انتهاء مهامهم، وفي إطار ممارسـة السـلطة الوطنية للتأدية مهامها قامت بإنشـــاء الســـجل الوطني لحماية المعطيات، الذي يعد وســـيلة تنظيمية لحماية حقوق الأشـخاص ومعطياتهم الشـخصـية بطريقة امنة وفعالة ومنع اسـتغلال تلك البيانات الشـخصـــية بدون تصـــريح مسـبق، وهذا اسـتنادا للمادة 28 من نفس القانون واســـتخلاص لما تم ذكره فيها، ان تقيد الملفات التي تكون الســـلطات العمومية والخواص

---

[1]– عائشـــة بن قارة مصـــطفى، آليات حماية المعطيات ذات الطابع الشـــخصـــي بالتشـــريع الجزائري وفقا لأحكام القانون 18-07، مجلة العلوم القانونية والسـياسـية، مجلد 10، العدد 01، جامعة عبد الحميد بن باديس مسـتغانم، السـنة 2019، ص784.

[2]– المادة 22 من القانون رقم 18-07.

[3]– المادة 23 من القانون رقم 18–07.

[4]– خضرة شنتيرة، المرجع السابق، ص 184.

[5]– المادتين 24 و25 من القانون رقم 18–07.

مســـؤولة عن معالجتها والملفات اللازمة للترخيص للأشـــخاص المعنيين بمزاولة حقوقهم المنصوصة طبقا للقانون، وتقيد التصريحات والتراخيص المقدمة من طرف السلطة[1].

ثانيا: المهام المسندة للسلطة الوطنية

أسند المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مهام حيث يمكن تقسيمها الى ستة محاور بموجب المادة 25 من القانون السالف الذكر:

- الإخبار والتحسيس والتي تضم الفقرة (2).
- الاستشارات والاقتراحات والتي تضم الفقرات (3)، (8)، (10).
- الطعون والشكاوى والتي تضم الفقرة (4).
- التراخيص والتي تضم الفقرات (1)، (5)، (9).
- الحماية والتي تضم الفقرات (6)، (12)، (13).
- العقوبات التي تضم الفقرتين (11)، (7)[2].

كما يجب على رئيس وأعضـــاء الســـلطة الوطنية المحافظة على ســـرية البيانات الشخصية، بعد الانتهاء من مهامهم في إطار ما ينص عليه القانون، ونظرا للخطورة موضوع الأمن الشخصي المعلوماتي سعت الدولة للحماية الرئيس وأعضاء السلطة الوطنية من كل أشكال الضغط والتهديد التي قد يتعرضوا لها أثناء ممارسة مهامهم بموجب المادة 26 من القانون الذي تم ذكره[3].

الفرع الثاني: حقوق والالتزامات المرتبطة بمعالجة المعطيات الشخصية

أقر المشرع الجزائري قواعد لحماية الأشخاص الطبيعيين في معالجة البيانات الشخصية وذلك للضمان الحماية الفعالة لمعطياتهم الشخصية، والسماح لهم بالسيطرة عليها والالتزام بالمبادئ المنصوص عليها في القانون.

---

[1]– المادة 28 من القانون رقم 18–07.

[2]– المادة 25 القانون رقم 18–07.

[3]– المادة 26 من القانون رقم 18–07.

أولا: تحديد حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي

عدد المشـرع الجزائري في القانون 18-07 المتعلق بحماية الأشـخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي جملة من الحقوق وهي:

1.الحق في الإعلام: وفقا للمادة 32 من القانون رقم 18-07، فإن كل شـخص يحق له الحصول على المعلومات ومعرفة كافة الإجراءات المتعلقة بهذه العملية، ما لم يثبت علمه المسبق والمتمثلة في العناصر التالية، هوية معالج البيانات وعند الاقتضاء ممثله، الغاية من المعالجة أو أي معلومات إضافية مفيدة لاسيما المتلقي والالتزام بالرد وعواقبه وكذلك حقوقهم ونقل البيانات إلى الخارج.

ويسـتثنى من مجال إلزامية الإعلام تطبيقا للمادة 33 من نفس القانون، إذا تعلق الأمر بمعالجة المعطيات الشخصية لأغراض إحصائية أو تاريخية أو علمية او صحفية أو فنية أو أدبية او إذا كانت الحالة تمت فيها المعالجة نصت عليها النصوص التشريعية[1].

2.الحق في الولوج: استنادا للمادة 34 من نفس القانون فإن هذا الحق يسمح للشخص المعني بالاستفسار عن ما إذا تمت معالجة بياناته ام لا والغاية من المعالجة وفئات البيانات التي انصبت عليها وأيضا المرسل إليهم واعلامه بشأن البيانات التي تخضع لهذه المعالجة ومصدرها، كما يحق للمسؤول عن المعالجة الاعتراض على الطلبات التعسفية بشأن عددها وطابعها المتكرر وذلك من خلال تقديم طلب للسـلطة الوطنية لتحديد اجال الإجابة على طلبات الوصول المشروعة.[2]

3.الحق في التصحيح: بموجب المادة 35 من القانون 18-07 يحق للشخص المعني أن يتوجه إلى المسؤول عن المعالجة أو إيداع طلب التصـحيح لدى السـلطة الوطنية وذلك لتصـحيح المعطيات التي قد تكون غير صـحيحة (العمر أو العنوان الخاطئ) أو إتمامها مثلا العنوان بدون رقم [3]أو تحديث أو حذف ما يكون غير مطابق مع القانون الجديد وتجدر بنا الإشـارة إلى ان هذه الإجراءات من غير تكلفة واجلها 10 أيام من الاعلام أما في حالة

[1]– المادتين 32 و33 من القانون 18-07.

[2]– المادة 34 من القانون 18-07.

[3]–https://www.gaan.dz/، تاريخ الاطلاع 10-05-2024، الساعة 00 :11.

الرفض فيكون إيداع طلب التصحيح لدى السلطة الوطنية وتكلفة احد أعضائها بالقيام بهذا الاجراء ويتعين على المسؤول عن المعالجة أو السلطة الوطنية اعلامه بكل التدابير المتخذة بشأن هذا التصحيح إضافة إلى ذلك ان هذا الحق يمكن استعماله من طرف الورثة[1].

4.الحق في الاعتراض: من منطلق المادة 36 من نفس القانون، يحق للمعني بالأمر الاعتراض على معالجة بياناته الشخصية وذلك لأسباب مشروعة وجدية وإذا لم تستعمل في إطار ما نص عليه القانون، كما يحق له الاعتراض على إحالة معطياته الشخصية إلى الغير لاستعمالها لأغراض دعائية وتجارية، كما لا يجوز ان يمارس هذا الحق عندما تفي معالجة بياناته التزام قانوني، وتجدر بنا الإشارة على أن هذا الحق من الممكن ممارسته في أي مرحلة من مرحلة جمع البيانات[2].

5.منع الاستكشاف المباشر: لقد عرف المشرع الجزائري هذا الحق في المادة 03 من القانون 18-07 وأكدته المادة 37 من نفس القانون، حيث منع التنقيب المباشر بأي وسيلة كانت أو بواسطة استعمال التكنولوجيا وهذا حماية للبيانات الشخصية والحق في الخصوصية المعلوماتية، كما أجاز المشرع الجزائري في المادة 37 الفقرة 02 من نفس القانون على استعمال هذا الحق عن طريق البريد الإلكتروني إذا ما توافرت فيه الشروط التي تتمثل في ما إذا ما طلبت البيانات مباشرة من المرسل اليه أو ان يكون بمناسبة تقديم عمليات خدماتية او من خلال نفس الشخص الطبيعي أو المعنوي الذي يقوم بخدمات مشابهة او في حالة الاعتراض عند ارسال الرفض كما يمنع إخفاء هوية الشخص الذي أوصلت اليه الرسائل، وهذا لتوفير اكبر قدر من الحماية للأشخاص المعنين[3].

ثانيا: تحديد التزامات المسؤول عن المعالجة

لقد حدد المشرع الجزائري جملة من الالتزامات التي تقع على مسؤولية المسؤول عن المعالجة و التي تتمثل في:

---

[1]– المادة 35 من القانون18-07 .

[2]– المادة 36 من القانون 18-07.

[3]– المادتين 03 و37 من القانون 18-07.

1. **سرية وسلامة المعالجة:** وفق احكام قانون 18-07 تنص المادة 38 منه على أن يلتزم المسؤول عن المعالجة باتخاذ التدابير اللازمة من أجل حماية المعطيات والحفاظ على سلامتها، من الإتلاف أو الضياع أو النشر... وحمايتها من أي شكل من أشكال المعالجة غير المشروعة[1]، غير أن التدابير التقنية والتنظيمية تعد من العوامل الرئيسية للضمان الحماية الفعالة [2].

2. معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكتروني:

يلتزم مؤدون خدمات التصديق الإلكتروني بمعالجة المعطيات الشخصية لأغراض التسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص الذين لهم صلة مباشرة، كما لا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها، ماعدا في حالة موافقتهم الصريحة وهذا حسب ما جاءت به نص المادة 42 من القانون السالف الذكر.[3]

3. معالجة المعطيات الشخصية ذات الطابع الشخصي في مجال الاتصالات الإلكترونية:

في حالة لم تقرر السلطة الوطنية الضمانات اللازمة لحماية البيانات انه قد تم اتخاذها من قبل مقدم الخدمات، يجب اعلام السلطة الوطنية والشخص المعني فور حدوث اختلالات في البيانات من ضياع او اتلاف أو ولوج غير مصرح به، أسفر إلى المساس بخصوصية الشخص المعني استنادا لم تم ذكره في المادة 42 من القانون السلف الذكر [4].

4. نقل البيانات نحو دول الخارج:

تسمح السلطة بنقل المعطيات عبر الحدود خارج الجزائر إلى الجهة المتلقية بعد ضمان خصوصية الأفراد وحماية بياناتهم ومعالجتها، إلا في الأغراض المصرح به[5].باستثناء أحكام

---

[1]– المادة 38من القانون 18-07.

[2]– دليل نظام حماية البيانات الشخصية، الهيئة السعودية للبيانات والذكاء الاصطناعي، السنة 2023، ص27 .

[3]– المادة 42 من القانون 18-07.

[4]– نفس المادة نفس القانون.

[5]– دليل عملي: انشاء إطار عمل للخصوصية وحماية البيانات، مجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال افريقيا، السنة 2021، ص27.

المادة 44 من القانون 18-07 حيث يمكن نقل البيانات إلى بلد اخر دون إجراءات الحماية إلى في الحالات التي نص عليها القانون نذكر منها :

- في حالة الموافقة الصريحة من طرف الشخص المعني بالنقل.
- بناء على الحصول على ترخيص من السلطة.
- إذا كان النقل تنفيذا لإجراءات تعاقدية [1].

خلاصة القول أن المشرع الجزائري حاول من خلال قانون 18-07 انشاء هيئة تتميز بالاستقلال المالي والإداري وتتمتع بالشخصية المعنوية للحماية الأشخاص الطبيعيين في مجال المعلوماتية، فأقر جملة من الضوابط والقيود التي من شأنها أن يتعرض لها الفرد أثناء استخدامه للمجال المعلوماتي ابتداء بالمبادئ الأساسية لحماية المعطيات الشخصية إلى الأحكام الإدارية والجزائية.

[1]– المادة 44 من القانون 18-07.

خلاصة الفصل الثاني

من خلال هذا الفصل تناولنا الأليات العملية للحماية الأمن الشخصي المعلوماتي التي تعد اليات ردعية مهمة في وجه الأفعال الإجرامية المرتكبة في حق المجتمع المعلوماتي، إلى جانب الأليات الإجرائية المعتمدة للمتابعة مرتكبي جرائم المساس بأمن الشخصي المعلوماتي حيث تمثل إحدى السبل المهمة التي يمكن من خلالها الكشف عن الجريمة خاصة، وإن تمت وفقا للقانون.

من هذا المنطلق، أولى المشرع الجزائري أهمية بالغة للحماية البيانات الشخصية وتجلت هذه الأهمية في إنشاء اليات مؤسساتية تساهم في الوقاية والحد من هذه الجرائم والتي تتمثل في انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إضافة إلى القطب الجزائي المتخصص في هذه الجرائم، إلى جانب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بالإضافة الى جهاز الشرطة القضائية الذي يعمل إلى جانب الوحدات التابعة لأسلاك الأمن الوطني، الدرك الوطني وكذا رجال القضاء.

حيث تساعد هذه الآليات العملية المراقبة والمتابعة بشكل مستمر في الكشف عن مخاطر معالجة البيانات الشخصية المحتملة.

خاتمـــــــــة

بتحليل عناصـــر الدراســـة، وإجابة عن الاشـــكالية المطروحة، وترابطا مع الأهداف المسطرة توصلنا **للنتائج** التالية:

✓ أورد المشـرع الجزائري آليات للحماية الجزائية اسـتباقية، لمواجهة الاعتداءات والتجاوزات التي تمس بخصـوصـية الأفراد في مجال المعلوماتية، وذلك عن طريق الحماية الموضـوعية في جانبها الوقائي، فلقد أقر المشـرع الجزائري مجموعة من النصـوص القانونية التي تحمي خصـوصـــية الأشـــخاص المعلوماتية، من بينها قانون 18-07 المتعلق بحماية المعطيات الشـخصـية ذات لطابع الشـخصـي، الذي يوضـح الحقوق التي يتمتع بها أصـحاب البيانات الشخصية بموجب هذا القانون، كحق الاعلام والتصحيح وغيرها إضافة الى القانون المتعلق بالتوقيع الإلكتروني ليقر الحماية القانونية للبيانات الشـــخصـــية التي يتم تداولها في نطاق التعاملات الإلكترونية.

✓ كما رسـم سـياسـة ردعية من خلال تجريم كل مسـاس بحياة الخاصـة المعلوماتية يقابله عقوبة لكل من يتعدى على هذه الخصـوصـية، ومن صـور التجريم المعلوماتي الاعتداءات التي تطال الحياة الشـخصـية المعلوماتية الواردة منها في قانون العقوبات، ويجدر بنا الإشـارة إلى التعديل الأخير ق.ع، 24-06 الذي نص على بعض الانتهاكات بين التشديد والتخفيف ووســع نطاق الحماية الجزائية للأشــخاص وذلك لتحقيق الحماية الفعالة للأمن الشــخصــي المعلوماتي، كما أن هناك صـور أخرى لتجريم واردة خارج نصـوص ق.ع، منها ما تم النص على بعض هذه الجرائم في القانون 18-07 .

✓ تبني آليات يتم على أســاســها تحقيق التوازن بين حماية الخصــوصــية الفردية وتطبيق الإجراءات الجزائية، فالمكافحة الفعالة لهذه الاعتداءات يقتضــي اســتخدام أســاليب التحري والتحقيق المتطورة للكشف عن هذه الجريمة والتجاوزات.

✓ وللحفاظ على الأمن الشــخصــي المعلوماتي، تم وضــع قيود وضــوابط تمنع من انشــاء ومعالجة البيانات الشـخصـية دون ترخيص، تحت اشـراف السـلطة الوطنية لحماية المعطيات ذات الطابع الشخصي التي تتولى مراقبة المعالجة الالية للبيانات الشخصية .

تكملة للنتائج المتوصل إليها نورد **الاقتراحات** التالية:

- تنمية الوعي المجتمعي بشأن المخاطر التي تهدد الحياة الشخصية المعلوماتية، وذلك من خلال إنشاء دليل لحماية نظام البيانات الشخصية، على أن يتضمن مبادئ حماية البيانات الشخصية، معرفة البيانات التي يتم جمعها، صور الانتهاكات والعقوبات التي تترتب على هذه الجريمة، وضع التدابير التقنية والتنظيمية، نقل البيانات الشخصية خارج الجزائر، الآليات المؤسساتية لحوكمة البيانات الشخصية، تحت شعار ثقافة ووعي ومعرفة بالتعامل مع البيئة الرقمية .
- تعزيز الأمن الرقمي، من خلال اعتماد المؤسسات والأفراد على مجموعة من الإجراءات التي يجب تبنيها للحد من مخاطر انتهاكات الخصوصية الشخصية المعلوماتية، وذلك من خلال تحديثات برامج الحماية، التغيير الدوري لكلمات المرور وفرض استخدام كلمات مرور قوية ومعقدة، التحقق من موثوقية وصحة رسائل البريد الإلكتروني، الإبلاغ الفوري عن أي انتهاكات.
- توفير التقنيات والكتب وتطوير المواقع الإلكتروني الخاصة بالمحاكم القضائية ومنظومة الأمن، وذلك لتعزيز دراسات الباحثين بأحكام قضائية واحصائيات بشأن المجال المعلوماتي.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: قائمة المصادر:

أ. الدستور

1. المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، (ج ر) رقم 82 الصادرة سنة 2020.

ب. القوانين والأوامر والمراسيم التنفيذية:

1. الأمر 66-155 المؤرخ في 8 يونيو سنة 1966، المتضمن ق.إ.ج معدل ومتمم بـ: الأمر 21-11، المؤرخ في 25 غشت 2021، الجريدة الرسمية العدد 65، الصادرة 26غشت 2021.
2. الأمر 66-156 المؤرخ في 8 يونيو سنة 1966، المتضمن ق.ع معدل ومتمم بـ:
   - قانون 21-14، المؤرخ في 28 ديسمبر 2021، الجريدة الرسمية العدد99، الصادر بتاريخ 29 ديسمبر 2021.
   - قانون رقم24 -06 المؤرخ في 28 ابريل 2024، الجريدة الرسمية العدد 30، الصادر بتاريخ 30 أفريل 2024.
3. قانون 09-04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، الصادر بتاريخ سنة 2009.
4. قانون 15-04، المؤرخ في اول فبراير 2015، المتضمن بتحديد القواعد العامة المتعلقة بتوقيع والتصديق الالكترونيين، (ج ر) رقم 06، الصادر بتاريخ 10 فبراير 2015.
5. قانون رقم 18-04 المؤرخ في 10 مايو 2018، المتعلق بتحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر (27)، الصادر بتاريخ 13 ماي2018 .
6. قانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين مجال المعطيات ذات الطابع الشخصي، ج ر (34)، الصادر بتاريخ 10 يونيو 2018.
7. مرسوم رئاسي رقم 08-151المؤرخ في 26 ماي 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، المنشور (ج ر)، العدد 27، الصادر بتاريخ 28 ماي2008.

8. المرسوم الرئاسي 20-183، المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الصادرة ب (ج ر رقم 40)، الصادرة في 18 يوليو 2020.
9. المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجهورية وقضاة التحقيق معدل، المنشور (ج ر)، العدد 63، الصادرة بتاريخ 8 أكتوبر 2006.
10. المرسوم التنفيذي رقم 10-322 المؤرخ في 16 محرم عام 1432 الموافق 22 ديسمبر سنة 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، الصادر بال ج ر، العدد 78، بتاريخ 26 ديسمبر سنة 2010.

ثانيا: قائمة المراجع:

أ. الكتب:

1. أنطونيوس أيوب بولين، الحماية القانونية للحياة الشخصية في مجال المعلوماتية – دراسة مقارنة –، منشورات الحلبي الحقوقية، لبنان، ط1، السنة 2009.
2. بوبكر رشيدة، الحماية الجزائية للتعاملات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، السنة 2020.
3. الخلف علي حسين، الشاوي عبد القادر سلطان، المبادئ العامة في قانون العقوبات، بغداد (العراق)، المكتبة القانونية للنشر والتوزيع، السنة 2011.
4. الزعبي علي أحمد، حق الخصوصية في القانون الجنائي – دراسة مقارنة–، المؤسسة الحديثة للكتاب، طرابلس، ط1، السنة 2007.
5. الزيدي وليد، القرصنة على الأنترنت والحاسوب، دار أسامة للنشر والتوزيع، ط1، عمان، السنة 2003.
6. زين العابدين صالح مروة، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، ط1، السنة 2016.
7. شنتيرة خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية – دراسة مقارنة–، مؤسسة الكتاب القانوني، ط1، السنة 2022.

8. الشـوابكة محمد أمين، جرائم الحاسـوب والأنترنت – الجريمة المعلوماتية–، دار الثقافة للنشر والتوزيع، عمان، ط1، السنة 2007.
9. الطحطاوي أحمد يوســـف، الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراســـة مقارنة)، دار النهضة العربية، القاهرة، السنة 2015.
10. عدنان، ســلام راضــية، شــرعية الدليل الإلكتروني، جامعة النهرين، العراق، الســنة 2014.
11. مصـري عبد الصـبور عبد القوي على ، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض، ط1، السنة 2012.
12. المومني عبد القادر نهلا، الجرائم المعلوماتية، دار الثقافة للنشـر والتوزيع، الأردن، ط1، السنة 2008.
13. ياكر طاهر، الجرائم الإلكترونية – الأحكام الموضـــوعية والإجرائية–، دار بلقيس للنشر، الجزائر، السنة 2024.

ب. المقالات العلمية:

1. بن طاهر امنة، الأمن القضـــائي ودوره في مواجهة الجرائم المســـتحدثة " الجريمة المعلوماتية نموذجا "، مجلة البحوث القانونية والاقتصـــادية، كلية الحقوق والعلوم السياسية، جامعة ام البواقي، المجلد 06، العدد 02، السنة 2023.
2. بن عودة يوسـف سـليمان، الجرائم الماسـة بحرمة الحياة الخاصـة التي تقع عبر وسائل التقنية المعلومات الحديثة، كلية الرافدين الجامعة، قسم قانون، المجلد 16، العدد 29–30، السنة 2018.
3. بن قارة مصـطفى عائشـة، آليات حماية المعطيات ذات الطابع الشـخصـي في التشـريع الجزائري وفقا لأحكام القانون 18–07، مجلة العلوم القانونية والسـياسـية، مجلد 10، العدد 01، جامعة عبد الحميد بن باديس مستغانم، السنة 2019.
4. بومحراث خلوفي علمي ليندة، ضـــوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، جامعة الأمير عبد القادر للعلوم الإســـلامية قســـنطينة، مجلد 28، العدد01، السنة 2024.

5. حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية – قراءة في أحكام المرسوم الرئاسي 20/05، مجلة الحقوق والعلوم الإنسانية، العدد03، جامعة بومرداس، الجزائر، السنة 2020.
6. رحال عبد القادر، البناء القانوني لجريمة التقاط الصورة ونشرها في التشريع الجزائري والفرنسي – دراسة موضوعية إجرائية مقارنة–، المجلد 15، العدد 01، الجزائر، السنة 2022.
7. طباش عزالدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري– دراسة في ظل قانون 18–07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد 02، بجاية، السنة 2018.
8. عمتوت كمال، دور الشرطة الجزائرية في الوقاية من الجريمة المعلوماتية ومكافحتها، مجلة القراءة القانونية الدولية، جامعة طاهري محمد –بشار–، السنة 2020.
9. مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي مغنية، الجزائر، المجلد 06، العدد 03، السنة 2023.
10. مشتة نسرين، اخلاص بن عبيد، الحماية القانونية للمعطيات الشخصية في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، مجلد 06، العدد 01، باتنة، السنة 2021.
11. هارون نورة، برازة وهيبة، حق الفرد على صورته بين مقتضيات الحق في حرمة الحياة الخاصة وضرورات الكشف عن الجريمة، المجلد 35، العدد 03، بجاية (الجزائر)، السنة 2021.

ت. الملتقيات :

1. معزوزي نوال، " الطبيعة الخاصة للجريمة المعلوماتية "، ملتقى ألقيت في الملتقى الوطني الموسوم ب " الجرائم المستحدثة وآليات مكافحتها "المنظم من قبل مخبر

بحث نظام الحالة المدنية بالتعاون مع كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة، يومي 06-05 ماي 2019.

❖ **المقالات الإلكترونية:**

1. غالب العوادي اوس مجيد، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، السنة 2016، https://www.bayancenter.org/ .
2. هميسي رضا، الضمانات القانونية لحماية البيانات الشخصية في الفضاء الرقمي، جامعة قاصدي مرباح ورقلة، السنة 2019، http://www.researchgate.net.

ث. الأطروحات والمذكرات الجامعية:

❖ **أطروحات دكتوراه:**

1. برارديي نعيمة، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر (دراسة تحليلية استطلاعية بالجزائر العاصمة)، رسالة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر03، السنة الجامعية 2012-2013.
2. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، قانون خاص، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2017-2018.
3. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة باتنة 1، كلية الحقوق والعلوم السياسية، السنة الجامعية 2015-2016.
4. زرقيني راضية، الحماية الجزائية للمعطيات الشخصية، أطروحة دكتوراه، تخصص قانون عام، الوادي، الجزائر، جامعة الشهيد حمه لخضر، السنة الجامعية 2022- 2021.
5. سعيداني نعيم، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي، باتنة، جامعة باتنة 1، السنة الجامعية 2020-2021.

❖ **مذكرات الماجيستر:**

1. المنصوري سلامة محمد، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، رسالة ماجيستر في القانون العام، كلية الحقوق –قسم القانون العام–، جامعة الإمارات العربية المتحدة، السنة 2018.

ج. المواقع الإلكترونية:

1.https://Legale. Advice. Online/ تاريخ الاطلاع، 18/05/2024, الساعة 09: 15.
2.http://Revues.imist.ma/ ?journal=regs ، تاريخ الاطلاع ،19/05/2024 , الساعة 12: 15.
3.https://Radioalgerie.dz/،تاريخ الاطلاع 03/05/2024 , الساعة21 :15 .
4. https://Elmawkie.dz/،تاريخ الاطلاع 03/05/2024 , الساعة21 :15.
5. http://www.gaana.dz/ ، متوفر على الرابط، تاريخ الاطلاع، 11/05/2024 الساعة 18: 18.
6.https://www.researchgate.net/
7.https://pdfdrive.to/
8.https://www.springer.com/gp
9. https://www.refseek.com/
10. https://scholar.google.com
11. https://books.google.com/
12. https://typeset.io/
13. https://www.matecat.com/

ح. دليل علمي:

1. دليل نظام حماية البيانات الشخصية، الهيئة السعودية للبيانات والذكاء الاصطناعي، السنة 2023.
2. دليل عملي: انشاء إطار عمل للخصوصية وحماية البيانات، مجموعة الامتثال لمكافحة الجرائم الماليـــــة في منطقة الشرق الأوسط وشمال افريقيا، السنة 2021.

خ. المراجع الأجنبية

1. Aradji Riad, Loi N° 18-07 : Protection des données personnelles, https://www.gaan.dz/.

2. Borking John: Privacy Protecting Measure IN IT Environment Necessary , In formation Management ,10,1998,P 6-11, Reference indicated.
3. Hendrik Betzing Jean and others، The impact of transparence on mobile privacy decision making، http://doi.org/10.1007./s12525.019.00332.3.
4. Yadav Ruma, Analysis of Cryptography in information Technology 03, WWW.IJSREM.COM.
5. Zarei Koosha and others, Impersonation on social media –Adeep Neural Approach to Identify Ingenuine Content, Institute Polytechnique de Paris, http://2010.08438 (arxiv.org).

فهرس المحتويات

فهرس المحتويات:

إهـداء

شكر وتقدير

قائمة المختصرات

مقدمــة 1

الفصل الأول: الآليات الموضوعية لحماية الحياة الشخصية المعلوماتية..... 6

المبحث الأول: صور الحماية الموضوعية الوقائية للحياة الخاصة المعلوماتية 8

المطلب الأول: القواعد الوقائية لحماية الحياة الشخصية المعلوماتية 8

الفرع الأول: مبدأ الشرعية..... 8

الفرع الثاني: مبدأ الموافقة 11

الفرع الثالث: الشفافية 12

المطلب الثاني: وسائل حماية الحياة الشخصية في مجال المعلوماتية..... 13

الفرع الأول: الوسائل التقنية لحماية البيانات الشخصية 13

الفرع الثاني: الوسائل التنظيمية لحماية البيانات الشخصية 17

المبحث الثاني: الحماية الجزائية الردعية للحياة الشخصية في مجال المعلوماتية 19

المطلب الأول: نماذج عن الجرائم المنصوص عليها في قانون العقوبات..... 19

الفرع الأول: الاعتداء على المراسلات والمحادثات..... 19

الفرع الثاني: الاعتداء على الحق في الصورة وانتحال الشخصية 23

المطلب الثاني: الجرائم المنصوص خارج قانون العقوبات 27

الفرع الأول: الجرائم المنصوص عليها في قانون 18-07 27

الفرع الثاني: الجرائم المنصوص عليها في قانون 15-04..... 34

خلاصة الفصل الأول: 40

الفصل الثاني: الآليات العملية لحماية الأمن الشخصي المعلوماتي 41

المبحث الأول: الآليات الإجرائية لحماية الأمن الشخصي المعلوماتي 43

المطلب الأول: جهات البحث والتحقيق عن جرائم المساس بالأمن الشخصي المعلوماتي 43
الفرع الأول: دور الشرطة القضائية في متابعة مرتكبي جرائم المساس بالأمن الشخصي المعلومات..... 43
الفرع الثاني: انعقاد الاختصاص القضائي في جرائم المساس بالأمن الشخصي المعلوماتي 46
المطلب الثاني: خصوصية القواعد القانونية الإجرائية لحماية الحياة الشخصية 48
الفرع الأول: الآليات الإجرائية التقنية 48
الفرع الثاني: اجراءات التحري الخاصة..... 50
المبحث الثاني: الآليات المؤسساتية لحماية الأمن الشخصي المعلوماتي..... 53
المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها 53
الفرع الأول: تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها 53
الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في التصدي للجرائم الماسة بالأمن الشخصي المعلوماتي 54
المطلب الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي..... 55
الفرع الأول: النظام القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي والمهام المسندة اليها 55
الفرع الثاني: حقوق والالتزامات المرتبطة بمعالجة المعطيات الشخصية..... 57
خلاصة الفصل الثاني 62
خاتمـــــة 63
قائمة المصادر والمراجع 66
فهرس المحتويات 74
ملخص:..... 77

ملخص:

تبنت الجزائر استراتيجية مزدوجة للحماية الحياة الشخصية المعلوماتية من الانتهاكات التي تطالها فنجد من الجانب الموضوعي، أن المشرع الجزائري تبنى الحلول التكنولوجية والتشريعات القانونية الشاملة والملائمة للضمان فعالية حماية البيانات الشخصية في البيئة الرقمية من خلال الجانب الوقائي و التدابير التقنية والتنظيمية التي اعتمدها، إضافة إلى الإجراءات الردعية التي من شأنها أن تحد من هذه الانتهاكات و كخطوة جديدة قام بالتعديل الأخير للقانون العقوبات الذي وسع فيه نطاق الحماية الجزائية، أما من ناحية الجانب العملي، فتظهر الجهود التشريعية من خلال الأليات الإجرائية التي من شأنها مساعدة جهات البحث والتحقيق للمتابعة مرتكبي جرائم المساس بأمن الشخصي المعلوماتي وذلك من خلال التقنيات المستحدثة لمواكبة التحول الرقمي إضافة إلى الاليات المؤسساتية تم استحداث هيئات ومراكز جديدة تضطلع بأدوار مهمة للمكافحة هذه الجرائم وذلك لضمان نجاح تنفيذ الاستراتيجية واستمرارية العمل بها في سبيل حماية خصوصية الحياة الشخصية المعلوماتية.

الكلمات المفتاحية: الخصوصية الرقمية؛ الحياة الخاصة المعلوماتية؛ الحماية الجزائية.

Abstract:

Algeria has adopted a dual strategy to protect informational privacy from violations. On the substantive side, the Algerian legislator has embraced technological solutions and comprehensive and appropriate legal frameworks to ensure effective protection of personal data in the digital environment through preventive measures, technical and regulatory provisions, as well as deterrent measures to limit these violations. As a new step, the latest amendment of the Penal Code expanded the scope of Algerian protection. On the practical side, legislative efforts are reflected in procedural mechanisms designed to assist investigative authorities in tracking perpetrators of crimes against informational personal security. This is achieved through the adoption of innovative technologies to keep pace with digital transformation, in addition to institutional mechanisms that have established new bodies and centers playing significant roles in combating these crimes. These efforts aim to ensure the successful implementation and continuity of the strategy to protect the privacy of informational personal life.

Keywords: Digital privacy; Informational personal life; Algerian criminal protection.