وزارة التعليم العالي والبحث العلمي

جامعة باتنة1 الحاج لخضر

كلية الحقوق والعلوم السياسية

قسم الحقوق

أطروحة لنيل شهادة دكتوراه العلوم شعبة الحقوق

تحت عنوان

الحماية الجزائية للتوقيع الإلكتروني

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالب

فارس خطابي

إشراف الأستاذة الدكتورة

دليلة مباركي

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
بوهنتالة أمال	أستاذ محاضر "أ"	جامعة باتنة 1	رئيسا
مباركي دليلة	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
دلول الطاهر	أستاذ التعليم العالي	جامعة تبسة	مناقشا
مستاري عادل	أستاذ التعليم العالي	جامعة بسكرة	مناقشا
بولافة سامية	أستاذ محاضر "أ"	جامعة باتنة 1	مناقشا
بن الشيخ نور الدين	أستاذ محاضر "أ"	المركز الجامعي بريكة	مناقشا

السنة الجامعية 2020 – 2021

بسم الله الرحمن الرحيم

"وما توفيقي إلا بالله
عليه توكلت وإليه أنيب"

صدق الله العظيم

سورة هود الآية 88

شكر وعرفان

أتقدم بأسمى معاني التقدير والشكر والامتنان الجزيل، للأستاذ المشرف الأستاذة الدكتورة دليلة مباركي التي لم تبخل عليا بتوجيهاتها القيمة وبعلمها الغزير وبجهدها ووقتها، فكانت سراجا منيرا ينير طريقي ودربي في كل سطر من سطور هذا البحث أشكرها شكرا لن يفي بحقها، أدامك الله في خدمة العلم والمعرفة.

كما أتقدم بالشكر الجزيل والتقدير إلى الأساتذة الكرام والأفاضل أعضاء لجنة المناقشة كل باسمه نظير ما بدلوه من جهد لإبداء ملاحظاتهم وتوجيهاتهم القيمة لإثراء الأطروحة.

مقدمة

مقدمة

أصبح العالم في الوقت الراهن يشهد تطورا كبيرا وملموسا في مجال تكنولوجيات الإعلام والاتصال، ما جعل التكنولوجيا تغزو مناحي حياة الأفراد العادية والتجارية، كظهور التجارة الالكترونية التي نظم المشرع الجزائري أحكامها ضمن قانون التجارة الالكترونية لسنة 2018 ولم يقتصر على الأفراد فقط بل مس أيضا الحكومات والمؤسسات التي تتعامل وفق أنماط الكترونية، ولقد أدركت الجزائر منذ أزيد من عشرية أهمية التحكم في تكنولوجيا الإعلام والاتصال، نظرا لعلاقة هذه الأخيرة بنجاح مسار التنمية المستدامة، و بغية التوصل إلى تحقيق أهداف التنمية أضحى التوجه صوب استعمال التكنولوجيات في جميع الميادين ضرورة من أجل تمكين كل المواطنين والمؤسسات من هذه الخدمات بدون تمييز، وهذا ما كرسه المشرع الجزائري من خلال تعديل القانون المدني رقم 05-10 المؤرخ في 20 جوان 2005 المعدل والمتمم للقانون المدني، حيث اعتبر الإثبات بالشكل الالكتروني كالإثبات بالكتابة بتوافر شروط معينة في المادة 323 مكرر.

ونظرا للطابع الرقمي لشبكات الاتصال التي أدت إلى تطور الاتصالات الالكترونية عن بعد وشبكات المعلومات سواء على الصعيد الوطني أو الدولي، تحولت معه المعاملات تدريجيا من البيئة الورقية إلى البيئة الافتراضية ذات طبيعة الكترونية رقمية تتناسب مع هده البيئة كاستخدام الفيديو، والبريد الالكتروني، وأجهزة الصراف الآلي، وبطاقات الائتمان، والتوقيع الالكتروني، ما أضفت على البشرية الكثير من الايجابيات كتقليص الجهد والوقت، والمال، وتحسين أداء الخدمات، لكنها حملت في مقابل ذلك جملة من المخاطر والتهديدات كالاعتداء على البيانات الالكترونية المستحدثة، ما ترتب عنه ظهور نمط إجرامي حديث يسمى بالجرائم المرتكبة بالوسائل الالكترونية من ضمنها الجرائم الواقعة على التوقيع الالكتروني .

وتظهر أهمية استخدام التقنية الحديثة المتمثلة في التوقيع الالكتروني في الزيادة من مستوى الأمن والخصوصية والثقة في التعاملات، نظرا لقدرة هذه التقنية على حفظ سرية المعلومات

والرسائل المرسلة وعدم قدرة أي شخص آخر على الإطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكد من مصداقية الشخصية، ولأن التوقيع الالكتروني يمر عبر أوساط الكترونية فإنه يكون معرضا للتحايل والتلاعب، ما يجعل إضفاء حماية جزائية للمعاملات الموقعة الكترونيا ضرورة مؤكدة.

وبوادر الحماية الجزائية للتوقيع الالكتروني بوجه عام في التشريع الجزائري كان في تعديل قانون العقوبات لسنة 2004 الذي جرم المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر07 من قانون العقوبات، والتي تشمل جريمة الاعتداء على النظام المعلوماتي للتوقيع الالكتروني، وأول نص تجريم صريح وخاص يعاقب على المساس بالتوقيع الالكتروني في التشريع الجزائري كان في المادة 17 من قانون عصرنة العدالة 15-03 لسنة 2015 الذي جرم استعمال بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني.

وبصدور القانون رقم 15-04، المؤرخ في 01 فيفري 2015 الذي يحدد القواعد العامة للتصديق والتوقيع الالكترونيين، يكون المشرع الجزائري قد قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة المواتية لتعميم وتطوير المبادلات الالكترونية، وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في الجزائر، كما أضفى حماية جزائية للتوقيع الالكتروني وبخاصة المادة 68 منه التي تجرم حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير، وجرائم التوقيع الالكتروني المرتكبة في مرحلة التصديق الالكتروني في المواد من 66 إلى 74 .

أما بالنسبة للحماية الجزائية الإجرائية للتوقيع الالكتروني فقد جاء تعديل قانون الإجراءات الجزائية لسنة 2006 بإجراءات تحري خاصة لجرائم خطيرة منها جريمة المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني، وكان للتطور الحاصل في مجال الإجرام الالكتروني ضرورة تطوير إجراءات المتابعة الجزائية والتحقيق والمحاكمة لمرتكبي الجرائم

بالوسائل الالكترونية، لذلك أرسى المشرع الجزائري قانونا إجرائيا ينظم أحكام الحماية الإجرائية للجرائم المرتكبة ضمن بيئة الكترونية، كالجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني وهو قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الصادر سنة 2009 المستحدث لإجراءات خاصة كالمراقبة الالكترونية، وتفتيش أنظمة الحاسب الآلي .

أهمية الدراسة

لاشك أن موضوع الحماية الجزائية للتوقيع الالكتروني له مكانة هامة ضمن موضوعات الدراسات القانونية الجزائية الحديثة سواء من الناحية العلمية أو التطبيقية القضائية، فمن الناحية العلمية يثير موضوع الحماية الجزائية للتوقيع الالكتروني الكثير من الإشكالات القانونية والمتصلة بطبيعة المعاملات الالكترونية الموقعة الكترونيا التي تستوجب تأمينها، بسبب سرعتها وكثرتها بفضل شبكة الانترنت في العديد من المجالات كالتجارة الالكترونية، الخدمات المصرفية الالكترونية كبطاقات الدفع والائتمان، والخدمات الحكومية الالكترونية.

ومن الناحية العملية التطبيقية تستمد الدراسة أهميتها من خلال ما يطرح على القضاء من جرائم خطيرة تمس نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، والتلاعب في البيانات الالكترونية للتوقيع الالكتروني.

ولأن الحماية الجزائية للتوقيع الالكتروني تثير العديد من الإشكالات سواء في الفقه أو التشريع الجزائري والمقارن، وأن القضاء الجزائري في حاجة ماسة لدراسات متخصصة يستنير بها القاضي عند تطبيقه لقانون العقوبات، يجعل من موضوع الحماية الجزائية للتوقيع الالكتروني أهمية كبيرة في الجانب التطبيقي العملي والجانب الأكاديمي العلمي .

أسباب اختيار الموضوع

كان اختيارنا لموضوع الدراسة مبنيا على أسباب ذاتية وموضوعية تتجلى فيما يلي:

أسباب ذاتية: وهي رغبتنا النفسية الذاتية للبحث في موضوع الحماية الجزائية للتوقيع الالكتروني، لما للموضوع من أهمية علمية في الدراسات العلمية والعملية لتطور القانون الجنائي، وعلاقته بالتكنولوجيا الحديثة.

أسباب موضوعية: وتتمثل فيما تضيفه الدراسة من قيمة علمية لأجل التصدي لظاهرة الإجرام الالكتروني الواقع على المعاملات الموقعة الكترونيا، وحاجة الجامعة الجزائرية، والقضاء الجزائري لدراسات تخص الحماية الجزائية للتوقيع الالكتروني، بسبب قلتها، وعلى حد ما اطعنا عليه من بحوث في الجامعات الجزائرية فهناك العديد من الدراسات التي تناولت مواضيع الجرائم المرتكبة بالوسائل الالكترونية، إلا أننا لم نعثر على أطروحة دكتوراه تناولت موضوع الحماية الجزائية للتوقيع الالكتروني.

أهداف الدراسة

تهدف هذه الدراسة إلى تسليط الضوء على الحماية الجزائية للتوقيع الالكتروني من خلال بيان الإطار القانوني الذي يتم فيه تبادل بيانات التوقيع الالكتروني المعالجة الكترونيا، و خصوصيتها، والتركيز على الصور التي يقر المشرع الجزائي الجزائري والمقارن بأنها تشكل جرائم اعتداء على التوقيع الالكتروني، مع بيان أحكامها الموضوعية، والقواعد الإجرائية المطبقة على الحماية الجزائية للتوقيع الالكتروني.

مع الإسهام في الكشف عن أحد صور الإجرام الالكتروني الحديث، وما تضيفه الدراسة للباحثين في مجال جرائم التوقيع الالكتروني، والجريمة المرتكبة بالوسائل الكترونية، والجرائم المعلوماتية، من الاستفادة منها كدراسة سابقة.

الدراسات السابقة

على حد إطلاعنا تمكنا من الحصول على دراستين سابقتين تحملان نفس عنوان دراستنا وهما:

الأولى، أطروحة دكتوراه للطالب: أيمن رمضان محمد أحمد، بعنوان: **الحماية الجنائية للتوقيع الالكتروني**، جامعة عين شمس، مصر، منشورة في دار النهضة العربية، القاهرة، 2011، توصل فيها الباحث إلى مجموعة نتائج منها أن جرائم التوقيع الالكتروني تشمل جرائم المساس بخصوصية وسرية التوقيع الالكتروني، وجرائم ماسة بحجية التوقيع الالكتروني وهي تزوير وإتلاف التوقيع الالكتروني، وتتفق دراستنا مع دراسته في بعض صور جرائم التوقيع الالكتروني، إلا أننا نرى بأن مصطلح جرائم حجية التوقيع الالكتروني نستعمله عندما يكون التوقيع الالكتروني محلا لكل جرائم التوقيع الالكتروني وليس التزوير والإتلاف فقط، كما يمكن أن يكون للتوقيع الالكتروني حجة ودليلا لإثبات جرائم أخرى لا علاقة لها بجرائم التوقيع الالكتروني، كما توصل الباحث أيضا إلى أن الحماية التقنية للتوقيع الالكتروني تتداخل مع الحماية الجزائية له، إلا أننا نرى عكس ذلك فالحماية التقنية حماية وقائية قبل وقوع جرائم التوقيع الالكتروني، وتدخل القانون الجزائي لا يكون إلا عندما يتعرض التوقيع الالكتروني إلى اعتداء منصوص ومعاقب عليه، وفي الجانب الإجرائي تتفق مع دراستنا من أنه لابد من ضبطية ونيابة وجهات حكم متخصصة في جرائم الاعتداء على التوقيع الالكتروني، ولا سبيل لمكافحتها بغير تعاون دولي، إلا أن دراستنا تختلف عنها من أنها كانت على ضوء التشريع الجزائري سواء في الجانب الموضوعي أو الإجرائي.

والثانية، أطروحة دكتوراه للطالب: ياسر محمد الكومي بعنوان: **الحماية الجنائية والأمنية للتوقيع الالكتروني-دراسة مقارنة**، جامعة حلوان، مصر، منشورة في دار المعارف الإسكندرية، 2014، والذي توصل فيها الباحث إلى مجموعة نتائج منها ضرورة إدراج جريمة استغلال ضعف أو جهل المتعامل في البيع الالكتروني، ضمن جرائم التوقيع الالكتروني،

للمتعامل الذي يقع في غلط نتيجة لوسائل تدليسية، إلا أننا نرى عكس ذلك لأن البيع الالكتروني قد لا يكون في كل الحالات موقعا الكترونيا، وأنها جريمة تتعلق بالاستغلال في البيع وليس في التوقيع الالكتروني، وتوصل الباحث أيضا إلا أن جرائم التزوير والإتلاف تمس أهمية وحجية التوقيع الالكتروني في الإثبات، إلا أننا نفضل أن تكون حجية وأهمية التوقيع الالكتروني في الإثبات عندما يكون التوقيع الالكتروني وسيلة للإثبات، وليس محلا لجرائم التوقيع الالكتروني، وتتشابه الدراسة مع دراستنا في بعض صور جرائم التوقيع الالكتروني، وحمايتها الإجرائية الخاصة، إلا أن دراستنا كانت على ضوء التشريع الجزائري.

وهناك أطروحات تناولت أجزاء من دراستنا نذكر منها:

أطروحة دكتوراه للطالب: محمد خليفة ، بعنوان: جريمة التواجد غير المشروع في الأنظمة المعلوماتية– دراسة مقارنة، كلية الحقوق ، جامعة عنابة ، 2010 – 2011 .

أطروحة دكتوراه للطالب: صالح شنين ، بعنوان: الحماية الجنائية للتجارة الالكترونية– دراسة مقارنة ، كلية الحقوق ، جامعة تلمسان، 2012– 2013 .

أطروحة دكتوراه للطالبة: نبيلة هبة هروال ، بعنوان: جرائم الانترنت– دراسة مقارنة، كلية الحقوق، جامعة تلمسان، 2013 – 2014 .

إشكالية الدراسة

إن أهم ما يميز عالم اليوم هو ثورة تكنولوجيا المعلومات مما ساعد على ازدياد نطاق المعاملات الموقعة الكترونيا، ما يجعلنا نتساءل في هذه الدراسة عن: **مدى ملائمة إسقاط النصوص الجزائية التقليدية الموضوعية منها و الإجرائية في مواجهة الجرائم الواقعة على التوقيع الالكتروني؟ وهل كفل المشرع الجزائري حماية جزائية فعالة ليضفي الثقة في التعاملات الموقعة الكترونيا ؟ .**

لتتفرع عن هذه الإشكالية الرئيسية جملة من التساؤلات الفرعية التالية:

فما مفهوم التوقيع الالكتروني محل الحماية الجزائية في جرائم التوقيع الالكتروني ؟

وما هو نطاق تطبيق النصوص الجزائية التقليدية الموضوعية على جرائم التوقيع الالكتروني؟ وهل تستدعى الحماية الجزائية الموضوعية للتوقيع الالكتروني تجريما خاصا؟

وهل شملت الحماية الجزائية الموضوعية كافة صور جرائم التوقيع الالكتروني ؟

وكيف يمكننا الوصول إلى حماية جزائية إجرائية للتوقيع الالكتروني، تتماشى وطبيعة الجرائم المرتكبة بالوسائل الالكترونية؟، وهل تتطلب إجراءات خاصة لا تتضمنها الإجراءات التقليدية، في البحث والتحري، والمتابعة الجزائية، والتحقيق القضائي في جرائم التوقيع الالكتروني ؟

وهل هناك معايير خاصة غير التقليدية يتحدد بها الاختصاص القضائي في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني؟ وكيف يمكن للقاضي الجزائي التعامل مع الأدلة الالكترونية الحديثة في مجال إثبات جرائم التوقيع الالكتروني المرتكبة بالوسائل الالكترونية، وأثرها على الاقتناع الشخصي للقاضي الجزائي؟.

منهج الدراسة

سنستخدم في دراستنا المنهج الوصفي، ومنهج تحليل المحتوى، وذلك بغية وصف وتحليل مضمون النصوص القانونية المتضمنة الجرائم محل الدراسة ولاسيما الجرائم الواقعة على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، والجرائم الواقعة على التوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين لسنة 2015، واستنباط علمي لما تحويه من أحكام موضوعية متعلقة بتلك الجرائم، وتحليل وصفي أيضا لأحكامها الإجرائية الخاصة بالبحث والتحري والمحاكمة في الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني.

كما نستخدم المنهج المقارن، لمقارنة موقف المشرع الجزائري في المسائل محل الدراسة مع مواقف بعض التشريعات المقارنة، وذلك بغية الاستفادة من تجارب الدول الأخرى لفهم نصوص القانون الجزائري وتطبيقه وما يجب التعديل فيه.

خطة الدراسة

قسمنا دراستنا إلى بابين مع فصل تمهيدي حسب الخطة الآتية:

الفصل التمهيدي: مفهوم التوقيع الالكتروني

المبحث الأول: ذاتية التوقيع الالكتروني.

المبحث الثاني: الحماية التقنية للتوقيع الالكتروني.

الباب الأول: الحماية الجزائية الموضوعية للتوقيع الالكتروني

الفصل الأول: الحماية الجزائية الموضوعية التقليدية للتوقيع الالكتروني وفقا لجرائم الأموال والتزوير.

الفصل الثاني:الحماية الجزائية الموضوعية للتوقيع الالكتروني وفقا للقواعد الخاصة المستحدثة.

الباب الثاني: الحماية الجزائية الإجرائية للتوقيع الالكتروني

الفصل الأول: الحماية الجزائية الإجرائية للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني في مرحلة ما قبل المحاكمة.

الفصل الثاني: الحماية الجزائية الإجرائية للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني في مرحلة المحاكمة.

الفصل التمهيدي:
ماهية التوقيع الالكتروني

الفصل التمهيدي: ماهية التوقيع الالكتروني

التطور في المجالات الالكترونية أدى إلى الكشف عن تقنية تحل محل التوقيع التقليدي ألا وهي التوقيع الالكتروني، تكون مواكبة لعصرنه العديد من القطاعات في القطاع الخاص كالتجارة الالكترونية، وأيضا في القطاع العام بظهور الحكومة الالكترونية، ولا يمكن توقيع هذه المعاملات الالكترونية، إلا بواسطة التوقيع الالكتروني، ما يجعله دائما في حاجة إلى حماية تقنية، هذا ما يدعونا للتطرق في هذا الفصل إلى مفهوم التوقيع الالكتروني في المبحث الأول، ثم حمايته التقنية في المبحث الثاني.

المبحث الأول: مفهوم التوقيع الالكتروني

التوقيع الالكتروني يزيد الثقة ما بين المتعاملين عبر الأوساط الالكترونية ويضمن صحتها ما أضفى عليه ذاتية وخصوصية، وقبل نشأة التوقيع الالكتروني يمر بعدة مراحل حتى ينتج أثرا قانونيا يعبر عن إرادة المتعاقدين، لذلك سنتناول بالدراسة في هذا المبحث ذاتية التوقيع الالكتروني في المطلب الأول، ثم إنشاء التوقيع الالكتروني في المطلب الثاني.

المطلب الأول: ذاتية التوقيع الالكتروني

يأخذ التوقيع الالكتروني طابعا خاصا عن نظيره التقليدي في التعريف والخصائص ومجالات استخدامه وصوره العديدة، ولكونه تقنية تتميز بالدقة فقد عرفته العديد من التشريعات منها التشريع الجزائري، فما هو تعريف التوقيع الالكتروني، وما هي خصائصه ومجالات استخدامه وصوره.

الفرع الأول : تعريف التوقيع الالكتروني

غالبية التشريعات عرفت التوقيع الالكتروني في قوانينها وقد سار المشرع الجزائري على ذلك بأن عرفه في قانون التوقيع الالكتروني 15 – 04، كما حظي بالعديد من التعريفات الفقهية، سنتطرق أولا إلى التعريف التشريعي، ثم الفقهي.

أولا: التعريف التشريعي

عرف المشرع في المادة 02 من قانون 15 – 04 [1] ، المؤرخ في 11 ربيع الثاني 1436 الموافق ل أول فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين بأن التوقيع الالكتروني هو: "بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى تستعمل كوسيلة توثيق" .

وتعرفه المادة 249 من قانون التوقيع الكتروني الفرنسي الصادر في 13 مارس 2000 بأنه التوقيع المثبت بشكل الكتروني صحيح فقط باستخدام عمليه تسمح بتحديد هوية الموقع، يضمن ارتباط التوقيع مع الفعل الذي يعلق عليه ويضمن سلامة هذا العمل، و التوقيع الرقمي يتكون من توقيع مكتوب بخط اليد في شكل رقمي بعد تثبيته علي شاشة تعمل باللمس، من قبل جهاز ضمان سلامة الفعل بمجرد توقيع التوقيع [2] .

ولقد ورد تعريف التوقيع الالكتروني في قانون التجارة الالكترونية المصري بأنه حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره [3].

---

[1]– الجريدة الرسمية للجمهورية الجزائرية ، العدد 06 ، الصادرة بتاريخ 10 – 02– 2015 .

[2]– Alain Bensoussan, La signature numérique et électronique en procédure pénal.

اطلع على الموقع في: 11–08 – 2020 على الساعة 10:30 . www. De alain.bensoussan. com

[3] – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي ، الإسكندرية، 2005 ، ص 16 .

وعرفه قانون التجارة الالكترونية الإماراتي رقم 2 الصادر سنة 2002 بأنه "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذو شكل الكتروني وملحق ومرتبط منطقيا برسالة الكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة" [1].

وعرفه القانون الأمريكي الصادر في 20-07 -2000 "بأنه شهادة رقمية تصدر عن إحدى الهيئات المستقلة وتميز كل مستخدم يمكن أن يستخدمها في إرسال أي وثيقة أو عقد تجاري أو تعهد أو إقرار"[2] .

وفي التشريعات الدولية عرفه قانون الأونيسترال النموذجي بأنه يعني "بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[3] ، كما عرف التوقيع الالكتروني في الاتجاه الأوروبي لسنة 1999 في الأمر رقم 1999-93 الصادر في 13 ديسمبر 1999 بشأن وضع إطار أوروبي للتوقيع الالكتروني بأن "التوقيع الالكتروني هو معطيات تأخذ الشكل الالكتروني والتي ترتبط بمعطيات أخرى إلكترونية وتستخدم كوسيلة لإثبات صحتها، وأكد التوجه الأوروبي بأن التجارة الالكترونية تتطلب الاعتراف بالتوقيع الالكتروني والخدمات المرتبطة به التي تسمح بتقرير صحة المعطيات" [4].

---

[1] – عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، ط1 ، دار الفكر الجامعي، الإسكندرية ، 2006 ص 233 .

[2] – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص19 .

[3]– المادة 02 من قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية المعتمد من طرف الأمم المتحدة في 05 جوان 2001 .

[4]– مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية–دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص 27 .

ثانيا: التعريف الفقهي

عرف جانب من الفقه التوقيع الالكتروني بأنه كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطا وثيقا بالتصرف القانوني تسمح بتمييز شخص صاحبها وتحديد هويته وتتم دون غموض عن رضائه بهذا التصرف القانوني[1]، ويعرفه جانب آخر من الفقه بأنه هو مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هده الإجراءات وقبوله بمضمون التصرف الذي يصدر الواقع بمناسبته[2]، وعرف أيضا بأنه ملف رقمي صغير (شهادة رقمية) تصدر عن إحدى الهيئات المتخصصة والمستقلة ومعترف بها من الدولة وهذا الملف يخزن الاسم الشخصي وبعض البيانات الهامة الأخرى مثل رقم التسلسل وتاريخ انتهاء الشهادة ومصدرها، ويسلم لصاحب التوقيع مفتاحين أحدهما المفتاح الخاص وهو التوقيع الالكتروني للشخص ويميزه عن توقيعات الآخرين أما المفتاح العام فيتم نشره في الدليل وهو متاح للعامة من الناس[3].

ويمكننا تعريف التوقيع الالكتروني بأنه: "**ملف الكتروني يحمل بيانات الكترونية مرتبطة منطقيا ببيانات أخرى، تسمح بتمييز صاحبه عن غيره، تصدره أحد الجهات المختصة بذلك**".

الفرع الثاني: صور التوقيع الالكتروني

للتوقيع الالكتروني العديد من الصور نذكر أهمها: التوقيع الرقمي، التوقيع بالقلم الالكتروني، التوقيع باستخدام بطاقات الائتمان الممغنطة ذات الرقم السري، التوقيع البيومتري.

---

(1) – ثروت عبد الحميد ، التوقيع الالكتروني– ماهيته مخاطره وكيفية مواجهتها مدى حجيته في الإثبات، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص51 .

(2) -Jonathan rosenar , cyber law , the law of internet , springer , 1999 , p237 .
نقلا عن : ثروت عبد الحميد، المرجع السابق، ص 51 .

(3) – عبد الفتاح بيومي بيومي حجازي ، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 565 .

أولا: التوقيع باستخدام بطاقات الائتمان الممغنطة ذات الرقم السري

يستخدم هذا النظام في التعاملات البنكية وغيرها وأوضح مثال عليه بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى العميل الذي يدخل البطاقة في ماكينة السحب حين يطلب الاستعلام عن حسابه أو صرف جزء من رصيده وهي تعمل بنظامي أوف لاين أون لاين[1]، واعترف القضاء الفرنسي للتوقيع الالكتروني بهذا الشكل منذ عام 1989 في قضية كريديكاس حيث قرر أن استعمال البطاقة ذات الذاكرة من حاملها مع استعمال كود سري يعادل التوقيع الالكتروني[2].

ولقد اعترض البعض حول إبرام صفقات إلكترونية عن طريق الدفع الإلكتروني للبطاقات البنكية الممغنطة، حيث أن التوقيع في هذا الشكل ينفصل ماديا عن صاحب الأمر الذي قد يترتب عليه إمكانية حصول أي شخص من الغير على هذه البطاقة وإبرام صفقات من خلالها عندما ينجح في الوصول إلى الرقم السري الخاص لهذه البطاقة[3]، ولكن هذا الاعتراف تم الرد عليه مع الاعتراف بقيمة ما يبرم من صفقات بهذه الطريقة بالإضافة إلى وجود وسائل أمان كافية لإتمامها وعدم التلاعب فيها فمن ناحية لا يمكن لأي شخص أن يصل إلى الرقم السري إذا كان إرساله يتم بشكل رسمي بخطاب مسجل لا يستلمه أحد غيره وبالتالي فلا يعلم به أحد غيره[4]، وفي حالة عدم تعرف الجهاز على صاحب بطاقة الائتمان من خلال إدخال رقم سري خاطئ لا يمكن له إتمام العملية الالكترونية، كإدخال رقم سري خاطئ للبطاقة الذهبية لأجل

---

(1) – عبد الفتاح بيومي بيومي حجازي ، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 23 .

(2) – المرجع نفسه، ص 29 .

(3)- Sandrine muno 2 : quelque interrogation sur le paiement électronique, petite affiches, 28 Aout 2000. N 171. P3.

- olivier zilbertin. Notes sur le paiement par les cartes bancaires, le monde, 15 septembre, 1999. P8.

نقلا عن : السعيد قنديل، التوقيع الالكتروني– ماهيته صوره حجيته في الإثبات بين التداول والاقتباس، دار الجامعة الجديدة ، الإسكندرية، 2006 ، ص 68.

(4) – المرجع نفسه، الصفحة نفسها.

سحب المال، وفي حالة أيضا تكرار الخطأ لأكثر من ثلاث مرات، فنظام الجهاز يقوم بمنع وتوقيف العملية الالكترونية لاحتمال حاملها ليس صاحب التوقيع الالكتروني أو الرقم السري .

ثانيا: التوقيع بالقلم الالكتروني

وهي الصورة الثانية للتوقيع الالكتروني حيث تتم باستخدام طريقة Pen – op أو التوقيع بالقلم الالكتروني ويتم ذلك عن طريق استخدام قلم الكتروني حسابي يمكن عن طريقه الكتابة على شاشة الكومبيوتر وذلك عن طريق استخدام برنامج معين ويقوم هذا البرنامج بوظيفتين الأولى هي خدمة التقاط التوقيع والثانية هي خدمة التحقق من صحة التوقيع حيث يتلقى البرنامج أولا بيانات العميل عن طريق بطاقته الخاصة التي يتم وضعها في الآلة المستخدمة وتظهر بعد ذلك التعليمات في الشاشة ويتبعها الشخص ثم تظهر رسالة تطالب بتوقيعه باستخدام قلم على مربع داخل الشاشة ودور هذا البرنامج قياس خصائص معينة للتوقيع الالكتروني من حيث الحجم والشكل والنقاط والخطوط و الالتواءات ويقوم الشخص بالضغط على مفاتيح معينة تظهر له على الشاشة بأنه موافق أو غير موافق على هذا التوقيع فإذا تمت الموافقة تتم تشفير تلك البيانات الخاصة بالتوقيع ثم يأتي دور التحقق من صحة التوقيع وهي تقوم بفك رموز الشفرة البيومترية ثم تقارن المعلومات مع التوقيع المخزن وترسلها إلى برنامج الكومبيوتر الذي يعطي الإشارة فما أن كان التوقيع صحيحا آم لا[1] ، ويؤخذ على هذا التوقيع على أنه على الرغم من الدقة والأمان والثقة المتوافرة فيه، إلا أنه ليس بعيد عن التزوير فيمكن أن تخضع الدبدبات الحاملة للصوت أو صورة بصمة الأصبع للنسخ وإعادة الاستعمال وإدخال تعديلات عليها كذلك الشأن بالنسبة لبصمة العين فيمكن تزويرها بتقليدها عن طريق بعض أنواع العدسات اللاصقة المصنوعة من رقائق السليكون والتي تحمل نفس اللون والشكل والخصائص المخزنة على الحاسب الآلي [2]، وكمثال عن ذلك تطبق وزارة الداخلية على مستوى البلديات التوقيع بالقلم

[1]– عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 33 .

[2] – ثروت عبد الحميد، المرجع السابق، ص 61 .

الالكتروني، عند طلب الحصول على بطاقة التعريف الوطنية أو جواز السفر البيومتري، فيطلب من الشخص التوقيع الالكتروني بالقلم الالكتروني على شاشة الكترونية يتم حفظها الكترونيا.

ثالثا: التوقيع الرقمي

يقصد بالتوقيع الرقمي بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة في صورة مشفرة [1]، ويقوم التوقيع الرقمي على فكرة الرموز السرية والمفاتيح الغير متناسقة العامة والخاصة، ويعتمد هذا التوقيع في الوصول إليه على فكرة اللوغارتميات والمعادلات الرياضية المعقدة من الناحية الفنية كإحدى وسائل الأمان التي يبحث عنها المتعاقدون عند إبرام صفقات إلكترونية [2].

كما ينشأ التوقيع الرقمي ويتحقق من صحته باستخدام التشفير، فإذا أراد الموقع إرسال بيانات عبر البريد الالكتروني مثلا فإنه يقوم بإعداد ملخص الرسالة باستخدام برنامج تشفير المفتاح الخاص وإرسالها للشخص المستلم الذي يستخدم المفتاح العام للتحقق من صحة التوقيع الرقمي، ثم ينشأ المرسل إليه ملخص رسالة باستخدام نفس برنامج التشفير ويقارن بين ملخصي الرسالتين، فإذا كانتا متطابقتين فهذا دليل على أن الرسالة وصلت سليمة كما هي ولم يحدث بها أي تغيير أو تحريف، أما إذا ما تغيرت فسيكون ملخص الرسالة التي أنشأها المستلم مختلفة عن ملخص الرسالة التي أنشأها الموقع [3].

---

[1]– خالد ممدوح إبراهيم، حجية البريد الالكتروني في الإثبات– دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2018، ص 214 .

(2)- Armand Fausse, La signature électronique transaction et confiance sur internet, DU NOD, 2001. P 25.

نقلا عن : السعيد قنديل، المرجع السابق، ص 72.

[3] - digital signature guidelines, American bar association, usa, 1996, p 09.

نقلا عن : خالد ممدوح إبراهيم، المرجع السابق، ص 215 .

رابعا: التوقيع باستخدام القياسات البيومترية

وفقا لهذه الطريقة يتم تخزين بصمة الشخص داخل الدائرة الإلكترونية للجهاز الذي يتم التعامل معه أو من خلاله بحيث لا يتم الدخول إلا عندما ينطق الشخص كلمات معينة ويضع بصمات الأصبع المتفق عليه أو بصمة شفتاه بحيث يتم التعامل عندما يتأكد الجهاز من عملية المطابقة الكاملة [1].

وتتألف الأنظمة البيومترية من جزئين متكاملين الكيان الصلب الذي يتمثل في الأدوات والدوائر والكيان اللين المتمثل في البرمجيات، وتشكل عملية التقاط مواصفات المحدد البيومتري في مرحلة التسجيل في النظام، حيث يتم إدخال بيانات التوقيع الالكتروني إلى النظام بواسطة الأداة المناسبة كأن تكون ماسح أو كاميرا، أو ميكرفون، وبعد ذلك تقوم برمجيات النظام باستخلاص السمات المناسبة من الشكل الذي تم إدخاله وتخزين البيانات العائدة له على شكل قالب وعندما يتعامل النظام البيومتري ثانية، فإن النظام يقوم بمقارنة بيانات التوقيع الالكتروني للمستخدم المدخلة مع القالب المخزن مسبقا عنه، فإن حصل التطابق يتم التعرف عليها[2].

ويثير النظام البيومتري العديد من المشاكل منها [3]:

– عدم تمكن استخدام هذه التقنية الحديثة في كل الحاسبات المتوفرة نظرا لاختلاف نظم التشغيل وأساليب التخزين وخصوصيات حزم البرامج المتنوعة .

– فقدان السرية والكفاءة الضمانية لهذه التقنية نظرا لمحاولة الشركات المصنعة لنظم البيومتري، والتي تعلن أن نسبة دقة منتجاتها أي التحقق من الشخصية بنسبة 99,99 بالمئة إلا أنه من غير الممكن التأكد من هذه النسب المرتفعة نوعا ما حيث يوجد حاليا حالات احتيال باستخدام

(1) – السعيد قنديل، المرجع السابق، ص 70.

(2) – هلالي عبد اللاه أحمد ، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة، دار النهضة العربية، القاهرة، 2015 ، ص ص 66 – 67 .

(3) – عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن والتأمين في شبكة الانترنيت، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، 2003 ، ص 295 .

البصمة الشخصية المقلدة البلاستكية وعدم استطاعة أجهزة التحقق البصرية المصنوعة من رقائق السليكون من كشفها أو تمييزها.

الفرع الثالث: أهداف ووظائف التوقيع الالكتروني الرقمي

يهدف التوقيع الالكتروني إلى تحقيق مايلي[1] :

1. **التوثيق:** يقصد به التحقق من هوية الموقع وأن الرسالة الموقعة منه تنسب إليه.

2. **السلامة:** يقصد بالرسالة أن محتويات الرسالة الموقع عليها الكترونيا لم يتم تغيير مضمونها ولم يتم التلاعب في بياناتها لا عمدا ولا عن غير عمد .

3. **السرية:** يحقق التوقيع الالكتروني سرية المعلومات التي تتضمنها المعاملات والرسائل الالكترونية حيث لا يمكن قراءتها إلا ممن أرسلت إليه باستخدام المفتاح العام للمرسل.

4. **عدم الإنكار:** مع التوقيع الرقمي لا يمكن للموقع إنكار أن الرسالة أو المعاملة الموقعة منه لا تنسب إليه، ويرجع ذلك إلى الارتباط التام بين المفتاح العام والخاص.

الفرع الرابع: مجالات استخدام التوقيع الإلكتروني

التعاملات الالكترونية تشمل كل تعامل يتم باستخدام وسيط الكتروني أيا كانت أطرافه بين أفراد أو بين جهات حكومية أو غير حكومية، أو بين دول ومؤسسات دولية أو بين بعض من هذه الجهات المذكورة وبعض آخر، كتعامل فرد مع الشركات التجارية، أو التعامل مع المصارف سواء فيما بينها أو مع عملائها[2]، ويستعمل التوقيع الالكتروني في الكثير من المجالات والمعاملات الالكترونية التي لا يمكن حصرها نذكر أهمها استخدامه في مجال الحكومة الالكترونية، التجارة الالكترونية، والمعاملات الالكترونية المدنية.

---

[1]– إبراهيم الدسوقي أبو الليل، توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، 2003 ، ص 1859.

[2]– المرجع نفسه، ص 1847 .

أولا: الحكومة الالكترونية

وتشمل المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية [1]، لذلك سنتطرق إلى علاقة الحكومة الالكترونية بالتوقيع الالكتروني، ثم إلى أهدافها.

أ.علاقة الحكومة الالكترونية بالتوقيع الالكتروني

لقد حرصت العديد من التشريعات تحديث قوانينها وتغييرها حتى تتلائم مع الحكومة الالكترونية مثل التشريع الفرنسي الذي حرص على الاهتمام بها، بهدف تحسين العلاقة بين الإدارة والمواطن وتبسيط الإجراءات الإدارية وتطويرها من أجل تلبية وسرعة إنهاء الخدمات العامة ومن أهم القوانين قانون العقود الإدارية بوسائط إلكترونية الصادر سنة 2001 .

والجزائر تتجه تدريجيا نحو إحداث حكومة الكترونية، نذكر على سبيل المثال تطبيق وزارة الداخلية للتوقيع الالكتروني عند طلب استخراج جواز السفر أو بطاقة التعريف البيومترية، إذ يتم التوقيع بواسطة القلم الالكتروني، وعند منح الوثيقة لصاحبها يتم التحقق من هويته عن طريق التوقيع باستخدام القياسات البيومترية.

إلا أن ظهور تطبيقات الحكومة الالكترونية في الولايات المتحدة الأمريكية كانت مند الثامنينات، وهي تقدم أعمال الخدمة العامة والمرافق حتى أن عمليات الانتخاب بالاقتراع المباشر تتم عن طريق الكمبيوتر، وكذلك تطوير إجراءات إبرام العقود الإدارية وتحديثها[2]، وتطبيق التوقيع الالكتروني في التشريع الفرنسي تضمنه الأمر الصادر في 08 ديسمبر 2005 بشأن المبادلات الالكترونية بين المستخدمين والهيئات الإدارية التي تنص علي أن " الإجراءات التي تتخذها السلطات الإدارية قد تكون بالتوقيع الالكتروني" [3].

---

[1]– خالد ممدوح إبراهيم، المرجع السابق، ص 212 .

[2]– إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008 ، ص 25.

[3]- Alain Bensoussan, op- cit .

ب. أهداف الحكومة الالكترونية

للحكومة الالكترونية الكثير من الأهداف لا يمكن حصرها لأنها تشمل الميادين الاقتصادية، السياسية، الاجتماعية، القانونية الإدارية، نذكر على سبيل المثال تحسين مستوى الخدمات، التقليل من التعقيدات الإدارية، تبسيط إجراءات التقاضي في المسائل الجزائية بواسطة التوقيع الالكتروني.

1. تحسين مستوى الخدمات

مما لاشك فيه أن الحكومة الالكترونية والإدارة الالكترونية تهدف في النهاية لتقديم الخدمات إلى الجمهور بشكل لائق وبمواصفات تتفق وجودة الحكومة الالكترونية، لتفادي الأخطاء التي يقع فيها الموظف العادي لأن الحاسب الآلي حسب البرنامج وقاعدة البيانات المزود بها يعطي نتائج يقينية لا مجال للخطأ فيها وهو ما يحقق سهولة في انجاز المعاملات[1].

2.التقليل من التعقيدات الإدارية

بعد ثورة المعلومات والاتصالات التي تحياها البشرية ظهرت بوادر ما يسمى بطريق المعلومات السريع، والذي عن طريقه يمكن للشخص الذي يرغب في معلومات معينة أيا كانت طبيعتها وغير تلك المحظورة بالطبع أن يحصل عليها في ثوان معدودة من خلال شبكة الحكومة الالكترونية ومقوماتها المتمثلة في كابلات الألياف البصرية والحواسيب الآلية الضخمة عالية السرعة والبرامج المطورة [2].

---

[1] – عبد الفتاح بيومي حجازي، الحكومة الالكترونية بين الواقع والطموح– دراسة متأصلة في شان الإدارة الالكترونية التنظيم – البناء – الأهداف – المعوقات – الحلول ، دار الفكر الجامعي، الإسكندرية ، 2008 ، ص 105 .

[2] – بيل جيتس، ترجمة عبد السلام رضوان، المعلوماتية بعد الانترنيت طريق المستقبل، مجلة الثقافة والفنون والآداب ، الكويت، 1990 ، ص 149 .

3.تبسيط إجراءات التقاضي في المحاكم الجزائية بواسطة التوقيع الالكتروني

نذكر على سبيل المثال في التشريع الفرنسي أنه يمكن للمتقاضين استخدام التوقيع الرقمي أو الالكتروني للاتصالات المتعلقة بالإجراءات الجنائية، ومن أجل تبسيط الإجراءات الجنائية، أدرج القانون المؤرخ 12 ماي 2009 في قانون الإجراءات الجنائية نص المادة 801 فقرة 01 التي تنص علي ما يلي: "جميع الأفعال المذكورة في هذا القانون، سواء كانت أوامر تحقيقية أو قضائية، يمكن توقيعها علي النحو المناسب رقميا أو الكترونيا" [1].

ثانيا: التجارة الالكترونية

للتجارة الالكترونية العديد من المزايا، من أهمها أنها توفر أكثر فعالية وتحقيق أرباح أكثر وتساعد على تخفيض مصاريف الشركات والقدرة أيضا على تحليل الأسواق والاستجابة لتغير متطلبات السوق، وتساعد على تقديم الخدمة للعملاء على مدار أربع وعشرين ساعة، وخلق العديد من فرص العمل الحر [2].

وتزايد تجارة البيع والشراء بواسطة المواقع الالكترونية عبر الانترنت، جعل المشرع يدرج في القانون رقم 18 –05 ، المؤرخ في 10 ماي 2018، كل ما يتعلق بالتجارة الالكترونية[3].

وقد عرفت المادة 06 فقرة 01 التجارة الالكترونية بأنها " النشاط الذي يقوم بموجبه مورد الكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك الكتروني، عن طريق الاتصالات الالكترونية ".

وهناك العديد من التعريفات للتجارة الالكترونية ينظر كل تعريف إليها من منظور معين ومن أبرز هذه التعريفات أنها أعمال تجارية تبرم وتتم بطريقة الكترونية سواء أكانت المعاملات التجارية تحدث بين طرفي العملية التجارية أو بين الشركة وعملائها، والبعض عرفها بأنها

---

[1] - Alain Bensoussan, op- cit .

[2]– صالح شنين، الحماية الجنائية للتجارة الالكترونية–دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان، 2012 – 2013 ، ص 02 .

[3] – الجريدة الرسمية للجمهورية الجزائرية ، عدد 28 ، الصادرة في 16 ماي 2018 .

استغلال تكنولوجيا المعلومات والاتصالات لتطوير وتحسين تدبير الشؤون العامة ويتمثل في إنجاز الخدمات الحكومية الرسمية سواء بين الجهات الحكومية أو بينها وبين المتعاملين معها بطريقة معلوماتية تعتمد على الانترنيت وفق ضمانات أمنية تحمي الجهة صاحبة الخدمة، كما تعني أيضا إمكانية تبادل السلع والخدمات عبر حدود الدول ودون التقيد بإقليم معين أو جنسية معينة فهي تؤدي إلى سهولة إبرام الصفقات الدولية دون حاجة إلى وسيط الأمر الذي يؤدي إلى تقليل النفقات وتخطي العقبات والحواجز الجغرافية بين الدول[1].

أما التجارة الالكترونية الموقعة الكترونيا فإنها تشمل كل معاملة ذات طابع تجاري في مجالات التعاملات المختلفة مثل البيوع والتصرفات القانونية التجارية والمعاملات المصرفية بكل أنواعها والتي تتم في شكل محرر إلكتروني موقع توقيعا إلكترونيا [2].

ونعني أيضا بالتجارة الالكترونية الموقعة الكترونيا بأنها كل خدمة تجارية يقدمها مورد الكتروني، تكون موقعة الكترونيا بينه وبين المستهلك الالكتروني بواسطة الاتصالات الالكترونية.

وعلاقة التجارة الالكترونية بالتوقيع الالكتروني تكاد تكون لصيقة لأن كل معاملة تجارية الكترونية عبر الانترنيت حتى تكتسب مصداقيتها وخصوصية بيانات التجارة الالكترونية لابد أن تكون موقعة الكترونيا.

ثالثا: المعاملات المدنية الإلكترونية

وتشمل كل معاملة إلكترونية مدنية الطابع بالنظر إلى طرفيها[3]، أي المعاملات الالكترونية المدنية الموقعة الكترونيا، والتي تتم عبر وسيط الكتروني بين الأفراد فيما بينهم، وبالتالي حماية التوقيع الالكتروني تعتبر حماية للمستهلك الالكتروني.

---

(1) – إيهاب فوزي السقا، المرجع السابق، ص22 .

(2) – خالد ممدوح إبراهيم، المرجع السابق، ص 212 .

(3) – المرجع نفسه، ص 212 .

وتنقسم الحقوق المدنية إلى حقوق مادية ومعنوية كحقوق الملكية الفكرية والذهنية ، فهل يكمن اعتبار التوقيع الالكتروني من ضمن الحقوق الذهنية ؟.

فمن الممكن اعتبار تماثل وتشابه التوقيع الالكتروني مع المصنف لأن لصاحب كل منهما الاستئثار به، ويحق له كشف محتواه أو تقييد الاطلاع عليه، ويتماثلان أيضا في أن المشرع يبسط حمايته لمحتوى كل منهما فلا تمتد إليه يد العبث أو التدمير أو التشويه، كما أن لصاحب الحق فيهما سلطة محو مضمونها أو سحبه أيا كان الشكل الذي يفرغ فيه [1]، إلا أنهما يختلفان من أن الحقوق الذهنية هي نتاج الفكر والإبداع، أما التوقيع الالكتروني فإنه لا يتطلب ذلك، ما يجعل محل الحماية القانونية لكل منهما يختلف عن الآخر.

المطلب الثاني: إنشاء التوقيع الالكتروني

التوقيع الالكتروني لا ينشأ بمجرد العملية المادية للتوقيع وإنما يمر بمراحل حتى ينتج أثره القانوني ويعبر عن صحة التوقيع والشخص المنسب له منها مرحلة التصديق الالكتروني على التوقيع الالكتروني، وعلى هذا الأساس قضت هيئة الاستئناف فرساي بتاريخ 12 ديسمبر 2019 بأن التوقيع المستنسخ SCAN لا يعتبر توقيعا الكترونيا لفقدانه للمصداقية [2]، وهذا ما يدفعنا للتطرق إلى شروط التوقيع الالكتروني حتى ينتج أثره القانوني، ثم إلى ضرورة المحافظة على التوقيع الالكتروني.

الفرع الأول: شروط التوقيع الالكتروني الحائز للحجية القانونية

للتوقيع الالكتروني شرطان أساسيان حتى تكون له حجية قانونية، وهو أن يكون تحت السيطرة المباشرة للموقع، ومصادق عليه.

---

[1] – أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الالكتروني، دار النهضة العربية، القاهرة، 2011 ، ص 109.
وكذلك: ياسر محمد الكومي، الحماية الجنائية والأمنية للتوقيع الالكتروني–دراسة مقارنة، منشأة المعارف، الإسكندرية، 2014، ص 108 .

[2] -htp :// www.dalloz.fr.
اطلع على الموقع بتاريخ 20 أفريل 2020 على الساعة 11:15

أولا: أن يكون التوقيع الالكتروني تحت سيطرة الموقع

حتى يمكن تحديد هوية الشخص المنسوب إليه المحرر الالكتروني بصورة قاطعة فلابد أن يكون موقعا الكترونيا يتخذ شكل حروف أو أرقام أو رموز أو إشارات يكون له طابع منفرد يسمح بتحديد شخصية الموقع وتمييزه عن غيره فهو وسيلة موثوقة بين التوقيع ومضمون المحرر المنسوب للموقع حيث يلتزم الأخير بذلك المضمون الذي وقع عليه، وينبغي لذلك سيطرة الموقع على الوسيط الالكتروني على نحو يطمئن إلى سلامة توقيعه وعدم تعرضه في صورته السرية لأي تلاعب كي نضمن نسبة التوقيع لصاحبه وارتباطه بمضمون المحرر [1].

ولقد قضت محكمة استئناف Besançon في الحكم الصادر لها بتاريخ 20 أكتوبر 2000 على ضرورة أن تكون وسائل التوقيع الالكترونية تحت سيطرة الموقع وحده دون غيره[2]، ومقتضى هذا الحكم أن التوقيع الالكتروني يكون له قيمة قانونية إذا كانت الوسائل التي يتم بها تحت السيطرة المباشرة للموقع دون غيره، كما يجب أن تكون هناك صلة بين هذا التوقيع وبين التصرف المتضمن لهذا التوقيع أي أن يكون صحيحا، وإن لم تتوافر هذه الشروط فلا ينتج التوقيع الالكتروني أثرا قانونيا، ولا يكون له أي حجة في الإثبات لأنه لا يعبر عن هوية الموقع[3]، وحتى يضمن التوقيع الالكتروني صحته لابد من طرف ثالث محايد بين الشخص الموقع والجهة المتعامل معها يسمى بجهة التصديق الالكتروني.

---

(1) - Piète coudol, signature de la facture électronique, com elec, 2003, p12.

نقلا عن : محمد حسين منصور، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، 2006 ، ص 274 .

* وتتلخص وقائع هذه القضية كان محامي لأحد الأشخاص احتج بالتوقيع الالكتروني لموكله أمام المحكمة وقدم في صحيفة دعواه بيانات هذا التوقيع السرية والتي من المفترض أن الموقع يعلمها وحده دون غيره كما أن هذه البيانات كان يعرفها أيضا أشخاص آخرون يعملون في مكتب المحامي وقد رفضت المحكمة الحكم بصحة هذا التوقيع الالكتروني لأن دوره في إثبات شخصية الموقع لا يصبح مشكوكا فيه ولأن بيانات التوقيع خرجت من تحت يد الموقع إلى شخص آخر وهو محاميه ومعاونوه في مكتبه. الوقائع مشار إليها في: ياسر محمد الكومي، المرجع السابق، ص 95.

(3) – أيمن سعد، التوقيع الالكتروني–دراسة مقارنة، دار النهضة العربية، القاهرة، 2013 ، ص30 .

ثانيا: أن يكون التوقيع الالكتروني مصادق عليه

لحماية البيانات[1]، الاسمية الشخصية والمعاملات الالكترونية التي ظهرت نتيجة المعاملات المالية عن طريق الانترنيت، فلا بد من الحاجة إلى شخص ثالث لا يعد من أطراف العقد ليوثق البيانات المتبادلة والتوقيع الالكتروني ويشهد بصحته دون أن تكون له مصلحة شخصية في هذه البيانات[2]، يسمى بجهة أو مقدم خدمات التصديق الالكتروني، لذلك سنتطرق إلى مقدم خدمات التصديق الالكتروني، نماذج التصديق الالكتروني، سلطات التصديق الالكتروني.

أ. مقدم خدمات التصديق الالكتروني

عرفت المادة 02 فقرة 12 من قانون التوقيع والتصديق الالكترونيين 15-04 مقدم خدمات التصديق بأنه "شخص طبيعي أو معنوي يمنح شهادات تصديق الكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الالكتروني"، والذي جاء مطابقا لتعريف قانون الأونسترال النموذجي للتوقيع الالكتروني الذي عرفه بأنه "يعني شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات الصلة بالتوقيعات الالكترونية ".

فمؤدي خدمات التصديق الالكتروني يمنحون ما يسمى بشهادة التصديق الالكتروني التي عرفتها المادة 02 فقرة 07 من قانون التوقيع الالكتروني "بأنها وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع"[3] ، يكون الغرض من شهادة التصديق الالكتروني تأكيد أن التوقيع الالكتروني أو الرسالة الالكترونية بصفة عامة صدرت

---

* البيانات dataيمكن أن تكون في أي شكل ومن ضمنها البيانات الألفبائية والرقمية التقليدية التي تمثل وتوصف المعاملات وتعتبر البيانات موارد ذات قيمة عالية. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008، ص 23 . وقد عرفت المادة 02 من قانون التوقيع والتصديق الالكترونيين 15-04 بيانات التوقيع الالكتروني بأنها "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الالكتروني".=

والمادة 01 من نظام مكافحة جرائم تقنية المعلومات المصري تعرف البيانات بأنها "المعلومات أو الأوامر أو الرسائل أو الأصوات أو الصور التي تعد أو التي يتم إعدادها لاستخدامها في الحاسب الآلي وكل ما يمكن تخزينه ومعالجته ونقله وإنشاؤه بواسطة الحاسب الآلي كالأرقام والحروف والرموز وغيرها". ياسر محمد الكومي، المرجع السابق، ص457 .

[2] – أيمن سعد، المرجع السابق، ص 32 .

[3] – المادة 02 فقرة 7 من قانون التوقيع والتصديق الالكترونيين 15-04.

ممن نسبت إليه وأن توقيعه صحيح، و تؤكد الشهادة أن البيانات الموقع عليها بيانات صحيحة صادرة من الموقع، ولم يتم التلاعب فيها فلم يطرأ عليها أي تبديل سواء بالحذف أو الإضافة أو التغيير، فهذه البيانات تصبح موثوقة ولا يمكن إنكارها [1].

ولممارسة نشاط خدمات التصديق الالكتروني لابد من ترخيص تمنحه السلطة الاقتصادية للتصديق الالكتروني[2]، كما أن مقدمي خدمات التصديق الالكتروني يقع عليهم مجموعة من الالتزامات القانونية، من بينها أنهم ملزمون بالسرية، لأن الأمان والسرية تأتي في مقدمة الضمانات التي يجب توافرها في التعاملات الالكترونية لدعم الثقة بين المتعاملين بالوسائل الالكترونية، خاصة وأن هذه المعاملات تتم بين أشخاص لا يشملهم مجلس عقد واحد ، فإذا لم تتوفر ضمانات كافية لهؤلاء الأشخاص فمن الصعب إقبالهم على إبرام عقود وصفقات بالطرق الالكترونية، إضافة إلى أنهم ملزمون أيضا بمسك سجل الكتروني لشهادات التصديق الالكتروني [3].

ب: نماذج شهادات التصديق الالكتروني

المشرع الجزائري نص في المادة 15 من قانون التوقيع والتصديق الالكترونيين 15-04 على نموذج واحد وهو شهادة التصديق الالكتروني الموصوفة، أما في فرنسا فقد نظم المرسوم الصادر في 20 مارس 2001 الصادر عن مجلس الدولة الفرنسي الخاص بالتوقيع الالكتروني نموذجين من شهادات التصديق على التوقيع الالكتروني، الأول هو نموذج التصديق الالكتروني العادي، والثاني هو نموذج التصديق الالكتروني المعتمد أو الموصوف وكل منهما تدرج فيه بيانات معينة تميزه عن النموذج الأخر[4]، سنتطرق إلا كلا من النموذجين العادي والموصوف.

---

[1] – إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 1874 .

[2] – المادة 33 من قانون التوقيع والتصديق الالكترونيين 15 -04 .

[3]– رضوان قرواش، هيئات التصديق الالكتروني في ظل القانون 15 -04 المتعلق بالتوقيع والتصديق الالكترونيين، مجلة العلوم الاجتماعية، العدد 24 ، جوان ، 2017 ، ص 417 .

[4] – أيمن سعد، المرجع السابق، ص 35 .

1. التصديق الالكتروني العادي

هو وثيقة الكترونية تصدر من الجهة المختصة بالتصديق على التوقيع الالكتروني تقر فيها بصحة بيانات التوقيع الالكتروني وصلته بالموقع ولا يتضمن هذا النموذج بيانات أخرى [1].

2. التصديق الالكتروني المعتمد أو الموصوف

هذا النموذج متميز لأنه يجب أن يتضمن عدة بيانات نص عليها المرسوم في المادة السادسة توفر أمانا أكثر لصاحب الشأن، تضمن له صحة بيانات التوقيع الالكتروني وصلته بالموقع ويجب على جهة التصديق على التوقيع الالكتروني المختصة أن توضح في هذا النموذج البيانات الآتية:

- أنه نموذج التصديق الالكتروني المعتمد.
- هوية مقدم خدمة التصديق على التوقيع الالكتروني المعتمد .
- اسم صاحب التوقيع، أو اسمه المستعار، كما هو موضح لدى مقدم خدمة التصديق على التوقيع .
- وظيفة صاحب التوقيع .
- بيانات التحقق من صحة التوقيع الالكتروني ، والتي تقابل بيانات إنشاء التوقيع الالكتروني .
- بيان مدة عمل هذا النموذج محددة بدقة منذ بدايتها إلى نهايتها.
- الرقم الكودي لبطاقة إثبات الهوية الالكترونية .
- أن هذا التوقيع مضمون بواسطة مقدم خدمة التصديق على التوقيع الالكتروني.
- عند الضرورة بيان الحد الأقصى للمبلغ المسموح به في التعامل بمقتضى هذه الشهادة [2].

---

[1] – أيمن سعد، المرجع السابق ، ص 36

[2] – السعيد قنديل، المرجع السابق، ص ص 36 –37 .

وقد تطرقت المادة 15 من قانون التوقيع الالكتروني لكل هذه البيانات، بأن نصت على شروط التصديق الالكتروني الموصوف بنصها " شهادة التصديق الإلكتروني الموصف هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

– أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني ، طبقا لسياسة التصديق الإلكتروني الموافق عليها .

– أن تمنح للموقع دون سواه.

– يجب أن تتضمن على الخصوص:

أ– إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة.

ب– تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه .

ج– اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته.

د– إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني.

هـ– بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الالكتروني.

و– الإشارة إلى بداية و نهاية مدة صلاحية شهادة التصديق الإلكتروني .

ز– رمز تعريف شهادة التصديق الإلكتروني .

ح– التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني.

ط– حدود استعمال شهادة التصديق الإلكتروني، عند الاقتضاء.

ي- حدود قيمة المعاملات التي قد تستعمل من أجل شهادة التصديق الإلكتروني، عند الاقتضاء.

ك- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر، عند الاقتضاء.

ج. سلطات التصديق الالكتروني

أفرز قانون التوقيع الالكتروني على ثلاث سلطات للتصديق الالكتروني، وهي السلطة الوطنية للتصديق الالكتروني، السلطة الحكومية للتصديق الالكتروني، السلطة الاقتصادية للتصديق الالكتروني.

1.السلطة الوطنية للتصديق الالكتروني

حسب المواد 16 17 18 من قانون التوقيع والتصديق الالكترونيين 15-04 السلطة الوطنية للتصديق الالكتروني هي سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي ينشأها الوزير الأول، التي لم يتحد بعد مقرها لعدم صدور مرسوم تنظيمي يحدده.

وتتجلى مهمة السلطة ترقية استعمال التوقيع والتصديق الالكترونيين وتطويرهما وضمان موثوقية استعمالهما.

ويناط بها حسب المادة 18 من قانون التوقيع الالكتروني المهام الآتية:

- إعداد سياستها للتصديق الإلكتروني و السهر على تطبيقها، بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة .

- الموافقة على سياسات التصديق الإلكتروني الصادرة عن السلطتين الحكومية و الاقتصادية للتصديق الإلكتروني.

- إبرام اتفاقيات الاعتراف المتبادل على المستوى الدولي .

- اقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الإلكتروني أو التصديق الإلكتروني على الوزير الأول .

– القيام بعمليات التدقيق على مستوى السلطتين الحكومية و الاقتصادية للتصديق الإلكتروني، عن طريق الهيئة الحكومية المكلفة بالتدقيق .

تتم استشارة السلطة عند إعداد أي مشروع نص تشريعي أو تنظيمي ذي صلة بالتوقيع أو التصديق الإلكترونيين.

2.السلطة الحكومية للتصديق الالكتروني

وفقا للمواد 26 27 28 من قانون التوقيع والتصديق الالكترونيين 15-04 السلطة الحكومية للتصديق الالكتروني ينشأها الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال تتمتع بالاستقلال المالي والشخصية المعنوية، التي لم يتحدد بعد طبيعتها، تشكيلها، تنظيمها لعدم صدور مرسوم تنظيمي ينظمها، تتجلى مهمتها في متابعة و مراقبة نشاط التصديق الالكتروني للأطراف، وكذلك توفير خدمات التصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي.

وتتجلى مهام السلطة الحكومية للتصديق الالكتروني حسب المادة 28 من قانون التوقيع الالكتروني في:

– إعداد سياستها للتصديق الإلكتروني و عرضها على السلطة للموافقة عليها و السهر على تطبيقها .

– الموافقة على سياسات التصديق الصادرة عن الأطراف الثالثة الموثوقة و السهر على تطبيقها.

– الاحتفاظ بشهادات التصديق الإلكتروني المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق، بغرض تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء طبقا للأحكام التشريعية و التنظيمية المعمول بها .

– نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة .

– إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناء على طلب منها .

– القيام بعملية التدقيق على مستوى الطرف الثالث الموثوق، عن طريق الهيئة الحكومية المكلفة بالتدقيق، طبقا لسياسة التصديق .

3.السلطة الاقتصادية للتصديق الالكتروني

وفقا للمواد 29 و 30 من قانون التوقيع والتصديق الالكترونيين 15-04 يتم تعيين السلطة الاقتصادية للتصديق الالكتروني من قبل السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، مهمتها متابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذين يقدمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور.

وتتجلى مهام السلطة الاقتصادية للتصديق الالكتروني حسب المادة 30 من قانون التوقيع الالكتروني في:

– إعداد سياستها للتصديق الالكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها .

– منح التراخيص لمؤديي خدمات التصديق الالكتروني بعد موافقة السلطة.

– الموافقة على سياسات التصديق الصادرة عن مؤديي خدمات التصديق الالكتروني والسهر على تطبيقها.

– الاحتفاظ بشهادات التصديق الالكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من طرف مؤديي خدمات التصديق الالكتروني بغرض تسليمها إلى السلطات القضائية المختصة عند الاقتضاء طبقا للأحكام التشريعية و التنظيمية المعمول بها.

– نشر شهادة التصديق الالكتروني للمفتاح العمومي للسلطة .

– اتخاذ التدابير اللازمة لضمان استمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الالكتروني عن تقديم خدماته .

– إرسال كل المعلومات المتعلقة بنشاط التصديق الالكتروني إلى السلطة دوريا أو بناء على طلب منها.

– التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الالكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة.

– السهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية أو استعادة المنافسة بين مؤدي خدمات التصديق الالكتروني.

– التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق الالكتروني فيما بينهم أو مع المستعملين طبقا للتشريع المعمول به.

– مطالبة مؤدي خدمات التصديق الالكتروني أو كل شخص معني بأي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها بموجب هدا القانون.

– إعداد دفتر الشروط الذي يحدد شروط وكيفية تأدية خدمات التصديق الالكتروني وعرضه على السلطة للموافقة عليه .

– إجراء كل مراقبة طبقا لسياسة التصديق الالكتروني ودفتر الشروط الذي يحدد شروط و كيفيات تأدية خدمات التصديق الالكتروني.

– إصدار التقارير والإحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطاتها مع احترام مبدأ السرية.

– تقوم السلطة الاقتصادية للتصديق الالكتروني بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية مهامها.

الفرع الثاني: ضرورة المحافظة على التوقيع الالكتروني

الحفاظ على صحة المحرر والتوقيع الالكتروني يجب أن يكون بنفس الصورة التي صدر فيها من مصدرها حتى وصوله إلى المرسل إليه، بمعنى أن تتطابق بيانات المحرر والتوقيع الالكتروني المرسل مع بيانات التوقيع الالكتروني الذي وصل إلى المرسل إليه، لكن ليس معنى ذلك أن لا يستطيع المرسل إليه إضافة أو تعديل في مضمون الوثيقة الالكترونية التي تضمنت التوقيع، فالمرسل إليه بمثابة الشخص الذي وجه إليه الإيجاب يستطيع إما قبوله جملة وتفصيلا، وإما رفضه جملة وتفصيلا، وإما قبوله موصوفا بتعديل بعض بنوده، ودائما لا يستطيع أن يمس التوقيع الالكتروني للمرسل بالتغيير أو التعديل فيجب أن يكون محميا [1].

كما يجب أيضا المحافظة على سلامة الدعامة الالكترونية التي تحمل التوقيع الالكتروني والبيانات الالكترونية، مع ضرورة حفظها عبر الزمن إذ لا يمكن تغييرها إلا من المحتفظ بها عن طريق تجميع كل الوثائق و البيانات الالكترونية المراد حفظها، ليقوم بعدها بالتوقيع عليها وتسمى بعملية التوقيع على التوقيع (signer la signature)، ثم يرسلها عبر الطريق الالكتروني إلى المسئول عن حفظ الوثيقة الالكترونية [2].

وللحفاظ على التوقيع الالكتروني من لحظة إنشائه حتى المصادقة عليه مرورا إلى مرحلة حفظه الكترونيا، فإن ذلك لا يكون إلا بواسطة وسائل الكترونية حديثة تحميه من الاعتداءات الالكترونية، أو ما يسمى بالحماية التقنية للتوقيع الالكتروني.

---

[1] – أيمن سعد، المرجع السابق، ص 51 .

[2] – المرجع نفسه، ص 57 .

المبحث الثاني: الحماية التقنية للتوقيع الالكتروني

أهم ما يهدد المعاملات والتجارة الالكترونية هو أمن البيانات وتأمين عملية التوقيع الالكتروني والتحقق من شخصية المتعاقدين وتأمين سلامة تداول البيانات لا تمام الصفقة التجارية وهو ما يدعو لإيجاد وسائل حماية تقنية لأنظمة التوقيع الالكتروني[1]، لذلك سنتناول بالدراسة الحماية التقنية لأنظمة التوقيع الالكتروني بوجه عام، ثم الحماية التقنية للتوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين لسنة 2015 .

المطلب الأول: الحماية التقنية لأنظمة التوقيع الالكتروني بوجه عام

تتمثل الحماية التقنية في إيجاد أنظمة أمان لحماية نظم المعلوماتية وتقنية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج أو تشفير البيانات بمعرفة أصحاب الشأن[2]، لذلك سنتطرق إلى مجالات وأنواع الحماية التقنية للتوقيع الالكتروني، أساليب اختراقه، آليات حمايته تقنيا.

الفرع الأول : مجالات الأمن المعلوماتي التقني المرتبط بمعلومات التوقيع الالكتروني

هناك مجالات وأنواع للأمن المرتبط بنظم المعلومات لا يمكن حصرها نذكر أهمها [3]:

1. أمن المعلومات: وهو المرتبط بالمعلومات التي هي أساس أو هدف نظام المعلومات القائم والذي يشكل عصب أو حياة المنشأة الحديثة، وهو يعمل على حماية المعلومات ذاتها أو مخازنها بمعناها الفني والاصطلاحي الدقيق.

2. أمن الوصول إلى الأنظمة: وهو يعني عملية التأمين المعلوماتي المرتبطة أساسا بعمليات التعامل مع البيانات القائم عليها نظام المعلومات وتشمل تلك الإجراءات تأمين أو عمليات

---

[1]– هدى حامد قشقوش، الحماية الجنائية للتوقيع الالكتروني، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، 2003 ، ص 590 .

[2]– طارق الدسوقي إبراهيم عطية، الأمن المعلوماتي– النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة، الإسكندرية ، 2009 ص 576 .

[3]– المرجع نفسه، ص ص 518 – 519 .

التحكم في الدخول لنظام المعلومات ذاته، والتحكم في التطبيقات التي يعمل عليها نظام المعلومات بالمنشأة، وهو لمستخدم هذا النظام ودرجة احتياجه للمعلومات المراد التعامل معها.

3. أمن برمجيات نظم المعلومات: تستهدف عمليات البرامج التي تشتغل أو يقوم عليها نظام المعلومات ذاته وهي البرامج التي تحدد مسار البيانات وكيفية التعامل معها، وتشمل عمليات التأمين ضد القرصنة من الداخل أو الخارج أو أعمال التخريب والإتلاف المعتمدة لها.

4. أمن الاتصالات: وهي عمليات تأمين وسائل الاتصال التي تعتمد عليها المنشأة في أعمالها الوظيفية وتشمل تأمين وسائل الاتصال السلكي من خطوط تلفونية وكوابل نقل المكالمات وأجهزة نقل وتداول الاتصالات المركزية أو الرئيسية الداعمة والمقوية للاتصالات الالكترونية، كما تشمل عمليات التأمين وسائل الاتصال اللاسلكي المستقلة منها أو الملحقة بأجهزة أخرى.

الفرع الثاني: أساليب اختراق أنظمة التوقيع الالكتروني

النمط المستخدم في عمليات الهجوم على نظام معلوماتي متصل بشبكة الانترنيت يتمحور في خطوات أولها ترقيم الشبكة أي الكشف عن معلومات حول الهدف المقصود ويتم ذلك من خلال مجموعة من التقنيات منها كسر كلمة السر وهي عملية استعادة كلمات السر من البيانات التي تم تخزينها أو إرسالها عبر نظام الحاسب والأسلوب الشهير هو بالمحاولة المتكررة لتخمين كلمة السر[1].

وهناك العديد من أساليب اختراق أنظمة التوقيع الالكتروني لا يمكن حصرها سنركز على أهمها، ومن أشهر أساليب الاختراق المعلوماتي[2]:

- **هجمات الحرمان من الخدمة:** يتنوع مفهوم الحرمان من الخدمة تبعا للهدف المبتغى تحقيقه فقد يقوم المهاجم بإغراق الأجهزة المزودة بسيل جارف من الطلبات والأوامر التي تفوق قدرة الجهاز المزود على المعالجة، كذلك قد يستخدم برنامجا يقوم بتجربة الدخول إلى حسابات

[1]- هلالي عبد اللاه أحمد، المرجع السابق، ص181.

[2] – المرجع نفسه، ص ص 184 – 185 .

المستخدمين ضمن خدمة معينة من خلال تجربة كافة أسماء المستخدمين، واستعمال كلمات سر خاطئة عمدا وعند استخدام هذه البرمجيات فإن بعض المزودات إذا لم يكن هناك تأخير معين بين محاولات الدخول تقوم بمنع المستخدمين الشرعيين من النفاد إلى النظام المعلوماتي.

-**استغلال الثغرات الأمنية:** الثغرة الأمنية عبارة عن تطبيق معد ليستغل نقطة ضعف معلومة فبعد أن يتعرف المجرم المعلوماتي على البرامج التي تدير السير المستهدف يبحث عن ثغرات في تلك البرامج ليستغلها أو يفسدها .

-**أحصنة الطراودة والفيروسات:** أحصنة الطراودة عبارة عن برنامج يبدو أنه يقوم بشيء ما لكنه يقوم بشي آخر يفتح المخترق من خلاله ثغرة أمنية ليتسلل من خلالها ويبدأ نشاطه الإجرامي، أما الفيروسات فهي عبارة عن برامج يضاعف نفسه بنفسه وينتشر بإدخال نسخ منه داخل رمز أو مستندات تنفيذية، فهو يتصرف بشكل مشابه للفيروسات الحيوية التي تنشر بإدخال نفسها إلى الخلايا الحية .

-**ديدان الحاسب:** وهي عبارة عن برنامج يضاعف نفسه بنفسه لكنه يختلف عن الفيروس من ناحيتين: الأولى أنه ينتشر عبر شبكات الحاسب دون تدخل المستخدم، والثانية أنه لا يحتاج إلى ربط نفسه ببرمانج موجود.

ومن وسائل اختراق النظم المعلوماتية والالكترونية للتوقيع الالكتروني هنالك أيضا:

- **الشمام sniffer:** عبارة عن أي جزء من عتاد الحاسوب أو برمجياته، التي تسترق السمع وتتحسس جميع أنواع المرور المعلوماتي على الشبكة لأغراض انتزاع المعلومات المتنقلة بين أجزائها.

وتكمن التهديدات المعلوماتية التي تنشب عن أنظمة الشمام في:

- القدرة على اقتناص كلمات العبور pas Word .
- القدرة على اقتناص المعلومات الخاصة التي تمتاز بدرجة عالية من السرية .

– إمكانية استخدامها في خرق النظم الأمنية للشبكات الحاسوبية بشتى مستوياتها[1].

– **قنبلة البريد الالكتروني:** قنبلة البريد الالكتروني عبارة عن برنامج حاسوبي يعمد إلى القصف المستمر للعنوان المستهدف عن طريق إرسال حزمة من رسائل البريد الالكتروني في توقيت محدد وبعدد معين، وخلال بعد زمني يتم اختياره من قبل الشخص المخترق بقصد الإضرار به، فتلك الرسائل تكون محملة بملفات كبيرة الحجم نظرا لصغر المساحة المحدودة للبريد الالكتروني والتي تصل إلى هذا الجهاز مرة واحدة وفي وقت واحد تقريبا فتؤدي إلى توقفه عن العمل على الفور نظرا لما تسببه من ملئ منافذ الاتصال أو المساحة المتاحة للمستخدم ما يؤدي إلى توقف الجهاز وإلغاء صندوق البريد [2].

– **انتحال الشخصية:** وهو أسلوب انتحال الشخصيات كأن يتصل المخترق بمدير النظام ويطرح نفسه على أنه مستخدم عجز عن الوصول إلى نظامه المعلوماتي وينشد المساعدة، أو أن يقدم نفسه بوصفه موظفا جديدا يحاول تسجيل الدخول على هذا النظام ويحتاج إلى بعض المساعدة وبالتالي يطلب تزويده بالخطوات التي يجب إتباعها لتسجيل الدخول على شبكة الاتصال كذلك يمكن أن ينتحل المخترق شخصية فني في قسم الحاسبات، يعتمد هذا النوع من انتحال الشخصيات على عنصر المفاجأة حيث يقوم المخترق بالاتصال بالهدف، ليقوم بعدها بإغرائه بالعديد من الأسئلة حتى يتمكن في النهاية من الحصول على كلمة المرور[3].

الفرع الثالث: آليات المواجهة التقنية للتوقيع الالكتروني

تعد الحماية التقنية لأنظمة التوقيع بمثابة الجدار الواقي من الاعتداءات الالكترونية التي ممكن أن تواجه التوقيع الالكتروني، ولتكريسها لابد من آليات تقنية، التي بدورها تنقسم إلى مرحلتين، الأولى وهي آليات المواجهة في المرحلة الوقائية، والثانية في المرحلة العلاجية.

---

[1]– طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 528 . وكذلك: خالد ممدوح إبراهيم، المرجع السابق، ص 141 .

[2]– المرجع نفسه، ص 534 .

[3]– هلالي عبد اللاه أحمد، المرجع السابق، ص 187 .

أولا: آليات المواجهة التقنية في المرحلة الوقائية

تعد المرحلة الوقائية من مخاطر جرائم المعلوماتية العابرة للحدود الواقعة على التوقيع الالكتروني من أهم مراحل المواجهة التي ينبغي أن تكرس لها كل الجهود لأن الوقاية خير من العلاج وأدوات الحماية والأمن في هذه المرحلة عبارة عن مجموعة من البرامج يتم تثبيتها أو تحليلها على الحاسبات حتى تكون النظم المعلوماتية بمأمن من مخاطر واختراقات هذه النوعية من الأنشطة الإجرامية، وتنقسم برامج الحماية والأمن إلى المجموعات الآتية[1] :

- برامج الحماية من الفيروسات أو برامج مضادات الفيروسات.
- برامج جدران النار أو برامج الجدران النارية.
- برامج تشفير المعلومات.
- برامج المضاهات الالكترونية.

النوع الأول: برامج مضادات الفيروسات: تعتبر برامج مضادات الفيروسات بمثابة الرقيب على أي ملف يتم استخدامه في النظم المعلوماتية، حيث يقوم بحصه والتأكد بخلوه من الفيروسات قبل أن يسمح باستخدامه، وتتنوع وظائف هذه البرامج فهناك برامج تفتيش وبرامج تبحث عن الفيروسات المعروفة بفحص أشكال معرفة عن طريق فحص سلاسل أو البحث عن السلاسل، كذلك برامج التفتيش المقيمة وهي برامج مقيمة تفحص الفيروسات أثناء عمل البرامج، وقد تكون لها خصائص مراقبة ومنع، والبرامج المساعدة لفحص الملفات التنفيذية بحثا عن شفرة تستخدم العمليات التي تقوم بها الفيروسات المعروفة، وبرامج المراقبة والمنع هي برامج مقيمة تراقب البرامج للبحث عن تصرف الفيروسات، وبرامج لاكتشاف وفحص المجموع وفحص السلامة وهي برامج تقوم بحفظ قاعدة بيانات لخصائص الملفات التنفيذية على النظام وتراجع وتفحص التغيرات التي تتم نتيجة غزو فيروس معروف، كما تستخدم أيضا برامج مضادات الفيروسات ضد عمليات الاختراق والتسلل بغرض التجسس على المعلومات، فلقد قامت الشركات المنتجة

[1]– هلالي عبد اللاه أحمد، المرجع السابق، ، ص 226 .

لبرامج antivirus بتوسيع نطاق عملها لتشمل التصدي لعمليات الاختراق، بالإضافة إلى استخدامها الأساسي للتصدي لفيروسات الحاسب[1].

النوع الثاني: برامج الجدران النارية: هي عبارة عن برامج[2] صغيرة يتم تثبيتها داخل نظام معلوماتي بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى النظام المعلوماتي أثناء التعامل مع شبكة الإنترنت، وظيفتها مراقبة كل البيانات الداخلية والخارجية من الشبكة، والتأكد من مطابقتها لشروط المستخدم التي يحددها البرنامج من قبل [3].

ومهما اختلفت أشكال الجدران النارية ومع تعدد الشركات الصناعية فإن جميعها تعمل بنفس الفكرة والتقنية وتقريبا تتساوى في قدراتها في حماية الشبكة، ولكن الاختلاف يكون في طريقة تركيبها وبرمجيتها، إلا أنه عندما يقرر المرء تركيب جدار ناري في شبكته الداخلية، يجب معرفة أن إسناد هذه المهمة بالجدار لا يفيد في شي أن لم يتم تركيبه بالشكل المناسب مثل الحارس الذي يتم وضعه أمام باب ولم يحدد مهامه، فلن يمنع أحد من الدخول إن لم يطلب منه ذلك، والجدار الناري ضروري جدا لكل شبكات الحاسب الآلي في أي مؤسسة إذا ما تقرر الارتباط بالانترنت وإلا فالعواقب وخيمة[4] .

النوع الثالث: برامج التشفير: التشفير هو إجراء يسمح بتوفير الثقة في المعاملات الالكترونية الموقعة الكترونيا، ويتم بأدوات وأساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون استخدامها أو تعديلها غير المشروع بحيث يتم التأكد من المعلومات التي تسلمها المرسل إليه وهي تلك البيانات التي قام المرسل بالتوقيع عليها ويتأكد المرسل أيضا أن المعلومات لم يتسلمها شخص سوى المرسل إليه الذي يستطيع باستخدام الوسائل الفنية من الاطلاع على محتويات المعلومات وبالتالي فإن التشفير يسمح بتفادي المخاطر المتوقعة من استخدام الطرق

---

[1]– هلالي عبد اللاه أحمد، المرجع السابق، ص ص 228 229 .

[2]– ومن أمثلة برامج الجدران النارية ZONEALARM- MCAFEE FIREWALL- NORTON SECURITY- BLACK ICE DEFENDER . المرجع نفسه، ص 229 .

[3]– طارق ابراهيم الدسوقي عطية ، المرجع السابق، ص 558 .

[4]– المرجع نفسه، ص 586 .

الالكترونية في المعاملات التجارية ويتم الاطلاع على المعلومات المشفرة باستخدام ما يسمى بالمفتاح العام وهو نظام معلن للشفرة ومفتاح خاص وهو تشفير سري ويتعين استخدام المفتاحين معا للتعرف والتأكد من شخصية المرسل ومن قيامه من التعبير على إرادته [1]، ويقصد بالتشفير أيضا معالجة البيانات قبل إرسالها بهدف عدم فهم الغير لمضمونها، وتعتمد فكرة التشفير على وجود مفتاح معين تتشكل بها الرسالة قبل إرسالها، وعند الاستقبال يتم تفسير الرسالة باستخدام نفس المفتاح، ومن هذا المنظور يأتي مصطلح CRYPTOGRAPHY والذي يعني استخدام الشفرات لضمان سرية المراسلات، بحيث يكون مفتاح الشفرة مقصورا على المرسل والمستقبل[2].

ويمكن أن يتم تشفير البيانات قبل تخزينها على محركات الأقراص الصلبة، كما يمكن تشفيرها كجزء من عملية النقل الإلكتروني، ومن أشهر نظم تشفير المعلومات قبل إرسالها عبر الإنترنت تقنية SECURE SOCKET LAYER ، والتي يطلق عليها اختصار SSL وهي تجمع بين كل من تقنية PUBLIC KEY في RSA، وتقنية PRIVATE KEY التقليدية التي يتم إتباعها في نظام التشفير القياسي، وهذه التقنية تقوم بإدخال طبقة من التشفير وفك الشفرة بين التطبيقات التي تقوم بإرسال المعلومات على شبكات الاتصالات وشبكة الانترنت باستخدام TCP/IP، ويتم استخدام تقنية SSL على نطاق واسع على شبكة الانترنت لإرسال المعلومات الهامة مثل رقم كارت الفيزا خلال الصفقات التجارية عبر الانترنت، وكذلك من نظم التشفير التي لا يمكن اختراقها نظام ROP الذي يستخدم في التعامل مع الاتصالات المهمة كما يحدث في الخط الساخن بين واشنطن وموسكو[3].

النوع الرابع: برامج المضاهاة الإلكترونية: يتضمن التنظيم الفني التقني للتوقيع الإلكتروني الأخذ بوسائل تقنية لإجراء المضاهاة الإلكترونية للتوقيع الإلكتروني والتي يمكن بمقتضاها

---

[1]– مدحت عبد الحليم رمضان، المرجع السابق، ص 31 .

[2]– هلالي عبد اللاه أحمد، المرجع السابق، ص 230 .

[3] – المرجع نفسه، ص ص 230– 231 .

الوقوف على هذا التوقيع وتختلف الطرق الفنية للمضاهاة إلى عدة طرق تكفل كل واحدة قدرا معينا من الطمأنينة والثقة في المستند وتضمن سلامته وحمايته[1]، ومن هذه الوسائل مطالبة الشخص الذي يريد التعامل مع المستند الإلكتروني الإدلاء ببيانات شخصية معينة ومضاهاتها بالبيانات المسجلة سلفا عنه وذلك قبل قيامه بالتوقيع الإلكتروني[2].

ثانيا : آليات المواجهة التقنية في المرحلة العلاجية

تلعب التقنية الرقمية في المرحلة العلاجية دورا مزدوجا فهي من ناحية تقوم بمتابعة الوسيلة التي استخدمها المخترقين وما تحدثه من آثار ضارة ومن ناحية أخرى تقوم بتتبع المخترقين أنفسهم من خلال وسيلة من الوسائل التي قاموا باستخدامها.

أ. متابعة الوسيلة التي استخدمها المخترقين وما نجم عنها من آثار

في حالة اكتشاف وجود فيروس فإنه ينبغي على هذه التقنية أن تتعامل معه وتتخلص منه، فهناك أساليب عديدة للتخلص من آثار الفيروس بحسب ما إذا كان اسم الفيروس موجود في الحاسب معلوما أو غير معلوما، كذلك هناك ما يسمى RESCUE DISCK أي ملفات الإنقاذ التي يقوم برنامج NORTO N بتخزينها على بعض الأقراص المرنة FLOPPY DISKS حيث يمكن لهذه الملفات العمل من خلال نظام DOS ، وذلك بالتخلص من الفيروسات كما يجب معالجة الملفات المصابة بالفيروس، وهناك ثلاث احتمالات للمعالجة، الأول هو إزالة أوامر الفيروس من داخل كل ملف مصاب، والثاني هو الحجر الصحي للفيروسات المصابة وهو عزلها داخل مجلد خاص ولا يسمح بالتعامل معها، والثالث الحذف أي حذف الملفات المصابة نهائيا من الحاسب، ونظرا لأن هذا الاختيار الأخير قد يؤدي إلى فقدان العديد من البرامج الموجودة على الحاسب فإنه يحبذ عمل نسخة احتياطية مسبقة من البيانات المعلوماتية المخزنة

(1) – أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، 2003 ، ص 514 .

(2) – المرجع نفسه، ص 517 .

في الحاسب تجنبا لمسحها أو إتلافها، فإستراتيجية النسخ الاحتياطي أفضل حماية للبيانات من خطر الفيروسات[1].

لذلك فمضادات الفيروسات وظيفتها حماية الحواسيب من الشبكات والرسائل الالكترونية والملفات التي يتم تحميلها من شبكة الانترنت أو أي مستخدم داخل الشبكة الداخلية، وتنقية المعلومات الشبكية من أي موقع فيه بحث عن البرامج الغير مرغوب فيها ، وبرنامج لإيقاف البرمجيات الضارة التي قد تنتقل للجهاز أثناء التجول على الانترنت والشبكات [2].

ب. تتبع المخترقين

تقوم برامج الجدران النارية بتتبع محاولات الاختراق التي تتعرض لها النظم المعلوماتية، ولتتبع القراصنة يمكن استخدام أمر التتبع من سطر الأوامر، أو البرامج مثل برنامج MY NEW WATCHMAN ليقوم بمهمة جدار النار ليجمع المعلومات من المستخدمين ويقوم بإرسال تقارير إلى مزود خدمة الانترنت في الزمن الحقيقي قبل أن يتمكن القراصنة من تغيير عناوين الـ IP الخاص بهم، ويوفر برنامج جدار النار معلومات عن الـ IP للمكان القائم بالاختراق، كما تتيح أداة التتبع معرفة عنوان مزود خدمة الانترنت الذي بدأت عنده محاولة الاختراق، وعند التعرض للاختراق يمكن التوجه للموقعSEMONTEC SECURITY باستخدام برنامج تتبع لمعرفة عنوان الـ IP ومعرفة عنوان مزود الخدمة، يمكن القيام بالإجراءات الآتية:

- إبلاغ مزود خدمة الانترنت الذي يستخدمه المخترق.
- إبلاغ سلطات الانترنت بعنوان مزود الخدمة.
- تصميم قاعدة تمنع استقبال اتصالات من رقم مزود الخدمة ip [3].

---

[1]– هلالي عبد اللاه أحمد، المرجع السابق، ص 234 – 235 .

[2]– طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 583 .

[3]– هلالي عبد اللاه أحمد، المرجع السابق، ص 236 .

المطلب الثاني: الحماية التقنية للتوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين 15-04

التوقيع الالكتروني يرتب أثارا قانونية في حق من قام به وفي حق الغير، ففي عقد التجارة الالكترونية المبرم عبر الانترنيت يقوم الأطراف بالتوقيع على العقد توقيعا الكترونيا، كذلك فإن رسائل البيانات التي تتضمن المفاوضات حول العقد ثم الإيجاب والقبول كلها يتم تداولها عبر وسائط إلكترونية تدون أو تحفظ على دعامة هي وسيط الكتروني قد يكون جهاز الحاسب نفسه أو قرص مدمج أو شريط ممغنط[1]، كل هده المجالات وغيرها المستعملة للتوقيع الالكتروني لابد لها من حماية تقنية ضمن أجهزة مخصصة لهدا الغرض تناولها المشرع لأهميتها في قانون التوقيع والتصديق الالكترونيين لسنة 2015- 04، يكون من خلال مرحلتين، في الأولى أثناء إنشاء التوقيع الالكتروني، و الثانية في مرحلة التحقق منه، وهو ما سنتطرق له بالدراسة تحت عنوان الحماية التقنية لإنشاء التوقيع الإلكتروني في الفرع الأول، ثم الحماية التقنية للتحقق منه في الفرع الثاني.

الفرع الأول: الحماية التقنية في مرحلة إنشاء التوقيع الالكتروني الموصوف

التوقيع الالكتروني محل الحماية التقنية في قانون التوقيع والتصديق الالكترونيين 15 - 04 هو التوقيع الالكتروني الموصوف، الذي عرفته ونصت على شروطه المادة 07[2]، من قانون 15 - 04 بأنه التوقيع الالكتروني الذي تتوافر فيه المتطلبات الآتية:

- أن ينشأ على أساس شهادة تصديق الكتروني موصوفة .
- أن يرتبط بالموقع دون سواه .
- أن يمكن من تحديد هوية الموقع .
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني .

---

[1] - عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 461 .

[2]- المادة 07 من قانون 15 - 04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع .

- أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات .

ولحماية التوقيع الالكتروني الموصوف تقنيا فلابد من آلية لإنشائه تسمى الآلية المؤمنة لإنشاء التوقيع الالكتروني حسب المادة 11[1] ، من قانون التوقيع الالكتروني 15-04، والذي لابد أن تتوافر فيها مجموعة من الشروط التقنية تضمنتها نفس المادة تتمثل في أنه يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي :

- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء توقيع الكتروني إلا مرة واحدة وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

- أن لا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الالكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.

- أن تكون البيانات المستعملة لإنشاء التوقيع الالكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين .

- يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع.

الفرع الثاني: الحماية التقنية في مرحلة التحقق من التوقيع الالكتروني

الآلية الموثوقة للتحقق من التوقيع الالكتروني نصت عليها المادة 13[2] من قانون التوقيع والتصديق الالكترونيين 15- 04، والتي عرفتها وحددت شروط تطبيقها، و هي عبارة عن آلية

[1]- المادة 11 من قانون 15 - 04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين .

[2]- المادة 13 من قانون 15 -04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

تحقق من التوقيع الالكتروني تتوافر فيها الشروط الآتية:

– أن تتوافق البيانات المستعملة للتحقق من التوقيع الالكتروني مع البيانات المعروضة عند التحقق من التوقيع الالكتروني .

– أن يتم التحقق من التوقيع الالكتروني بصفة مؤكدة وأن تكون نتيجة هذا التحقيق معروضة عرضا صحيحا .

– أن تكون مضمون البيانات الموقعة إذا اقتضى الأمر محددا بصفة مؤكدة عند التحقق من التوقيع الالكتروني .

– أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الالكتروني .

– أن يتم عرض نتيجة التحقق وهوية الموقع بطريقة واضحة وصحيحة.

خلاصة الفصل التمهيدي

نخلص مما سبق بيانه من هذا الفصل التمهيدي إلا أن التوقيع الالكتروني يلعب دورا أساسيا في عصب الاقتصاد الرقمي الالكتروني، لعلاقته بالأداء الوظيفي للحكومة الالكترونية، وبالبيع والشراء عن بعد بواسطة الاتصالات الالكترونية، وبالخدمات المصرفية الالكترونية كبطاقات الدفع والائتمان الالكترونية الموقعة الكترونيا، وأن الحماية التقنية نظرا لأهميتها الكبيرة في تأمين التوقيع الالكتروني فقد تضمنها قانون التوقيع والتصديق الالكترونيين لسنة 2015 في مرحلتي إنشاء التوقيع الالكتروني والتحقق منه، إلا أنه وإن كانت الحماية التقنية لازمة وضرورية حتى يصبح أكثر أمان من الاعتداء عليه، إلا أن هذه الحماية التقنية لا تكفي لوحدها فلابد من بسط حماية جزائية للتوقيع الالكتروني.

الباب الأول:

الحماية الجزائية الموضوعية للتوقيع الالكتروني

الباب الأول: الحماية الجزائية الموضوعية للتوقيع الالكتروني

كلما تطورت الجريمة تتطور معها وسائل مكافحتها، وكلما ظهرت أنماط إجرامية مستحدثة تدخل المشرع لمواجهتها، لأنه قد تكون النصوص القديمة غير كافية للمواجهة، وتماشيا أيضا مع مبادئ القانون الجنائي كالتفسير الضيق للنص الجنائي، ومبدأ الشرعية الجنائية، كظهور جرائم المساس بأنظمة المعالجة الآلية للمعطيات التي جرمها المشرع في ظل تعديل قانون العقوبات لسنة 2004 التي تشابه في بعض صورها الجرائم التقليدية للسرقة والنصب وخيانة الأمانة والإتلاف والتزوير، وتشابه أيضا صور التجريم الواقعة على التوقيع الالكتروني وبياناته، ولأن التوقيع الالكتروني يتم معالجته ضمن نظام معالجة آلية للمعطيات، وبصدور قانون التوقيع والتصديق الالكترونيين لسنة 2015 الذي نظم فيه المشرع أحكام الحماية الجزائية الموضوعية للتوقيع الالكتروني، كل ذلك سيقودنا في هذا الباب أن نتناول بالدراسة الحماية الجزائية الموضوعية للتوقيع الالكتروني وفقا لقواعد الجرائم التقليدية من خلال جرائم الأموال والتزوير في الفصل الأول، ثم سنتطرق إلى الحماية الجزائية الموضوعية للتوقيع الالكتروني وفقا لقواعد الجرائم المستحدثة الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني وجرائم التوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين 15- 04 في الفصل الثاني.

الفصل الأول: الحماية الجزائية الموضوعية التقليدية للتوقيع الالكتروني وفقا لقواعد جرائم الأموال والتزوير

يلعب الحاسب الآلي والوسائل الالكترونية دورا هاما وأساسيا في جميع المجالات الفردية والحكومية، ولأن بيانات ومعلومات التوقيع الالكتروني قد تكون محلا للتغيير أو التدمير، فلابد أن تكون محمية تقنيا وذلك بهدف تحصينها ومنع الاعتداء عليها، إلا أن هذه الحماية التقنية لا تكفي فلابد من بسط حماية جزائية لكل من تسول له نفسه الاعتداء على التوقيع الالكتروني

وبياناته، لذلك سنتناول في هذا الفصل الحماية الجزائية الموضوعية للتوقيع الالكتروني من خلال جرائم الأموال التقليدية في المبحث الأول، ثم التزوير في المبحث الثاني.

المبحث الأول: التوقيع الالكتروني وجرائم الأموال التقليدية

تعد جرائم الأموال أكثر الجرائم انتشار في مجال الإجرام الالكتروني، لأجل الحصول على منافع مادية، وخاصة أن الجرائم الالكترونية لا تتطلب جهدا عضليا كالجرائم التقليدية، وإنما تتطلب جهدا فكريا، بالإضافة لعدم المواجهة بين الجاني والمجني عليه، لذلك سنتناول بالدراسة جرائم الاعتداء بالسرقة، والنصب، وخيانة الأمانة، والإتلاف الواقعة على بيانات التوقيع الالكتروني في المطلب الأول، ثم موقف التشريعات من تطبيق النصوص الجزائية التقليدية في المطلب الثاني.

المطلب الأول: جرائم السرقة والنصب وخيانة الأمانة والإتلاف الواقعة على التوقيع الالكتروني

جرائم الأموال التقليدية تتداخل مع جريمة الاعتداء على البيانات الالكترونية للتوقيع الالكتروني إذا ما اعتبرنا هذه البيانات من الأموال والأشياء القابلة للتملك، لكن طبيعتها المعنوية أحدثت صعوبة في تطبيق النصوص الجزائية التقليدية لجرائم الأموال، لذلك سنتطرق في هذا المطلب إلى أهم هذه الجرائم وهي السرقة، والنصب، وخيانة الأمانة، والإتلاف.

الفرع الأول: السرقة

السرقة من الجرائم التقليدية الأكثر قدما وانتشارا في كل أنحاء العالم، والتي شهدت في كل مراحلها تطورا سواء في وسائل ارتكابها، أو في محلها وهو الشيء المختلس، لأنها هدف الجاني من وراء الاختلاس، وإن كانت الأشياء المادية لا جدال في عدم مشروعية اختلاسها فإن المعلومات والبيانات الالكترونية و منها بيانات التوقيع الالكتروني غير ذلك، وقد أثير بشأنها جدل فقهي وقضائي، لذلك سنتطرق إلى مدى اعتبار بيانات التوقيع الالكتروني من الأموال، ثم سنتطرق إلى فعل الاختلاس وظهور فكرة سرقة منفعة الحاسب.

أولا: مدى اعتبار بيانات ومعلومات التوقيع الالكتروني من الأموال

موضوع السرقة هو الشيء الذي تتعلق به الحقوق والمصالح المعتدى عليها وينصب عليه الفعل الإجرامي، ويشترط أن يكون موضوع السرقة مالا ذا طبيعة مادية وعلة ذلك أن جريمة السرقة هي اعتداء على الملكية، فيجب أن يكون محلها صالحا للملكية، ولا يصلح محلا للملكية إلا شيء له صفة المال[1].

أما عن طبيعة معلومات وبيانات التوقيع الالكتروني، فلقد اختلف الفقه والقضاء في مدى اعتبار بيانات التوقيع الالكتروني مالا ماديا بين اتجاهين من يعتبر أن المعلومات والبيانات لا تعتبر من الأشياء المادية وبالتالي غير قابلة للسرقة، وبين من اعتبرها من الأشياء المادية من نوع خاص وبالتالي قابليتها للسرقة .

أ. الاتجاه القائل بعدم صلاحية المعلومات وبيانات التوقيع الالكتروني للاختلاس

استبعد هذا الاتجاه الفقهي أن تقع جريمة السرقة على المعلومات والبيانات مستقلة عن دعامتها نظرا للطبيعة غير المادية وأنصار هذا الاتجاه لم يكن لهم رأي واحد حول تفسير أحكام محكمة النقض الفرنسية، فمنهم من رأى أن السرقة وقعت على الأصل، ومنهم من اعتبر أنها وقعت على الجهاز، فذهب مؤيدو فعل الاختلاس على الأصل أن هذا الفعل يتمثل في الاستيلاء على هذا الأصل مدة الوقت اللازم لتصويره وأن الجاني في هذه الحالة يتوفر في حقه سرقة الاستعمال لهذا الأصل حتى لو لم يكن هذا الاستيلاء قد استمر لفترة طويلة من الزمن، ويستند هذا الرأي إلى ما استقر عليه التطور القضائي بشأن سرقة الاستعمال وبصفة خاصة استعمال السيارات، ففي هذا النوع من السرقة لا يشترط الاستيلاء على سبيل التملك وإنما يكون قد ظهر بمظهر المالك حتى ولو لفترة قصيرة لأنه يبدو وكأنه المالك الحقيقي للسيارة [2].

---

[1] - كامل السعيد، شرح قانون العقوبات- الجرائم الواقعة على الأموال، ط1 ، دار الثقافة، عمان ، 2008 ، ص 57 .
وكذلك: محمود نجيب حسني ، شرح قانون العقوبات– القسم الخاص، دار النهضة العربية، القاهرة، 1988 ، ص 810.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2010، ص 94.

كما أن موقف القضاء الفرنسي بعد تردد عبرت عنه بعض الأحكام التي رفضت اعتبار المعلومات من قبل الأموال مستندة في ذلك أن المنقول يجب أن يكون شيئا ماديا وفي ذلك تقول محكمة الاستئناف GRONOBLE لا يوجد في الأوراق ما يسمح بالقول بوقوع سرقة للديسكات أو أي دعامة مادية للمعلومات[1]، ولأن هذه الدعامة هي التي تكون قابلة للسرقة بغض النظر عن قيمتها وذلك لتحقق صفة المنقول فيها والمال بذاته بينما تبقى المعلومة خارج دائرة السرقة لعدم تحقق وصف المال فيه وإن أمكن تحييزها في إطار مادي[2].

فالأشياء الناتجة عن الاختلاس في السرقة تتحدد تبعا لطبيعتها، وتتباين الطرق التي يتم بها اختلاس المعلومات عن غيرها من الأشياء الأخرى، لأنه قد يتحقق بمجرد قراءة المعلومة أو الاستماع إليها وهو ما لا يمكن العقاب عليه أو بنقلها من الوسيط المادي الذي يحتوي عليها إلى وسيط آخر، وفي فعل النقل يتحقق الاختلاس المكون للركن المادي في جريمة السرقة، لأنه لا يتوقف الفعل عند الالتقاط الذهني للمعلومات، وإنما يتعدى ذلك إلى عمل مادي يقوم به الفاعل ما يحفظ لهذا الفعل ماديته الذي تتطلبه الشرعية الجنائية، وتفسير ذلك أنه لا يمكن التسليم بمادية الاختلاس ما لم يكن المحل الذي ينصب عليه ذا طبيعة مادية[3].

وهناك أيضا من الفقه من ينفي صفة المال عن المكونات المنطقية على أساس أن النبضات الإلكترونية والإرشادات الإلكترونية الممغنطة لا تعد من قبل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا [4].

(1)– شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 48.

(2)– عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003، ص 339.

(3)– نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية– دراسة نظرية وتطبيقية، ط1 ، منشورات الحلبي الحقوقية، بيروت، 2005 ، ص 153 .

(4) - GROZE ,h, l'apport du droit pénal à la trérorie general du droit de l'informatique c p . 1988, 1988, 3333. N 16.

- (R) gassin, le droit pénal de l'informatique, D 1982, P 38.=

ب. الاتجاه القائل بصلاحية المعلومات وبيانات التوقيع الالكتروني للاختلاس

لتحديد مدى انطباق وصف المال على معلومات وبيانات التوقيع الالكتروني ذهب بعض الفقه ومنهم « catala » حيث اعتبر أن المعلومة استقلالا عن دعامتها المادية تعد من قبل المال القابل للحيازة وذات قيمة مادية[1].

فالمعلومات الأصل أنها ليست ملكا لأحد ذلك أن المعلومات كالأفكار لا يمكن نسبة ملكيتها إلى شخص محدد وهي شائعة بين كل الناس، حيث يصعب الاستئثار بها والمعلومات ليست موضوعا لحق الملكية، ففي مجال الإبداع غير المادي لا يمكن تصور الحصول عليها إلا في إطار الحقوق المتعلقة بالملكية الفكرية وبراءات الاختراع ولا يمكن أن تكون هذه الأعمال محلا للسرقة وتنطبق عليها جريمة التقليد « contrefaçon » [2].

والمعلومة من الأشياء، حسب رأي الفقيه « vivant » وأيده كل من « planiol » و « ripert » وأسس رأيه على حجتين[3]:

الأولى أن فكرة الشيء أو القيمة لها صورة معنوية وأن أي نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي جديرة بالحماية القانونية.

والثانية أن الإنسان الذي يكشف عن معلومة بصرف النظر عن شكلها فهو يقدم قيمة ولا وجود للقيمة المعنوية بدون الإقرار بالقيمة المعلوماتية.

نقلا عن : هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني،، دار النهضة العربية، القاهرة، 2013 ، ص 152.

(1)- Katala pierre , Ebanche d'une théorie juridique de l'information, D, 1984, P 264.

نقلا عن : حسام محمد نبيل الشنراقي، الجرائم المعلوماتية–دراسة تطبيقية على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013 ص 205.

(2)– نائلة قورة، المرجع السابق، ص 157.

(3) - Vivant, aprapes des biens informationnels, j.c.p. 1984, p 3132.

نقلا عن : أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005 ، ص 128.

وعلى الرغم من الطبيعة المعنوية للمعلومات الالكترونية إذا لم تكن مسجلة على دعامة مادية وتم الاستيلاء عليها بدون الاستيلاء على تلك الدعامة، فإن اتجاها في الفقه والقضاء نحو الاعتداد بصفة المنقول لهذه المعلومات الالكترونية، فيرى أنها أموال يصلح أن يعد عليه النص الخاص بالسرقة [1].

وهناك من يرى بأن البيانات تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، وفي هذا تشبه التيار الكهربائي الذي اعتبره الفقه والقضاء من قبل الأشياء المادية[2]، فالقضاء الفرنسي اعتبر أن الماء والكهرباء قابلين للسرقة إذا تم التغيير في جهاز العداد للحصول على كمية أكبر من الماء والكهرباء[3]، وإذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية فإن الفقه الحديث يرى العكس لأن المعيار في اعتبار الشيء مالا ليس على أساس ما له من كيان مادي وإنما على أساس قيمته الاقتصادية وأن القانون يرفض إسباغ صفة المال على شيء له قيمة اقتصادية، فهو بلا جدال كما قال الأستاذ « carbonnier » بأنه قانون ينفصل تماما عن الواقع، ويضاف إلى ذلك أن تحديد مفهوم الشيء أو المال كما قال الأستاذان « planiol et rippert » نابع من الدهن وليس من طبيعة هذا الشيء[4] .

وترى أيضا الأستاذة de leyssac وهي واحدة من أبرز المدافعين عن صلاحية المعلومات كمحل في جرائم الاعتداء على الأموال بصفة عامة ويسايرها في أنصار هذا الاتجاه أن أحكام القضاء التي طبقت نصوص السرقة على المعلومات لم تحدث ثورة قانونية بالمعني الحرفي للكلمة، إذ أن اعتبار المعلومات محلا للنشاط الإجرامي في جريمة السرقة لا يمكن أن يتعارض

(1) - Michelle vivant, c, le stanc,. n 2212.

نقلا عن : شيماء عبد الغني محمد عطا الله، المرجع السابق ، ص 34.

(2) – شيماء عبد الغني محمد عطا الله، المرجع نفسه، ص 154.

(3) - Michelle laure rassat, infraction contre les biens, les personnes, la famille, les mœurs et la paix public, 4eme edition, tome 1, DALLOZ, PARIS 1976, p 32.

(4) – علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط3 ، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 2003 ، ص 577 .

مع المبادئ الأساسية للقانون الجنائي، وتمثل نتيجة منطقية للتطور والثورة القانونية التي لحقت بجريمة السرقة بوجه عام، ويبرزون حججهم على أساس أن تطبيق النصوص الخاصة بالسرقة على المعلومات وبيانات التوقيع الالكتروني لا يتعارض مع المبادئ الأساسية للقانون الجنائي، لأنه ليس من الضروري أن يكون المحل في جريمة السرقة ماديا، ويتضح ذلك من نصوص قانون العقوبات الفرنسي[1]، والجزائري فكلمة شيء الواردة بنص المادة 350 من قانون العقوبات الجزائري، تسمح بإدراج الأشياء غير المادية كالمعلومات وبيانات التوقيع الالكتروني.

كما أن تطبيق النصوص الخاصة بجريمة السرقة للحصول غير المشروع على معلومات التوقيع الالكتروني نتيجة منطقية للتطور القانوني لجريمة السرقة إذ يذهب أنصار هذا الاتجاه إلى أن تطبيق النص الخاص بجريمة السرقة على المعلومات وحدها بمعزل عن وسيطها المادي هو نتيجة منطقية للتطور القانوني في مجال السرقة، وبصفة خاصة فما يتعلق بالاختلاس، لأن المعلومات في ذاتها تتعارض وفكرة الاختلاس إذا نظرنا إليه من النظرة التقليدية التي عرفته بأنه نزع الشيء أو أخده أو نقله من حيازة المجني عليه إلى حيازة الجاني دون رضا مالكه بقصد تملكه، لذا يجب أن يكون الشيء محل الاختلاس ذا طبيعة مادية خاصة وهو ما يتعارض مع المعلومات، ومن ناحية أخرى فإن النظرية التقليدية للاختلاس تقتضي انتزاعا أو نقلا أو أخدا للشيء من حيازة المالك إلى حيازة الجاني بقصد تملكه، وبفعل التطور لم يعد الاختلاس يتطلب نقل الحيازة، كما في حالة سرقة المنفعة، بالإضافة أنه يمكن الاستئثار بواحدة من سلطات المالك على الشيء دن أن يتطلب بالضرورة نقل الشيء من المكان الذي وضعه فيه مالكه[2]، والباحث مع هذا الاتجاه إذ نرى بأن بيانات التوقيع الالكتروني تصلح أن تكون محلا للسرقة، وكما اعتبر التشريع الجزائري في نص المادة 350 من قانون العقوبات والقضاء والفقه صلاحية اختلاس الكهرباء، فإنه يمكن أيضا اختلاس البيانات الالكترونية، وأن الحماية الجزائية من الاختلاس وفق النظرة التقليدية كانت مقصورة

[1]– نائلة قورة، المرجع السابق، ص ص 151–152 .

[2]– المرجع نفسه، ص 153 .

فقط على العقارات والمنقولات، والفقه والقضاء الحديث قد ساير التطور في مفهوم الأشياء بأن جعل البيانات الالكترونية من الأشياء والقيم القابلة للاختلاس.

ثانيا: فعل الاختلاس وظهور فكرة سرقة منفعة الحاسب الآلي

المعلومات وبيانات التوقيع الإلكتروني هو تسجيل لواقع قائم كحالة أو رقم أو صفة، والمعلومة قد تكون سرية بمعنى أن يكون الاطلاع عليها أو حيازتها محظورا على غير الصفة في ذلك ويمثل الحصول عليها انتهاكا لسرية المعلومة وليس سرقة، أما إذا كانت المعلومة غير سرية أي أن العلم بها مباح للكافة فلن يخرج الأمر هنا عن أحد الفرضيين، وهي أن تكون مجانية فلا عقاب في الحصول عليها، والثانية أن تكون متاحة بمقابل مادي وهنا فإن الحصول عليها بغير المقابل المحدد لها وبغير رضا من له الحق في تقاضي هذا المقابل، يكون في حقيقته سرقة للمنفعة أو الفائدة المرجوة من هذه المعلومة، كما أن جهد الآلة ما هو إلا خدمة تتاح بمقابل مادي أيضا، ومنه فالحصول على هذه الخدمة بغير المقابل المقرر وبغير رضا صاحب الحق في اقتضاء ذلك المقابل يعد أيضا سرقة للمنفعة بالمعنى المتقدم، كما أن المكونات غير المادية من النظام الآلي لمعالجة البيانات لا يتحقق فيها وصف المال بالمعنى المتداول وأن تسميه هذا الجانب بالأموال المعلوماتية يتعين فهمها على أنها تعني القابلية للاستغلال المالي لهذه المعلومات[1]، وهذا ما يقودنا للتطرق إلى مفهوم سرقة منفعة الحاسب، ثم إلى موقف القضاء والتشريعات من سرقة منفعة الحاسب.

أ. مفهوم سرقة منفعة الحاسب الآلي

تعددت التسميات التي أطلقت على هذه الجريمة فهناك من يطلق عليها سرقة وقت الحاسب [2]

---

[1]– عمر فاروق الحسيني، المرجع السابق، ص 333.

[2]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ، القاهرة، 2003 ، ص187. وكذلك: محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية–دراسة مقارنة ، رسالة دكتوراه، كلية الحقوق، جامعة عنابة، 2011، ص 73 .

وهناك من يطلق عليها الاستعمال غير المصرح به لنظام الحاسب الآلي[1]، لذلك سنتناول بالدراسة صعوبة فعل اختلاس بيانات التوقيع الالكتروني وظهور فكرة سرقة منفعة الحاسب، ثم بيان تعريف سرقة وقت الحاسب، والتكييف القانوني لسرقة منفعة الحاسب .

1. صعوبة فعل اختلاس بيانات التوقيع الالكتروني وظهور فكرة سرقة منفعة الحاسب

هناك صعوبتان قانونيتان الأولى تتمثل في اعتبار المعلومات من المنقولات، وقد جانب المشرع الجزائري هذه الصعوبة في تعديل قانون العقوبات لسنة 2006 بأن نص في المادة 350 من قانون العقوبات بعبارة "كل من اختلس شيء"، وبالتالي نلاحظ هنا أن المشرع يوسع في مفهوم المنقولات والتي من الممكن أن تتضمن المعلومات والبيانات الالكترونية، أما الصعوبة الثانية فتتمثل في الاختلاس بعدم خروج الحيازة المادية من المجني عليه إلى الجاني، ما أدى إلى ظهور جريمة منفعة الحاسب أو استغلال وقت الحاسب.

2. تعريف سرقة منفعة الحاسب الآلي

قد تباينت الآراء الفقهية في إعطاء تعريف موحد هناك من يركز على السلوك الإجرامي وهناك من يركز على المحل الذي ينصب عليه السلوك الإجرامي وهناك من يركز على الباعث.

فالذين يعتمدون على السلوك الإجرامي بدورهم هناك من اعتمد على سلوك الاختلاس ويعرفونه كل نشاط إجرامي ينطوي على اختلاس لوقت الحاسب الآلي.

وهناك من اعتمد على سلوك فعل استعمال نظام الحاسب الآلي ويعرفونه "بأنه كل استعمال غير مصرح به للحاسب الآلي سواء عن طريق العاملين أو عن طريق أشخاص خارج المؤسسة"، أو هو كل استعمال غير مشروع للحاسب الآلي".

[1]– نائلة قورة، المرجع السابق، ص 371 .

ومن اعتمد على محل السلوك الإجرامي لم يتفقوا فما بينهم على تحديد هذا المحل، فارتكزت بعض المحاولات على الحاسب الآلي نفسه، أو على الوقت الذي ينفقه الحاسب الآلي لأداء العمل، أو على الطاقة المستخدمة [1].

والذين يعتمدون على الباعث يعرفونه بأنه" استخدام الحاسب الآلي لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانوني"[2].

وهناك اتجاه يجمع بين هذه الاتجاهات وهو الأقرب إلى الصواب، ويعرفونه "كل استعمال للوظيفة التي يؤديها الحاسب الآلي خلال فترة زمنية دون أن يكون مصرحا بذلك للفاعل، أو بمعنى أخر كل استخدام أو نظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي يمارس هذا الاستخدام الحق في ذلك، وقد يتم عن طريق شخص مرخص له باستخدام الحاسب الآلي في أوقات أخرى أو لإغراض غير التي استخدم لها أو عن طريق شخص غير مرخص له باستخدامه، وينصب الاستخدام غير المصرح به لنظام الحاسب الآلي بصفة أساسية على الخدمات التي يقدمها النظام وهي التي تتعلق بمعالجة، وتخزين، وإرسال بيانات التوقيع الالكتروني التي تتم عن طريق المكونات المادية للحاسب الآلي، وفي كثير من الحالات أيضا عن طريق استخدام برامج الحاسب والبيانات والمعلومات الأخرى المخزونة داخل الحاسب الآلي[3] .

3.التكييف القانوني لسرقة منفعة الحاسب الآلي

تثار مسألة التكييف الجزائي لهذا الفعل الغير مشروع، هل يعد من قبل السرقة، النصب، خيانة الأمانة.

---

[1]– التعاريف واردة في: نائلة قورة، المرجع السابق، ص ص 375 – 376.

[2] – محمد سامي الشوا، المرجع السابق، ص 187.

[3]- Sieber ulrich, criminal liability for the transfer of data in intrenational computer networks, new problems for german law, european journal of crime, criminal law and criminal justice, vol5, issue 1, 1997, p18.

نقلا عن : نائلة قورة ، المرجع السابق، ص 377 .

ولقد تباينت المواقف الفقهية لإضفاء الوصف القانوني لهذا الفعل الغير مشروع إلى ثلاث اتجاهات ما بين وصف السرقة، النصب، خيانة الأمانة [1]:

- **وصف السرقة**

يرى جانب من الفقه أن بالإمكان العقاب على سرقة منفعة الحاسب الآلي بوصفها سرقة طاقة أو تيار كهربائي، بيد أن جانبا من الفقه لا يؤيد هذا الرأي ويرى بأنه لا يوجد في مثل هذا الفرض باستخدام لموصل مخصص لسحب الطاقة بانتظام، كذلك لا يمكن القياس هذا الفعل على فعل اختلاس سيارة بصفة مؤقتة، لأنه بهذه الحالة هناك استيلاء مادي ولو مؤقتا للشيء المختلس، بينما في شبكة الاتصالات لا يوجد أي نوع من الاتصال المادي مع أجهزة الحاسب الآلي المعتدى عليه.

- **وصف النصب**

يرى جانب من الفقه بأن استخدام الشفرة أو كلمة السر للولوج إلى الحاسب الآلي يمكن اعتباره من قبل انتحال اسم كاذب أو صفة غير صحية التي يتحقق بها مباشرة الطرق الاحتيالية.

- **وصف خيانة الأمانة**

يميز جانب من الفقه بين سرقة الحاسب الآلي والتي ترتكب بواسطة مستخدم بدون علم رب العمل وبين سرقة هذه المنفعة التي يمكن أن تحدث بمنأى عن عقد العمل أو عقد الخدمات، إذ يرى في الفرض الأول أن الجاني خالف عقد العمل أو عقد الخدمات، وهذا ما يسمح بتكييف الفعل أنه خيانة الأمانة، أما إذا كان الحاسب الآلي قد سلم إليه خارج العقود الخاصة بخيانة الأمانة فلا يقع تحت أي وصف جزائي[2]، والباحث من رأي أن تكييفها

[1]– محمد سامي الشوا، المرجع السابق، ص188.

[2] – المرجع نفسه، ص189.

القانوني هي سرقة إذا لم تربط بين الجاني والضحية أية علاقة، أما إذا كان بينهما عقد من عقود الأمانة فإنها توصف وتكيف بأنها جريمة خيانة أمانة .

ب. موقف القضاء والتشريعات من سرقة منفعة الحاسب

لم نعثر على موقف القضاء الجزائري من مسألة سرقة منفعة الحاسب، ما دعانا للتطرق لموقف القانون المقارن الأمريكي والفرنسي.

1. الموقف الأمريكي

أصدرت المحكمة العليا لولاية أنديانا الأمريكية حكما بتاريخ 17 يوليو 1985 بموجبه رفضت المحكمة إضفاء وصف السرقة على سرقة منفعة الحاسب الآلي، في قضية تتلخص وقائعها بمتهم يدعىMC GRAW كان يعمل مستخدما لدى بلدية أنديانا والتي استأجرت حاسبها الآلي نظير مبلغ اتفاقي لا يراعى عدد الساعات الفعلية للتشغيل، وبدأ MC GRAW خلال ساعات عمله باستخدام هذا الحاسب لأغراضه الشخصية بهدف برمجة معلومات لحساب الغير، وقد فصل عن عمله عقب اكتشاف عمله غير المشروع، ثم أقيمت عليه دعوى جزائية بوصفه مرتكبا لجريمة سرقة، وفي بداية الأمر أيدت محكمة استئناف أنديانا حكم أول درجة والذي قضي بإدانته عن جرم السرقة، حيث اعتبرت محكمة الاستئناف أن الاستعمال غير المسموح به للحاسب الآلي يقاس على سرقة الخدمات التليفونية التي تقدم بمقابل مادي، وذكرت في حيثيات حكمها أن الخدمات المعلوماتية المؤجرة أو المباعة تشكل جزءا من الاقتصاد القومي وأنها تنطوي على قيمة تماثل الخدمات التليفونية التي تقدم نظير أجر، ويمكن أن تعد هذه الخدمات من قبيل رأس المال بالنسبة لأصحابها وبهذا السبب يمكن أن تكون محلا للسرقة وفقا لقانون العقوبات، واعتبرت المحكمة أن عدم استعمال الحاسب الآلي من قبل مالكه لحظة ارتكاب الجريمة لا يعد عذرا معفيا من العقاب [1].

[1]– محمد سامي الشوا، المرجع السابق، ص 190.

وعلى النقيض رفضت المحكمة العليا لولاية أنديانا تأييد هذا الحكم حيث قررت أن مفهوم السرقة كما هو محدد في قانون العقوبات يستلزم انتهاك مال الغير على نحو غير مشروع بقصد حرمان مالكه الشرعي منه، فالتساؤل يثور حول الشيء الذي تم انتزاع حيازته من مالكه فالحاسب الآلي وفقا لتقدير المحكمة العليا تم استئجاره نظير مبلغ إجمالي ولم تتحمل بلدية أنديانا أي مبلغ إضافي نظير الاستعمال غير المشروع للمتهم، ومن جهة أخرى لم ينسب إلى هذا الأخير استعماله على نحو غير مشروع للبطاقات أو البيانات أو قيامه بسرقتها بل اكتفى بأن يبرمج لحسابه بعض البيانات، وترتيبا على ما تقدم قضت المحكمة العليا بأن الوقائع المنسوبة للمتهم لا تنطوي على جريمة سرقة [1].

2. الموقف الفرنسي

أتيح للقضاء الفرنسي أن يعرب عن رأيه أول مرة فيما يتعلق بسرقة منفعة الحاسب الآلي من خلال حكم أصدرته محكمة جنح ليل Lille في قضية تتخلص وقائعها أنه بتاريخ 28 مارس 1986 قدم مدير عام شركة café grand mère شكوى ضد مجهولين لانتهاكهم النظام المعلوماتي الخاص بهذه المنشأة حيث تمكنوا من إنشاء خط بريدي خاص بهم بداخله وتحملت الشركة المدعية تكلفت تشغيله حيث أعدت الشركة نظام معلوماتي لإدارة فروعها المنتشرة في أنحاء فرنسا وبحيث يمكن لممثلي هذه الفروع أن يتبادلوا الرسائل مع المقر الرئيسي للشركة أو بين بعضهم والبعض الآخر عن طريق جهاز معلوماتي مرئي أو حاسب آلي ميكروي، وذلك بالضغط على رقم الشفرة واسم الفرع وشفرة المستخدم وكلمة السر، ولاحظ أحد المسئولين عن الإدارة المعلوماتية وجود 967 رسالة بريدية في صندوق البريد الخاص بالنظام ومعظمها لا يخص الشركة حيث تمكن مجهولون من إنشاء بنك جديد للمعلومات بعد ولوجهم في هذا الخط البريدي الالكتروني، وقد أثمر فحص الرسائل بواسطة الشرطة القضائية على أن اثنين من المختلسين أحدهم انتحل اسم appel et moi والآخر اسم jo le dingue ، هما اللذان قاما

[1]– محمد سامي الشوا، المرجع السابق، ص ص 190–191.

بارتكاب هذا الفعل غير المشروع، وتمكنت الشرطة من التواصل والقبض عليهما بعد أن أفشى كل منهما رقم تيليفونه الشخصي، ليتبين أن أحدهما يدعى Arnaud والآخر يدعى Laurent وهما شابان يقطنان الإقليم الباريسي ولديهما شغف بالمعلوماتية، ليحيلهما قاضي التحقيق إلى محكمة الجنح لارتكابهما جريمة السرقة بوصفهما قد استعملا بدون وجه حق حاسبا آليا خاصا بالغير وأظهر إرادتهما في الاستيلاء عليه وعلى نحو غير مشروع، بالإضافة إلى استخدامهما لوظيفة الحاسب الآلي ذاته[1].

وبعد أن تم النظر فيها أمام محكمة الجنح قضت ببراءة المتهمين وأسست حكمها على أنه طبقا للمادة 379 من قانون العقوبات التي تعرف السرقة بأنها الاختلاس المقترن بالغش لشيء يخص الغير، فإنه يلاحظ أولا وفقا لوقائع الدعوى عدم وجود استيلاء مادي على الحاسب الآلي ولكن هناك مجرد استخدام من بعد لهذا الحاسب الآلي الخاص بالشركة المدعية وبدون إذن منها ومن جهة أخرى لم يمنع المتهمان ولو مؤقتا مستخدمي الشركة من استعمال الحاسب الآلي، ومن جانب آخر فالمتهمان لم يستأثرا على نحو مطلق بشيء يخص الغير ولم يرتكبا اختلاسا وفقا للمادة 379 من قانون العقوبات، ومراعاة لمبدأ التفسير الضيق لقانون العقوبات وفي ظل عدم وجود نص جنائي خاص يجرم هذا السلوك غير المشروع للمتهمان، فإنه يتعين الحكم ببرائتهما [2].

أما الاتجاهات الحديثة التي تنادي بإضفاء صفتي المال والمنقول على البيانات المعالجة آليا يرون أنه يمكن في الركن المادي للسرقة تطبيق فعل الاختلاس على السرقة المعلوماتية إذا كان الجاني يقصد حرمان مالك المعلومة أو حائزها حرمانا دائما، و في حالة سرقة وقت الحاسب أو منفعته أو الاطلاع على المعلومات أو سماعها أو غيرها من الحالات التي لا يتم حرمان صاحب بيانات التوقيع الإلكتروني نهائيا، وإنما يقتصر فقط على الاستفادة من الوسيلة ذاتها أي النظام المعلوماتي الذي تعد من قبل سرقة المنفعة، وفيما تعلق بالركن المعنوي فإن السرقة

---

[1] – محمد سامي الشوا، المرجع السابق، ص ص 191 – 192 .

[2]– المرجع نفسه، ص ص 192 – 193 .

المعلوماتية جريمة عمدية يتطلب لتوافرها لتحقيق القصد الجنائي، وترتيبا لذلك يجب أن تتجه الإرادة إلى السلوك بالاستيلاء على بيانات التوقيع الالكتروني كما يجب أن تتجه الإرادة أيضا إلى النتيجة وهي امتلاك هذه الأشياء وحرمان مالكها منها مع العلم من أنها مملوكة للغير[1].

الفرع الثاني: النصب على التوقيع الالكتروني

جرم المشرع الجزائري النصب التقليدي في نص المادة 372 من قانون العقوبات باستعمال الجاني لطرق احتيالية لأجل الحصول على أموال أو منقولات أو سندات، فهل يمكن تطبيق جريمة النصب بالاحتيال للحصول على بيانات التوقيع الالكتروني ؟ وهو ما سنجيب عليه من خلال التطرق إلى مدى خضوع النشاط الإجرامي للاحتيال على بيانات التوقيع الالكتروني، ثم الاحتيال على الحاسب الآلي .

أولا: مدى خضوع النشاط الإجرامي للاحتيال على بيانات التوقيع الالكتروني

إذا لجأ الجاني إلى إحدى الطرق الاحتيالية وحمل المجني عليه على تسليمه دعامة مادية مثبتا عليها بيانات التوقيع الالكتروني، ثم استولي عليها بعد ذلك فإن النشاط الإجرامي في جريمة النصب يتحقق[2]، إذ أن الحصول غير المشروع على المعلومات باستعمال الطرق الاحتيالية لا يثير أي صعوبة إذا تعلق الأمر بالمستند أو الأسطوانة المدمجة أو القرص الممغنط الذي يحتوى على معلومات التوقيع الالكتروني[3] .

لكن هل من المتصور أن تقع الجريمة على معلومات وبيانات التوقيع الالكتروني ؟، وهل من المتصور أن يتحقق النشاط الإجرامي في جريمة النصب من خلال الطرق الاحتيالية التي يلجأ إليها الجاني والتي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى أن ينقل إليه شفهيا أي عن طريق القول محتويات التوقيع الالكتروني؟.

---

[1]– هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، المرجع السابق، ص ص 156-157.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق ، ص 97 .

[3]– نائلة قورة ، المرجع السابق، ص 173 .

فيتبين من نص المادة الثامنة من اتفاقية بودابست أن جوهر الاحتيال هو التلاعب بمدخلات النظم المعلوماتية بمعنى تغذية الحاسب الآلي ببيانات غير صحيحة للإيهام بصحتها، أو من خلال التلاعب في البرامج عن طريق تعديلها أو تقليدها أو اصطناعها أو الدخول عليها باسم وصفة المستخدم الأصلي لها على غير الحقيقة أو عبر التلاعب في معالجة البيانات بالحذف أو بالإضافة عليهما معا، وذلك بهدف الحصول على مبالغ نقدية أو سندات أو أية أموال منقولة أخرى سواء لنفسه أو للغير، وهو ما ينطبق النص المتعلق بالنصب على التلاعب المعلوماتي[1].

ويمثل هذا الاتجاه الذي يطبق النصب المعلوماتي تشريعات الدول الأنجلوسكسونية والتي جاءت نصوصها في مجال النصب على نحو أعم وأشمل من نظيرتها الأوروبية بحيث يمكن تطبيقها على النصب المعلوماتي، ففي انجلترا ودول الإقليم الغربي من بريطانيا فإن التفسير الضيق لنصوص قانون السرقة يشمل التلاعب في البيانات من أجل الحصول على منفعة مالية، إذ تنص المادة 16 من قانون السرقة على أنه يعاقب كل من حصل على نحو غير مشروع وبأي وسيلة خداع سواء لنفسه أو للغير على منفعة مالية، إلا أنه وعلى الرغم من ظاهر هذه النصوص أنه يوحي بإمكانية تطبيقها على النصب المعلوماتي إلا أن القضاء الانجليزي لم يطبقها في قضية Regina [2] .

لكن يجب الإشارة أنه لقيام جريمة النصب أن يكون تسليم المال قد تم بناءا على الطرق الاحتيالية التي قام بها الجاني، فالاحتيال يسبق تسليم المال، ومنه لا يمكن تطبيق النص الخاص بجريمة النصب في حالات الاحتيال المعلوماتي التي تنطوي على التلاعب ببيانات

---

[1]– هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، المرجع السابق، ص 184.

*وتتلخص وقائع القضية بتلاعب أحد الأشخاص في البيانات المعالجة الكترونيا بواسطة الحاسب الآلي والخاصة بسداد الضريبة بهدف التهرب منها حيث اعتبرت المحكمة الغش الواقع على الآلة لا يعد من قبيل الاحتيال المعاقب عليه جنائيا وهذا مادفع البرلمان الانجليزي إلى إجراء تعديل عام 1984 يهدف إلى اعتبار خادع الآلة بنية ارتكاب غش مالي من قبيل الاحتيال المعاقب عليه قانونا. الوقائع مشار إليها في : محمد سامي الشوا، المرجع السابق، ص 124 .

التوقيع الالكتروني المبرمجة آليا من أجل إخفاء ما تم الحصول عليه بطريقة غير مشروعة [1]، وفي حالة النصب على معلومات التوقيع الالكتروني التي تم نقلها بالقول، فإنه لا يوجد نشاط إجرامي مجسم يتحقق به التسليم والإستلاء في هذه الحالة، وبالتالي لا ينتج عن ذلك حرمان المجني عليه من معلومات التوقيع الالكتروني التي تظل بحوزة الجاني وتحت سيطرته وهو ما لا يتفق والنشاط الإجرامي في جريمة النصب [2].

ثانيا: الاحتيال على الحاسب الآلي بوصفه آلة

تنطوي كثير من حالات الاحتيال المعلوماتي على اتصال بين الجاني والمجني عليه والذي يكون في أغلب الحالات هو الإنسان، وهناك حالات يكون تعامل الجاني مع نظام الحاسب الآلي وليس الإنسان، كما هو الحال في الاستعمال غير المشروع لبطاقات الائتمان لسحب النقود من أجهزة الصراف الآلي أو الحالات التي يتم فيها تحويل الأموال إلكترونيا دون تدخل لأي عنصر بشري، أو الحصول على خدمات يقدمها الحاسب الآلي بمقابل ويتم الاحتيال عليه دون دفع الثمن، وظهر هذا الشكل بظهور الانترنت وما تقدمه من خدمات يتم الحصول عليها بإدخال الرقم الخاص بالبطاقة الائتمانية لطالب الخدمة والذي يقوم بإدخال بيانات غير سليمة للبطاقة كإدخال الرقم السري للبطاقة[3]، والذي يعد نوعا من أنواع التوقيع الإلكتروني، فيلجأ الجاني في هذه الحالة إلى الاحتيال على صاحب التوقيع الالكتروني من أجل انتزاعه منه ما يجعله يسلك طريقا غير مشروعا للحصول على توقيع إلكتروني بطريق الاحتيال، ولا يمكن أن تقع جريمة النصب على الآلة فإذا لم يوجد شخص طبيعي وقع ضحية احتيال نتيجة للتلاعب بالبيانات ومعطيات الحاسب من الصعب القول بوجود احتيال بمعنى تقليدي، وفي مجال

---

[1]– نائلة قورة، المرجع السابق، ص 568 .

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 97 .

[3]– نائلة قورة، المرجع السابق، ص 557.

المعلوماتية لا بد من وجود من يتحكم في نظام الحاسب أثناء إتيان الجاني لفعل الاحتيال بأن يكون له القدرة على اتخاذ القرار أو التحقق من سلامة العملية التي تتم[1].

الفرع الثالث: خيانة الأمانة

جرم المشرع الجزائري خيانة الأمانة في نص المادة 376 من قانون العقوبات والتي يقتضي النشاط الإجرامي فيها بتسليم المال بناء على عقد من عقود الأمانة وهي الإجارة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو استعمالها أو لاستخدامها في عمل معين، ليقوم بعدها المؤتمن بالاستيلاء على الحيازة الكاملة للمال المسلم إليه لحسابه الخاص من خلال أي فعل من الأفعال التي حددها القانون وهي الاختلاس، التبديد، الاستعمال.

ولا جدال في وقوع جريمة خيانة الأمانة بالنسبة للأشرطة أو الأقراص الممغنطة المثبت عليها التوقيع الالكتروني ، في حالة تجاوز الأمين حدود الاتفاق، أو في حالة عدم رد الأقراص أو الأشرطة التي تحوي التوقيع الالكتروني، أو إذا تصرف فيها شخص آخر[2]، لذلك سنتطرق إلى الاتجاه القائل بتطبيق خيانة الأمانة التقليدية الواقعة على البيانات الالكترونية للتوقيع الالكتروني، والاتجاه المعارض له.

أولا:الاتجاه القائل بعدم تطبيق خيانة الأمانة التقليدية الواقعة على البيانات الالكترونية للتوقيع الالكتروني

اتجه القضاء الفرنسي في بعض أحكامه إلى عدم انطباق وصف خيانة الأمانة على إفشاء معلومات مؤتمن عليها وأكدت ذلك محكمة النقض الفرنسية في قضية « DACF »، وتتلخص وقائع هذه القضية في قيام مدير فرع مكتب « DAFC » بالمحاسبات القانونية بتسليم العقود التي سلمت إليه بمقتضى وظيفته إلى رؤسائه وذلك بمناسبة إنهاء عمله وقد كان من بين هذه

[1]– نائلة قورة ، المرجع السابق، ص 561.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 99 .

العقود عدد كبير تم فسخه من قبل العملاء الذين اتفقوا مع المدير السابق بتقديم ذات الخدمات التي كانت منصوصا عليها في العقود الملغاة المبرمة بينهم وبين مكتب المحاسبة القانونية والتي كان يتولى تنفيذها على أن يكون ذلك لحسابه الخاص، وقدم المتهم للمحاكمة بتهمة خيانة الأمانة بقيامه باختلاس العقود التي تعد ملكا للمكتب الذي يعمل به، وقد سلمت إليه للقيام بعمل محدد إضرار بالضحية، وذهبت محكمة أول درجة إلى أن جميع العناصر المكونة لجريمة خيانة الأمانة قد تحققت، إلا أن محكمة الاستئناف برأت المتهم من التهمة المنسوبة إليه وهو ما أيدته محكمة النقض الفرنسي في حكمها الصادر في 09 مارس 1987[1].

ويلاحظ بعض الفقه أن وضع المعلومات المؤتمن عليها الأمين موضع التنفيذ لحسابه الخاص بواسطة آخر يصدق عليه وصف الاستعمال الذي يتحقق به النشاط الإجرامي في جريمة خيانة الأمانة، لأنه يعتبر نشاطا ماديا ينتج عنه استنزاف قيمة المعلومات، أما صورة التعامل في هذه المعلومات كبيعها من خلال النقل الشفوي فقط فإنه لا تتحقق جريمة خيانة الأمانة لعدم توافر الاختلاس أو التبديد أو الاستعمال [2].

ثانيا: الاتجاه القائل بتطبيق خيانة الأمانة التقليدية الواقعة على البيانات الالكترونية للتوقيع الالكتروني

على العكس فلقد اتجه القضاء الفرنسي إلى انطباق وصف خيانة الأمانة على الاستيلاء غير المشروع على أموال متحصل عليها عن طريق التلاعب في البيانات المعلوماتية الخاصة بحسابات عملاء لدى إحدى شركات توظيف الأموال، وتتلخص وقائع القضية في شاب يدعى HIVAR عمل كمستخدم في قسم الصرافة لشركة TUFFIER HAVIRRY لتوظيف الأموال وقد ألحق للعمل بها عام 1987 وهو نفس عام بداية اقترافه لأفعاله الاحتيالية وقد أسندت إليه وظيفة مراجعة حسابات العملاء المؤسسين ووضع تحت تصرفه بعض الأساليب المعلوماتية الخاصة لنظام المعالجة الآلية للبيانات، فاستثمر لصالحه عن طريق الاستقطاع من حسابات

[1]– محمد سامي الشوا، المرجع السابق، ص 290.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 98 .

العملاء من أرصدتهم الراكدة وتحويلها إلى حسابات أخرى مفتوحة عن طريق أشخاص آخرين، وقد تمكن المتهم من الحصول على شفرة الولوج إلى إدارة التحويلات من حساب إلى آخر، وكان له في الواقع لكي يكشف هذه الشفرة أن يطلع على قائمة LISTING ، وقد خاطب المتهم صديقا له يدعى BLOT ، وصهرا له يدعى CARISTAN وفتح لكل منهما حساب عميل لدى الشركة التي كان يعمل بها [1].

وقد أيد هذا الاتجاه القائل بإمكانية تطبيق خيانة الأمانة على بيانات التوقيع الالكتروني بعض الفقه وحجته بأن محل جريمة خيانة الأمانة المعلوماتية كما هو الحال في جريمة السرقة والنصب المعلوماتي هو المال المعلوماتي، فبيانات التوقيع الالكتروني التي يقوم الشخص بإيداعها لدى مزود الخدمة لتخزينها مثلا فيقوم هذا الأخير بتغيير حيازتها أو يستعملها لمصلحته أو يبيعها يعد خائنا للأمانة المعلوماتية [2].

وتتحقق جريمة خيانة الأمانة المعلوماتية من خلال مايلي[3]:

1. إمكانية تطبيق فعل خيانة الأمانة بصوره الثلاث الاختلاس أو الاستعمال أو التبديد على جريمة خيانة الأمانة المعلوماتية إذا تحقق صورة الاختلاس المكونة لجريمة خيانة الأمانة في حالة قيام المجني عليه المعلوماتي بتسليم بيانات التوقيع الالكتروني إلى مزود الخدمة لمعالجتها آليا فيقوم هذا الأخير بمعالجتها لحسابه الخاص ، كما تتحقق صورة التبديد إذا قام مزود الخدمة ببيع هذه البيانات .

2. يستوي في مقدم الخدمة حسب اتفاقية بودابست أن يكون جهة عامة أو خاصة ، وسواء أكانت الخدمة موجهة لجميع الأفراد أو تخص فئة معينة، كذلك يستوي أيضا أن تكون الخدمة بمقابل أو بالمجان.

---

[1]– محمد سامي الشوا، المرجع السابق، ص 290.

[2]– هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة، المرجع السابق، ص 204 .

[3]– المرجع نفسه، ص 206 .

3. يمكن أن يكون مزود الخدمة من الأشخاص الذين يعرضون خدمة الاستضافة أو التخزين المؤقت.

وتميل بعض التشريعات المقارنة إلى التطبيق الضيق للنصوص الجنائية الخاصة بخيانة الأمانة والتي لا يمكن تطبيقها في الغش المعلوماتي سواء في مرحلة التلاعب في بيانات التوقيع الالكتروني المدخلة إلى الحاسب الآلي أو في مرحلة البرمجة، سوى على طائفة محددودة من الأشخاص وهم الذين يشغلون درجة وظيفة عالية، ومنه يستبعد تطبيقها على الذين يعملون في لوحة المفاتيح والمحللين والمبرمجين وسائر الأشخاص الآخرين الذين يستعملون الحاسب الآلي، ومن أمثلة هذه التشريعات النمساوي والألماني والسويسري[1]، ونرى بأنه يمكن تطبيق خيانة الأمانة على بيانات التوقيع الالكتروني، لسببين الأول هو أنه يمكن اعتبار البيانات الالكترونية من المال ذو قيمة خاصة، والسبب الثاني أنه يمكن أن تكون مؤتمنة لدى شخص ملزم بالمحافظة عليها في إطار عقد من عقود الأمانة.

الفرع الرابع: جريمة إتلاف بيانات التوقيع الالكتروني

جريمة إتلاف بيانات التوقيع الالكتروني تجمع مابين الجرائم الالكترونية والتقليدية، ولا تثير أي صعوبة في تطبيق الأحكام الخاصة بجريمة الإتلاف والتخريب في حالة إتلاف العناصر المادية لنظام المعالجة الآلية للمعطيات باعتبارها أموالا منقولة[2]، إلا أن الكيانات المنطقية للتوقيع الالكتروني تثير إشكال فيما تعلق بإتلافها، لذلك سنطرق إلى مفهوم إتلاف بيانات التوقيع الالكتروني، ثم إلى أركان جريمة إتلاف بيانات التوقيع الالكتروني.

أولا: مفهوم إتلاف بيانات التوقيع الالكتروني

من أخطر الأفعال الواقعة على التوقيع الالكتروني تكون عن طريق إتلافه، لذلك سنتطرق إلى بيان تعريف إتلاف التوقيع الالكتروني ، ثم وسائل أو طرق إتلافه.

---

(1)– محمد سامي الشوا، المرجع السابق، ص 131 .

(2)– نائلة قورة، المرجع السابق ص 190 .

أ. تعريف إتلاف التوقيع الإلكتروني

ويقصد بها محو أو تدمير تعليمات البرامج أو البيانات ذاتها ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها، ولكن يبقى ببساطة إحداث ضرر بنظام المعلومات وإعاقته عن أداء وظيفته[1] ، وهناك من يعرف إتلاف التوقيع الالكتروني بأنه استخدام أي من الوسائل التكنولوجية أو البرامج لإحداث تعديل أو محو أو تدمير لنظم معلومات التوقيع الالكتروني أو أي من مكوناتها المنطقية للإضرار بالمؤسسة أو الشخص صاحب التوقيع الالكتروني بقصد جعل النظام المعلوماتي غير صالح للاستخدام [2]، كما ورد مصطلح الإتلاف في الفقرة الأولى من المادة الرابعة لاتفاقية بودابست وهو يعني تغيير البيانات الموجودة، وكذلك إدخال شفرات عدوانية كالفيروسات وأحصنة الطراودة والتي من شأنها تغيير البيانات التي تنتج عن هذا التصرف[3]، وجريمة الإتلاف التقليدية تحقق حماية جزائية لأفعال الإتلاف والتخريب التي تؤدي إلى عدم صلاحية الاستعمال أو التعطيل لبرامج الحاسب الآلي وبيانات التوقيع الالكتروني المعالجة آليا [4].

ب. وسائل إتلاف بيانات التوقيع الالكتروني المبرمجة آليا

الإتلاف بواسطة فيروسات وبرامج أخرى.

1. الإتلاف بواسطة الفيروس

الفيروسات هي برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة للاتصالات بحيث يمكنه من أن ينتقل عبر الحدود من أي

---

[1]– محمد سامي الشوا، المرجع السابق، ص 165 .

[2]– محمد نبيل الشنراقي ، المرجع السابق، ص296 .

[3]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة، المرجع السابق، ص202 .

[4]– علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص104 .

مكان إلى آخر في العالم وهو يسمى عادة باسم أول مكان اكتشف فيه[1] ، ولا يستطيع مستخدمو الحاسب معرفة الفيروسات الملوثة بدون وجود برامج أخرى تستخدم لاكتشافه تنشط في وقت محدد ليقوم بتدمير البيانات والمعلومات المختزنة داخل الجهاز دون أن يفسد المكونات المادية التي يتكون منها هذا الجهاز[2].

أو بمعنى آخر الفيروسات هي مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا لدرجة تصيب النظام المعلوماتي بالشلل التام، أي عبارة عن خلية كهرومغناطيسية نائمة ومبرمجة بحيث تنشط في وقت محدد لتخريب البرنامج الأصلي وتنشر في الأجهزة الأخرى التي تضمنتها الشبكة بحيث تفسد ما تحويه من معلومات.

وتتمتع هذه الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسبات الآلية والشبكات العامة والخاصة، ويسفر عن ذلك تدمير البرامج والمعلومات وتعيق الاتصالات وتشوه البيانات، بل وتضلل المستخدم أحيانا ببيانات خاطئة، وتسلل هذه الفيروسات إلى الحاسبات الآلية في صمت عند اتصالها بإحدى الشبكات الملوثة أو عند نقل برنامج مصاب لذاكرة الحاسب، حيث لم تلبث أن تتكاثر خفية دون دراية من المستخدم أو من نظام تشغيل الحاسب حتى تصيبه بالشلل التام[3].

(1) - Fish rigrir deborah, natinal and international aspects of computer crime : the emerging need for statutory controls, thesis university of london, center for criminal law studies, queen mary and westfield college, january, 1993 , P 189.

نقلا عن: نائلة قورة، المرجع السابق، ص 192.

(2)– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 104.

(3) – محمد سامي الشوا، المرجع السابق، ص 166.

ويمكن تقسيم الفيروسات والملوثات المعلوماتية إلى عدة أقسام مختلفة تبعا لاختلاف وجهات النظر التي يتأسس عليها التقسيمات [1] :

- ✓ **من حيث النوع**

يمكن تقسيمها إلى أربعة أنواع رئيسية:

– الفيروسات المعلوماتية، الديدان المعلوماتية، أحصنة الطراودة، القنابل المعلوماتية المنطقية.

- ✓ **من حيث سرعة الانتشار**

هناك فيروسات سريعة الانتشار وهناك البطيئة.

- ✓ **من حيث توقيت النشاط**

هناك فيروسات تنشط في أوقات محددة أو دائمة النشاط.

- ✓ **من حيث مكان الإصابة**

هناك فيروسات مقطع التشغيل boot sector على الأقراص ، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات.

- ✓ **من حيث حجم الضرر**

يمكن تقسيمها إلى ثلاثة أنواع: الفيروسات المدمرة للأجهزة والعتاد ، الفيروسات المدمرة للبرامج، فيروسات عديمة الضرر وهي التي تم برمجتها لإثبات الذات.

- ✓ **من حيث درجة الخطورة**

يمكن تقسيمها إلى خمسة أنواع:

– **الفيروس العادي trivial virus :** ويقتصر عمله على مجرد التكاثر دون إحداث ضرر أو تخريب للمعلومات .

[1]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت، المرجع السابق، ص ص 153 – 145 .

- **الفيروس الثانويminor virus:** وهو يصيب الملفات التنفيذية دون تأثير على البيانات .

- **الفيروس المعتدل moderate virus :** وهو يقوم بتدمير جميع الملفات الموجودة على القرص إما باستبدال المعلومات لا معنى لها، أو عن طريق إعادة التهيئة .

- **الفيروس الرئيسي major virus :** وهذا الفيروس يؤدي إلى تخريب المعلومات بإجراء تغييرات للبيانات دون أن يترك أثرا يشير إلى التغيير الحاصل، كأن يقوم بتبديل كتل المعلومات المتساوية في الطول بين الملفات، كما أن تأثيره يكون على المدى الطويل ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام.

- **الفيروس اللامحدود unlimited virus :** وهذا الفيروس يستهدف الشبكات والملفات المشتركة ، وكذلك معرفة كلمة السر للمستخدمين الأكثر فاعلية.

2. الإتلاف بواسطة البرامج الخبيثة

كبرامج الدودة التي تستغل فجوات في نظام التشغيل لكي تنتقل من حاسب إلى آخر أو من شبكة إلى أخرى عبر الوصلات التي تربط بينهما، وتتكاثر أثناء عملية انتقالها كالبكتيريا بإنتاج نسخ منها، وتهدف هذه البرامج إلى شغل أكبر حيز ممكن من سعة الشبكة، ومن ثمَ العمل على تقليل أو خفض كفاءتها، وأحيانا تتعدى هذا الهدف لتبدأ بعد بالتكاثر والانتشار في التخريب الفعلي للملفات والبرامج ونظام التشغيل.

ومن أمثلة برامج الدودة INTERNET WARM التي عن طريقها تمكن طالب أمريكي يدعى روبرت موريس طالب دراسات عليا في جامعة كورنيل لولاية نيويورك من تدمير 16000 شبكة حاسب، وترتب على هذا الهجوم في خسائر تمثلت في تأخير الأبحاث، وفي إعادة البرمجة في تكاليف بلغت العديد من ملايين الدولارات[1].

(1) – محمد سامي الشوا، المرجع السابق، ص 169.

وفضلا عن استخدام البرامج الخبيثة كوسيلة لإتلاف المكونات المنطقية للحاسبات الآلية توجد وسائل أخرى يتم الاستعانة بها من أجل إحداث هذا التلف على سبيل المثال محو البيانات عن طريق تعريض الأسطوانات أو الأقراص الممغنطة المسجلة عليها لقوى مغناطيسية أو قطع التيار أثناء معالجة بيانات التوقيع الالكتروني أو وضع شريحة أو دائرة مطبوعة في غير مكانها الصحيح أو التلاعب في البيانات بتغييرها بحيث تفقد قيمتها وحقيقتها التي كانت عليها[1].

ثانيا: أركان جريمة إتلاف بيانات التوقيع الالكتروني

جريمة إتلاف بيانات التوقيع الالكتروني تقوم على ركنين مادي ومعنوي.

أ.الركن المادي لجريمة الإتلاف

المشرع الجزائري لم يدرج نص خاص يعاقب على إتلاف البيانات الالكترونية، بينما قرر المشرع الفرنسي صياغة نص مادة جديد يجرم فيها إتلاف البرامج والمعلومات وهو نص المادة 274 فقرة 03 ويبين فيه صور الإتلاف وهي عن طريق محو البيانات ويقصد بها تدمير البيانات إلكترونيا كلها أو بعضها supprimé les donne أو إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة intoduire des donnes dans le système de traitement automatisé أو تعديل البيانات أو طرق معالجتها أو وسائل انتقالها Modifie les donnes qu'il contient que leur mode de traitement ou de transmission [2]، لذلك يتخذ الركن المادي لجريمة إتلاف بيانات التوقيع الالكتروني إما صورة تعديلات غير مشروعة، أو تدمير البيانات، أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسب الآلي.

---

[1] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية–دراسة مقارنة، ط1 ، دار الفكر الجامعي، الإسكندرية، 2018 ، ص 431 .

[2]– هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الالكتروني، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثالث، ط3، جامعة الإمارات العربية المتحدة، 2003 ، ص896 .

1.التعديل غير المشروع للمعلومات

يشكل التعديل غير المشروع للمعلومات المبرمجة آليا واحد من أكثر صور الإتلاف المعلوماتي الواقع على التوقيع الالكتروني والذي هو كل تغيير غير مشروع للمعلومات والبرامج التي تتم عبر استخدام إحدى وظائف الحاسب الآلي.

وقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلقة بجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات والبرامج، وبين التعديلات الغير مصرح بها والتي لا تؤدي إلى إحداث هذه النتائج، بل قد تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ونظامه، وقد تضمنت التوصية بندا يطالب بإدراج التعديلات الأولى ضمن القائمة الأساسية لجرائم المعلوماتية، ولكنه اكتفى في خصوص الثانية بإدراجها ضمن القائمة الاختيارية إلا أن الدول التي جرمت المعلومات لم تعتد بهذه التفرقة حيث تم تجريم كافة أشكال التعديل [1].

2. تدمير المعلومات

يعد تدمير المعلومات أحد صور الإتلاف وإن كان أبعد أثرا من مجرد إجراء تعديلات للمعلومات، وقد استخدمت جميع القوانين التي جرمت الإتلاف المعلوماتي تعبيري إخفاء المعلومات ومحوها للتعبير عن تدمير المعلومات باعتباره صورة متميزة من صور الإتلاف، ويرى البعض أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تدميرا لها، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو للمعلومات التي يحوي عليها من ذاكرة الحاسب الآلي وإنما يؤدي فقط إلى تعديل في قائمة الملفات، وهو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو إلا أن يكون تعديلا وليس تدميرا لها [2]، وتدمير نظم معلومات التوقيع الإلكتروني أشد من التعديل، وقد فرقت التوجيهات الأوروبية في مسألة تدمير

---

[1]– نائلة قورة، المرجع السابق، ص 217 .

[2]– المرجع نفسه، ص 218 .

المعلومات بين فرضيتين أولهما محو المعلومات تماما والثاني إخفاؤها بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محو المعلومات، وقد استخدمت معظم التشريعات هذين اللفظين للدلالة على تدمير المعلومات، إلا أن المشرع الانجليزي اعتبر التعديل من صور الإتلاف المعلوماتي[1]، ونرى بأن الإخفاء لا يعد تدميرا لمعلومات التوقيع الإلكتروني لأنها ما زالت مخزنة ضمن نظام الحاسب الآلي ويمكن الاطلاع عليها في مرحلة لاحقة.

3. الإدخال غير المشروع للمعلومات

نصت الكثير من قوانين العقوبات التي جرمت الإتلاف المعلوماتي على الإدخال غير المشروع للمعلومات كصورة من صور الركن المادي لهذه الجريمة ومنها فرنسا السويد هولندا، وقد ذهب القضاء الفرنسي في جريمة إتلاف المكونات المنطقية لأنظمة الحاسبات الآلية إلى اعتبار إدخال المعلومات والبرامج على نحو غير مشروع مكونا لهذه الجريمة، حيث أدانت محكمة باريس عام 1990 أحد الأشخاص بتهمة إتلاف معلومات لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي، كما أدانت أيضا محكمة ليموج عام 1994 أحد المتهمين بتهمة إتلاف المكونات المنطقية للحاسب الآلي لقيامه بإدخال برنامج خبيث حصان طراودة إلى نظام الحاسب الآلي مما ترتب عليه إتلاف المعلومات فضلا عن إعاقة النظام عن أداء وظيفته[2].

ويتخذ السلوك الإجرامي في جريمة الإتلاف وفقا للمادة 04 من اتفاقية بودابست إحدى الصور التالية وهي الإضرار أو محو أو تعطيل أو إتلاف أو طمس لبيانات الحاسب، وتشير المذكرات التفسيرية أن الهدف من تقرير هذا النص أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمدا بالمصالح القانونية المحمية وهي سلامة وحسن تشغيل أو حسن استخدام البيانات أو برامج الحاسب المسجلة، وقد ورد في الفقرة الأولى من المادة الرابعة مصطلح الإضرار، ومصطلح التعطيل،

[1]– حسام محمد نبيل الشنراقي، المرجع السابق، ص 317.

[2]– نائلة قورة، المرجع السابق، ص 219 .

وهي من الأعمال المتراكمة التي تتصل على وجه الخصوص بالإتلاف السلبي لسلامة ومحتوى البيانات والبرامج، كما ورد في هذه الفقرة أيضا مصطلح محو البيانات، وهذا المصطلح يعادل تدمير الأشياء المادية، فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها [1].

أما مصطلح طمس البيانات فهذا المصطلح يمتد ليشمل كل تصرف من شأنه أن تجعل هذه البيانات غير كائنة أو غير متاحة للشخص الذي له حق الولوج إلى داخل الحاسب، أو الاعتماد على تلك البيانات التي كانت مخزنة، وفيما تعلق بمصطلح الإتلاف فهو يعني تغيير البيانات الموجودة وكذلك إدخال شفرات عدوانية مثال ذلك فيروسات أو أحصنة طروادة والتي من شأنها تغيير البيانات التي تنتج عن هذا التصرف[2].

ب.الركن المعنوي

جريمة إتلاف بيانات التوقيع الالكتروني جريمة عمدية تتطلب قصدا جنائيا عاما، أي علم الجاني أنه يقوم بأحد الأفعال التي من شأنها أن تؤدي إلى الإتلاف أو إعاقة نظام الحاسب الآلي عن أداء وظيفته، وأن تتجه إرادته إلى تحقيق هذه النتيجة، ومن التشريعات كالتشريع الانجليزي تتطلب أن يسبق فعل الإتلاف دخول غير مصرح به إلى نظام الحاسب، لذلك فإنه يجب أن تنصرف إرادة المتهم أولا إلى أن الدخول الذي يقوم به غير مصرح به، وهناك من التشريعات من تتطلب قصدا خاصا، كالقانون البرتغالي والفلندي والتركي الذي يتطلب أن تتجه نية المتهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير[3].

وقد انتقد بعض الفقه تطلب القصد الخاص في جريمة الإتلاف وإعاقة النظام، خاصة متى تعلق هذا القصد بتحقيق ربح مادي غير مشروع، لأن اشتراط هذا القصد سوف يؤدي إلى استبعاد تطبيق جريمة الإتلاف المعلوماتي في الحالات التي تتجه فيها نية الفاعل إلى تحقيق الربح على الرغم من أهمية المعلومات التي قد يتم إتلافها، كما تطلب الإضرار بالغير كقصد

---

[1]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت، المرجع السابق، ص 201 .

(2)– المرجع نفسه، ص 202.

[3]– نائلة قورة، المرجع السابق، ص 223 .

خاص يجب أن يفسر تفسيرا واسعا بحيث لا يقتصر على مجرد الخسائر أو الأضرار المادية التي قد تلحق بالمجني عليه، وعلى إثر هذا النقد تراجع المشرع الفرنسي من تطبيق القصد الخاص في جريمة إتلاف المعلومات وإعاقة النظام عند تعديل النصوص الخاصة بالإتلاف المعلوماتي[1]، وقد اشترطت المادة 04 من اتفاقية بودابست في سلوكات الإضرار أو المحو أو التعديل أو الإتلاف أو طمس البيانات أنه لا يتم المعاقبة عليا إلا إذا كانت بدون وجه حق[2] .

المطلب الثاني: موقف التشريعات من تطبيق النصوص الجزائية التقليدية في جرائم الاعتداء على بيانات التوقيع الالكتروني

لقد تباينت المواقف بين اتجاه يطبق النصوص التقليدية مع إدخاله تعديلات عليها تتلاءم وطبيعة الإجرام الالكتروني المستحدث، وبين اتجاه آخر نص على نصوص مستحدثة تحوي الأنماط الإجرامية المستحدثة للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني.

الفرع الأول: الاتجاه القائل بتطبيق النصوص التقليدية

لا يثير هذا النوع من الأفعال (النصب، السرقة، خيانة الأمانة) أدنى مشكلة في الدول التي تبنت تصورا شاملا للغش المعلوماتي كما هو الحال في السويد والولايات المتحدة الأمريكية وعلى سبيل المثال فالمادة 21 من قانون السويد الخاص بالبيانات الشخصية الصادر سنة 1973 والتي لها مجال أعم تنص على كل من ولج بوسائل غير مشروعة في سجل معلومات خصص للمعالجة الآلية للبيانات وكل من أتلف أو نقل على نحو غير مشروع هذا السجل في ملف يعاقب على سرقة البيانات، وفي الولايات المتحدة فإن بعض الولايات الفيدرالية حذت حذو القانون الفيديرالي الخاص بحماية أنظمة الكمبيوتر الصادر سنة 1977 فأصدرت قوانين تعرف

---

(1) - vergutch pascal, la répression des délits informatiques dans une perspective international, thèse, université de Montpellier, 1996 , p 233

نقلا عن : نائلة قورة، المرجع السابق، ص 224

(2)– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت، المرجع السابق، ص ص 201 – 202.

المال بأنه كل شيء يمثل قيمة، ويشمل هذا التعريف الأموال المعنوية والبيانات المعلوماتية، كما يعاقب كل من دبر عن إرادة وعلم أو نفد خطة أو حيلة أيا كانت بغرض ارتكاب نصب أو سلب للأموال[1].

الفرع الثاني: الاتجاه القائل بتطبيق نصوص خاصة وموقف المشرع الجزائري

نظرا للصعوبات السابق ذكرها التي تواجه الحماية الجزائية للبيانات الالكترونية للتوقيع الالكتروني من خلال جرائم الأموال التقليدية، اتجه الفكر القانوني إلى البحث عن وضع نصوص خاصة لتحقيق تلك الحماية، فظهر اتجاه ينادي بتطويق النصوص المتعلقة بجرائم الأموال التقليدية وتعديلها بحيث تتلاءم مع طبيعة المال المعلوماتي ومع النشاط الذي يتحقق به الاعتداء على هذا المال كجرائم السرقة النصب خيانة الأمانة والتخريب والإتلاف والتعييب، لكن تلك المحاولات لم تكلل بالنجاح لأن الأخذ بها يؤدي إلى تشويه المبادئ المستقرة التي تقوم عليها تلك الجرائم، كما أنها لا تحقق الحماية الكافية لبيانات التوقيع الالكتروني[2]، والمشكل الأكثر جسامة ينبع من أن غالبية النصوص الجزائية التقليدية قد وضعت في مرحلة سابقة على ظاهرة الغش المعلوماتي[3]، وذلك لعدم ملائمة القواعد التقليدية في قانون العقوبات لمواجهة جرائم السرقة والنصب وخيانة الأمانة إذا وقعت على معلومات وبيانات التوقيع الالكتروني بسبب طبيعتها الخاصة إذا ما قورنت بغيرها من المنقولات، وأن النصوص التقليدية تتطلب الاستيلاء على الحيازة بإخراج المال من حوزة المجني عليه فتقع السرقة بالاختلاس، وبالتسليم في النصب، أو بالاختلاس أو بالاستعمال أو بالتبديد في جريمة خيانة الأمانة، وهو مالا يمكن تطبيقه في الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، ولا تكتسب المعلومات

---

[1]– محمد سامي الشوا، المرجع السابق، 139.

[2]– علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، المرجع السابق ، ص 589 .

[3]– محمد سامي الشوا، المرجع السابق ، ص 97 .

صفة المال المنقول الذي تحميه جرائم الأموال إلا إذا كانت على دعامة مادية [1]، ولا يمكن التوسع في تفسير النصوص التقليدية على اختلافها، وعليه يلزم توفيرها عن طريق حماية تشريعية خاصة، ولتوفير حماية المعلومات وبيانات التوقيع الالكتروني يجب تجريم الحصول عليها بطريق غير مشروع بأن تتضمن أنماط السلوك المختلفة التي يمكن أن تؤدي إلى حصول الغير عليها سواء أكان ذلك بالاستيلاء أو الحصول على معلومات يعلم المتهم بأنها متحصله من جريمة معلوماتية أخرى أو عن طريق الاحتيال أو إفشائها للغير.

وفي إتلاف بيانات التوقيع الالكتروني فلا يمكن تطبيق النصوص التقليدية الخاصة بإتلاف الأموال في مجال المعلوماتية، ما لم ينصب الإتلاف على الحاسب الآلي ذاته أو أي من مكوناته المادية أما الإتلاف الذي ينصب على المكونات المنطقية للحاسبات الآلية والأفعال التي تستهدف إعاقة النظام عن أداء وظيفته فلا يمكن تطبيق النصوص التقليدية بشأنها، لذا لابد من نصوص قانونية خاصة لحماية معلومات التوقيع الالكتروني في جرائم الأموال[2].

وقد كان القضاء الفرنسي قبل صدور قانون الغش المعلوماتي لسنة 1988، ولوقت طويل يعطى حلولا في الكثير من الحالات، لكنه لم يستطع في حالات أيضا إعطاء التكييف الصحيح لوقائع إجرامية متعلقة بالحاسب الآلي بالنصوص التقليدية، إذ أصبح القضاء متناقض، لنعطي مثالين عن هذا التناقض، المثال الأول قضاء محكمة bordeau الصادر في 25 مارس سنة 1987 بأنه تشكل جريمة نصب، وانتحال لصفة الغير، للمتهم الذي عثر على بطاقة ائتمان، ثم استعملها لسحب المال من بطاقة الصراف الآلي، ومثال ثاني آخر ما قضت به محكمة النقض الفرنسية بأن من يقوم بسحب مبلغ أكثر من رصيده من الصراف الآلي بواسطة بطاقته

---

[1]– غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط3 ، جامعة الإمارات العربية المتحدة، 2003 ، ص 659 . وأنظر كذلك: مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنيت، دار النهضة العربية، القاهرة، 2000 ، ص37 .

[2]– نائلة قورة، المرجع السابق، ص 227 .

الائتمانية، لا يشكل لا جريمة نصب ولا سرقة ولا خيانة أمانة [1]، وأمام هذا الوضع وجب وضع حد لتطبيق النصوص الجزائية التقليدية في مجال المعلوماتية، مع ضرورة تدخل المشرع لسد الفراغ القانوني في الكثير من الحالات[2].

وتظل هناك العديد من الإشكالات التي تثار عند تطبيق النصوص الجزائية التقليدية على الأنماط المستحدثة للإجرام المعلوماتي والالكتروني الواقع على بيانات التوقيع الالكتروني، ما دعا بالمشرع الجزائري إلى إدراج جرائم المساس بأنظمة المعالجة الآلية للمعطيات في تعديل قانون العقوبات لسنة 2004، وذلك لأجل سد الفراغ القانوني الذي يكتنف جرائم المعلوماتية، ومن بينها جرائم المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني والتي سنتناولها بالدراسة في الفصل الثاني.

المبحث الثاني: تزوير التوقيع الالكتروني في المحررات الالكترونية

تتنوع الجرائم المخلة بالثقة العامة وتتعدد في قانون العقوبات ورغم هذا التعدد فتكاد أن تتوحد المصلحة القانونية المعتدى عليها أو المعرضة لخطر الاعتداء في كافة هذه الجرائم حماية ثقة الأفراد والأشياء والمحررات التي يضفي عليها المشرع حماية قانونية والتي تعتبر في الوقت ذاته أدوات لاغني عنها في تسيير الحياة اليومية لأفراد المجتمع يترتب على ذلك أن كل انحراف في المظهر القانوني الذي يصبغه المشرع على هذه المحررات وكل تعطيل لها عن إنتاج أثارها القانونية يعد انتهاكا للثقة العامة التي يحرص النظام القانوني على توافرها في هذه الصور، والانتقاص من مظهرها والكذب بشأنها يستوجب العقاب[3]، ويعد التزوير من الجرائم الماسة بالثقة العامة، التي نص عليه المشرع الجزائري في الفصل السابع من الكتاب الثالث من قانون العقوبات.

---

[1]- Jean Pradel, les infraction relative a l informatique, revue international de droit compare, vol 42, n 02, juin, 1990. P 816 .

[2]- Ibid , p 817 .

[3] – محمد زكي أبو عامر، سليمان عبد المنعم – قانون العقوبات– القسم الخاص، منشورات الحلبي الحقوقية، بيروت ، 2009 ، ص521 .

وفي ظل الانتشار الواسع لنطاق المعاملات الموقعة الكترونيا، وكثرة استخدام المحررات الالكترونية، كان لزاما على المشرع الجزائري أن يفرض حماية جنائية على المحررات الموقعة الكترونيا، لذلك سنتناول بالدراسة في هذا المبحث مفهوم تزوير التوقيع الالكتروني، ثم أركان جريمة تزوير التوقيع الالكتروني واستعماله.

المطلب الأول: مفهوم تزوير التوقيع الالكتروني

تزوير التوقيع الالكتروني من الجرائم الخطرة التي تمس الثقة في التعاملات الالكترونية نتيجة لزعزعة الأمن القانوني والالكتروني للتوقيع الالكتروني الذي نجد صوره في مجال التجارة الالكترونية، والعقود الالكترونية والسجلات الالكترونية وغيرها، وهو ما دفع بالمشرع إلى إصدار قانون التوقيع والتصديق الالكترونيين 15- 04، الذي نوه فيه على خطورة تزوير التوقيع الالكتروني، لذلك سنتناول بالدراسة في هذا المطلب تعريف التزوير، والعلة من تجريمه، خصائص جريمة تزوير التوقيع الالكتروني ومجالات استخدامه، ثم أخير موقف بعض التشريعات من تجريم تزوير التوقيع الالكتروني، ومنها موقف المشرع الجزائري.

الفرع الأول: تعريف التزوير

التزوير عرفه الفقيه garçon بأنه تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون، تغييرا من شأنه أن يسبب ضررا [1]، أو هو تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المحرر المزور فما أعد له[2].

الفرع الثاني: علة التجريم

علة تجريم التزوير في المحررات أنه يهدر الثقة العامة فيها ، ويخل تبعا لذلك بالضمان واليقين والاستقرار في المعاملات وسائر مظاهر الحياة القانونية في المجتمع ، فالناس يعتمدون

[1] – محمد زكي أبو عامر، سليمان عبد المنعم، المرجع السابق ، ص 525 .

[2]– محمود نجيب حسني، المرجع السابق، ص 215.

على الأوراق المكتوبة لإثبات علاقاتهم، والدولة تعتمد عليها في ممارسة اختصاصاتها المتنوعة وهي وسيلة أساسية لحسم منازعات القضاء، إذ تقوم بها الأدلة الكتابية التي تعد أهم وسائل الإثبات القانونية، ولا يتاح للكتابة أداء هذا الدور إلا إذا منحها الناس ثقتهم، فامنوا بصدق البيانات التي تثبتها، أما إذا كان تعارضها والحقيقة هو الوضع الغالب ، فإن ذلك يؤدي إلى رفض الناس الاعتماد عليها دون أن تكون لديهم الوسيلة التي تحل محلها، وتعثر التعامل وتعقيده، وعرقلة نشاط الدولة واضطرابه، ويحمي المشرع بتجريم التزوير الثقة العامة في المحررات[1] .

الفرع الثالث: خصائص جريمة تزوير التوقيع الالكتروني

لكل جريمة خصائص تميزها عن باقي الجرائم، حتى وإن كان هناك تشابه بينهم، ولجريمة تزوير التوقيع الالكتروني الكثير من الخصائص نذكر أهمها والمتمثلة في جمعها بين الجرائم التقليدية والمعلوماتية، وأنها من الجرائم المركبة، وأيضا من الجرائم التي تترتب عنها الكثير من الأضرار.

أولا: جريمة تزوير التوقيع الالكتروني تجمع بين خصائص الجرائم التقليدية والمعلوماتية

تتميز بأنها تجمع بين خصائص الجرائم المعلوماتية والعادية، وهي الخصائص المرتبطة بجريمة سرقة منظومة التوقيع الالكتروني وبين الخصائص المميزة للجريمة المعلوماتية كون الجريمة الأساسية تتم عبر استخدام التوقيع الالكتروني إلا انه في كثير من الأحيان قد لا تكون متوافرة على أساس أن سرقة التوقيع الالكتروني قد تتم عبر إحدى جرائم الانترنيت والحاسب الآلي، ولا تعتبر إحدى الجرائم التقليدية بل من الجرائم المعلوماتية [2]، وما يجمع بين تزوير التوقيع الالكتروني في الجرائم المعلوماتية والتقليدية هو في حالة استخدام التوقيع الالكتروني المزور أو التقليدي في كلا الحالتين يعاقب الجاني على استخدام توقيع مزور، والفرق بينهما

[1] – محمود نجيب حسني، المرجع السابق، المرجع السابق، المرجع السابق، 216 .

[2] – عبد الحليم فؤاد الفقي ، جريمة تزوير التوقيع الالكتروني ، دار النهضة العربية، القاهرة، 2016، ص 46 .

هو أنه في تزوير التوقيع الالكتروني يتم عبر أوساط الكترونية واستخدامه أيضا كاستخدام التوقيع الالكتروني الرقمي لبطاقة الائتمان من شخص غير صاحبها، وفي الجرائم التقليدية يكون استخدامه في مجالات أخرى .

ثانيا: جريمة تزوير التوقيع الالكتروني جريمة مركبة

تعتبر جريمة تزوير التوقيع الالكتروني جريمة مركبة لأنها تتكون من جريمتين الجريمة الأولى تتمثل في سرقة منظومة التوقيع الالكتروني لشخص ما، أما الجريمة الثانية فهي جريمة استخدام هذه المنظومة المسروقة بدون إذن مالكها، والسرقة هنا قد تتم بطريقة تقليدية كالتلصيص، وقد تتم عبر الشبكة المعلوماتية من خلال القرصنة الالكترونية والتجسس الالكتروني[1]، وفي نظرنا نرى بأن سرقة منظومة التوقيع الالكتروني جريمة مستقلة عن تزوير التوقيع الالكتروني، وتجمع بين السرقة التقليدية المعاقب عليها بنص المادة 350 من قانون العقوبات، وجريمة الاعتداء على نظام المعالجة الآلية للمعطيات المعاقب عليها بنص المادة 394 من قانون العقوبات .

ثالثا: خصائص متعلقة ب الأضرار

ضرر التزوير في التوقيع الالكتروني يمكن إجماله في[2] :

1.إلحاق الضرر بالسمعة التجارية للشخص: يعتبر التوقيع الإلكتروني من أهم الأدوات التي يستعين بها التاجر عند إبرام صفقاته عبر التجارة الإلكترونية، لذلك فالسمعة التجارية للتاجر تعد من أكبر الأضرار التي قد تصيبه ويفقد ثقة من حوله من التجار والزبائن.

2.إضعاف الثقة في المحرر الإلكتروني: من أهم أضرار جريمة تزوير التوقيع الإلكتروني إضعاف الثقة في المحررات الموقعة إلكترونيا، ذلك أن الثقة في التوقيع الإلكتروني تكتسب

---

(1) – راشد بن حمد البلوشي ، التوقيع الالكتروني والحماية الجزائية المقررة له ، ط1 ، منشورات الحلبي الحقوقية، بيروت، 2018 ، ص 87 . وكذلك: عبد الحليم فؤاد الفقي، المرجع السابق، ص 43 . وكذلك: منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006 ، ص 98 .

(2) – منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص ص 97 إلى 101 .

ذات الحجية والثقة في المحررات التقليدية العادية، وإذا تمَ تزوير التوقيع فإن ذلك أيضا يضعف الثقة في منظومة التوقيع الالكتروني، ويحتاج الشخص المتضرر إلى وقت طويل حتى تنتهي تلك الآثار الضارة.

3,تعد أحد التهديدات الموجهة إلى التجارة الإلكترونية: هناك العديد من التهديدات الموجهة إلى التجارة الإلكترونية، وتعد جريمة تزوير التوقيع الإلكتروني أحد أهم التهديدات التي توجه إلى نمو التجارة الإلكترونية واتساع عدد مستخدميها عبر إضعاف ثقة مستخدمي تلك الوسيلة في إبرام الاتفاقات التجارية، وحماية التوقيع الإلكتروني عن طريق خدمات التصديق يكفل أكبر قدر من الثقة في احتمال عمليات تزوير التوقيع الإلكتروني.

بالإضافة إلى الأضرار السالف ذكرها نضيف ضررا آخر وهو إلحاق الضرر بالشخص ذاته الموقع إلكترونيا.

الفرع الرابع: مجالات استخدام المحررات الموقعة الكترونيا

هناك العديد من المجالات التي تستخدم فيها المحررات الالكترونية، خاصة بعد ظهور التجارة الالكترونية والحكومة الالكترونية مما استلزم وجود عقود تجارية تناسب البيئة التي تحدث فيها هذه الصفقات وبظهور العقود الالكترونية حدث انقلاب جدري في المفهوم التقليدي للمحررات[1]، ونظرا لطبيعتها الالكترونية فإنه لا يمكن توقيعها إلا الكترونيا[2]، ونذكر على سبيل المثال استخدام المحررات الالكترونية في مجال العقود الالكترونية، والسجلات الالكترونية.

[1]– ايهاب فوزي السقا، المرجع السابق، ص 34 .

[2]– فارس خطابي، حجية التوقيع الالكتروني في الإثبات الجنائي– دراسة على ضوء القانون 15 –04 ، مجلة دفاتر السياسة والقانون، عدد خاص، جوان، 2018 ، ص 283 .

أولا: العقود الالكترونية

التطور السريع للتبادل الالكتروني للبيانات من خلال شبكة الانترنت كان له تأثير جوهري على الطريقة التي تتم بها إبرام المعاملات والصفقات التجارية، حيث بدأ التبادل الالكتروني للبيانات عن طريق المحررات الالكترونية ليحل محل المحررات الورقية ، واستطاع الأشخاص بفضل ذلك وعبر استخدام هذه الشبكة إلى إجراء العديد من المعاملات عن بعد دون أن يكونوا في مكان واحد عن طريق عقود أطلق عليها العقود الالكترونية كونها تبرم عن طريق الوسائل الالكترونية وفي مقدمتها العقود المبرمة باستخدام الحاسب الآلي سواء عن طريق المواقع التجارية الموجودة على الشبكة الدولية أو عن طريق البريد الالكتروني.

وقد واجهت هذه العقود تحديات منها صعوبة تحديد شخصية المتعاقدين والتحقق من وجود إرادة المتعاقدين وسلامتها ومدى جدية هذا التعاقد وحقيقة مضمونه وكيفية إثباته[1]، لذلك تدخل المشرع الجزائري في قانون التجارة الالكترونية 2018 لتنظيم المعاملات المبرمة عبر التعاقد الالكتروني .

ثانيا: السجل الالكتروني

يعتبر السجل الالكتروني من الأمور الهامة التي يتعين مراعاتها في مجال التبادل الالكتروني للبيانات، خاصة إذا ثار نزاع بين أطراف التعامل به، ولذلك فإنه غالبا ما يتم وضع المحررات الالكترونية في سجل الكتروني بهدف تخزينها والرجوع إليها عند وقوع الضرر [2] .

ونظرا للتوسع في استخدام التجارة الالكترونية حول العالم، فإن الاتفاقات الدولية والتشريعات الحديثة بشان تنظيم التجارة الالكترونية، تسعى لحفظ المعلومات المتبادلة بين أطراف التعامل وتوثيق البيانات المدونة فيه، ومن هذه التشريعات ما نص عليه التوجه الأوروبي الصادر عام

---

[1]– خالد حسن أحمد لطفي ، المستند الالكتروني ووسائل اثباته وحمايته ، دار الفكر الجامعي، الإسكندرية ، 2019 ، ص194 .

[2] – ايهاب فوزي السقا ، المرجع السابق، ص 38 .

2000 في بشأن التجارة الالكترونية من أن الشخص الذي يعرض منتجات وخدمات من خلال نظم المعلومات يمكن للجمهور الوصول إليها، يلزمه أن يوفر وسائل لتخزين أو طباعة العقد.

كما حرصت الاتفاقات النموذجية للتبادل الالكتروني للبيانات على إلزام أطراف التبادل الالكتروني للبيانات بالاحتفاظ بسجل الكتروني يمكن الرجوع إليه عند الحاجة ومنها الاتفاق النموذجي الأوروبي للتبادل الالكتروني للبيانات حيث نص على أنه " يجب على كل طرف من أطراف التعاقد أن يخزن بدون تعديل أو تحريف، وباستخدام وسائل أمان، سجلا كاملا ومسلسلا زمنيا لجميع رسائل البيانات التي يتبادلها الأطراف الكترونيا أثناء القيام بالعملية التجارية" [1].

الفرع الخامس: موقف بعض التشريعات من تجريم تزوير التوقيع الالكتروني

اختلفت التشريعات بشأن تجريم تزوير التوقيع الالكتروني بين من يجرمه بنص خاص صريح كالتشريع المصري والعماني وبين من يعطي تجريما عاما لجرائم التزوير الالكتروني من دون تخصيص تزوير التوقيع الالكتروني كالتشريع الفرنسي، أما موقف المشرع الجزائري فإنه لم يتبنى أي من الموقفين السابقين ولم يجرمه بنص خاص أو عام، لذلك سنتناول بالدراسة في هذا الفرع موقف كلا من المشرع الجزائري والمصري والعماني والفرنسي.

أولا : موقف المشرع الجزائري

موقف المشرع الجزائري بشأن تجريم تزوير التوقيع الالكتروني يمكن أن نستشفه من خلال قانون التوقيع والتصديق الالكترونيين 15 – 04 من أنه لم يجرمه بنص خاص واكتفى فقط بالتنويه على ضرورة حماية التوقيع الالكتروني من التزوير في المادة 11 فقرة ب من 11 قانون 15 – 04 بعبارة " أن يكون التوقيع الالكتروني محميا من أي تزوير عن طريق الوسائل التقنية وقت الاعتماد ".

وبالرجوع إلى النصوص الجزائية التي تعاقب على التزوير في قانون العقوبات الواردة ضمن الفصل السابع من الكتاب الثالث الموسوم بعنوان الجنايات والجنح وعقوبتها، يمكننا القول بأنه

[1] – ايهاب فوزي السقا ، المرجع السابق، ص 39 .

يمكن احتمال تطبيقها على جريمة تزوير التوقيع الالكتروني، لأن المشرع في نص المواد من 214، 215 ، إلى 229 من قانون العقوبات استعمل مصطلح "محرر"، من دون أن يميز بين المحررات الكتابية والالكترونية، لكن باعتبار أن القياس غير جائز في المواد الجزائية ما على المشرع الجزائري إلا تجريم تزوير التوقيع الالكتروني بنص خاص.

ولذلك فللمشرع خيارين إما أن يعدل في القواعد العامة للتزوير بأن يضيف إلى جانب المحررات الورقية منها والإلكترونية، وإنما ينص على تجريم خاص بتغيير الحقيقة في البيانات الالكترونية ومنها التوقيع الالكتروني وبياناته .

ثانيا: موقف المشرع الفرنسي

جريمة التزوير الالكتروني من أخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي يقوم به الحاسب الآلي والذي اقتحم كافة المجالات وأصبحت تجرى من خلاله كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة التي لا يصدق عليها وصف المكتوب أو الصك أو المستند في القانون المدني والجنائي، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع التزوير عليها، وقد حاول بعض الفقه اعتبار التزوير الحاصل على التزوير الالكتروني بمثابة شروع في التزوير على أساس أنه مقدمة لإنشاء مستند مزور، لكن هذا الرأي لم يحظى بتأييد لأن ما صدر من الجاني حتى هذه اللحظة لا يعتبر بدءا في التنفيذ يتحقق به الشروع أو المحاولة، وإنما لا يعد إلا أن يكون عمل تحضيري لا عقاب عليه[1].

وقد تقدم النائب Godfrain باقتراح مشروع إدخال تعديل على جريمة التزوير في المحررات بحيث تشمل التسجيلات المعلوماتية، وقد هاجم البرلمان الفرنسي هذا الاقتراح بشده على أساس أن الأخذ به يؤدي إلى تشويه مفهوم التزوير في المحررات والقول بتحققه على الرغم من عدم توافر محرر أو مكتوب، فأقترح مجلس الشيوخ تعديلا يتمثل في اعتبار تزوير المستندات المعالجة آليا جريمة مستقلة عن التزوير في المحررات، وكذلك جريمة استعمال تلك المستندات

[1]– علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، المرجع السابق، ص 137 .

المزورة، وتمت الموافقة في البرلمان بمجلسيه على هذا التعديل، وتضمن القانون رقم 19 -88 الصادر في 05 -01-1988 بشأن غش المعلوماتية في المادتين 462 فقرة 05 و 06 حيث نصت الأولى على تجريم تزوير المستندات المعالجة آليا، بينما جرمت الثانية استعمال تلك المحررات، ولكن بصدور قانون العقوبات الفرنسي الجديد سنة 1994 ألغيت المادتين السابقتين حيث قرر المشرع الفرنسي عدم الإبقاء على التجريم الخاص بتزوير المستندات المعالجة آليا واستعمالها والاكتفاء بإضافته إلى جريمة التزوير العادية[1]، وهذا الحذف له ما يبرره وهو اختلاف المصلحة التي يحميها القانون في هاتين المجموعتين من الجرائم فالمصلحة التي يحميها المشرع من تجريم الاعتداء في نظام المعالجة الآلية للمعطيات هي النظام ذاته وبمعنى أدق مصلحة صاحب الحق في هدا النظام أو مصلحة من له السيطرة عليه بينما المصلحة التي يحميها القانون بصدد جريمة التزوير هي الثقة العامة في المستندات ذات القيمة القانونية أيا كان شكلها [2] .

ثالثا : المشرع المصري

المشرع المصري جرم تزوير التوقيع الالكتروني في موضعين مختلفين وهما المواد 23 و15 من قانون التوقيع الالكتروني رقم 15 لسنة 2004 في المادة 23 التي تعاقب كل من زور توقيعا الكترونيا بطريق الاصطناع أو التعديل أو التحوير أو بأي الطرق.

وفي المادة 15 التي تعاقب على كل من زور أو تلاعب في توقيع الكتروني سواء تم ذلك بالاصطناع أو التعديل أو التحوير أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته[3] .

[1] – علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي المرجع السابق، ص ص 138 .

[2] – المرجع نفسه، ص143 .

[3] – محمد حسين على محمود، التزوير باستخدام الوسائل الالكترونية، دار النهضة العربية، القاهرة، 2016 ، ص 136.

رابعا : موقف المشرع العماني

حرصا من المشرع العماني على إيجاد الثقة لدى الناس في التعاملات التي تتم عبر الشبكة المعلوماتية والمضي قدما نحو تحقيق أعلى استفادة من التطور التكنولوجي والعلمي في مجال الاتصالات فقد صدر قانون المعاملات الالكترونية بموجب المرسوم السلطاني رقم 69 – 2008، وذلك من أجل تنظيم المعاملات التي تتم عبر الشبكة العالمية سواء فما يتعلق بتحريرها وحفظها وتبادلها وتوفير الحماية والتغطية لها وإضفاء الحجية القانونية عليها.

ومن بين المسائل التي تضمنها القانون تجريم تزوير التوقيع الالكتروني واستعماله بنص صريح في نص المادة 52 فقرة 14 إذ نصت على انه " يعاقب بالسجن لمدة لاتتجاوز سنتين وبغرامة لا تتجاوز خمسة ألاف ريال عماني أو بإحدى هاتين العقوبتين كل من زور سجلا الكترونيا أو توقيعا الكترونيا أو استعمل أيا من ذلك مع علمه بتزويره " [1].

المطلب الثاني: أركان جريمة تزوير التوقيع الالكتروني واستعماله في المحررات الالكترونية

لا تقوم أي جريمة إلا باكتمال أركانها وعناصرها الأساسية التي يتطلبها القانون، ولارتباط جريمة تزوير التوقيع الالكتروني مع جريمة استعمال هدا التوقيع، سنتناول بالدراسة أركان كل جريمة لوحدها في المطلب الأول نخصصه إلى أركان جريمة تزوير التوقيع الالكتروني، ثم المطلب الثاني أركان جريمة استعمال هدا التوقيع الالكتروني المزور.

الفرع الأول: أركان جريمة تزوير التوقيع الالكتروني

التزوير في المحررات هو تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شانه إحداث ضرر ومقترن بنية استعمال المحرر المزور فيما أعد له [2]، وأكدت المحكمة العليا في العديد من قراراتها من أن التزوير يتم بتغيير الحقيقة مع علمه بأنه يغيرها

[1] – راشد البلوشي، المرجع السابق، ص ص 77 – 78 .

[2]– محمود نجيب حسني، المرجع السابق، ص 215 .

وبأن من شأن هذا التغيير أن يلحق ضررا بالغير وقد نقضت وأبطلت المحكمة العليا أحد قرارات الغرفة الجنائية لأنها لم تتضمن هده العناصر في التزوير[1].

والركن المادي في جريمة تزوير التوقيع الالكتروني لا تختلف عن الركن المادي في جريمة التزوير التقليدية من حيث عناصره فالركن المادي يقتضي عنصران الأول تغيير الحقيقة، وأن يتم التزوير بإحدى الطرق المحددة قانونا، والعنصر الثاني وهو الضرر الذي لا يكتمل الركن المادي إلا به فيشترط تحقق الضرر للغير وهذا الضرر قد يكون ماديا أو معنويا أدبيا بفقدان الثقة في المعاملات الالكترونية والمجتمع عموما[2]، وبالتالي فأركان تزوير التوقيع الالكتروني تقوم على الركن المادي المتكون من محل التزوير وهو المحرر الالكتروني، وفعل تغيير الحقيقة، مع الركن المعنوي، والضرر.

أولا : الركن المادي

السلوك الإجرامي في جريمة تزوير التوقيع الالكتروني لا يمكن أن يكون محله إلا محررا الكترونيا، لذا ارتأينا أن نتناول بالدراسة في الركن المادي لمحل الجريمة وهو المحرر الالكتروني، ثم فعل تغيير الحقيقة في التوقيع الالكتروني.

أ. المحرر الإلكتروني محل التزوير

التطور في مجال الكتابة الالكترونية أدى إلى ظهور المحرر الالكتروني، كبديل عن المحرر الكتابي، لذلك سنتطرق إلى تعريف المحرر الالكتروني، ثم تمييزه عن المحرر التقليدي، وموقف بعض التشريعات منه.

---

[1]– قرار المحكمة العليا رقم 27199 ، الصادر بتاريخ 26–10–1982. وكذلك : القرار رقم 39130، الصادر في 02–01 –1985 .

[2]– هدى حامد قشقوش، الحماية الجنائية للتوقيع الالكتروني، المرجع السابق، ص 581 .

1. تعريف المحرر الالكتروني والتقليدي

عرفه المشرع المصري في القانون رقم 15 سنة 2004 والخاص بقانون التوقيع الالكتروني في مادته الأولى الفقرة ب بأنه رسالة تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية أو رقمية أو ضوئية أو بأنه وسيلة أخرى متشابهة[1].

وفي المجال الفقهي قد عرف المحرر الالكتروني بأنه كل دعامة مادية مهيأة لاستقبال المعلومات والتي يتم تسجيل المعطيات عليها من خلال تطبيق إجراءات المعالجة المعلوماتية[2] والبعض عرفه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات وقد سجلت عليه معلومات معينة سواء كانت معدة للاستخدام بواسطة نظام معالجة آلية أو يكون متسقا من هذا النوع[3].

أما المحرر التقليدي فهو كل ما يتضمن عبارات خطية مدونة بلغة يمكن أن يفهمها الناس، أو أنه كل مسطور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شخص لآخر، أو هو كل مكتوب يفصح عن شخص من صدر عنه ويتضمن ذكرا لواقعة أو تعبيرا عن إرادة من شانه إنشاء مركز قانوني أو تعديله أو إنهاؤه أو إثباته، سواء أعد المحرر لذلك أساسا أو ترتب عليه هذا الأثر بقوة القانون[4] .

2. تمييز المحرر الالكتروني عن المحرر التقليدي

مفهوم المحرر طبقا للنص التقليدي لا يتفق مع مفهوم المحرر الالكتروني، وهو ما ذهب ببعض الفقه إلى عدم دخول المحرر الالكتروني في الحماية الجنائية للمحرر التقليدي، وحججهم أن النصوص التقليدية وضعت لتنظيم المعاملات بالمحررات الورقية، ولكن المشرع

---

[1]– إيهاب فوزي السقا، المرجع السابق، ص 15.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 139 .

[3]– إيهاب فوزي السقا، المرجع السابق، ص 16.

[4] – هذه التعريف مشار إليها في: سليمان عبد المنعم، قانون العقوبات– القسم الخاص– الجرائم المضرة بالمصلحة العامة، دار الجامعة الجديدة، الإسكندرية، 2018 ، ص 355 .

عند وضعه هذه النصوص لم يرد إلى ذهنه المحررات الالكترونية، كما أن التزوير الواقع في المحررات الالكترونية يخرج عن المفهوم الواقع على المحررات الورقية باعتبار أن فكرة التزوير في المحرر تقتضي أن يعبر المحرر عن فكرة إنسانية وأن يكون وجوده ماديا ملموسا يمكن رؤيته بالعين المجردة على خلاف البيانات الالكترونية التي لا يمكن رؤيتها بغير الوسائل التقنية [1] .

3. موقف بعض التشريعات من المحرر الالكتروني

نأخذ نموذجين من التشريعات الجزائري والفرنسي.

1.3 موقف المشرع الجزائري

المشرع الجزائري اعترف بالكتابة الالكترونية في المادة 323 من تعديل القانون المدني لسنة 2005، إلا أن المحررات الموقعة الكترونيا، فأول قانون يعترف بها، وينظمها هو قانون التوقيع الالكتروني 15 – 04، وهذا ما يعني بأن قانون التوقيع الالكتروني 15 – 04 قد اعتبر المحرر الموقع الكترونيا يتخذ الشكل الالكتروني وبالتالي يعتبر من قبل المحررات الالكترونية، الذي يكون محلا للتزوير.

2.3 موقف المشرع الفرنسي

محل التزوير كان قاصرا إلى ما قبل تعديل قانون العقوبات الفرنسي على المحرر المكتوب الذي يتخذ شكل الكتابة أي العبارات الخطية أو العلامات أو الرموز التي تصلح لسرد واقعة أو التعبير عن إرادة أي التي تصلح لنقل المعنى من شخص لأخر، وكان يستبعد استنادا إلى هذا التحديد الكتابة الالكترونية، ولكن المشرع الفرنسي في التعديل الأخير وسع من محل التزوير بحيث أصبح لا يقتصر على ما يصدق عليه وصف المكتوب فقط وإنما يمتد ليشمل أيضا أي دعامة أخرى تحتوي على الفكر ويدخل فيه دعامات الحاسب الآلي التي يسجل عليها تعبيرا عن الفكر يصلح لأن يرد عليه التزوير، وليس التعبير عنها فقط ، وإنما يلزم أيضا أن تكون

[1] – إيهاب فوزي السقا، المرجع السابق، ص ص 54 – 55 .

هذه البيانات مما يصلح التمسك بها والاحتجاج بها إذا كانت تقرر حق بإنشائه أو تعديله أو بإلغائه [1].

ب. فعل تغيير الحقيقة وطرقه

جوهر التزوير هو فعل تغيير الحقيقة، والذي يتم بإحدى الطرق المحددة في قانون العقوبات.

1. فعل تغيير الحقيقة

يقصد بفعل تغيير الحقيقة في جريمة تزوير المستندات المعالجة ألليا ، كل تغيير للحقيقة أو تحريف لها يرد على محتوى أو مستند الكتروني وهذا يعني أنه لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية التي لا تتحقق إلا أثناء تكوين المستند من ذلك أن فعل تغيير الحقيقة آليا لا يتحقق إلا باستخدام طرق التزوير المادية دون المعنوية بشرط أن يقع هذا الفعل على محتوى مستند أصلى معالج آليا و موجود سلفا ويستوي أن يقع داخل نظام المعالجة الآلية للمعطيات أم خارجه كما يستوي أن يقع ذلك قبل أم بعد دخوله إلى ذلك النظام[2]، ويتم تغيير الحقيقة باستخدام وسيلة معلوماتية، بتغيير التوقيع الالكتروني أو معلوماته في ذاكرة الحاسب مباشرة أو بتعديل البرنامج للحصول على نتائج غير صحيحة، وليس لطبيعة الوسيط المادي الذي يحمل معلومة التوقيع الالكتروني بعد ذلك من أهمية [3]، كما يتخذ التزوير في المحررات الالكترونية صورتين تتمثل الأولي في التلاعب في معلومات المحرر بتعديلها والثانية تتمثل في إدخال معلومات غير صحيحة[4]، وقد تضمنت المادة 07 من اتفاقية بودابست تغيير الحقيقة في التزوير الالكتروني بإحلال أمر غير صحيح محل أمر صحيح يتعلق به حق الغير، سواء تم ذلك بإدخال بيانات توقيع الكتروني غير صحيحة أو محوها أو طمسها أو غير ذلك من أنواع التلاعب بالبيانات، وكل تصرف من شانه أن يجعل بيانات

---

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 144 .

[2]– المرجع نفسه، ص 141 .

[3]– نائلة قورة، المرجع السابق، ص 587 .

[4]– إيهاب فوزي السقا، المرجع السابق، ص 47 .

التوقيع الالكتروني غير كائنة أو غير متاحة للشخص الذي له الحق في الولوج إلى داخل النظام أو الاعتماد على تلك البيانات التي كانت مخزنة [1].

ويثار التساؤل حول التغيير الذي ينصب على معلومات التوقيع الالكتروني التي تتم طباعتها، فيذهب البعض إلا انه ينبغي في هذه الحالة التفرقة فما إذا كان التغيير قد طرأ على المعلومات قبل أو بعد طباعتها، ففي الحالة الأولى يعتبر تزويرا معلوماتيا، بينما يعتبر تزويرا تقليديا في الحالة الثانية[2]، ومعلومات التوقيع الالكتروني التي يتم طباعتها قد تتخذ الشكل الورقي أو الالكتروني كالأشرطة الممغنطة والأقراص المغناطيسية والمصغرات الفيلمية وغيرها من الأشكال الالكترونية للتكنولوجيا الحديثة التي تتوافر عن طريق الوصول المباشر حيث يقوم المستخدم بإدخال البيانات والحصول على المخرجات في نفس الوقت [3].

2.طرق التزوير

طرق تغيير الحقيقة في التزوير حددها المشرع الجزائري على سبيل الحصر في نص المادة 216 من قانون العقوبات عن طريق الحالات التالية:

- إما بتقليد أو تزييف الكتابة أو التوقيع.

- وإما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هده المحررات فيما بعد.

- وإما بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها.

- بانتحال شخصية الغير أو الحلول محلها.

---

[1] – هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة ، المرجع السابق، ص 244 .

[2] – نائلة قورة ، المرجع السابق، ص 588 .

[3] – هلالي عبد اللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية– دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2008 ، ص 141 .

ومن هذه الطرق يتضح وأن للتزوير طرق مادية ومعنوية.

1.2 الطرق المادية

ذهب جانب من الفقه إلى أن التزوير الالكتروني لا يقع إلا بالطرق المادية ولا يتصور فعل تغيير الحقيقة بالطرق المعنوية، بشرط أن يكون تزوير التوقيع الالكتروني بعد نشأة المحرر الالكتروني[1]، ومن وجهة نظرنا نرى عكس ذلك بأن تزوير التوقيع الالكتروني قد يقع بالطرق المعنوية لأنه قد يكون فعل تغيير الحقيقة أثناء تكوين المحرر الالكتروني، سنتناول بالدراسة الطرق المادية المتمثلة في تزييف الكتابة أو التوقيع، الاصطناع، التقليد.

- **تزييف الكتابة أو التوقيع**

وذلك بأن ينسب المزور محررا إلى شخص لم يصدر عنه ذلك أن ظهور إمضاء شخص أو ختمه أو بصمته في محرر يعني أن ما تضمنه قد صدر عنه إذ الإمضاء و ما في حكمه هو رمز الشخصية ودليلها ، أما البصمة المزورة فإنها تأخذ حكم الإمضاء بالنسبة للتزوير [2].

وإذا كانت الوسائل السابقة تتم بطرق تقليدية تتناسب مع المحررات التقليدية فإنها يمكن أن تتم بطريقة حديثة تتناسب مع المحررات الالكترونية، وقد يكون ذلك بإدخال معلومات وهمية إلى الجهاز الذي يصدر منه المحرر الالكتروني أو عن طريق استبدال المعلومات الصحيحة بغيرها أو القيام بمحو التوقيع الالكتروني أو بعض بياناته أو قد تتم بتعديل البرنامج الخاص بالحاسب الآلي أو تغيير نظام التشغيل غير أنه في بعض الحالات تكون المعلومات صحيحة وتنسب إلى شخص لم يصدر عنه بإضافة توقيعه الالكتروني[3].

---

[1] – على عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص140 .

[2]– محمود نجيب حسني، المرجع السابق، ص 230 .

[3] – محمد حسين على محمود، المرجع السابق ، ص94 .

- **الاصطناع**

التزوير بطريق الاصطناع نصت عليه المادة 23 فقرة من قانون التوقيع الالكتروني المصري بقولها" من أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا أو زور شيء من ذلك بطريقة الاصطناع أو التعديل أو التحرير أو بأي طريقة أخرى".

والاصطناع هو الإنشاء الكامل للمحرر ونسبته إلى شخص أو جهة لم يصدر عنها المحرر، ويكون الاصطناع إما بتقليد التوقيع ولما كان الأصل في المحررات أن تحمل توقيعا، فالغالب أن يصطحب الاصطناع وضع توقيع أو ختم مزور، ولكن غير لازم دائما كما في اصطناع محرر غير موقع عليه، فالجمع بين الاصطناع ووضع توقيع مزور غير مطلوب بالضرورة، فالاصطناع طريقة مستقلة للتزوير فيقوم بها بصرف النظر عما إذا كان هناك توقيع مزور أم لا، ويعاقب على تزوير المحرر بطريق الاصطناع حتى ولو لم يكن موقعا طالما استوفى في ظاهره الشكل الذي يمكن أن يرتب عليه القانون أثارا معينة[1] .

كما أن تزوير التوقيع الالكتروني بطريق الاصطناع أمر وارد إذ يمكن للجاني أن يدخل ما يريد من معلومات أو بيانات إلى جهاز الحاسب الآلي وينسب صدورها لشخص ما أو جهة ما ثم يقوم باستخراجها من جهاز الحاسب بوصفها منسوبة إلى ذلك الشخص، فتزوير التوقيع الالكتروني بطريق الحاسب الآلي تعد من طرق الاصطناع كما هي من طرق التقليد، وذلك لأن الاصطناع هو خلق محرر بأكمله ونسبته إلى غيره، وليس هناك صعوبة في عملية إدخال عناصر المحرر الموقع الكترونيا إلى جهاز الحاسب الآلي عن طريق الماسح الضوئي أو لوحة المفاتيح أو عن طريق الانترنيت ثم صياغتها في هيئة المحرر المزور توقيعه الالكتروني[2] .

---

[1] – سليمان عبد المنعم ، المرجع السابق، ص286 .

[2] – عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، منشأة المعارف ، الإسكندرية، 2009 ص202 .

- **التقليد**

يقصد بالتزوير بطريق التقليد تحرير المتهم كتابة بخط يشبه خط شخص آخر ساعيا بذلك أن ينسب لهذا الأخير البيانات التي تضمنتها الكتابة .

ويتداخل التقليد مع طرق تغيير الحقيقة السابقة، فالتقليد قد يتناول إمضاء أو ختما للغير، وقد يتناول محررا تجري محاكاته في صلبه وفي أختامه أو إمضاءاته، وقد يكون باصطناع محرر بغير نقل من محرر سبق إعداده، وكل ما يراد بالتقليد أن يتم التزوير المادي بإحدى هذه الطرق مع مراعاة الإتقان في محاكاة توقيع الشخص أو الجهة المراد أن ينسب التوقيع أو المحرر إليها [1]، ولذلك فتزوير التوقيع الالكتروني بطريق التقليد يكون عن طريق إتيان الفاعل بتوقيع الكتروني ينسب إليه يشابه صاحب التوقيع الصحيح، وليس دائما التقليد متصلا بوسائل أخرى فقد يقع التقليد على التوقيع الالكتروني فقط، أو على تقليد إحدى بياناته .

2.2الطرق المعنوية للتزوير

التزوير لا يتم فقط بالطرق المادية وإنما بالطرق المعنوية أيضا والمتمثلة في تغيير إقرار صاحب التوقيع الالكتروني، وجعل واقعة مزورة في صورة واقعة صحيحة.

- **تغيير إقرار صاحب التوقيع الالكتروني**

تغيير الحقيقة بهذه الطريقة لا يتصور وقوعه إلا أثناء تدوين المحرر، كما لا تدل عليه أثار مادية ظاهرة في المحرر، وإنما بتطلب إثباته الرجوع إلى صاحب الشأن نفسه لمعرفة حقيقة البيانات التي كان يريد اثباتها ومقارنتها بتلك التي أبثثت بالمحرر فعلا [2]، ويتحقق ذلك أثناء كتابة المحرر الالكتروني، فمن يقوم بالكتابة يدون بيانات غير تلك التي أدلى صاحب التوقيع الالكتروني.

---

[1] – سليمان عبد المنعم، المرجع السابق، ص687 .

[2] – إيهاب فوزي السقا، المرجع السابق، ص 73 .

- **جعل واقعة مزورة في صورة واقعة صحيحة**

والمراد بهذه الطريقة من طرق التزوير المعنوي كل اثباث لواقعة على غير حقيقتها، ويشمل ذلك كل صور التشويه والتحريف التي يدخلها كاتب المحرر على الوقائع التي يثبتها أثناء تدوينه، وتتسع هذه الطريقة لكل طرق التزوير المعنوي، ويستوي فيها أن تقع على محرر رسمي أو عرفي[1]، ومثال عن ذلك كأن يدون في عقد التجارة الالكترونية بأن السلع أصليه في حين أنها مغشوشة .

وبما أن غالبية الدول في عصرنا الحالي متجهة نحو الحكومة الالكترونية، لذلك فمن المتصور أن يقوم الموظف في العدالة بالتلاعب في مقدار الرسم في الدعاوى بمقتضى القسيمة التي يستخرجها من الحاسب الآلي ويدون عليها هذه البيانات، وهناك أخطاء قد تحدث في التحقيق الجنائي العادي تعد تزوير كإثبات واقعة لم يتم الإدلاء بها خاصة اعتراف المتهم، أو عدم إثبات واقعة معينة، وكل هذه الوقائع كما يحدث التلاعب فيها في التحقيق الجنائي الورقي فمن الوارد وقوعها في التحقيق الالكتروني أو التحقيق الجنائي عن بعد، ويعد مثالا نموذجيا لجعل واقعة مزورة في صورة واقعة صحيحة بالطريق الالكتروني [2].

- **انتحال شخصية الغير**

يمثل إحدى صور التزوير المعنوي إدا لم يترك في المحرر أثرا ماديا يدل عليه حيث يعد من قبيل جعل واقعة مزورة في صورة واقعة صحيحة ويستوي لقيام التزوير بهذه الطريقة أن ينتحل المتهم شخصية خيالية أو شخصية ذات وجود فعلي في محيط بيئته [3]، وإمكانية انتحال شخصية صاحب التوقيع الالكتروني لا يمكن التحقق منه إلا بواسطة الوسائل الالكترونية، لأنه قد يقع عليه تزوير مادي كالتلاعب في البيانات المادية لصاحب المحرر، فتصبح البيانات غير

---

[1] – سليمان عبد المنعم، المرجع السابق، ص 691 .

[2] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 210 .

[3] – سليمان عبد المنعم، المرجع السابق، ص 392 .

مطابقة لصاحب المحرر الالكتروني، وفي هذا الفرض فإن التزوير يتضمن تزويرا ماديا ومعنويا.

ثانيا: الركن المعنوي

تتطلب الجريمة قصدا جنائيا عاما وخاصا، يتمثل القصد العام في العلم والإرادة أي علم الجاني بأنه يغير الحقيقة وان هذا الفعل ينصب على محرر وأن من شان فعله إحداث ضرر[1]، أما الإرادة فتتجه إلى ارتكاب الركن المادي لجريمة تزوير التوقيع الالكتروني في المحررات الالكترونية والمتمثلة في تغيير الحقيقة للمحرر الموقع الكترونيا.

وقصد خاص يتمثل في توفر نية استعمال المحرر المزور فما زور لأجله، والاستعمال هو الذي يكسب التزوير الخطورة الإجرامية، ونية الاستعمال تتوافر حتى ولو لم يستعمل التوقيع الالكتروني المزور مستقبلا، لأن الاستعمال ليس ركنا في التزوير ومفصول عنه، باعتبار أن من يزور التوقيع الالكتروني قد لا يستعمله، وكل جريمة مستقلة عن الأخرى[2] .

ويضيف الفقه قصد خاص للتزوير وهو نية استعمال المحرر المزور فيما زور من أجله [3]، وتبعا لذلك لا يعتبر تزويرا من يصطنع توقيعا الكترونيا مزورا بهدف اثبات قدراته في التزوير أو التقليد .

ثالثا: الضرر

هناك جانب من الفقه اعتبر الضرر ركن أساسي في جريمة التزوير، وهذا ما يدعونا للتطرق إلى تعريف الضرر في التزوير، ثم صوره، ومعايير تحديد الضرر.

---

[1] – راشد البلوشي، المرجع السابق، ص 100 .

[2] – المرجع نفسه، ص 101 .

[3] – محمد زكي أبو عامر، سليمان عبد المنعم، المرجع السابق، ص 579 . وكذلك : محمود نجيب حسني، المرجع السابق ص 274 . و كذلك: عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 141 .

أ, تعريف الضرر في التزوير

هو إهدار حق أي الإخلال بمصلحة مشروعة يعترف بها القانون ويكفل حمايتها، وليس من عناصر فكرة الضرر أن يحل بشخص معين لأن الناس سواسية من حيث جدارتهم بالحماية إزاء أضرار التزوير، فإذا استهدف المتهم أن ينال الضرر شخصا معينا فنال شخص آخر قام التزوير على الرغم من ذلك، ولا تقتضى فكرة الضرر أن يمثل جسامة معينة فأقل الأضرار جسامة يقوم به التزوير، والضرر ركن أساسي في التزوير فإذا ثبت تخلف الضرر انتفى التزوير ولو توافرت سائر أركانه[1].

ب. صور الضرر في جريمة تزوير التوقيع الالكتروني

الضرر في جرائم التزوير الالكتروني كالضرر في تزوير المحررات الكتابية، فيستوي أن يكون مادي أو معنوي حال أو محتمل، فردي أو اجتماعي[2]، لذلك سنتناول بالدراسة الضرر المادي والمعنوي، ثم الضرر المحتمل والحال ثم الفردي والاجتماعي.

1.الضرر المادي والأدبي

الضرر المادي هو الذي يمس عناصر الذمة المالية فيترتب عليه الإنقاص من عناصرها الايجابية أو الزيادة في عناصرها السلبية وهذا الصرر أبرز أنواع الضرر وأكثرها شيوعا، ولا يشترط لتوفر هذه الصورة قدرا معينا من الضرر، إذ أن أي قدر من الضرر المادي يكفي ولو كان ضئيلا لقيام التزوير، أما الضرر المعنوي فهو الضرر الذي يصيب الشخص في شرفه واعتباره أو بصفة عامة في حق من حقوقه غير المالية، وقد يقترن الضرر المادي بالضرر المعنوي [3]، ومثال عن الضرر المادي تغيير الحقيقة في الرقم السري لبطاقة الائتمان لأجل

---

[1] – محمود نجيب حسني، المرجع السابق، ص 251 .

[2] – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي ، المرجع السابق، ص 141 .

[3] – محمد زكي أبو عامر، سليمان عبد المنعم، المرجع السابق، ص572 .

الحصول على المبالغ المالية التي تحويها البطاقة، أما الضرر المعنوي ومثاله انتحال بيانات وتوقيع الكتروني لشخص آخر في عقد زواج أو في إشهار طلاق.

2.الضرر المحتمل والحال

الضرر الحال هو الذي يتحقق بالفعل باستعمال المحرر المزور وفي هذه الحالة تتوافر جريمة استعمال المحرر المزور بالإضافة إلى جريمة التزوير نفسها [1]، أما الضرر الاحتمالي هو ضرر لم يتحقق فعلا، ولكن تحققه منتظر ، ففعل الجاني لم يحدث ضررا حالا ولكنه ينطوي على خطر إحداث الضرر، ويستخلص احتمال الضرر من احتمال استعمال ضار للمحرر الموقع الكترونيا [2].

3.الضرر الفردي والاجتماعي

الضرر الفردي هو الذي يلحق بفرد أو بهيئة خاصة كالشركات، أما الضرر الاجتماعي فهو مالا يصيب فردا معينا بذاته أو هيئة خاصة بل يلحق بالمصلحة العامة للمجتمع إذ هو يصيب مجموع الأفراد في المجتمع، وقد يكون الضرر الاجتماعي الناشئ عن التزوير في المحرر الموقع الكترونيا ماديا أو معنويا [3].

ج. ضابط أو معيار الضرر

تقدير الضرر من عدمه مسألة موضوعية، إلا أنه من المنطق و ضع معيار دقيق حتى لا تتفاوت أحكام القضاء، لذا فكر الفقه في معيار لتبيان الضرر ، وأبرزها ما قام به الفقيه جارو Garraud الذي يوضح بأن التزوير المعاقب عليه هو الذي يقع في محرر يصلح لأن يتخذ أساسا لاكتساب حق أو صفة أو حالة فإذا لم يكن للمحرر قيمة في الإثبات فتغيير الحقيقة فيه لا يعد تزويرا، ويعد معيار جارو في نظر غالبية الفقهاء هو الضابط المنشود في وضع أساس

---

[1] – محمد زكي أبو عامر، سليمان عبد المنعم، المرجع السابق، ص 573 .

[2] – محمود نجيب حسني، المرجع السابق، ص 255 .

[3] – محمد زكي أبو عامر، سليمان عبد المنعم، المرجع السابق، ص 574 .

للتزوير المعاقب عليه على الأقل عند غموض الضرر والتباس القول بالعقاب من عدمه[1]، وقد اعتبرت المحكمة العليا في أحد قراراتها أن معيار قيام الركن المادي للتزوير يجعل الضرر متوافرا ولو من الناحية المعنوية [2].

الفرع الثاني : جريمة استخدام التوقيع الالكتروني المزور

استعمال التوقيع الالكتروني المزور من الأفعال الخطرة، فبعد ارتكاب الجاني لفعل التزوير تأتي المرحلة الثانية من وراء التزوير هو استعمال التوقيع الالكتروني، سنتناول بالدراسة تمييز استعمال التوقيع الالكتروني عن تزويره، ثم أركانه.

أولا : تمييز جريمة استعمال التوقيع الالكتروني المزور عن التزوير

أقرت المحكمة العليا في القرار الصادر في 07 -01 - 2010 غرفة الجنح والمحالفات أن جريمة استعمال الوثيقة المزورة، جريمة مستقلة عن التزوير[3]، ويمكن إجمال التمييز بينهما في:

- اختلاف مفهوم الاستخدام عن مفهوم التزوير ذاته، وعلى الرغم من وجود علاقة بين النصين التجريميين وهي المتعلقة بوجود التزوير إلا أنه يبقى لمفهوم التزوير ذاتية تختلف عن الاستخدام يترتب عنها أن الفاعل في الاستعمال يختلف عنه في التزوير، والفاعل في التزوير لا تطبق عليه عقوبة الاشتراك في جريمة التزوير، وإذا كان الفاعل متهم في جريمتي التزوير والاستخدام فإنه من الممكن أن يبرأ عن أحد الجريمتين دون الأخرى.

---

[1] - هلالي عبد للاه أحمد ، الجرائم التقليدية والمستحدثة ، المرجع السابق، ص ص 232 -233 . و كذلك: سليمان عبد المنعم، المرجع السابق، ص 400 .

[2] - قرار المحكمة العليا رقم 559251 ، الصادر بتاريخ 22 10 -2008 ، غرفة الجنح والمخالفات، مجلة المحكمة العليا، العدد الثاني، 2008 ، ص 373 .

[3] - قرار المحكمة العليا رقم 522390 ، الصادر بتاريخ 07 - 01 - 2010 ، غرفة الجنح والمخالفات ، مجلة المحكمة العليا، العدد الأول ، 2012 ، ص 343 .

– يعد الاستخدام تاما ومكتملا في حالة تقديم وإبراز أو نقل المستند المزور، وفي هذه الحالة لا يشترط أن يؤدي هذا الاستخدام إلى تحقيق النتيجة المطلوبة، ويعد العدول اللاحق على الاستخدام نتيجة الندم أو التوبة غير مؤثر على النتيجة والمسؤولية الجنائية[1].

– تتقادم جريمة استعمال المزور من يوم استعمال الوثيقة المزورة ، بينما تتقادم جريمة التزوير من يوم العلم بالطبيعة المزورة للوثيقة موضوع الدعوى العمومية [2].

ثانيا : أركان جريمة استخدام التوقيع الالكتروني المزور

الذي يقدم على جريمة تزوير التوقيع الالكتروني غالبا يكون هدفه استعماله في غرض غير مشروع، وهي جريمة لها أركانها وعناصرها مستقلة عن التزوير لأن من يستعمل قد يكون هو مرتكب التزوير، وقد يكون شخصا غيره، لذلك سنتناول بالدراسة ركنيها المادي والمعنوي.

أ. الركن المادي

جريمة استعمال التوقيع الالكتروني المزور من جرائم السلوك المادي المتمثل في استعمال التوقيع الالكتروني المزور في الغرض الذي زور من أجله، ويراد بالاستعمال كل فعل يقوم به الجاني بدفع التوقيع الالكتروني المزور أو المحرر إلى مجال التعامل والاحتجاج والتمسك به، حتى ولو عدل المتهم عن التمسك بهذا التوقيع أو المحرر بعد ذلك أو لم يتحقق له غرضه من الاحتجاج به، لذلك لا يتوقف الاستعمال على قبول المحرر المزور بل يتم وينتهي بمجرد تقديمه للاستفادة منه في غرض معين ولو لم يتحقق هدا الغرض[3] .

واعتبار الفعل استعمالا مرتهن بتوافر شروط: تتمثل في أن تتوافر له صفة إرادية، فلا يعد استعمالا إكراه شخص على إبراز محرر مزور، فإذا ضبط المحرر المزور في حوزة المتهم

---

[1]- Zousmam, Faux en ecriture, dalloz, Paris, P 5.

مشار إليه في : أحمد خليفة الملط، المرجع السابق، ص 586.

[2] – قرار المحكمة العليا رقم 572259 ، الصادر بتاريخ 18 –02 –2009 ، مجلة المحكمة العليا العدد الثاني ، 2009 ، ص 347 .

[3] – راشد البلوشي، المرجع السابق، ص 110 .

فادعى صحته أثناء التحقيق فلا يعد ذلك استعمالا، ولا يتحقق الاستعمال كذلك بتقديم المحرر المزور استجابة لأمر القاضي أو المحقق، وتفترض فكرة الاستعمال إبراز المحرر المزور، إذ هي تعني الاستعانة بالبيانات التي يتضمنها للتأثير على الغير وحمله على التصرف بنحو معين، أما إذا لم يبرز المتهم المحرر، إنما اقتصر ذكره و الإشارة إلى أنه يدعم موقفه، فلا يعد ذلك استعمالا، ويتطلب السلوك الإجرامي للاستعمال الاحتجاج بالمحرر على أنه صحيح أما إذا قدمه المتهم إلى الغير على أنه مزور فليس ذلك استعمالا، ولا يكفي لتحقق الاستعمال مجرد تقديم المحرر، بل يتعين الاحتجاج والتمسك به لتحقيق غرض معين [1].

وقد يقع استعمال المحرر المزور من نفس الشخص الذي ارتكب التزوير فتقوم في حقه حالة من حالات تعدد النصوص الأصلية الاحتياطية، ويعتبر التزوير هنا الوصف الأصلي واستعمال المحرر هو الوصف الاحتياطي، ومع ذلك قد يقع استعمال المحرر المزور من شخص أخر غير الذي ارتكب التزوير، وفي هذا الفرض يعاقب هذا الشخص باعتباره مرتكبا لجريمة مستقلة مستمرة يسري عليها كافة الأحكام التي تسري على الجرائم المستمرة [2].

ب. الركن المعنوي

جريمة استعمال التوقيع الالكتروني المزور جريمة عمدية، يتخذ ركنها المعنوي صورة القصد الجنائي، وقوامه علم المستعمل بتزوير التوقيع الالكتروني، واتجاه إرادته إلى دفعه لتحقيق غرض من شانه أن يحققه، ويجب أن يثبت له العلم اليقيني بالتزوير، ولكن إذا كان المستعمل هو المزور نفسه وتبث قصد التزوير لديه، فإنه يفيد بالضرورة علمه بتزوير التوقيع الالكتروني وتوافر القصد المتطلب في الاستعمال، وينتفي القصد الجنائي إذا لم تتجه إرادته إلى الاستعمال، وإذا سرق منه واستعمله سارقه فلا ينسب إليه القصد، ولا عبرة بالبواعث التي دفعت المتهم إلى استعمال التوقيع الالكتروني المزور [3].

---

[1] – محمود نجيب حسني ، المرجع السابق، ص 311 .

[2] – سليمان عبد المنعم، المرجع السابق، ص ص 422– 423 .

[3] – محمود نجيب حسني، المرجع السابق، ص 313 .

الفصل الثاني: الحماية الجزائية الموضوعية للتوقيع الالكتروني وفق القواعد الخاصة المستحدثة

التطور التكنولوجي أضفى على قانون العقوبات بعض المميزات وهي التوجه نحو حماية القيم والمصالح الحديثة للأفراد نتيجة للتطور في مفهوم المصالح التي كانت مقتصرة على القيم المادية فقط.

كما أن القيم والمصالح الاجتماعية للأفراد المتغيرة والمتطورة يجب حمايتها عن طريق التجريم، وللمشرع أن يدرج هذا التجريم في قانون العقوبات أو في القوانين الخاصة، وقد كان لهذا التطور أثرا على قانون العقوبات الجزائري بأن أدرج ضمن تعديل قانون العقوبات لسنة 2004 تجريمه للاعتداء على نظم المعالجة الآلية للمعطيات، ولحماية المصالح الفردية والاجتماعية من جراء الاعتداء على التوقيع الالكتروني، نظم المشرع كل ما يتعلق بالتوقيع الالكتروني ومنها أحكام حمايته الجزائية في القانون 15 – 04 المتعلق بالتوقيع والتصديق الالكترونيين، لذلك فالحماية الجزائية الموضوعية للتوقيع الالكتروني تتطلب حماية نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، سنتطرق له في المبحث الأول، أما الصورة الثانية للحماية الجزائية فتشمل الحماية الجزائية الموضوعية المقررة في قانون 15 – 04 المتعلق بالتوقيع والتصديق الالكترونيين .

المبحث الأول: الحماية الجزائية الموضوعية في ظل جرائم المساس بأنظمة المعالجة الآلية للمعطيات

أضفى المشرع الجزائري حماية جزائية للأنظمة المعلوماتية ومعطيات الحاسب الآلي بوجه عام ضمن تعديل قانون العقوبات لسنة 2004 في نص المواد 394 مكرر إلى 394 مكرر7، ولأن التوقيع الالكتروني بإمكانه أن يكون ضمن نظام معلوماتي فهو يتمتع بحماية جزائية ومصلحة قانونية محمية وفقا لقواعد المساس بالنظام المعلوماتي ومعطياته، وهذا ما يدعونا إلى

التطرق لمفهوم جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ثم إلى لصور تجريمها والعقوبات المقررة لها.

المطلب الأول: مفهوم جرائم المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني

جرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني تندرج ضمن الإطار العام للجريمة المعلوماتية، لذلك في هذا المطلب سنتطرق إلى بيان تعريفها، ثم المصلحة المحمية جنائيا، وخصائصها، وموضوعها .

الفرع الأول: تعريف الجريمة المعلوماتية

تتعد المصطلحات الدالة على هذه النوعية من الجرائم [1]، فتعددت معها التعريفات التي قام بها الفقهاء والباحثون التي يعتمد عليها كل منهم والمعيار الذي يتبناه، ورغم كثرة هذه التعريفات إلا أنه يمكن بلورتها في ثلاث معايير وأسس وهي معيار وسيلة ارتكاب الجريمة، معيار موضوعها، معيار توافر المعرفة بتقنيات المعلومات:

فالتعريفات المرتكزة على وسيلة ارتكابها يعرفها الفقيه الألماني تاديمان Tiedmann الجريمة المعلوماتية بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب، وعرفت بأنها فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية وعرفت أيضا بأنها الفعل غير المشروع الذي يكون الحاسب داخلا في ارتكابه.

*هناك من يطلق عليها جرائم الحاسب الآلي، أو الجرائم المعلوماتية، أو الجرائم الالكترونية، أو جرائم الانترنت السيبرانية، أو جرائم الغش المعلوماتي، ومن جهتنا نحبذ مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما جاء في المادة 394 مكرر من قانون العقوبات، إذا ما كنا بصدد الاعتداء على نظام معالجة آلية لمعطيات التوقيع الالكتروني، ومصطلح الجرائم بالمرتكبة بالوسائل الالكترونية إذا ما كان التوقيع الالكتروني قد وقع عليه الاعتداء في وسط الكتروني.

وجانب آخر يرتكز على معيار توافر المعرفة بتقنيات المعلومات كتعريف David Thompson أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب [1].

وهناك من يرتكز على معيار موضوع الجريمة منها تعريف الفقيه الأمريكي Peter stephson الجريمة السيبرانية أو المعلوماتية بأنها الجرائم الواقعة على الحاسوب أو نظام الحاسوب[2]، فالجريمة المعلوماتية في منطق واضعي هذه التعريفات ليست هي التي يكون الحاسب الآلي أداة ارتكابها بل التي تقع على الحاسب أو على نظامه، والطائفة الثانية استندت إلى محل أو موضوع الجريمة لاعتباره أساسا لتعريف هذه النوعية من الجرائم، وعرفتها بأنها كل سلوك أو نشاط غير مشروع يتعلق بنسخ أو تغيير أو حذف البيانات أو المعلومات المخزنة داخل النظام أو الوصول إليها، وتلك التي يتم تحويلها عن طريقه، أو هي كل سلوك أو نشاط غير مشروع موجه إلى المعالجة الآلية للبيانات أو نقلها [3].

وهناك من حاول الجمع بين هذه المعايير فيعرفها بأنها كل فعل أو امتناع يأتيه شخص طبيعي أو معنوي عن طريق ممثليه، باستعمال نظام معلوماتي معين يتمثل في الحاسبات أو ما يقوم مقامها من نظم مطمورة، مشاركات الاتصال، إضرار بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية تمثل نماذج معلوماتية مستحدثة، أو كانت تدخل في نطاق المصالح والحقوق التي كان يحميها مسبقا قانون العقوبات بالطرق التقليدية وسواء كان الاعتداء واقعا داخل حدود الدولة أو كان يمس أقاليم عدة دول[4].

---

[1]– هشام محمد فريد رستم، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني، مؤتمر القانون والكمبيوتر و الانترنت، المجلد الثاني ، ط3 ، جامعة الإمارات العربية المتحدة ، 2003 ، ص 407 .

[2] - Peter Stephenson, investigating computer – related crime , crc press , new york ,2000 , p 19 .

[3]– هشام رستم ، المرجع السابق، ص 407 .

[4]– هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة، المرجع السابق، ص 101 .

ومن جهتنا نعرف الجريمة المعلوماتية بأنها كل مساس يترتب عنه الدخول أو البقاء أو التغيير في أنظمة المعالجة الآلية للمعطيات بغض النظر عن صفة مرتكبها أو ما يحدثه من أضرار.

الفرع الثاني: المصلحة المحمية في الجرائم الواقعة على نظام المعالجة الآلية لمعطيات التوقيع

المشرع الجزائري أخذ بعين الاعتبار ثلاث مصالح متعلقة بمعطيات الحاسب الآلي، وقام بحمايتها وتجريم العدوان عليها، وهذه المصالح هي سرية الأنظمة المعلوماتية والمعطيات "confidentialité" وسلامتها وتكاملها Intégrité وإتاحتها ووفرتها "Disponibilité"، ولحماية سرية المعطيات قام المشرع بتجريم الدخول غير المصرح به والبقاء في أنظمة المعالجة الآلية للمعطيات، وجرم التعامل في المعطيات المتحصلة من جريمة، ولحماية مصلحة سلامة المعطيات أو تكاملها جرم التلاعب بالمعطيات، إدخالا وإزالة وتعديلا، ما لم يكن مصرحا بذلك، سواء كجريمة خاصة، أو كظرف مشدد لجريمة الدخول أو البقاء غير المصرح بهما، وكذلك تخريب أنظمة المعالجة الآلية للمعطيات كظرف مشدد لهذه الجريمة الأخيرة، والنص على هذه الجرائم يحمي المعطيات في إتاحتها ووفرتها[1].

الفرع الثالث : خصائص الجريمة المعلوماتية

تتميز جرائم المعلوماتية بمجموعة من الخصائص والسمات منها لا نجد لها مثيل في الجرائم التقليدية، لذلك سنتطرق إلى أهم خصائصها وهي أنها من الجرائم العابرة للحدود، يصعب إثباتها، تتسم بالنعومة، أنها من جرائم الرقم المظلم، وعالية التقنية، سمات تميز ضحايا ومجرمي المعلوماتية.

[1]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007 ، ص ص 82 – 83 .

أولا: أنها من الجرائم المنظمة و العابرة للحدود

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحاسبات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بعض دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع من جاني في دولة معينة على مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر لاسيما مع تعاظم الدور الذي تقدمه شبكة الانترنت، خاصة في مجال التجارة الالكترونية وازدياد اعتماد البنوك عليها [1]، وبذلك حولت الشبكة العالم إلى قرية الكترونية تتدفق المعلومات بين أرجائها بسهولة وسرعة وغزارة وينتقل فيها روادها بين الدول والقارات دون الحاجة إلى وسيلة نقل أيا كان نوعها [2].

وبما أن الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني تمس حدود عدة دول، سينعدم معه مسرح الجريمة المادي، وتثار معه مشاكل تتعلق بالاختصاص القضائي والقانون الواجب التطبيق و إجراءات التحقيق والملاحقة والضبط و التفتيش والمحاكمة .

كما أن القدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل فيها آلاف الأميال قد أدت إلى نتيجة أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في أن واحد كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عنها قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة [3].

والجريمة المعلوماتية في تطور يوم بعد يوم وبخاصة الجرائم الماسة بالمراسلات الشخصية وسرقة المعطيات، الاتجار بالمعطيات الشخصية، صنع وتوزيع البرامج، ما أدى إلى ظهور

---

[1]– محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص 37 .

[2]– نبيلة هبة هروال، جرائم الانترنت– دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان، 2013 – 2014، ص39 .

[3]– نائلة قورة، المرجع السابق ، ص 52 .

مؤسسات إجرامية منظمة، وأثبت التطبيق القضائي اليوم أن غالبية الأنشطة الإجرامية ترتكب بطريق منظم، فيقوم التنسيق بين مجموعة من عدة دول لأجل الهكر واختراق الأنظمة والغش والنصب [1].

ثانيا: أنها جرائم يصعب إثباتها وتتسم بالنعومة

صعوبة إثباتها سيؤدي ذلك إلى سهولة إتلاف الأدلة الإلكترونية من قبل الجناة، وصعوبة الوصول إليها نظرا لتشتتها في أكثر من دولة، مع صعوبة تحديد شخص الفاعل خاصة عندما يستخدم اسما مستعارا، أو يكون اتصاله عبر مقاهي الانترنت، كما هذه النوعية من الجرائم لا عنف فيها ولا دماء، إذ ليس هناك جثث أو إصابات كما هو الحال في الجرائم التقليدية، لأنها لا تتطلب الجهد العضلي أو البدني بل إلى مجهود ذهني والدراية الفائقة بتقنيات الحاسبات والمعلومات [2].

ثالثا: أنها من جرائم الرقم المظلم وعالية التقنية

لا يتم الإبلاغ عنها في أغلب الأحيان إما لعدم اكتشاف الجريمة، أو خشية المسئول من عواقب الإبلاغ خاصة في مجال الأعمال الذي ينتمي إليه، وزعزعة المتعاملين معه، كما تستوجب أن يكون الجاني ذو خبرة كبيرة ودراية فائقة في الحاسب الآلي والانترنت وتقنية المعلومات [3].

رابعا: أن لها ميزات خاصة بالضحايا والمجرم المعلوماتي

لها ميزات تميز الضحايا ومرتكبي الجرائم المعلوماتية لا نجدها في الجرائم التقليدية.

---

[1] - Emilio c vino, societe de linformation et le droit penal , revue international de droit pénal , vol 84 , 2013 ,p314.

[2]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت، المرجع السابق، ص 129 .

[3]– المرجع نفسه، الصفحة نفسها .

أ.سمات متعلقة بالضحية

تميل غالبية الضحايا إلى الحفاظ على سمعتهم التجارية ومكانتهم المرموقة والقليل منهم هو الذي يكشف عن أفعال الغش التي وقعوا ضحية لها ويعترفون بنتائجها، وغالبا جدا ما يشغل مرتكبوها مركز المسئولية ويحتلون مراتب عليا في التدرج الوظيفي بالمنشات التي يعملون بها وهذا ما يدفع مديروها إلى التستر على الفعل وحلها داخليا بالمؤسسة، وهناك حالات عديدة تمكن فيها مرتكبو أفعال الغش المعلوماتي من تحسين أوضاعهم المالية نتيجة لمهاراتهم في اقتراف الأفعال غير المشروعة وكان قد سبق وعدهم بشغل مراكز مهمة في محطة المراقبة أو إدارة الأمن المعلوماتي، وما يبعث القلق حقيقية إزاء سلبية هؤلاء الضحايا هو إصرارهم على إخفاء الجرائم التي وقعوا ضحية لها على الرغم من التوصيات العديد من المنظمات في هذا الشأن، مع إقناعهم محاولة مقاومة ظاهرة الجريمة المعلوماتية، وتكمن في المعرفة الجيدة بمرتكبيها والتقنيات المستعملة والقطاعات الأساسية التي يستهدفونها ويبقى الكثير في جميع الحالات من أجل فهم ظاهرة الجريمة المعلوماتية والياتها وهي مهمة على قدر من الصعوبة بالنظر إلى التقنية العالية للوسائل المستخدمة من أجل اقتراف الغش وإلى تعقد التكنيك المعلوماتي ذاته[1].

ب.سمات خاصة بالمجرم المعلوماتي

يعد الفقيه Parker أحد الباحثين الذين عنو بدراسة الجريمة المعلوماتية بصفة عامة والمجرم المعلوماتي بصفة خاصة، ويرى بأن المجرم المعلوماتي ينتمي إلى مجموعة خاصة من المجرمين تقترب في سماتها من جرائم دوي الياقات البيضاء وإن كانت لا تتطابق معها، فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز، كما أنه على درجة من العلم والمعرفة وهو ما يميز بشكل عام دوي الياقات البيضاء، وإن كان ليس من الضروري أن ينتمي المجرم المعلوماتي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو

[1]– محمد سامي الشوا، المرجع السابق، ص 70 .

الحال في جرائم دوي الياقات البيضاء كما يتفق مجرم المعلوماتية مع دوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق [1].

وخلص Parker من خلال دراسته للأنماط المختلفة لمجرمي المعلوماتية إلى أن أغلبهم غير قادرين على اقتراف الجرائم التقليدية، وخاصة تلك التي تتطلب مواجهة مع الضحية، فالمجرم المعلوماتي لا يستطيع الاعتداء على الضحية بطريقة مباشرة [2].

وما يميز أيضا المجرم المعلوماتي هو الهدف و الدافع الذي يكون الطمع و الاستيلاء على المال وبريق الكسب السريع محرك مرتكبها، وقد ترتكب أحيانا لمجرد خرق نظام الحاسب وتخطي حواجز الحماية أو بدافع الانتقام من رب العمل أو حد الزملاء، ومؤخرا تجاوز اختراق شبكات المعلومات الهواة الباحثين عن الشهرة وإثبات الذات في مجال أنظمة الحاسبات والشبكات ليشمل بعض محترفي الابتزاز وشركات لها مصلحة في زيادة الطلب على إنتاجها من أنظمة حماية المعلومات أو شركات تخترق مواقع منافسيها عبر الانترنت بوجه خاص لإضعاف مركزها المالي في وقت قد يكون حاسما وحساسا، بالإضافة إلى نوع آخر من الاختراقات يرتبط بأهداف سياسية أو اقتصادية لبعض الجماعات أو الحكومات[3].

الفرع الرابع: موضوع الجريمة المعلوماتية

الإشكالات التي تطرحها المعلوماتية تتعلق أساسا بوجود الحاسب الآلي واستعمالاته، والذي يمكن بالطبع أن يحمل في طياته العديد من الأفعال الضارة على جميع المستويات[4]، ما يجعل موضوع الجريمة المعلوماتية يختلف بحسب ما إذا كانت موجهة ضد أحد مكونات النظام

---

[1]– نائلة قورة ، المرجع السابق، ص ص 56 –57 .

[2]– المرجع نفسه، ص 61 .

[3]– هشام رستم ، المرجع السابق، ص446 .

[4]- Jean pradel , op- cit, P815.

المعلوماتي بحيث يكون هذا الأخير موضوعها، أو مرتكبة من خلال هذا النظام بحيث يكون هو وسيلة تنفيذها وأداتها [1].

فيما تعلق بالحالة الأولى تجتمع الجرائم التقليدية البحتة والجرائم المعلوماتية بمعناها الفني فتتوافر أولاهما إذا كانت المكونات المادية للنظام كالأجهزة والمعدات والكابلات هي محل الاعتداء أو موضوع الجريمة ولم يكن ثمة أهمية للتقنية في ارتكاب الجريمة كما هو الحال في سرقة أو إتلاف الحاسب أو شاشته، وتتوافر الثانية حينما تكون المكونات الغير مادية للنظام كالبيانات والبرامج في ذاتها هي محل الاعتداء كما هو الحال في الاعتداء على البيانات المخزنة في ذاكرة الحاسب أو المنقولة عبر شبكات الاتصال بالسرقة أو التزوير، أو الاعتداء على البرنامج ذاته بإدعاء ملكيته أو سرقته أو تقليده أو إتلافه أو محوه أو تعطيله، وفي الحالة الثانية نكون أمام إزاء جرائم تقليدية أداة ارتكابها ووسيلة تنفيذها هي الحاسب أو النظام المعلوماتي عامة ومن الوجهة النظرية وكما تشهد بعض الحالات الواقعية يمكن استخدام الحاسب لارتكاب طوائف من جرائم شتى كالسرقة والنصب وخيانة الأمانة وانتهاك الحياة الخاصة والتزوير والتجسس والمخدرات وتجارة الجنس[2]، وغسيل الأموال [3]، أما موضوع دراستنا للجريمة المعلوماتية بعنوان جريمة المساس بأنظمة المعالجة الآلية للمعطيات سينصب على الحالة الأولى وهي عندما يكون نظام المعالجة الآلية لمعطيات التوقيع الالكتروني محل اعتداء.

المطلب الثاني: صور جرائم المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني

الجريمة التي نحن بصدد دراستها والمتمثلة في جريمة المساس بأنظمة المعالجة الآلية للمعطيات قد وضع لها المشرع عدة صور للتجريم في المواد من 394 مكرر إلى 394

---

[1]– هشام رستم ، المرجع السابق، ص 443

[2]– المرجع نفسه، الصفحة نفسها .

[3]– للاطلاع أكثر حول موضوع غسيل الأموال راجع: دليلة مباركي ، غسيل الأموال، أطروحة دكتوراه، جامعة باتنة، كلية الحقوق، 2007 – 2008 .

مكرر07، تشمل جريمة الدخول أو البقاء في النظام المعلوماتي للتوقيع الالكتروني، وجريمة الاعتداء القصدي على معطيات التوقيع الالكتروني، جريمة الاتفاق الجنائي، جريمة التعامل في معطيات غير مشروعة، لذلك سنتناول في هذا المطلب بيان أركان كل جريمة وعقوبتها.

الفرع الأول:جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني

جرم المشرع الجزائري الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات من دون أن يفرد نص خاص بذلك للتوقيع الالكتروني، على عكس بعض التشريعات التي جرمت الدخول بطريق الغش إلى نظام أو قاعدة بيانات تتعلق بالتوقيع الالكتروني بنص خاص [1]، سنتطرق لهذه الجريمة من خلال بيان أركانها وعقوبتها.

أولا: أركان جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني

جريمة الدخول أو البقاء في نظام التوقيع الالكتروني تقوم على ركنين مادي ومعنوي، بالإضافة إليهما فمحل الجريمة هو النظام المعلوماتي كركن مفترض، لذلك سنتطرق إلى ركنها المادي والمعنوي.

أ. الركن المادي

الركن المادي في جريمة الدخول أو البقاء في النظام المعلوماتي للتوقيع الالكتروني، يتكون من فعلي الدخول أو البقاء، ونتيجتهما الإجرامية التي كانت بسبب الدخول أو البقاء، ولأن هذا السلوك الإجرامي للركن المادي لا يقع إلا على نظام معلوماتي، سنتناول بالدراسة الركن المفترض في الركن المادي وهو نظام المعالجة الآلية للمعطيات، ثم إلى السلوك الإجرامي لفعلي الدخول والبقاء والشروع في الدخول.

* كالتشريع المصري الذي جرم الدخول إلى قاعدة بيانات تتعلق بالتوقيع الالكتروني في نص المادة 26 من قانون التجارة الالكترونية التي تنص على " مع عدم الإخلال بأي عقوبة أشد وردت في أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن 3000 جنيه أو بإحدى هاتين العقوبتين ، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الالكترونية ، ويعاقب بنفس العقوبة من اتصل أو بقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة ".

1. الركن المفترض (نظام المعالجة الآلية للمعطيات)

نظرا لأهمية المعلومات في الوقت الحاضر، فقد استحدثت وسائل كثيرة لحمايتها، وحماية أنظمة معالجتها وقد تنوعت هذه الوسائل بين مادية ومعنوية، ويلجأ أصحاب الأنظمة المعلوماتية كثيرا إلى مثل هذه الأساليب وغيرها لتأمين الحماية للمعلومات التي تحويها أنظمتهم[1]، لذلك سنتطرق إلى تعريف النظام، ثم إلى مدى ضرورة الحماية التقنية للنظام.

فلقد عرفت الفقرة ب من المادة 02 من قانون رقم 09 – 04[2] ، المؤرخ في 14 شعبان عام 1430 الموافق ل 05 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه "يقصد بمنظومة معلوماتية أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

كما عرفه مجلس الشيوخ الفرنسي أنه كل مركب يتكون من وحدة ومجموعة وحدات معالجة والتي يتكون منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط التي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات[3].

أما النظام المتعلق بالتوقيع الالكتروني، فهو عبارة عن بيانات أو معلومات تم معالجتها بعد إتباع طرق وإجراءات الكترونية معينة، فصارت برنامجا تطبيقيا تم تحميله على الحاسب الآلي من أجل تشغيله والحصول على نتائج معينة خاصة بالتوقيع الالكتروني، لذلك فإن قاعدة البيانات، عبارة عن معلومات مخزنة يتم الرجوع إليها عند الحاجة، والنظام المعلوماتي قد يكون صورة برنامج تطبيقي لتشغيل الحاسب الآلي ، وكلاهما يتعلق بالتوقيع الالكتروني [4].

---

[1]– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 136 .

[2]– الجريدة الرسمية للجمهورية الجزائرية، العدد 47 ، ص 05 .

(3)– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 110 .

[4]– عبد الفتاح بيومي حجازي ، التجارة الالكترونية في القانون العربي النموذجي ، المرجع السابق، ص 185 .

ويمثل نظام أو نظم المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة الاعتداء على نظام متعلق بالتوقيع الالكتروني، فإذا ثبت تخلف هذا الشرط الأولي لا يكون هناك مجال للبحث في جريمة الاعتداء على نظام التوقيع الالكتروني، وبتوافر شرط النظام يمكن الانتقال والبحث في مدى توافر أركان جريمة الاعتداء على النظام أو الجرائم الملحقة والمرتبطة به[1].

أما فيما تعلق بمدى ضرورة الحماية الفنية والتقنية للنظام، فلقد أثير جدل فقهي بشأن الدخول للأنظمة التي لا يوفر المسئولون عنها تدابير أمنية، فهناك جانب يذهب إلى أن الحماية الجنائية تكفل فقط الأنظمة التي وفر لها مسئولوها حماية أمنية و تقنية، فمن غير المعقول حماية معلومات هامة تركها المسئولون عنها دون أيه إجراءات تكفل لها الحماية، ويرون أن الدخول شبيه بجريمة انتهاك حرمة مسكن الغير حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بغير رضا صاحبه، وإنما يجب أن يتم الدخول بغير رضا صاحب المسكن كالتهديد والاحتيال ويستندون إلى عدة أسباب منها[2] :

– أن هذه الأنظمة المعلوماتية بانفتاحها على شبكة المعلومات رغم أهميتها في أغلب الأحوال لزم عليها توفير حماية أمنية لها.

– السبب الأخر وهو أنه كلما كانت الأنظمة محمية فنيا كلما كانت سهولة في إقامة الدليل على قيام الركن المادي للجريمة، وفي التحقق من توافر القصد الجنائي لدى مرتكبها، لأن دخول هذه النظم يترك أثرا ماديا يسهل معه التحقق من وقوع الجريمة .

وبعض أعضاء البرلمان أثناء مناقشة قانون الغش المعلوماتي الفرنسي قالوا أن الحماية الجنائية في نظرهم تقتصر على الأنظمة المحمية فنياً لأن في نظرهم أن من يقوم باستغلال نظم المعالجة الآلية للمعطيات ويحقق ربحا من هذا الاستغلال يضع الوسائل الفنية لمنع الغش وأن

(1)– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 110.

(2)– نائلة قورة، المرجع السابق، ص ص 353 – 354.

القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم وليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله، كما أن الضرورة تتطلب حماية فنية ما يدفع مشغلي تلك الأنظمة إلى استخدام الحماية الفنية ويكون دور القانون الجنائي هو دور وقائي[1].

أما الاتجاه الثاني يرى أنه ينبغي على أن تكون حماية جنائية لأنظمة الحاسب والمعلومات بغض النظر عن كونها تتمتع بحماية أمنية أم لا، وحججهم في ذلك[2] :

– أن جريمة الدخول شبيهة بجريمة السرقة سواء تمتع المال المسروق بحماية صاحبه أو لم يتمتع بهذه الحماية لا يؤثر على قيام جريمة السرقة، فالجريمة قد تمت على الرغم من الصعوبة التي واجهت الجاني في تنفيذها.

– استبعاد تطبيق الحماية الجنائية على الأنظمة الغير مؤمنة يضيق على نحو كبير من حالات تطبيق جريمة الدخول غير المصرح به إلى نظم التوقيع الالكتروني، كما أنه يتجاهل الحالات التي يتم فيها الدخول نتيجة خطأ قام بها المسئولون عن أمن النظام.

ومهما كانت وجهات النظر إلا أن المسألة واضحة من خلال النصوص المتعلقة بجرائم الاعتداء على نظم المعالجة الآلية للمعطيات أنها لا تتضمن شرط الحماية الفنية، ومن المبادئ المستقر عليها في القانون الجنائي أنه لا يجوز إضافة شرط لم ينص عليه القانون، لذلك إذا لم يذكر المشرع شرط الحماية الفنية فإنه أراد استبعادها[3]، ومن وجهة نظرنا نؤيد الاتجاه الثاني الذي يرى بأن الحماية الجزائية مبسوطة على الأنظمة التي تتمتع أو لا تتمتع بحماية تقنية، بهدف عدم إفلات مرتكبي جريمة الدخول إلى نظام معلوماتي متعلق بالتوقيع الالكتروني من المتابعة الجزائية، وهو ما سار عليه المشرع الجزائري في نص المادة 394 من قانون العقوبات التي لم تشترط حماية فنية تقنية لأنظمة المعالجة الآلية للمعطيات.

(1)– علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 111.

(2)– نائلة قورة، المرجع السابق، ص ص 354 – 355.

(3) – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 112.

2. السلوك الإجرامي (الدخول أو البقاء)

السلوك الإجرامي لركنها المادي يكون بأحد الأفعال، إما الدخول أو البقاء، ثم سنتطرق للشروع في الدخول كأحد صور الجريمة الغير تامة في ركنها المادي، ثم النتيجة الإجرامية للدخول.

- **الدخول**

فعل الدخول غير المصرح به هو الوصول إلى المعلومات أو البيانات المخزنة داخل نظام الحاسب دون رضاء المسئول عن هدا النظام أو المعلومات التي يحتويها أو بمعنى آخر إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزونة بداخله[1].

ومن القضايا التي تناولت تفسير معنى الدخول قضية لولاية كانساس في الولايات المتحدة الأمريكية ضد "Allen" وذلك عام 1996 ، تتلخص وقائع القضية في قيام Allen باستخدام الحاسب الآلي الخاص به في الدخول المتكرر بنظام "Dial up" إلى حاسب شركة الهاتف الجنوبية الغربية وتلاعب بها بحيث تسمح للمستخدم بالقيام بمكالمات بعيدة المدى مجانا، ولما اتصل Allen بحواسيب الشركة المذكورة واجهته شاشة تطلب منه اسم المستخدم و كلمة العبور بحيث قام بتخمين كلمة العبور بدقة وأزال الدليل على نشاطه بإلغاء سجلات "logs"، ولقد اتضح للمحققين أن Allen خمن كلمة المرور بدقة وأزال الدليل على نشاطه بإلغاء سجلات "logs"، بعدها قام المحققين بإعداد ما يفيد أن Allen قام باستخدام الاتصال الهاتفي للشركة المذكورة ورأى مؤشر كلمة العبور[2] .

---

[1] – نائلة قورة، المرجع السابق، ص 317 .

[2] – أورين كير، ترجمة عمر محمد بن يونس، نطاق الجريمة الافتراضية– تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، مجلة القانون، جامعة نيويورك، العدد78، نوفمبر، 2003 ، الأكاديمية الدولية للتجارة الالكترونية، دون ذكر مكان النشر، 2008 ، ص 73 .

ولقد تمت إدانته بالدخول لحسابات الشركة دون تصريح انتهاكا لتشريع جرائم الحاسوب بولاية كانساس، وقد جادل Allen بأنه لا يوجد دليل على دخوله إلى حاسوب الشركة، إلا أن الحكومة اعتمدت على التعريف التشريعي لعبارة accès وذلك لعموميته بين التشريعات الولائية المبكرة لجرائم الحاسوب التي تقرر أن الدخول هو الاقتراب وإصدار أمر أو الاتصال أو تخزين بيانات أو استردادها أو أي شيء آخر يؤدي إلى استخدام مصادر الحاسب الآلي، وقد أجابت المحكمة بأن هذا التعريف كان واسعا وإذا أخد بجدية فإنه يؤدي إلى القول بعدم دستورية التشريع لغموضه، ولا حظت المحكمة أنه إذا كان الدخول يعني الاقتراب من أي جهاز حاسوب مادي بدون تصريح يمكن أن يشكل جريمة وفي ضوء هدا الاتساع رفضت تطبيق التعريف منتهية إلى أن التعريف الكامل والعادي يجب أن يطبق عوضا عن الترجمة المشوهة للتعريف، وقد فسرت المحكمة ذلك بقولها يعرف قاموس Webster الدخول accès كحرية أو قابلية للحصول أو الاستخدام وهدا مشابه للبناء الذي أعدته محكمة الموضوع للوصول إلى عدم وجود دليل ظاهر يقرر أن تحصل على دخول إلى حواسيب الشركة أو الحصول على أي شيء لذا فإنه لا يستطيع القول بأن دخوله إلى نظم حواسيب الشركة هو أمر معروف بشكل عام [1].

ومعنى الدخول يبرز كما لو كان مبنيا على الافتراض، بحيث أن الاسم الصحيح وكلمة العبور تسمح للمستخدم بالدخول إلى الملفات المتواجدة بالداخل، ولكن الاسم الخاطئ وكلمة العبور غير الصحيحة تمنع المستخدم من الدخول للوصول إلى المعلومات بالداخل يؤدي إلى القول بأنه لم يدخل إلى حواسيب الشركة[2].

فالدخول إذا له طبيعة معنوية غير مادية، أي أنه يختلف عن مفهوم الدخول كما هو متصور في العالم المادي، والحقيقة أن هذه النظرة هي التي تتفق مع العالم المعلوماتي ومكوناته غير المادية [3].

---

[1]– أورين كير، المرجع السابق، ص ص74 – 75 .

[2]– المرجع نفسه، ص75 .

[3]– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 147 .

بالإضافة أيضا أن الدخول لابد أن يكون غير مصرحا به [1]، فمجرد الدخول إلى نظام الحاسب الآلي لا يشكل فعلا غير مشروع، وإنما يشكل الفعل عدم مشروعيته من كونه غير مصرح به أو بدون وجه حق، ويرتبط أساسا من له الحق في الدخول إلى نظام الحاسب الآلي أو في التصريح بالدخول إليه فمناط التجريم هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك، ويكون الدخول غير مصرح به في حالتين، الأولى إذا كان هناك مسئول عن نظام الحاسب الآلي وكان دخول الفاعل إلى هذا النظام قد تم دون الحصول على تصريح منه، أي الدخول يكون من قبل أشخاص خارج المؤسسة التي يوجد بها نظام الحاسب الآلي، والحالة

* من القضايا التي تطرق لها القضاء الجزائري التي تتعلق بالدخول دون ترخيص قضية تعرض شركة أمريكية تسمى sago net works للاختراق من طرف شاب جزائري ، حيث انطلقت هذه القضية على إثر إرسالية صادرة من وزارة العدل الأمريكية مفادها تعرض المنظومة المعلوماتية لمؤسسة أمريكية تسمى صاقونات ووركس ، والتي تعتبر بنك معلوماتية جهوية كبيرة في ولاية فلوريدا الأمريكية وتعود الوقائع إلى تاريخ 08 – 04 – 2009 عندما تلقت المؤسسة المذكورة في بريدها الالكتروني من طرف شخص مجهول يدعي من خلاله انه اكتشف طريقة للدخول عن طريق الغش إلى المعطيات الالكترونية لهذه المؤسسة عبر برنامج التشغيل المرتبط بشبكة الانترنت، وبتاريخ 10 – 04 – 2009 تلقت نفس المؤسسة بريدين الكترونيين من نفس العنوان الأول يحمل تصريح صاحبه بأن جميع المعطيات والمعلومات الخاصة بالمؤسسة قد تم استنساخها وهي بحوزته ، وتضمن البريد الأول صورة شاشة لقائمة المواقع الالكترونية التابعة للمؤسسة ، أما الثاني فجاء فيه عبارة محاولة ناجحة كرد للمؤسسة بعد اكتشافها للاختراق الواقع على نظامها المعلوماتي ، وبتاريخ 10 -04 – 2009 تلقت نفس المؤسسة رسالة مجهولة يطلب من خلالها مبلغ مالي مستعملا عنوان الكتروني التابع لمؤسسة اتصالات الجزائر متعامل فوري، وبتاريخ 16- 04 – 2009 تلقت المؤسسة بريدا الكترونيا من طرف صندوق بريد يخطرهم بأن نظامهم قد تم اختراقه ، وأن المعلومات الخاصة بالطرق التي تسمح باختراقه مروضة للبيع على موقع unknown . ws وبعد البحث والتحري من قبل الضبطية القضائية بالجزائر تم تحديد هوية الشخص الذي قام باختراق مواقع ومعطيات الكترونية لشركات أجنبية بما فيها sago الأمريكية.

وبعد فتح تحقيق قضائي في الوقائع اعترف المتهم باختراقه عدة مواقع الكترونية لشركات أجنبية ، وذلكعن طريق القرصنة من خلال الإبحار في شبكة الانترنت ، انطلاقا من غرفته بمقر سكنى والده ببانتة، باستعمال خط هاتف المنزل وبالاشتراك في شبكة الانترنت مع المتعامل الفوري، بإستعممال عدة عناوين الكترونية بأسماء وهمية وأرقام سرية خاصة ، وأكد اختراقه مؤسسة sago عبر ثغرة في برنامج " ubrersmith" مند سنة 2006 ، كما أفاد بأنه حصل على مبالغ مالية من وراء عمليات القرصنة التي قام بها ، كما أن مصدر الحوالات المالية التي ضبطت بحوزته مصدرها كان مقابل نشاطه في الغش والقرصنة وأن تلك الصفقات كانت عن طريق الغش وحصوله على المعلومات التي يروجها باختراق الأنظمة المعلوماتية المحمية . الحكم الصادر عن محكمة باتنة بتاريخ 01 – 06 – 2010 تحت رقم 05272 /10 . الوقائع والحكم مشار إليها في: محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص ص 149 – 150 .

الثانية إذا كان دخول الفاعل إلى نظام الحاسب الآلي في غير الحالات المرخص له بذلك، أي يتجاوز التصريح الممنوح له بالدخول إلى معطيات لا يشملها التصريح[1].

وهذه الحالة الثانية لا تثير مشكلة في حالة الدخول غير المصرح به، إلا أن المشكلة تكون في حالة الدخول غير المصرح به من قبل العاملين في المؤسسة الذي يوجد بها نظام الحاسب الآلي الذي تم الدخول إليه ، ففي هده الحالة يتجاوز العامل السلطة المخولة له بدخوله إلى هذا النظام في غير الحالات المرخص له فيها بذلك ويصعب في كثير من الأحيان معرفة ما إذا كان العامل قد تجاوز بالفعل اختصاصه ، ولهذا ينبغي تحديد اختصاصات العاملين بالمؤسسة في شأن استخدام الحاسب الآلي بها تحديدا دقيقا حتى يسهل تحديد التجاوزات كما يتعذر في كثير من الأحيان معرفة ما إذا كان العامل قد تجاوز اختصاصه عن عمد نظرا لكثرة احتمالات دخوله إلى نظام الحاسب الآلي ودخوله إلى معلومات غير مرخص له الوصول إليها عن طريق الخطأ والصدفة[2] .

- **البقاء في النظام المعلوماتي**

البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[3]، والسلوك الإجرامي في البقاء يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والاطلاع فقط ويتحقق أيضا بالنسبة للخدمات الموجهة للجمهور مثل الخدمات التليفونية والتي يستطيع فيها الجاني الحصول على خدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة [4]، وقد يجد شخص نفسه داخل نظام لحاسب آلي غير مسموح له بالدخول إليه عن طريق الخطأ معتقدا أنه

---

[1]– نائلة قورة، المرجع السابق، ص 333 .

[2]– المرجع نفسه، ص ص 333 – 334 .

[3]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 122 .

[4]– المرجع نفسه، ص 123 .

في انه في نظام له الحق في الدخول إليه، وفي هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه للخطأ الذي وقع فيه، وقد يستمر البقاء في هذا النظام على الرغم من معرفته من أن هذا النظام غير مصرح له بالدخول إليه [1].

وما يجمع بين حالة البقاء بعد دخول مصرح به أو بعد دخول عن طريق الصدفة أو الخطأ أن الدخول في جميع الحالات كان مشروعا وبالتالي لا يمكن أن نطبق بشأنه أحكام جريمة الدخول غير المصرح به، لذلك تدخل المشرع الجنائي ليضيف سلوكا آخر إلى جانب الدخول غير المشروع وهو البقاء غير المشروع أو وغير المصرح به لأن المصلحة القانونية المحمية هي واحدة بالنسبة للفعلين معا[2].

ويرى البعض أن البقاء غير المصرح به داخل نظام الحاسب الآلي لا يقتصر فقط على حالة الدخول إلى نظام غير مصرح بالدخول إليه على سبيل الخطأ والبقاء داخل النظام على الرغم من العلم بذلك ، وإنما ينطبق أيضا على حالة الدخول إلى نظام الحاسب الآلي بموافقة المسئول عن هذا النظام إذا كانت هذه الموافقة مشروطة بزمن محدد وحدث تجاوز لهذا الزمن فإن البقاء في هذه الحالة غير مصرح به [3]، في حين يرى البعض الآخر عكس ذلك لأن الحكمة من تجريم البقاء غير المصرح به داخل نظام الحاسب الآلي هي ذات الحكمة من تجريم الدخول ألا وهي حماية المعلومات من الوصول إليها من قبل أشخاص غير مسموح لهم من البداية بالدخول إلى هذا النظام ، فإذا كان الدخول بموافقة المسئول عن النظام، أي يعني رضاءه باطلاع هذا الشخص على المعلومات التي يحويها هذا النظام فلا مجال للمساس بالمصلحة من التجريم، لذلك إذا تجاوز الوقت والزمن المحدد لهذا الدخول فإنه لا يشكل بقاءا في النظام المعلوماتي، وإن كان يشكل جريمة أخرى وهي الاستعمال غير المصرح به، أو ما

---

[1]– نائلة قورة ، المرجع السابق، ص 346 .

[2]– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 161.

[3] - champy guillaume, fraude informatique, thèse, tom1et 2, université Aix –marseille, 1990, p261.

نقلا عن : نائلة قورة، المرجع السابق، ص 347

يطلق عليها بسرقة وقت الحاسب[1]، ومن وجهة نظرنا نؤيد هذا الرأي لأن الدخول المشروع والمصرح به داخل النظام المتعلق بالتوقيع الالكتروني، يترتب عنه بالضرورة بقاء مشروعا ومصرح به داخل النظام، حتى ولو تجاوز الوقت المحدد والمسموح له.

والدخول والبقاء مختلفين من ناحية الركن المادي داخل نظام المعالجة الآلي للبيانات[2]، ولكل جريمة سلوكها الإجرامي الخاص بها دون الأخرى ويعتمد هذا الرأي على حجتين الأولى استقاها من المبادئ التي تحكم تفسير القانون، وهي تقضي بأن المشرع عندما يستخدم كلمتان أو مصطلحان مختلفان فلابد أن يكون لكل مصطلح معناه ومدلوله المختلف عن المصطلح الآخر، فمصطلح بقاء لا يحتوي مصطلح دخول والعكس كذلكصحيح، أما الحجة الثانية فسندها المنطق، وهي أن صفة الغش لا تنطبق فقط على الدخول وإنما تنطبق على البقاء أيضا[3].

- **الشروع في الدخول**

نكون أمام شروع في الجريمة كلما تكون العناصر المكونة لها غير مكتملة[4]، فتباينت مواقف التشريعات فدهب البعض إلى استبعاد ما يسمى بالدخول الذهني ويعني أن يقوم الفاعل بنشاط الدخول فمجرد قراءة المعطيات على الشاشة لا يكفي لتحقق الركن المادي للجريمة واستلزمت بعض التشريعات أن يقوم الفاعل قبل الدخول ببعض الإجراءات التقنية كاستخدام شفرة غير صحيحة أو إجراءات مخافة لقواعد الحماية التقنية لهده المعلومات على عكس دلك فان بعض التشريعات لم تتطلب نشاط ما يسبق الدخول إلى النظام أو استلزم وسائل محددة كالتشريع النرويجي والبرتغالي والفرنسي، وقد تبنى المشرع الجزائري الموقف الثالث للتشريعات التي لم تشترط وسائل محددة قبل قيام الفاعل بالدخول[5] .

---

(1)– نائلة قورة، المرجع السابق، ص 348 .

(2)– أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة ، 2000 ، ص 120 .

(3) - Raymond gassin, fraude informatique, 1995 , p20 .

نقلا عن : محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 163 .

(4) - Georges Vermelle , le nouveau droit pénal, Dalloz, paris, 1994, p 88.

(5)– نائلة قورة ، المرجع السابق، ص 341 .

- **النتيجة الإجرامية في جريمة الدخول**

هل تتم الجريمة بمجرد الدخول ونكون بصدد جريمة شكلية أم تتطلب نتيجة إجرامية وهي الحصول على المعلومات والمعطيات ونكون بصدد جريمة مادية.

يرى جانب من الفقه أنه ليس بالضرورة أن يصل الفاعل إلى المعلومات والمعطيات حتى يكتمل النشاط الإجرامي للدخول لأنها تمثل عدوانا محتملا على الحق[1]، وقد تبنى المشرع الجزائري والفرنسي هذا الرأي في نص المادة 394 من قانون العقوبات الجزائري والمادة 323 من قانون العقوبات الفرنسي وجرم الدخول بطريق مباشر أو غير مباشر على الحاسب ليوفر حماية خاصة للمعلومات ولبرامج الكمبيوتر من كشفها والاطلاع عليها أو التلاعب فيها أو تدميرها وجرم الدخول غير المشروع على أجهزة الحاسب ذاته دون النظر إذا كان الجاني استهدف الإضرار أم لا[2]، إلا أنه هناك بعض التشريعات تجرم كل فعل منهما بنص خاص كالتشريع الأمريكي في القانون الفدرالي لجرائم الحاسب، فالمادة 103 فقرة 01 تعاقب على الدخول بواسطته يتم الحصول على المعلومات، أما المادة 1030 فقرة 02 تعاقب على دخول المجرد[3].

وذهب جانب من الفقه أن فعل الدخول لا يتم إلا بفعل إيجابي بوصول الفاعل إلى المعلومات المخزنة داخل الحاسب الآلي، لأن الحكمة من تجريم الدخول هو حماية المعلومات والبرامج من الوصول إليها، أما الدخول المجرد فيمكن اعتباره الشروع في الدخول لأنه يحقق للنظام والعقاب على تجريم النشاط المتمثل في تشغيل الحاسب الآلي للدخول إلى النظام والمعلومات لأسباب خارجة عن إرادته[4].

---

(1)–نائلة قورة ، المرجع السابق، ص 344

(2)– مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000، ص 39 .

(3)– نائلة قورة، المرجع السابق، ص 344.

(4) – المرجع نفسه، 345 .

ب. الركن المعنوي في جريمة الدخول

أولى عناصر العلم هو موضوع الحق المعتدى عليه فيتعين علم الجاني أن فعله ينصب على نظام الحاسب الآلي، بما يتضمنه من معلومات وبيانات، فإذا اعتقد الفاعل بناء على أسباب معقولة أنه يقوم بحسابات عن طريق الحاسب دون أن يتجه علمه إلى أنه يقوم بالدخول إلى نظام الحاسب بما يحتوي عليه من معلومات وبيانات فإن قصد الدخول لا يتوافر لديه والحقيقة إن هذا الغرض على الرغم من أهميته القانونية إلا أنه يفتقر إلا هذه الأهمية من الناحية العملية فنادرا ما يدخل الفاعل إلى نظام الحاسب الآلي وهو على غير علم بذلك لتمتعه بالخبرة في المجال المعلوماتي، ومع ذلك إذا ثبت انتفاء العلم ينتفي معه القصد الجنائي[1].

وتنص المادة 394 مكرر من قانون العقوبات الجزائري صراحة على وجوب كون جريمة الدخول الدخول والبقاء في غير المصرح بهما جريمة عمدية، ويستشف ذلك من قولها كل من يدخل أو يبقى عن طريق الغش وعلى هذا أيضا نصت المادة 323 فقرة 01 من قانون العقوبات الفرنسي بقولها frauduleusement ، وهذا التعبير يعني أن الفاعل يقدم على فعله أو امتناعه وهو يعلم بأنه غير مرخص له بذلك، وإذا كانت الجريمة وهي مخالفة لأوامر المشرع ونواهيه فإن إرادة تحقيق تلك المخالفة تشكل أقصى درجات الإثم باعتبار أن الجاني قد عبر عن ذلكبإرادته في عدم الامتثال للقانون، والحقيقة أن المنطق يحتم أن تكون هذه الجريمة عمدية، لأن عمليات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها هي عمليات تتكرر بشكل مذهل في اليوم الواحد، وتقع من عدد هائل من المستخدمين، ولاسيما مع عدد ارتفاع مرتادي شبكة الانترنيت، وليس من المستبعد في كل هذه الحركة دخولا وخروجا أن تكون هناك عمليات دخول أو بقاء غير مصرح بها لكنها غير عمدية، ولو كانت جريمة غير عمدية لوقع الكثير من مستخدمي هذه الشبكة والحاسب الآلي تحت طائلة العقاب، وعلى هذا كان من اللازم أن

[1]– نائلة قورة ، المرجع السابق، ص 365.

تكون عمدية، وذلكمن أجل خلق توازن بين حماية خصوصية الأنظمة المعلوماتية وحماية حرية الأفراد في استخدام الانترنت[1] .

ولا يتوفر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به أي مشروع كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو البقاء أو في نطاق هدا الحق كمن يجهل حظر للدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له الدخول، وإذا توافر القصد الجرمي بعنصريه العلم والإرادة، فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل قائما حتى ولو كان الباعث من الدخول أو البقاء الفضول أو التنزه أو إثبات القدرة على الانتصار على النظام[2] .

ثانيا: عقوبة الدخول أو البقاء في النظام المعلوماتي للتوقيع الإلكتروني

هناك عقوبات أصلية وعقوبات تكميلية.

أ. العقوبات الأصلية

العقوبات الأصلية هي العقوبات الواجب على القاضي النطق بها في جريمة معينة، فلا عقوبة جنائية بدون عقوبة أصلية [3]، وتقسم إلى عقوبات أصلية بسيطة ومشددة.

1.العقوبات الأصلية البسيطة

تعاقب المادة 394 مكرر أنه إذا لم ينجم عن الدخول أو البقاء غير المصرح بهما إعاقة أو إفساد لنظام المعالجة الآلية للمعطيات أو إزالة أو تعديل لمعطياته فإن العقوبة تكون الحبس لثلاث أشهر إلى سنة والغرامة من 50000 إلى 100000 دينار جزائري.

---

[1]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص ص 162 – 163 . .

[2] – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 126 .

[3] - Bernard bouloc,haritini mastopolou, droit pénal général et procédure pénal, Dalloz, paris, 2009 , p 476 .

2. العقوبات الأصلية المشددة

تعاقب المادة 394 مكرر فقرة 01 و 02 أنه إذا ترتب عن الدخول أو البقاء غير المصرح بهما إزالة أو تعديل لمعطياته فإن العقوبة تكون الحبس من ستة أشهر 06 إلى سنتين 02 والغرامة من 100.000 إلى 400.000 دينار جزائري.

والظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة القصدية الأساسية وهي جريمة الدخول أو البقاء علاقة سببية للقول بتوافره، كما لا يشترط أن تكون النتيجة غير مقصودة أي على سبيل الخطأ غير العمدي، إلا إذا أثبث الجاني انتفاء تلك العلاقة كأن يبثث أن إزالة أو تعديل المعطيات يرجع للقوة القاهرة أو الحادث المفاجئ ، كما لا يشترط أن تكون النتيجة غير مقصودة أي على سبيل الخطأ غير العمدي ويكفي لتوافر هذا الظرف وجود علاقة سببية بين الدخول أو البقاء غير المشروع والنتيجة الضارة المتمثلة في إعاقة أو إفساد النظام، أي بمعنى عدم قدرة هذا النظام للقيام بوظيفة المعالجة الآلية لمعطيات التوقيع الالكتروني، مع عدم اشتراط القصد للنتيجة، لأن الظرف المشدد هنا هو ظرف مادي[1].

وإذا ترتب عنه إعاقة أو إفساد لنظام المعالجة الآلية للمعطيات فتكون العقوبة الحبس من ستة 06 أشهر إلى سنتين 02، والغرامة من 100.000 إلى 300.000 دينار جزائري.

وإفساد أو إعاقة النظام يكون إما بفعل توقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظر منه القيام به، وإما في فعل إفساد نشاط أو وظائف هذا النظام ولا يشترط أن يقع فعل التعطيل أو الإفساد على كل عناصر النظام جملة بل يكفي أن يؤثر على أحد هذه العناصر فقط، ولم يشترط المشرع أن يتم التوقف أو التعطيل بوسيلة معينة فقد تكون مادية أو معنوية، والمادية تكون مقترنة بعنف أم لا إذا وقعت على الأجهزة المادية للنظام أو منعت من الوصول إليها مثل تخريبها بكسرها أو تحطيم أو قطع شبكات الاتصال ، وتكون وسيلة التحطيم معنوية إدا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، .ص ص 126 –127 .

وذلك بإدخال برنامج فيروس أو بإشغالها بمعلومات ومعطيات تفوق سعتها الحقيقة أو تعديل برنامج كلمة السر أو الدخول أو جعل النظام يتباطأ في أداء وظيفته[1].

ويستوي أن يكون التوقف أو التعطيل دائما أو مؤقتا، فقد يتم تدمير النظام بأحد الفيروسات، وقد يكون التوقف مؤقتا أو منقطعا على فترات منتظمة ينجم عنها شل النظام عن البدء في تشغيله مثلا أو عند استخدام أحد برامج التطبيق، ويشترط في التوقف أو التعطيل أن يكون إيجابيا أي يصدر عن الجاني نشاطا إيجابيا يؤدي إلى توقف النظام، فإذا كان ما صدر عنه امتناع مجرد فلا يتوافر الركن المادي، ولا تقوم الجريمة، أما إذا كان يقع على عاتق الجاني واجب قانوني أو اتفاقي يكون تشغيل النظام بموجبه يتوقف على تدخله وإذا امتنع على التدخل بقصد تعطيل النظام يتوافر الركن المادي وتقع الجريمة والامتناع هنا ليس امتناع مجرد وإنما هو امتناع مختلط بنشاط إيجابي يتمثل في تعسف الجاني ورفضه القيام بما يفرضه عليه القانون والاتفاق من واجب تشغيل النظام، أما الإفساد فيقصد به كل فعل وإن كان لا يؤدي إلى التعطيل، سيؤدي إلى جعل نظام المعالجة الآلية لمعطيات التوقيع الالكتروني غير صالحة للاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها [2].

وتضاعف وتشدد أيضا العقوبات المشار إليها في المادة 394 مكرر و394 مكرر 01 و02 إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر 3.

مع إمكانية تطبيق عقوبات على الشخص المعنوي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر4.

---

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص ص 128 – 129.

[2]– المرجع نفسه ص ص 129– 130 .

ب. العقوبات التكميلية

العقوبات التكميلية هي عادة لا يمكن النطق بها دون العقوبات الأصلية، وهي تكون دائما لتكملة العقوبات الأصلية، بهدف إعطاء أكثر فعالية للردع [1]، وتشمل في جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني عقوبة المصادرة، وإغلاق المواقع .

1 .المصادرة

المصادرة هي نقل ملكية مال أو أكثر للدولة، فهي عقوبة ناقلة للملكية جوهرها حلول الدولة محل المحكوم عليه أو غيره في ملكية مال[2]، وقد نصت عليها المادة 394 مكرر 06 بمصادرة الأجهزة والبرامج والوسائل المستخدمة في جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني.

2. غلق المواقع

نصت عليها أيضا المادة 394 مكرر 06 بإغلاق المواقع التي تكون محلا لجرائم المساس بالمعالجة الآلية للمعطيات، مع إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

الفرع الثاني: جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني

تضمن المشرع الجزائري تجريم الاعتداء القصدي على معطيات التوقيع الالكتروني في نص المادة 394 مكرر 01 بقولها "كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، لذلك سنتطرق إلى تمييز الاعتداء على النظام والمعطيات، ثم سنتطرق إلى أركانها وعقوبتها.

---

(1) -Bernard bouloc – hartini matos poulon , op-cit, p 477.

(2)– محمود نجيب حسني، قانون العقوبات– القسم العام ، ط8 ، دار النهضة العربية، القاهرة، 2018 ، ص 956 .

أولا: التمييز بين الاعتداء على النظام والاعتداء على المعطيات

إذا كانت جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني كجريمة الاعتداء القصدي على نظام المعالجة الآلية للتوقيع الإلكتروني يهدفان إلى الحماية من أفعال التخريب والقرصنة، إلا أنهما يختلفان في أن جريمة الاعتداء على النظام إن كانت تقع على البرامج وشبكات الاتصال فينتج عنه أيضا الاعتداء على المعطيات والعكس فإن المساس بالمعطيات لا يترتب عنه المساس بالنظام [1].

وقد وضع جانب من الفقه معيار المحل الذي تقع عليه، فإذا كان الفعل يقع على العناصر المادية للنظام فإن الجريمة تكون الاعتداء القصدي على النظام، أما إذا كانت تقع على عناصر معنوية فإننا نكون أمام جريمة اعتداء على المعطيات، وما يؤخذ على هذا المعيار أن كلا من الجريمتين قد تقع على العناصر المادية والمعنوية معا، لذلك ذهب جانب من الفقه إلى الأخذ بمعيار الغاية، فإذا كان غاية الجاني الاعتداء على النظام نكون أمام جريمة الاعتداء القصدي على نظم المعالجة الآلية لمعطيات التوقيع الإلكتروني، وإذا كان غاية الجاني الاعتداء على معطيات التوقيع الإلكتروني نكون أمام جريمة الاعتداء على معطيات التوقيع الإلكتروني[2].

ثانيا: أركان جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني

نص المادة 394 فقرة 01 تضمن ثلاث أفعال بطريق الغش وهي الإدخال، المحو، التعديل، سنتطرق لهم في الركن المادي، ثم ركنها المعنوي.

أ.الركن المادي

النشاط الإجرامي يتخذ ثلاث صور وهي الإدخال، المحو، التعديل، ولا يشترط اجتماعها فإحدى الصور تكفي لتوافر الركن المادي، وهذه الصور تنطوي على التلاعب في المعطيات

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص ص 135 – 136 .

[2]– المرجع نفسه، ص 136 .

التي يحويها نظام المعالجة المادية للمعطيات سواء بإضافة معطيات جديدة أو بمحو أو تعديل معطيات كانت موجودة، ويقصد بالإدخال، المحو ، التعديل لقيام الركن المادي ما يلي[1]:

1. الإدخال: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم كان يوجد عليها معطيات من قبل، كإدخال برنامج غريب يضيف معطيات جديدة.

2.المحو: ويقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

3.التعديل: وهو تغيير المعطيات داخل النظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو و التعديل عن طريق برامج تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديله، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برامج الفيروسات بصفة عامة.

والأفعال السابقة الإدخال المحو التعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة بصور أخرى.

ب. الركن المعنوي

جريمة قصدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة إلى فعل الإدخال أو المحو أو التعديل وعلمه إلى أن نشاطه الإجرامي يترتب على التلاعب في المعطيات بما ليس له الحق في ذلك وباعتدائه على صاحب الحق والسيطرة على تلك المعطيات أو بدون موافقته[2].

---

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 133 .

[2]– المرجع نفسه، ص 134.

ثالثا: عقوبة الاعتداء القصدي على معطيات التوقيع الالكتروني

تعاقب المادة 394 مكرر 01 بالحبس 06 ستة أشهر إلى 03 ثلاث سنوات وبغرامة من 500.000 دج إلى 4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر 3 .

مع إمكانية تطبيق عقوبات على الشخص المعنوي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر 4 .

وتطبق أيضا العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة اعتداء قصدي على معطيات التوقيع الالكتروني بعلم مالكها وفقا لنص المادة 394 مكرر 6.

الفرع الثالث: جريمة الاتفاق الجنائي للمساس بأنظمة المعالجة الآلية للمعطيات

المشرع الجزائري لم يكتف بتجريم الشروع في الجريمة فقط وإنما جرَم قبل ذلك الاتفاق على الإعداد لارتكاب هذه الجريمة إذا تجسد في أعمال مادية وجرَم التعامل في معطيات غير مشروعة والتي تعتبر من جرائم الخطر ومن خلالهما يهدف المشرع إلى تجريم وقائي لسد كل الأبواب أمام ارتكاب جريمة التواجد غير المشروع وامتد أيضا التجريم إلى مراحل لاحقة بالجريمة وهو ما يتجلى في الصورة الثانية من جريمة التعامل في معطيات غير مشروعة والمتمثلة التعامل في المعطيات المتحصلة من الجريمة [1]، لذلك سنتطرق إلى الحكمة من تجريم الاتفاق، وتمييزه عما يشابهه، ثم أركان الاتفاق لارتكاب جرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني، ثم عقوبتها .

(1)- محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص ص 202-203.

أولا: الحكمة من تجريم الاتفاق

الحكمة من تجريم الاتفاق على الإعداد لارتكاب جريمة التواجد غير المشروع للأنظمة المعلوماتية إذا تجلى ذلك في أعمال مادية تظهر في رغبة المشرع في التصدي لجريمة التواجد في مرحلة مبكرة جدا، تسبق حتى مرحلة الشروع ذلك أن الاتفاق على ارتكاب تلك الجريمة يعطي لهده الأخيرة بعدا تنظيميا يتطلب التصدي المسبق لأنه يشكل خطرا جديا وحقيقيا، ومن شان تركه أن يؤدي إلى ارتكاب جريمة التواجد وإلحاق ضرر، فتجريم الاتفاق هو حرب استباقية من المشرع ضد جريمة التواجد غير المشروع في الأنظمة المعلوماتية[1].

ثانيا: التمييز بين الاتفاق ومايشابهه

هناك ما يشابه الاتفاق في ارتكاب الجرائم كالاشتراك والشروع.

أ. الاتفاق الجنائي والاتفاق كوسيلة اشتراك

يتلخص وجه الشبه بين الاتفاق الجنائي والاتفاق كوسيلة اشتراك في أن كليهما من صنف واحد، فليس ثمة فارق بين النوعين من حيث طبيعتهما .

أما من حيث الاختلاف بينهما يتلخص في:

– أن الاتفاق الجنائي على خلاف الاتفاق كوسيلة اشتراك محدد بجرائم معينة .

– لا يقوم الاتفاق الجنائي إلا في الجرائم العمدية بينما في الاتفاق كوسيلة اشتراك قد يكون موضوعه جرائم عمدية كالجنايات أو الجنح أو المخالفات وهي في الغالب غير عمدية.

– أن الاتفاق الجنائي قد يكون موضوعه الأعمال التحضيرية المحضة على خلاف الاتفاق كوسيلة اشتراك.

[1]– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 205 .

– أن الاتفاق قد يكون موضوعه جريمة معينة أو غير معينة، أما الاتفاق كوسيلة اشتراك فيتعين أن يكون موضوعه جريمة معينة.

– أن الاتفاق الجنائي لا يتطلب نتيجة معينة فهو من قبيل الجرائم ذات الطابع الشكلي، أما الاتفاق كوسيلة اشتراك فهو على خلاف ذلك لأنه يحدد المسؤولية عن جريمة ارتكبت فعلا[1].

ب.الاتفاق الجنائي والشروع

يتشابه الاتفاق الجنائي والشروع في أن كليهما يعتبر من الجرائم الناقصة وذلك لعدم إتمام الفعل الإجرامي الذي قصده الجاني كما أنهما يعتبران من قبيل جرائم الخطر نظرا لأن طبيعتهما تتنافى مع تحقيق الضرر، وأخيرا فإن كليهما يتطلب تنفيذ الغرض غير المشروع، أما من حيث الاختلاف، فالشروع ليس جريمة قائمة بذاتها بل يضيع ضمن ثنايا الجريمة الأخرى التي يقع فيها الشروع، لأنه يأخذ طابع تلك الجريمة من حيث التجريم والعقاب، في حين أن الاتفاق الجنائي يعتبر جريمة قائمة بذاتها ولا يضيع في ثنايا الجريمة موضوع الاتفاق لأن تنفيذ الجريمة موضوع الاتفاق لا ينهي جريمة الاتفاق، كما أن الشروع بخلاف الاتفاق محدد بجرائم معينة[2] .

ثالثا: أركان الاتفاق لارتكاب جرائم المساس بالمعالجة الآلية للمعطيات

يقوم الاتفاق الجنائي لارتكاب جرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني على ركنين مادي ومعنوي.

أ.الركن المادي

يتمثل في اتفاق بين شخصين على الأقل نحو هدف محدد هو التحضير لارتكاب إحدى جرائم الاعتداء على نظم المعالجة الآلية للتوقيع الالكتروني، ويستوي أن يكون أعضاء الاتفاق

---

[1]– مصطفى عبد اللطيف إبراهيم، الاتفاق الجنائي، جريمة الاتفاق الجنائي–دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2011 ، ص ص 84 – 85 .

[2]– المرجع نفسه، ص82 .

في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، كما يستوي أن بعرف أعضاء الاتفاق بعضهم بعض أو لا، ولكن اتفقوا فما بينهم على القيام بالنشاط الإجرامي المتمثل في الاعتداء على نظام التوقيع الالكتروني، فادا ارتكب الفعل التحضيري شخص بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة فالعقاب لا يتقرر إلا باجتماع شخص فأكثر، ويجب أن يتخذ هذا النشاط صورة العمل التحضيري المادي والذي لا يختلط مع البدء في التنفيذ الذي يتحقق به الشروع أو المحاولة في ارتكاب الجريمة أو المساهمة الجرمية وإلا لما كانت الحاجة لهذا النص، ومن أمثلة العمل التحضيري المادي المعاقب عليه تبادل المعلومات اللازمة لتنفيذ الجريمة من الكشف عن الرقم الكودي أو السري للدخول إلى النظام أو كيفية تجاوزها، فلا يكفي أن يكون الشخص عضوا في جماعة أو منظم لها، وإنما يجب أن يصدر عنه فعل تحضيري مادي حتى ولو تمثل في حضور اجتماع تناقش فيه مثل تلك الأفعال[1].

ب. الركن المعنوي

يجب أن يتوافر القصد الجنائي لدى أعضاء الجماعة والذي يتمثل في توافر العلم لدى كل منهم أنه عضو في جماعة إجرامية وأن تتجه إرادة كل عضو من أعضائها إلى تحقيق نشاط إجرامي معين، مع علمه بنشاط الأخر[2]، فمن ينظم إلى اتفاق معتقدا أنه للاتجار في برامج حاسب آلي ومعطيات عادية ثم يتبين أن الاتجار كان ببرامج خبيثة أو برامج اختراق، مثل هذا لا يعد القصد الجنائي متوافرا لديه، وذلك لانتفاء علمه بموضوع الاتفاق الجنائي، لكن القصد الجنائي يتوافر لدى هذا الشخص إذا علم بعد دخوله الاتفاق بموضوعه غير المشروع ومع ذلك بقي في الاتفاق [3].

---

[1]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 118 .

[2]– المرجع نفسه، ص119 .

[3]– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 220 .

رابعا: العقوبة

تعاقب المادة 394 مكرر 5 على جريمة الاتفاق الجنائي لارتكاب جرائم المساس بالمعالجة الآلية للمعطيات ، بالعقوبات المقررة للجريمة ذاتها التي تم الاتفاق و الإعداد لارتكابها .

فإذا كان موضوع الاتفاق الدخول أو البقاء في منظومة المعالجة الآلية للمعطيات وفقا لنص المادة 394 مكرر تكون العقوبة الحبس من ثلاثة أشهر إلى سنة والغرامة من 50000 إلى 200000 دج ، في صورتها البسيطة .

وتشدد العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، وإذا ترتب على هذه الأفعال تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 300000 دج .

ويعاقب على جريمة الاتفاق لإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها وفقا لنص المادة 394 مكرر1 ، بالحبس من ستة إلى ثلاث سنوات وبغرامة من 50000 دج إلى 4000.000 دج .

كما يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 إلى 10.000.000 دج على الاتفاق كل من يقوم عمد وبطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، أو حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها وفقا لنص المادة 394 مكرر 2 فقرة 1 و 2 .

وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر3 .

مع إمكانية تطبيق عقوبات على الشخص المعنوي الذي ينضم إلى اتفاق جنائي لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر 4.

وتطبق أيضا على جريمة الاتفاق الجنائي العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة اتفاق بعلم مالكها وفقا لنص المادة 394 مكرر 6.

الفرع الرابع: جريمة التعامل في معطيات غير مشروعة

تعاقب المادة 394 مكرر 02 كل من يقوم عمدا وبطريق الغش بمايأتي:

1- تصميم أو بحث أو تجميع أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أو ترتكب بها الجرائم المنصوص عليها في هذا القسم

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .

وبالتالي تتخذ جريمة التعامل في معطيات غير مشروعة صورتين، الأولى هي التعامل في معطيات صالحة لارتكاب جريمة، والثانية هي التعامل في معطيات متحصلة من جريمة[1]، لذلك سنتطرق إلى أركان جريمة التعامل في معطيات غير مشروعة، ثم عقوبتها .

أولا: أركانها

تقوم جريمة التعامل في معطيات غير مشروعة على ركنين مادي ومعنوي.

أ. **الركن المادي** : الركن المادي يقوم على محل الجريمة، والسلوك الإجرامي.

[1]- محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 13 ، العدد01 ، جوان، 2018 ص 74 .

1. محل الجريمة

المعطيات في جريمة الدخول أو البقاء غير المصرح بهما هي المعطيات الموجودة داخل النظام، أما المعطيات في جريمة التعامل في معطيات صالحة لارتكاب جريمة فهي المعطيات المخزنة أو المرسلة، والمشرع لم يرد حصر هذه الجريمة في المعطيات المعالجة وفق نظام معالجة آلية، وإنما أراد أن يتسع مجالها إلى مختلف المعطيات مهما كانت حالتها سواء كانت مخزنة ثابتة أو مرسلة متحركة أو معالجة، وهذا مسلك يبرره أن كثير من المعطيات التي يمكن أن ترتكب بها الجرائم قد لا توجد داخل النظم للمعالجة الآلية للمعطيات وإنما تكون مخزنة داخل وسائط أخرى أو تكون مرسلة بين نظم المعلومات، وإذا كان قانون العقوبات الجزائري قد اقتصر على المعطيات كمحل للجريمة فإن قانون العقوبات الفرنسي كان أكثر توسعا في ذلك عندما أقر في مادته 323 – 3–1 أن التعاملات المجرمة يمكن أن تقع على تجهيزات أو أدوات أو برنامج معلوماتي وعلى معطيات مصممة أو معدة لارتكاب واحدة أو أكثر من جرائم الدخول غير المصرح بهما أو إعاقة أو إفساد أنظمة المعالجة الآلية للمعطيات أو التلاعب بالمعطيات[1].

2. السلوك الإجرامي

السلوك الإجرامي يكون بأحد الأفعال المنصوص عليها في الفقرة 01 و02 من المادة 394 مكرر02 .

وتتحقق الأفعال الإجرامية المكونة لجريمة التعامل في معطيات صالحة لارتكاب جريمة بمايلي :

- **التصميم والبحث والتجميع**

التصميم هو أول عملية في سلسلة التعامل في المعطيات، وهي تتمثل في إخراج المعطيات إلى الوجود، أي القيام بخلق وإيجاد معطيات صالحة لارتكاب جريمة، وهذا العمل يقوم به

(1)– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص ص 196 – 197 .

مختصون في هذا المجال كالمبرمجين ومصممي البرامج ومثاله تصميم برنامج يحمل فيروسا وهذا ما يطلق عليه بالبرامج الخبيثة أو تصميم برنامج اختراق، أما البحث فهو كيفية البحث عن هذه المعطيات وإعدادها وليس مجرد البحث عن هذه المعطيات ولهذا جاءت عبارة البحث بعد عبارة التصميم مباشرة وإن كان النص قد جاء عاما، وفيما تعلق بفعل التجميع فهو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول أو البقاء في نظام معالجة آلية للتوقيع الالكتروني، ويفترض في هذا السلوك أن صاحبه يحتفظ بمجموعة من المعطيات التي تشكل خطرا والتي ممكن استعمالها في ارتكاب تلك الجرائم، وقد قدر المشرع أن تعدد المعطيات من شأنه أن يرفع درجة الخطر التي تشكلها [1].

- **التوفير (الوضع تحت التصرف أو العرض) و النشر و الاتجار**

الاتجار بالمعطيات هو تقديمها للغير بمقابل ولا يشترط أن يكون هذا المقابل نقديا بل قد يكون عينيا أو قد يتمثل في خدمات أو غير ذلك، فالاتجار كل المعاملات التي قد تقع على المعطيات الصالحة لارتكاب الجريمة، أما التوفير فهو من الأفعال التي تجرمها المادة 394 مكرر 02 من قانون العقوبات الجزائري أيضا فعل التوفير، أي توفير معطيات يمكن أن ترتكب بها جريمة دخول أو بقاء داخل نظام معلوماتي للتوقيع الالكتروني، أو جريمة تلاعب، وتعاقب المادة 323 فقرة 3 و 1 من قانون العقوبات الفرنسي على السلوك نفسه، كما تعاقب عليه المادة السادسة من اتفاقية بودابست تحت عبارة " أي شكل للوضع تحت التصرف "، والحقيقة أن الترجمة الفرنسية للمادة 394 مكرر 2 من قانون العقوبات الجزائري توافق هذه العبارة وهي الوضع تحت التصرف " met a disposition، والمراد بذلك هو تقديم المعطيات وإتاحتها لمن يريدها أي جعلها في متناول الغير، ووضعها تحت تصرفه، أما صورة فعل النشر فيقصد به

[1]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص ص 200 – 201 .

إذاعة المعطيات محل الجريمة وتمكين الغير من الاطلاع عليها وذلك عن طريق مختلف الوسائل التي يتصور النشر بها مهما كانت طبيعتها[1].

والفرق بين النشر والوضع تحت التصرف أن هذا الأخير يشير إلى وضع أجهزة على الخط ليتم استخدامها بواسطة الغير، كما يضم المصطلح من ناحية أخرى إنشاء وتجميع الروابط المتشعبة من أجل تسهيل الوصول إلى هذه الأجهزة وذلك عن طريق الإحالة لبرنامج يتصل ببرامج مصممة لإتلاف بيانات التوقيع الالكتروني، أو من أجل التدخل في عمل النظام، كبرامج الفيروسات، أو البرامج المصممة من أجل الوصول إلى نظام الحاسب المتعلق بالتوقيع الالكتروني [2].

أما الصورة الثانية لأفعال التعامل في معطيات غير مشروعة هي الأفعال المنصوص عليها في المادة 394 مكرر02 فقرة 02 وهي الحيازة، الإفشاء، النشر ، الاستعمال.

ب. الركن المعنوي

جريمة عمديه تتطلب قصدا جنائيا عاما وخاصا في صورة التعامل في معطيات صالحة لارتكاب جريمة، بينما يكفي في صورتها الثانية وهي التعامل في معطيات متحصلة من جريمة توافر القصد الجنائي العام، كما أنه لا يكفي لقيام جريمة التعامل في معطيات صالحة لارتكاب جريمة أن يتوافر لدى الفاعل القصد الجنائي العام وحده، وإنما يلزم فضلا عن هذا القصد أن يتوافر لدى الفاعل القصد الخاص، لأن التعامل في المعطيات الصالحة لارتكاب الجريمة لابد أن يكون بقصد الإعداد أو التمهيد لاستعمالها في ارتكاب هذه الجريمة [3]، وأن الصورة الثانية تتطلب قصد عام، لأن طبيعة هذه المعطيات واحدة، فكلها متحصلة من جريمة، وصفتها الثابتة

[1]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص ص 202 إلى 204 .

[2]– هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية و المستحدثة، المرجع السابق، ص 263 .

[3]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص 213 . .

هذه تجعل من القصد العام كافيا لقيام الجريمة، إذ لا يسأل الفاعل عن قصده الخاص من التعامل في هذه المعطيات ما دام يعلم أنها متحصلة من جريمة، وهذا ما يكون القصد العام[1].

ثانيا : العقوبة

يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 إلى 10.000.000 دج كل من يقوم عمد وبطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، أو حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها وفقا لنص المادة 394 مكرر 2 فقرة 1 و 2، وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر 3، مع إمكانية تطبيق عقوبات على الشخص بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر 4 .

وتطبق أيضا العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة التعامل في معطيات غير مشروعة بعلم مالكها وفقا لنص المادة 394 مكرر 6.

المبحث الثاني: الحماية الجزائية الموضوعية للتوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين 15 – 04

نظم المشرع الجزائري جميع أحكام التوقيع الالكتروني ضمن قانون التوقيع والتصديق الالكترونيين 15 – 04 من بينها أحكام الحماية الجزائية الموضوعية له، والتي تشمل نماذج صور التجريم الواقعة على التوقيع الالكتروني وبياناته، وباعتبار التوقيع الالكتروني يمر بجهة أخرى تسمى جهة التصديق الالكتروني لإعطائه أكثر مصداقية وموثوقية، فقد يتم الاعتداء على التوقيع الالكتروني سواء قبل المصادقة عليه أو أثنائها أو بعدها، وصور الاعتداء على

[1]– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص 215 .

التوقيع الالكتروني في قانون التوقيع الالكتروني، هي جريمة إفشاء أو استعمال أو حيازة بيانات التوقيع الالكتروني المنصوص عليها في المادة 68 من قانون التوقيع الالكتروني، سنتناولها بالدراسة من خلال عنوان الحماية الجزائية للإفشاء والتعامل غير المشروع في بيانات التوقيع الالكتروني ضمن المطلب الأول، وهناك صور أخرى للجرائم الواقعة على التوقيع الالكتروني أثناء وبعد المصادقة عليه أفردها المشرع في قانون التوقيع الالكتروني ضمن جرائم التصديق الالكتروني في المواد من 66 إلى 74 والتي سنتناولها بالدراسة في المطلب الثاني.

المطلب الأول: الحماية الجزائية للإفشاء والتعامل غير المشروع في بيانات التوقيع الالكتروني

السرية صفة لازمة لأنها تحصر حركة الرسالة التي تحمل المعلومة في دائرة محددة من الأشخاص، لأن المعلومة غير السرية لديها ميل للتداول لذلك تكون بمنأى عن أي حيازة، وتكتشف المعلومة وصفها إما بالنظر إلى طبيعتها، أو بالنظر إلى إرادة الشخص أو بالنظر إلى الأمرين معا، كما هو الحال بالنسبة للرقم السري للبطاقة الائتمانية، ويقلل الطابع السري في هذه الحالات المختلفة من استخدام المعلومات ويقصرها فقط على دائرة المؤتمنين عليها، والذين يجدون أنفسهم منتفعين بحق الاستئثار عليها [1]، ولكن القانون رتب آثارا قانونية ومتابعة جزائية على إفشاء أو استعمال أو حيازة بيانات التوقيع الالكتروني الخاصة بالغير في نص المادة 68 من قانون التوقيع الالكتروني حماية لخصوصية الموقع الكترونيا، لذلك سنتطرق إلى الأحكام الموضوعية لجريمة إفشاء بيانات التوقيع الالكتروني في الفرع الثاني، وقبلها سنتطرق إلى مفهوم جريمة إفشاء الأسرار في الفرع الأول، وقد يقوم الشخص باستخدام التوقيع الالكتروني في الكثير من المجالات الالكترونية ما يجعل إمكانية إفشاء بياناته يرتبط بجرائم أخرى سنتطرق إليها في الفرع الثالث، والمشرع في قانون التوقيع الالكتروني نص على جريمة واحدة لا تتم في مرحلة التصديق الالكتروني عليه وهي جريمة المادة 68 من قانون التوقيع الالكتروني، ما

[1]- محمد سامي الشوا، المرجع السابق، ص 185 .

يدعونا أيضا إلى التطرق لبعض صور التجريم الواقع على التوقيع الالكتروني في التشريع المقارن ضمن الفرع الرابع .

الفرع الأول: مفهوم جريمة إفشاء الأسرار

جريمة إفشاء الأسرار تتطلب بعض المميزات لا نجدها في جرائم أخرى كاشتراط صفة معينة في مرتكبها، وشروط السر محل الحماية الجنائية، وحالات جواز إباحة السر، وما مدى رضا صاحب السر بإفشائه، كل هذه التساؤلات سنحاول الإجابة عنها في هذا الفرع.

أولا: علة تجريم الإفشاء

العلة من التجريم هو أن يكفل المشرع المباشرة السليمة والمنتظمة لمهن يفترض فمن يمارسونها أن يودع عملائهم لديهم أسرارهم إذ أن هذه الأسرار هي موضوع نشاطهم المهني[1].

ثانيا: تعريف إفشاء الأسرار

هو الكشف عن واقعة لها صفة السر ممن علم بها بمقتضى مهنته ومقترن بالقصد الجنائي[2]، وعرف أيضا بأنه تعمد الإفضاء بسر ائتمن عليه بحكم عمله أو صناعته، في غير الأحوال التي يوجب فيها القانون الإفضاء أو يجيزه[3] .

وفكرة الإفشاء أن الإخبار بالسر والشخص المتعلق به كان إلى الغير، والغير يراد به الشخص الذي لا ينتمي إلى هذه الفئة من الناس الذين ينحصر فيهم نطاق العلم بالواقعة [4]، التي توصف بالسر [5].

---

[1]– محمود نجيب حسني، قانون العقوبات– القسم الخاص، المرجع السابق، ص 751 .

[2]– المرجع نفسه، ص750 .

[3]– رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مكتبة الوفاء القانونية، الإسكندرية، 2015 ، ص 457 .

[4] – محمود نجيب حسني، قانون العقوبات– القسم الخاص، المرجع السابق، ص735 .

* والسر هو واقعة أو صفة ينحصر نطاق العلم بها في عدد محدود من الأشخاص إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم بها محصورا في ذلك النطاق . أما الإفشاء فهو إطلاع الغير على السر والشخص الذي=

ثالثا: شروط السر المحمي قانونا

يتعين أن تكون المعلومة التي وصلت إلى علم المهني أو الموظف مكتسبة بسبب ممارسة مهنته أو وظيفته على أي صورة من الصور، لأن جوهر جريمة إفشاء الأسرار هو إخلال شخص ملزم قانونا بكتمان ما ائتمن عليه بحكم وظيفته أو مهنته [1]، بشرط أن تقوم صلة بين السر ومباشرة المهنة أي أن يكون السر مهنيا، وتطبيقا لذلك فإنه لا جريمة في إفشاء سر يصدر عن صديق أو قريب أودع لديه سر، ولا جريمة في إفشاء سر يصدر عن خادم في شأن سر أو دعه لديه رب العمل فمهنته ليست من المهن التي تفترض الإيداع الاضطراري للسر [2].

رابعا: حالات إفشاء الأسرار

في أحوال معينة يكون إفشاء السر واجبا بمقتضى القانون أو جائزا فحسب وفي أي من الحالتين لا تتحقق الجريمة وإفشاء السر يكون وجوبيا بمقتضى نصوص صريحة أو إذا تعلق الأمر بأعمال الخبرة أمام الجهات القضائية ويكون جوازيا إذا أريد منه التبليغ عن جريمة [3].

والسر المهني قد يعفى صاحبه أحيانا من عدم الإدلاء به حتى بالشهادة أمام الجهات القضائية، إذا كان من الأشخاص الملزمين بكتمان السر المهني فمن حقهم رفض الإدلاء بشهادتهم أمام الجهات القضائية في حالة الحماية للنظام العام والآداب العامة، ويكون إفشاء السر المهني عن طريق الإدلاء بشهادة أمام الجهات القضائية لا يشكل جريمة، إذا كان من الأشخاص الغير ملزمين بكتمان السر المهني المذكورين في نص المادة 378 من قانون العقوبات الفرنسي، والمقابلة لنص 301 من قانون العقوبات الجزائري، وهؤلاء الأشخاص

يتعلق به أي أن الإفشاء في جوهره هو نقل معلومات وتتحدد عناصره بالسر والشخص الذي يتعلق به . محمود نجيب حسني، قانون العقوبات– القسم الخاص، المرجع السابق، ص759 .

[1]– سامان عبد الله عزيز، المسؤولية الجنائية الناشئة عن إفشاء الأسرار المهنية والوظيفية– دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2017 ، ص 60 .

[2]– محمود نجيب حسني، قانون العقوبات، القسم الخاص، المرجع السابق، ص752 .

[3]– رؤوف عبيد، المرجع السابق، ص 472 .

الإدلاء بالشهادة عندهم لا يعتبر جريمة إفشاء سر مهني [1]، فمتى يكون إفشاء أسرار بيانات التوقيع الالكتروني وجوبا، ومتى يكون جوازيا .

أ. افشاء بيانات التوقيع الالكتروني وجوبا

مثل ما نص عليه القانون 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي [2]، في المادة 49 منه "أنه يمكن للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي القيام بالتحريات المطلوبة ومعاينة المحلات التي تتم فيها المعالجة باستثناء محلات السكن، ويمكنها للقيام بمهامها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها، ومن ضمنها بيانات التوقيع الالكتروني، ولا يعتد أمام السلطة الوطنية بالسر المهني ".

ب. إفشاء بيانات التوقيع الالكتروني جوازيا

الأصل أن حظر إفشاء الأسرار مقرر حتى ولو كان للتبليغ عن جريمة وقعت بالفعل، وإنما استثناء لهذا الأصل أجاز القانون للأمين عن السر تبليغ السلطات عما توصل إليه من معلومات[3]، مثلما أجازت الفقرة 13 من المادة 25 من قانون حماية المعطيات ذات الطابع الشخصي 18-07 أنه يمكن للسلطة الوطنية لحماية المعطيات الشخصية في حالة معاينة وقائع تحتمل وصف جزائي تعلم النائب العام المختص، كالوصول إلى علمها وقائع إفشاء معطيات شخصية لبيانات توقيع الكتروني، فتقوم بإعلام النائب العام المختص.

---

[1]- Michèle laure rassat, op-cit , p305.

[2]– الجريدة الرسمية للجمهورية الجزائرية، العدد 34 ، الصادرة في 10– جوان– 2018 .

[3]– رؤوف عبيد، المرجع السابق، ص 474 .

خامسا: رضا صاحب السر بإفشائه

انقسم الرأي حول رضا صاحب السر بإفشائه، وهل يحول دون قيام الجريمة أم لا إلى قسمين[1] :

الأول يرى أن الالتزام بكتمان سر المهنة مصدره العقد الذي بين صاحبه وصاحب المهنة، سواء أكان عقد عمل أو كالة، وان الإيداع للسر لدى الأمين يصبح أن يوصف بأنه وديعة، ولكنه قياس مع الفارق أن الوديعة يلتزم الوديع بالرد، أما هنا فلا التزام به ولعله إذا أريد القول بالتعاقد على كتمان السر يكون أرجح الآراء في وصفه القول بأنه عقد غير مسمى.

والاتجاه الثاني يرى أن أساس الالتزام بكتمان السر هو نص القانون لا العقد، فهو قاعدة مقررة لحساب الصالح العام، وقد أخذ القضاء في فرنسا بهذا التكييف الثاني واعتبر التقيد بالكتمان قاعدة تنظيمية مطلقة، فليس للأمين أن يتدرع بأن صاحب السر قد أحله من قيد الكتمان .

سادسا: صفة الجاني (من يفشي السر)

تتطلب جريمة إفشاء الأسرار صفة معينة، وهذه الصفة مستمدة من نوع المهنة التي يمارسها أي أنها صفة مهنية، والعلة في تطلب هذا الركن أن جوهر الجريمة هو الإخلال بالتزام ناشئ عن المهنة وما يتفرع عنها من واجبات بالإضافة إلى أن علة التجريم هي الحرص على السير المنتظم لمهن معينة ذات أهمية اجتماعية [2]، وهذه الصفة متطلبة في فاعل الجريمة، لذلك يجوز أن يكون الشريك فيها غير حائز على هذه الصفة، وهي متطلبة وقت إيداع السر دون وقت إفشائه، وبالتالي فالقائم على جهة التصديق الذي يودع سرا لبيانات التوقيع الالكتروني لا تقوم الجريمة في حقه إذا أفشى السر بعد اعتزاله المهنة [3].

---

[1]– رؤوف عبيد، المرجع السابق، ص 476 .

[2]– محمود نجيب حسني، قانون العقوبات–القسم الخاص، المرجع السابق، ص 863 .

[3]– المرجع نفسه، ص 864 .

الفرع الثاني: أحكام جريمة إفشاء أو استعمال أو حيازة توقيع الكتروني موصوف خاص بالغير

يؤدي التعامل عن طريق التوقيع الالكتروني في المعاملات الالكترونية إلى احتمال الاعتداء عليه سواء بإفشائه أو استعماله أو حيازته بطريقة غير مشروعة، التي ستؤدي حتما إلى المساس بمصلحة الخصوصية لصاحب التوقيع الالكتروني، ويبسط المشرع حمايته الجزائية للمصلحة والقيم الاجتماعية عن طريق التجريم والعقاب، ما أدى بالمشرع إلى تجريم إفشاء أو حيازة أو استعمال بيانات توقيع الكتروني موصوف خاص بالغير في نص المادة 68 من قانون التوقيع الالكتروني، هذا ما يقودنا إلى دراسة أركانها، ثم عقوبتها.

أولا: أركانها

أي جرم يظهر إلى الوجود لابد وأن له الأركان الأساسية التي يقوم عليها، وللجريمة مهما كانت ثلاث أركان أساسية و هي الركن الشرعي، الركن المادي، والركن المعنوي، أما الركن الشرعي فهو يكمن في الحقيقة أن الفعل منصوص ومعاقب عليه قانونا. أما الركن المادي فهو الذي يتكون من فعل أو امتناع مجرم قانونا، ويبقى الركن المعنوي فهو نسبة الفعل أو الجريمة إلى مرتكبها [1]، ولدراسة أركان جريمة إفشاء أو استعمال أو حيازة توقيع الكتروني موصوف خاص بالغير سنتطرق إلى محل وصفة الجاني فيها، ثم ركنها المادي والمعنوي.

أ. محل الجريمة وصفة الجاني

محل الجريمة لابد أن يكون توقيع الكتروني موصوف خاص بالغير، أما صفة الجاني فإن الأصل أن جريمة إفشاء الأسرار من جرائم دوي الصفة، فهي تتطلب قانونا أن يتم ارتكابها من شخص ينتمي إلى فئة معينة من المهن، وفي جريمة إفشاء أسرار التوقيع الالكتروني أو حيازتها أو استعمالها، قد ترتكب من مزودي خدمات التصديق الالكتروني، أو شخص عادي، فلذلك

(1) -Bernard bouloc,haritini mastopolou, op-cit, p27 .

المادة 68 من قانون التوقيع الالكتروني لا تشترط صفة معينة في مرتكبها لأنها لا تعاقب على الإفشاء فقط، وإنما أيضا على استعمال وحيازة التوقيع الالكتروني.

ب. الركن المادي

يقول الفقيه الفرنسي robert أن لا جريمة بدون ركن مادي[1]، والذي هو ماديتها، أي ما يدخل في كيانها وتكون له طبيعة مادية ملموسة، إذ أنه بغير ماديات ملموسة لا ينال المجتمع اضطراب ولا يصيب الحقوق الجديرة بالحماية عدوانا، بالإضافة إلى ذلك فإن قيام الجريمة على ركن مادي يجعل إقامة الدليل عليها ميسورا، حيث أن إثبات الماديات أسهل من إثبات الظواهر النفسية أو المعنوية، وللركن المادي ثلاثة عناصر رئيسية وهي الفعل، النتيجة، والعلاقة السببية[2]، لذلك سنتناول بالدراسة عناصر الركن المادي في جريمة إفشاء أو استعمال أو حيازة توقيع الكتروني موصوف خاص بالغير، وهي الفعل، والنتيجة ، والعلاقة السببية.

1.الفعل الإجرامي المادي

يتحقق السلوك الإجرامي بإحدى الأفعال الثلاث: الإفشاء، الاستعمال، الحيازة .

- **الإفشاء**

وهو الفعل المتمثل في إيداع ونشر بيانات التوقيع الالكتروني بحيث يمكن للغير الاطلاع على محتواها وقراءتها، وسواء تم الاطلاع على محتواها من قبل الغير أو لم يتم ذلك، لأن العبرة بالنشر هو خروج بيانات التوقيع الالكتروني من دائرة السرية، ما يجعل إمكانية واحتمال الاطلاع عليها من قبل الغير واردة الحصول .

(1) - « il n’ya pas d’infraction sans fait matériel », Abdelmadjid zaalani, Eric Mathias, la responsabilité pénal, Berti, Alger,2009, P179.

(2)– محمود نجيب حسني، شرح قانون العقوبات– القسم العام، المرجع السابق، ص 321.

أما عن مكان ووسائل النشر قد يكون في أوساط الكترونية كنشره في المواقع الالكترونية وشبكات التواصل الاجتماعية كالفيسبوك أو التويتر أو الواتس أب وغيرها، أو سمعية بصرية في إحدى القنوات التليفزيونية، أو كتابية في إحدى الجرائد أو المجلات .

وهذه البيانات التي يتم إفشاؤها قد تكون محمولة في أوساط إلكترونية كالأقراص الممغنطة والديسكات أو مكتوبة في مجلات أو أي دعامة سواء كانت ورقية أو إلكترونية.

- **الاستعمال**

جرم المشرع الجزائري في نص المادة 68 فعل استعمال بيانات التوقيع الالكتروني لأنها تشكل أخطر سلوك واقع على بيانات التوقيع الالكتروني، لما يسببه من أضرار على صاحب التوقيع نتيجة للآثار المترتبة عن الاستعمال والتي غالبا ما تكون في أعمال غير مشروعة .

وعند ارتكاب الجاني لفعل حيازة بيانات التوقيع الالكتروني فإنها تكون بسيطرة الجاني الحائز وحده، كما انه أيضا عند إفشائها سيعلم الغير ببيانات التوقيع، ما يجعل هذين الفعلين أقل خطورة من الاستعمال بسبب أن بيانات التوقيع الالكتروني لم تخرج إلى دائرة الاستعمال.

ولا يتصور أن يكون الجاني مرتكبا لفعل الاستعمال من دون أن يكون حائزا لبيانات التوقيع الالكتروني، فمن يرتكب فعل الاستعمال يكون مرتكبا لفعل الحيازة، والعكس غير ذلك فالحائز لبيانات التوقيع الالكتروني قد لا يقوم باستعمالها .

وتقوم جريمة فعل استعمال بيانات التوقيع الالكتروني سواء تم استعمالها لمرة واحدة أو للعديد من المرات لأن العبرة بالاستعمال ولو مرة واحدة وليس بتكرار الاستعمال.

- **الحيازة**

حيازة التوقيع الالكتروني تعني الاستئثار بالتوقيع الالكتروني وتحت تصرف الحائز، وأن تكون حيازته بدون مبرر قانوني أو اتفاقي، بمعنى مبرر قانوني أي أن القانون هو من خول له

صلاحية الحيازة كجهات التصديق الالكتروني، أما المبرر الإتفاقي فهو الذي يكون بموافقة صاحب التوقيع الالكتروني.

أما بالنسبة للشروع فإنه لا يكون في الجنح إلا بنص صريح في القانون ولا يعاقب عليه في المخالفات إطلاقا، وهذا ما نصت عليه المادة 31 من قانون العقوبات[1]، وبالرجوع إلى صريح المادة 68 من قانون التوقيع الالكتروني نجذ أنها تعاقب على الجريمة التامة فقط، ولا تعاقب على الشروع والمحاولة.

2. النتيجة الإجرامية

هناك نوعان من الجرائم تبعا لمدى ضرورة تحقق نتيجة معينة للسلوك الإجرامي واعتبارها عنصرا لازما في الركن المادي أو عدم ضرورة تحقق ذلك، فهناك جرائم الضرر أو الجرائم المادية أو الجرائم ذات السلوك والنتيجة وهي التي يتطلب المشرع لتمام ركنها المادي تحقق نتيجة معينة، ومثالها جرائم القتل والضرب والجرح والسرقة، وهناك أيضا الجرائم الشكلية أو الجرائم ذات السلوك المجرد وهي التي لا يتطلب المشرع لتمام ركنها المادي تحقق نتيجة معينة، ومثال هذا النوع جريمة الامتناع عن أداء الشهادة أمام سلطات التحقيق أو الحكم وجريمة تعريض الأطفال للخطر وجريمة شهادة الزور[2]، فهل تصنف جريمة إفشاء أو استعمال أو حيازة توقيع الكتروني موصوف خاص بالغير تبعا لمدى ضرورة تحقق نتيجتها الإجرامية إلى جرائم الضرر أم جرائم الخطر؟.

جرائم الضرر يترتب عليها عدوان حال على الحق أو المصلحة المحمية جنائيا، أما جرائم الخطر يترتب عليها احتمال العدوان على الحق أو المصلحة المحمية جنائيا [3].

---

[1] - Jean-Claude soyer, droit pénal et procédure pénale, 18ém Edition, libraire générale de droit et de jurisprudence, paris, 2004, p 85.

[2]– بكري يوسف بكري محمد، قانون العقوبات– القسم العام، ط 1، مكتبة الوفاء القانونية، الإسكندرية، 2012، ص 398.

[3]– سليمان عبد المنعم، النظرية العامة لقانون العقوبات–دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003 ، ص 477 .

وتبعا لذلك نرى بأن جريمة إفشاء أو استعمال أو حيازة توقيع الكتروني موصوف خاص بالغير، تجمع بين جرائم الخطر والضرر، لأنه يترتب على السلوك الإجرامي في فعل الاستعمال والإفشاء عدوان حال على المصلحة المحمية جنائيا بأن تم انتهاك خصوصية التوقيع الالكتروني، أما في الحيازة فهناك احتمال العدوان على المصلحة المحمية جنائيا، لذلك حيازة توقيع الكتروني تصنف ضمن جرائم الخطر، أما إفشاء أو استعمال التوقيع الالكتروني فهي من جرائم الضرر .

3. العلاقة السببية

يجب توافر صلة السببية بين السلوك و النتيجة، فإذا أمكن رد هذه النتيجة إلى عامل آخر غير السلوك الإجرامي تنقطع صلة السببية وتنتفي المسؤولية الجنائية، وهذا أمر منطقي إذ الشخص لا يتحمل التبعية القانونية لما اقترفه من فعل إلا إذا كان فعله وحده هو سبب حصول النتيجة المحظورة قانونا وليس من العدل مساءلة الشخص إذا كانت النتائج المحظورة ثمرة عامل أو عوامل أخرى بخلاف فعله [1]، لذلك لابد من علاقة سببية بين أفعال الحيازة والإفشاء والاستعمال التي تضمنتها المادة 68 من قانون التوقيع الالكتروني والنتائج الإجرامية الغير مشروعة من جراء هذه الأفعال، فإذا أثبت الفاعل بأن النتائج الإجرامية التي نالت بالعدوان على التوقيع كانت وراءها عامل أو عوامل أخرى لم يكن سببها تنتفي معه رابطة السببية، ولا يسأل جنائيا.

ب. الركن المعنوي

كل الجرائم تتطلب ركنا معنويا وبفضله ينسب الفعل الإجرامي إلى مرتكبه [2]، فهو العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني [3]، وجوهر الركن المعنوي القصد الجنائي في

---

[1]– سليمان عبد المنعم، النظرية العامة لقانون العقوبات، المرجع السابق، ص 478 .

[2] - Bernard bouloc,haritini mastopolou, op-cit , p 101 .

[3]– محمود نجيب حسني ، النظرية العامة للقصد الجنائي– دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، ط3 ، دار النهضة العربية، القاهرة، 1988 ، ص 10 .

الجرائم العمدية الذي هو علم بعناصر الجريمة، وإرادة متجهة إلى تحقيق هذه العناصر وقبولها[1]، لذلك سنتناول بالدراسة عناصر القصد الجنائي العام التي تقوم عليه جريمة إفشاء أو حيازة أو استعمال توقيع الكتروني موصوف خاص بالغير المتمثل في العلم و الإرادة.

1. العلم

القصد الجنائي يتطلب شمول العلم موضوع الحق المعتدى عليه بارتكاب الجريمة، فيجب أن يعلم الجاني بوجود الشيء الذي يقع عليه فعله وتتحقق فيه النتيجة التي يعاقب القانون عليها، ويتطلب القصد الجنائي أن يحيط العلم بعناصر الركن المادي، وإذا تطلبت بعض الجرائم أركانا إضافية كارتكاب الفعل الذي تقوم به في مكان أو زمان معين أو تتوافر صفة خاصة في المجني عليه أو الجاني، تعين أن محيط العلم بالوقائع التي تفترضها هذه الأركان، ولا تقتصر فكرة القصد الجنائي على العلم بالوقائع فقط، بل تتطلب العلم باكتساب بعض هذه الوقائع تكييفا معينا[2]، وعلم الجاني بموضوع الحق المعتدى عليه ليس الحماية المادية له وإنما الحماية القانونية والمصلحة محل الحماية، فعلم الجاني يتطلب في جريمة إفشاء أو حيازة أو استعمال توقيع الكتروني موصوف خاص بالغير المنصوص عليها في المادة 68 من قانون التوقيع الالكتروني بأن ينال بالاعتداء على حق خصوصية التوقيع الالكتروني، مع توقعه بالنتائج الإجرامية التي تصل إلى أفعال الحيازة أو الإفشاء أو الاستعمال، وعلم الجاني أيضا بأنه يحمل صفة موظف أو عامل بجهات التصديق الالكتروني إذا كان الجاني من مؤدي خدمات التصديق الالكتروني، فإذا انتفت لدى الجاني أحد هذه العناصر انتفى معه القصد الجنائي.

---

[1]– محمود نجيب حسني ، النظرية العامة للقصد الجنائي المرجع السابق، ص 43 .

[2]– المرجع نفسه، ص 51.

2.الإرادة

الإرادة قوة نفسية متحركة اتجاه واقعة إجرامية مخالفة للقانون وخطيئة جديرة بلوم الشارع، والإرادة حين تتجه إلى الفعل فهي تتجه إلى إقامة الرابطة الوثيقة بينه وبين هذه الآثار لإحداث النتيجة الإجرامية، بمعنى أن الإرادة تستمد صفتها من اتجاهها إلى ماديات الجريمة [1]، فبعدما تطرقنا إلى العلم بجميع عناصر الركن المادي لجريمة إفشاء أو حيازة أو استعمال توقيع الكتروني موصوف خاص بالغير، فلابد لاكتمال القصد الجنائي العام ألا يعلم الجاني بهذه العناصر المادية فقط ، وإنما لابد أن تتجه إرادته إلى إحداث هذه الماديات .

ثانيا: العقوبة

مثل لا جريمة إلا بنص فلا عقوبة أيضا إلا بنص، فشرعية الجرائم تتضمن وتستلزم شرعية العقوبات التي نصت عليها المادة 111 الفقرة 3 من قانون العقوبات الفرنسي الجديد، والمقابلة لنص المادة 01 من قانون العقوبات الجزائري[2]، والجوهر الأساس للتدابير الجنائية هي العقوبة[3]، لذلك سنتطرق إلى العقوبات الأصلية لجريمة إفشاء أو حيازة بيانات توقيع الكتروني موصوف خاص بالغير ، وإمكانية تطبيق عقوبة العمل من أجل النفع العام.

أ. العقوبات الأصلية

وتتفرع إلى العقوبات المطبقة على الشخص الطبيعي والمعنوي.

1.عقوبة الشخص الطبيعي

تعاقب المادة 68 من قانون التوقيع الالكتروني 15- 04 بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمسة ملايين أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.

---

[1]– محمود نجيب حسني، قانون العقوبات– القسم العام، المرجع السابق، ص 689 .

[2] - Georges vermelle , op-cit , p110.

[3] -Jean larguier, droit pénal général et procédure pénal, Dalloz, paris, 1977 , P50 .

وللقاضي السلطة التقديرية في تقدير العقوبة المناسبة للجاني، تتراوح بين حد أدنى وحد أقصى للحبس والغرامة المقررين في المادة 68 من قانون التوقيع الالكتروني، كما للقاضي أيضا السلطة التقديرية في الاختيار مابين عقوبة الحبس أو الغرامة.

2.عقوبة الشخص المعنوي

لقد أدرج المشرع الجزائري المسؤولية الجزائية للشخص المعنوي في تعديل قانون العقوبات 04-15 المؤرخ في 10-11-2004 في المادة 51 مكرر، التي نصت على "أن يكون الشخص المعنوي مسئولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين ".

والمسؤولية الجنائية للأشخاص المعنوية لم تكن مكرسة إلا في الدول الأنجلوساكسونية كالولايات المتحدة الأمريكية وكندا، ولم تعرفها الكثير من الدول إلا حديثا، مثال بلجيكا سنة 1999، فلندا سنة 1995، اسبانيا و فرنسا سنة 1994[1]، لأن الأصل في المسؤولية الجزائية أنها شخصية، فمن يرتكب جريمة هو المسئول جزائيا عنها [2].

ومن أنواع العقوبات التي تطبق على الشخص المعنوي التي حددها المشرع في نص المادة 18 من قانون العقوبات[3]، هي الغرامة التي تعاقب بها المادة 75 من قانون التوقيع والتصديق

---

(1) - Jean pradel, la mondialisation du droit pénal, revue juridique Thémis , édition Thémis, faculté de droit université de Montréal, -p250

(2) - Jean paul antona, Philippe colin, François lenglart, la responsabilité pénal des cadres et des dirigeants dans le monde des affaire, dalloz paris, 1996 , p10.

*العقوبات المطبقة على الشخص المعنوي حددها المشرع على سبيل الحصر في المادة 18 من قانون العقوبات وهي: – الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

– واحدة أو أكثر من العقوبات الآتية:

– حل الشخص المعنوي .

– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات .

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات .=

الالكترونيين الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في الفصل الثاني من الباب الرابع، من هذه الجرائم نص المادة 68 التي تجرم إفشاء أو حيازة أو استعمال بيانات توقيع الكتروني موصوف خاص بالغير، ومقدار غرامة الشخص المعنوي تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها للشخص الطبيعي، بمعنى أن المادة 75 من قانون التوقيع الالكتروني قد طبقت الحد الأقصى للغرامة المقررة في الفقرة الأولى المادة 18 من قانون العقوبات، وهي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

وبالرجوع إلى الحد الأقصى للغرامة المعاقب بها الشخص الطبيعي وفقا لنص المادة 68 من قانون التوقيع الالكتروني هي خمسة ملايين دينار جزائري، أي بمعنى الغرامة التي تطبق على الشخص المعنوي تصل إلى خمسة وعشرين مليون دينار جزائري .

وشروط تطبيق المسؤولية الجزائية للشخص المعنوي في قانون العقوبات الجزائري حددتها نص المادة 51 مكرر أو في المادة 121 من قانون العقوبات الفرنسي، والتي أوجبت أن ترتكب الجريمة لحساب الشخص المعنوي من طرف أعضائه أو ممثليه والقانون حدد مؤسسي

– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات .

– مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو ما نتج عنها .

– نشر وتعليق حكم الإدانة .=

– الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة وارتكب الجريمة بمناسبته .

ويعاقب أيضا المشرع المصري الشخص المعنوي في نص المادة 24 من القانون رقم 15 لسنة 2004 للتوقيع الالكتروني التي تنص على أن "يعاقب المسؤول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك ويكون الشخص الاعتباري مسؤولا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين به لصالح الشخص الاعتباري، المادة 24 من قانون التوقيع الالكتروني المصري. ياسر محمد الكومي، المرجع السابق، ص 200. وبالتالي فالمسؤولية الجزائية للشخص المعنوي لا تكون منفردة وإنما تكون بالتضامن مع المسؤول عن الإدارة فيما يتعلق بالتعويضات والغرامة المحكوم بها، كما نصت المادة 21 من نفس القانون على أن الجهات المرخص لها بإصدار شهادات التصديق للتوقيع الالكتروني لا يجوز لها بأي حال إفشاء سرية التوقيع الالكتروني .

الشخص المعنوي، قد يكون مجلس الإدارة، جمعية عامة، مجلس المراقبة، المسيرين، يستثنى من ذلك العمال البسطاء أو الأجراء لدى الشخص المعنوي[1]، وتبقى مسؤولية الشخص المعنوي قائمة حتى ولو قدموا ممثليه أو أعضائه استقالتهم[2].

وهناك نوعان من المسؤولية الجزائية للشخص المعنوي مسؤولية مباشرة ومسؤولية غير مباشرة، في المسؤولية المباشرة تسند الجريمة للشخص المعنوي فترفع عليه الدعوى ويحكم عليه بالجزاءات المقررة، أما المسؤولية غير المباشرة فتكون عندما ينص القانون على أن الشخص المعنوي يسأل بالتضامن مع الشخص الطبيعي عند تنفيد الجزاءات التي يحكم بها من غرامة ومصاريف وغيرها[3]، وهذه المسؤولية الغير مباشرة نصت عليها الفقرة 02 من المادة 51 مكرر من قانون العقوبات بقولها بأن المسؤولية الجنائية للشخص المعنوي لا تمنع مسائلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال.

ب. إمكانية تطبيق عقوبة العمل من أجل النفع العام

يؤدي اختلاط المحكوم عليه بعقوبة سالبة للحرية بغيره من المجرمين إلى عواقب وخيمة، بتعرفه على المجرمين الخطرين ومعتادي الإجرام واختلاطه اليومي بهم يصبح مجالا خصبا لتبادل الخبرات الإجرامية ولاكتساب ثقافة الجريمة واقتسام الإحساس المشترك بكراهية المجتمع وتغذية مشاعر الانتقام منه، وهكذا بدلا من أن يصيح السجن دار تهذيب وإصلاح وتقويم يتحول إلى دار لتخريج مجرمين جدد بمؤهلات إجرامية أعلى وخبرات لم تكن لبعضهم من قبل وفضلا عن ذلك يساهم الاختلاط في السجون في انتشار بعض الرذائل كالشدود الجنسي وفي انتقال الأمراض المعدية كالايدز[4]، ومن بين أخطر الأمراض المعدية مرض الكورونا كوفيد 19 والذي بسببه تم الإفراج عن 5037 محبوس بموجب مرسوم عفو رئاسي صادر عن رئيس

(1) - Georges vermelle, op-cit , p100.
(2) - ibid , p 101.
(3)– محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، ج1، ط2، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1979 ص 136.
(4)– سليمان عبد المنعم ، علم الإجرام والجزاء، ط1 ، منشورات الحلبي الحقوقية، بيروت، 2005 ، ص 484 .

الجمهورية في الجزائر تفاديا لانتشار العدوى بين المساجين في أفريل 2020 [1]، ويعد العمل للمنفعة العامة من الأنظمة المطبقة في السياسات العقابية الحديثة لتجنب سلبيات الحبس القصير المدة الذي يحمل الكثير من المساوئ كما سبق بيانه، وقد سايرت الجزائر هدا التطور العقابي بإدراج العمل للنفع العام ضمن تعديل قانون العقوبات 2009، ليساهم هدا النظام في التقليل من اكتظاظ السجون واختلاط المبتدئين في الإجرام مع المجرمين الخطرين، وفي إعادة تأهيل المحكوم عليهم [2].

ولقد استحدث المشرع الجزائري عقوبة العمل من أجل النفع العام بموجب قانون 01-09 المؤرخ في 25-02-2009 المعدل والمتمم لقانون العقوبات، كعقوبة بديلة للحبس المنطوق به، تتمثل في قيام المحكوم عليه بعمل للنفع العام بدون أجر لدى شخص معنوي من القانون العام في الجرائم التي لا تتجاوز عقوبتها 3 سنوات حبسا، وبالرجوع إلى نص المادة 68 من قانون 15 – 04 التي تعاقب على إفشاء أو استعمال أو حيازة بيانات توقيع الكتروني خاصة بالغير بالحبس من سنة إلى ثلاث سنوات فإنه يمكننا القول بأنه يمكن تطبيق عقوبة العمل من أجل النفع العام في هذه الجريمة.

ولتطبيق عقوبة العمل من أجل النفع العام في جريمة إفشاء أو استعمال أو حيازة بيانات التوقيع الالكتروني لابد من مراعاة شروط تطبيقها سيما المنصوص عنها في المادة 05 مكرر01 و مكرر06، ويكمن إجمالها في شروط متعلقة بالمتهم، وشروط متعلقة بالعقوبة والمدة.

---

* ويعرف أيضا باسم المرض التنفسي الحاد المرتبط بفيروس كورونا المستجد 2019 ، وهو مرض تنفسي إنتاني حيواني المنشأ، اكتشف الفيروس في مدينة ووهان الصينية في ديسمبر 2019 وانتشر حول العالم منها الجزائر، ويمكن أن يصاب الأشخاص بعدوى مرض كوفيد 19 عن طريق الأشخاص الاخرين المصابين بالفيروس. أنظر الموقعين المطلع عليهما في 05 مارس 2020 على الساعة 13:15 https://ar.m.wikipidia.org

وموقع منظمة الصحة العالمية: https://whoint/ ar- news-room q-a-detail .

[2] – فارس خطابي، العمل من أجل النفع العام كعقوبة بديلة في التشريع الجزائري، الملتقى الوطني حول العقوبات البديلة في التشريع الجزائري، جامعة خميس مليانة، كلية الحقوق، مداخلة غير منشورة، 02 ماي 2018 .

1.الشروط المتعلقة بالمتهم

أورد قانون العقوبات الجزائري في المادة 05 مكرر 01 الشروط المطلوبة في المتهم للحكم علية بعقوبة العمل للنفع العام وتتمثل فيما يلي:

- أن لا يكون المتهم مسبوقا قضائيا.

- أن لا يقل عمره عن 16 سنة وقت ارتكاب الوقائع المجرمة.

- الموافقة الصريحة للمتهم على عقوبة العمل للنفع العام ورضاه بها، وهو ما يستلزم حضوره جلسة الحكم.

2.الشروط المتعلقة بالعقوبة والمدة

أوردت المادة 05 مكرر 01 قانون العقوبات الجزائري شروط إصدار عقوبة العمل للنفع العام وقد جاء المنشور الوزاري رقم 02 المؤرخ في 21-04-2009 بتوضيح كيفية تطبيق هذه العقوبة وشروطها بالنظر لخصوصية العمل للنفع العام كعقوبة بديلة فيجب مراعاة ما يلي:

- أن لا تتجاوز العقوبة المنطوق بها مدة سنة حبسا نافدا.

- أن لا تتجاوز عقوبة الجريمة المرتكبة ثلاث 03 سنوات حبسا.

- أن لا يطبق العمل للنفع العام إلا بعد صيرورة الحكم أو القرار نهائيا، وفقا لنص المادة 05 مكرر 06 .

أما عن المدة فقد أوجبت المادة 05 مكرر 01 مدة العمل من أجل النفع العام أن تتراوح بين أربعين ساعة وستمائة ساعة بحساب ساعتين عن كل يوم حبس في أجل أقصاه ثمانية عشر شهرا لدى شخص معنوي من القانون العام.

وإذا كان المتهم قاصر فلا بد ألا تقل مدة العمل للنفع العام عن 20 عشرين ساعة وأن لا تزيد عن ثلاثمائة 300 ساعة، بمعنى نصف العقوبة المقررة للبالغ.

الفرع الثالث: جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بمجالات أخرى

التوقيع الالكتروني يشترط في الكثير من المعاملات الالكترونية، بما فيها عمليات التجارة الالكترونية، وحتى لا يتم انتهاك سرية البيانات والمعلومات الخاصة بها، فإن تشريعات التجارة الالكترونية تحرص على تنظيم أحكام التوقيع الالكتروني، بما فيها فيها الحماية الجنائية المقررة له [1]، كجريمة إفشاء بيانات التوقيع الالكتروني في إطار التجارة الالكترونية، ولأن التوقيع الالكتروني يحمل البيانات الشخصية للموقع فإن إفشائها أيضا يشكل جريمة، لذلك سنتطرق إلى جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بالتجارة الالكترونية، والبيانات الشخصية والحياة الخاصة.

أولا: جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بالتجارة الالكترونية

جرائم التوقيع الالكتروني تقع على مضمون التجارة الالكترونية ذاتها، وليس على بياناتها ذلك أن عقد التجارة الالكترونية سواء أكان عقد بيع أو شراء أو غيره من العقود يستلزم لصحته تمام توقيع الطرفين عليه ، كما في عقود التجارة التقليدية، إلا أن التوقيع في عقود التجارة الالكترونية تتم بواسطة التوقيع الالكتروني [2]، فإذا وقع اعتداء على التوقيع الالكتروني سيؤدي إلى المساس بالتجارة الالكترونية، لذا من الواجب إضفاء حماية جزائية للتوقيع الالكتروني لأجل حماية التجارة الالكترونية من الاعتداء عليها، ومن الجرائم الواقعة على التوقيع الالكتروني في إطار التجارة الالكترونية وهي جريمة إفشاء الأسرار الالكترونية في التجارة الالكترونية، لذلك سنتطرق إلى محل الجريمة، وأركانها.

---

[1]– عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 276 .

[2]– عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية ، دار الفكر الجامعي، الإسكندرية، 2004 ، ص 294.

أ. محل الجريمة

البيانات التي تمت معالجتها الكترونيا والذي تم التعامل فيها في نطاق التجارة الالكترونية والتي يجب الحفاظ على سريتها وخصوصيتها تأمينا لممارسة العملية التجارية، ويتكفل نظام الأمن بحماية هذه البيانات وتأمين سريتها[1]، ومنها البيانات المرتبطة منطقيا بالتوقيع الالكتروني في إطار التجارة الالكترونية .

ب. أركانها

تقوم جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بالتجارة الالكترونية على ركنين مادي ومعنوي:

فيما تعلق بالركن المادي فإن الجاني يكون قد اطلع على المعلومات الالكترونية المدونة في سجل الكتروني أو مستند الكتروني أو رسالة الكترونية، وأن يكون اطلاع الجاني عليها بمناسبة ممارسة مهامه كأن يكون من مزودي خدمة الانترنيت المنوط بهم توصيل هذه الخدمة إلى العملاء، وقد يكونوا من مزودي خدمات التصديق الذي يصدرون شهادة التصديق على التوقيع الالكتروني أو صحة بيانات المتعاقد في نطاق التجارة الالكترونية، وعقب اطلاع الجاني بشكلها السابق يقوم بإفشائها ويستوي أن يتم الإفشاء عن طريق النشر في صحيفة أو إعلان في وسيلة مرئية أو إذاعية، وقد يتم كذلك الإفشاء بطريقة الكترونية[2].

أما الركن المعنوي فهي من الجرائم العمدية التي تتطلب عنصري العلم و الإرادة، أي علم الجاني بأنه يطلع الغير على سرية البيانات المتعلقة بالتجارة الالكترونية، مع اتجاه إرادته إلى إفشائها.

ثانيا: جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بالبيانات الشخصية

---

[1] – هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000 ، ص41 .

[2] – عبد الفتاح بيومي حجازي ، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص 193 .

بإعتبار التوقيع الالكتروني هو ملف رقمي يصدر عن إحدى الجهات المتخصصة والمستقلة والمعترف بها من قبل الدولة، وهذا الملف يحتوي على الاسم الشخصي والبيانات الهامة لهوية الموقع [1]، فتكون البيانات الشخصية التي يحويها التوقيع الالكتروني محلا للإفشاء واطلاع الغير عليها، فما علاقة البيانات الشخصية بجريمة إفشاء الأسرار التقليدية، وجريمة إفشاء الأسرار المعالجة آليا ؟، هذا ما يقودنا إلى تبيان التفرقة بين البيانات الشخصية المشمولة بالحماية الجنائية للأسرار، ثم التمييز بين جريمة إفشاء البيانات الشخصية المعالجة آليا عن جريمة الإفشاء التقليدية، وعن جريمة إفشاء البيانات الشخصية للتوقيع الالكتروني.

أ. التفرقة بين البيانات الشخصية المشمولة بالحماية الجزائية للأسرار

يفرق الأستاذ Sieber في هذا الخصوص بين نوعين من البيانات الشخصية:

1.البيانات الشخصية المشمولة بالحماية الجزائية التقليدية للأسرار

هذا النوع من البيانات لا يثير أدنى شك في عدم مشروعية الإفشاء بها طالما سارت عليها النصوص الجزائية التقليدية الخاصة بحماية لأسرار خاصة في مجالات الطب والأعمال المصرفية، والبيانات الشخصية المخزونة في الحاسبات الآلية للبنوك هي الأكثر تعرضا للإفشاء[2]، والتي جرمها المشرع الجزائري في نص المادة 301 من قانون العقوبات التي أوجبت على الأطباء والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى لهم بها وأفشوها في غير الحالات التي أوجب عليهم القانون إفشاؤها ويصرح لهم بذلك، ولكن فيما تعلق بإفشاء بيانات التوقيع الالكتروني قد حماها المشرع الجزائري نظرا لأهميتها وخصوصيتها بنص خاص في المادة 68 بعدم إفشائها للغير، دون تطبيق الحماية الجزائية التقليدية للأسرار التي يعاقب عليها المشرع بنص المادة 301 من قانون العقوبات الجزائري .

---

[1]– عبد الفتاح بيومي حجازي ، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص 193 . ص 294 .

[2]– نائلة قورة، المرجع السابق، ص 237 .

2.البيانات الشخصية غير السرية

إفشاء البيانات الشخصية غير السرية التي تتمتع بالحماية القانونية من الصعوبة تحديد الضرر الذي قد يصيب المجتمع بسبب إفشاؤها، وأيضا في مشروعية أو عدم مشروعية إفشائها[1]، وبالنسبة لبيانات التوقيع الإلكتروني فإنها من البيانات السرية ويكون إفشاؤها يتسم بعدم المشروعية.

ب. تمييز جريمة إفشاء البيانات الشخصية المعالجة آليا عن جريمة الإفشاء التقليدية

المشرع الجزائري أخضع جريمة إفشاء البيانات الشخصية المعالجة آليا للحماية الجنائية للأسرار المنصوص عليها في المادة 301 من قانون العقوبات، وذلك حسب ما نصت عليه المادة 62 من القانون 18 – 07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أما المشرع الفرنسي فقد نص في المادة 226 من قانون العقوبات الفرنسي الجديد بتجريم كل فعل يرتكبه شخص قام بالكشف عن بيانات اسمية بمناسبة تسجيل أو فهرسة أو أي نقد أو أي شكل من أشكال معالجة البيانات الاسمية والتي يترتب على كشفها الاعتداء على اعتبار صاحب الشأن أو حرمة حياته الخاصة عن هذه المعلومات دون التصريح بذلك من صاحب الشأن للغير الذي لا توجد له أي صفة في تلقي هذه المعلومات، ولا تحرك الدعوى العمومية إلا من قبل صاحب الشأن وممثله القانوني، وهذه الجريمة تقترب من جريمة إفشاء الأسرار التقليدية ومع ذلك يوجد اختلاف بينهما حيث أن كشف البيانات الاسمية قد ينطوي على إفشاء الأسرار، وقد ينطوي على الكشف على بيانات لا تعد من الأسرار، وبالتالي تعد هذه الجريمة أوسع نطاقا من جريمة إفشاء الأسرار التقليدية[2]، ويشترط لتحقق الجريمة أن يكون من شأنها أن تضر

(1) – نائلة قورة، المرجع السابق، ص 238.

(2) – مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 104.

بالمجني عليه وحصر المشرع الضرر بالشرف والاعتبار وحرمة الحياة الخاصة، وأن يكون الإفصاح أيضا لشخص لا صفة له في تلقى هذه المعلومات[1].

ج. تمييز جريمة إفشاء البيانات الشخصية المعالجة آليا عن جريمة إفشاء بيانات التوقيع الالكتروني

جريمة الاعتداء على البيانات الشخصية تشترك مع جريمة الاعتداء على التوقيع الالكتروني من حيث المحل الذي تقع عليه الجريمة وهي البيانات الشخصية في كلتا الجريمتين، وأما ما يختلفان عن بعضهما البعض هو أن جريمة الاعتداء على البيانات الشخصية قد لا تكون موقعة من صاحبها أما في جرائم التوقيع الالكتروني فتكون موقعة.

ويختلفان أيضا في موضع الحماية الجزائية، فجريمة إفشاء البيانات الشخصية تخضع للحماية الجزائية للأسرار المنصوص عليها في المادة 301 من قانون العقوبات حسب ما نصت عليه المادة 62 من القانون 18 – 07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أما جريمة إفشاء بيانات التوقيع الالكتروني فموضع تجريمها في المادة 68 من قانون التوقيع والتصديق الالكترونيين 15 – 04.

ثالثا: جريمة إفشاء بيانات التوقيع الالكتروني المرتبطة بالحياة الخاصة

ضمانة حماية الحريات الفردية للأشخاص لا تعني فقط معالجة الوضع في الحبس المؤقت والعقوبات السالبة للحرية، وإنما تعني أيضا حماية الحياة الخاصة للأفراد، إذ لكل شخص الحق في حرمة حياته الخاصة [2]، وبيانات التوقيع الالكتروني في حالة إفشائها أو نشرها فإن ذلك يشكل مساسا بالحياة الخاصة للأفراد، كما يشمل أيضا هذا المساس بالحياة الخاصة الاستعمال

(1) – مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 105.

[2]- Michele laure rassat , op –cit, -p311.

غير المشروع لبيانات التوقيع الالكتروني، و التعديل غير المشروع لبيانات التوقيع الالكتروني، والجمع والتخزين غير المشروعان للبيانات الشخصية[1].

إلا أن الخصوصية تقترب من السر ولكنها لا ترادفه إذ أن السر يفترض الكتمان التام، أما الخصوصية فقد تتوافر بالرغم من عدم وجود السرية، والسر يقتضي قدرا من الكتمان أكثر مما تقتضيه الخصوصية فما يعتبر سرا يدخل في الغالب في نطاق الخصوصية، وما هو خصوصي قد لا يكون سريا بمعنى الكلمة إذ أن هذا لا ينفي أن السرية تعد طابعا مميزا للحق في الخصوصية لأنها تتطلب قدرا من الخفاء لذلك فالسر هو جوهر الحياة الخاصة، فالهدف من الحفاظ على الأسرار هو حماية حق الخصوصية[2] .

وجريمة الاعتداء على الحياة نص عليها المشرع في نص المادة 303 مكرر من قانون العقوبات التي تنص بأن "يعاقب كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك ب :

– إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه .

– إلتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه ".

وما يمكننا أن نستشفه من نص المادة 303 مكرر من قانون العقوبات التي تجرم الحياة الخاصة بأن حصرت الحماية الجزائية للحياة الخاصة للأفراد على المكالمات والأحاديث في الفقرة الأولى وعلى الصور في الفقرة الثانية، من دون ذكر حماية للبيانات أو المعطيات الالكترونية، ما يجعلنا نخلص إلا أن إفشاء بيانات التوقيع الالكتروني لا تعتبر من الجرائم الماسة بالحياة الخاصة في التشريع الجزائري.

[1]– نائلة قورة، المرجع السابق، ص 248.

[2] – جمال صالح عبد الحليم، الحماية الجنائية للحق في الحق الخصوصية في مواجهة نظم المعلومات ، ط1 ، دار النهضة العربية، 2018 ، ص 26 .

الفرع الرابع. نماذج صور تجريم واقعة على التوقيع الالكتروني في التشريع المقارن

نظرا لاتساع مجال استعمال التوقيع الالكتروني كان لصور تجريمه الكثير من الأوصاف الإجرامية لم يتطرق إليها المشرع في قانون التوقيع الالكتروني لسنة 2015، ما جعلنا نتطرق إلى بعض صور للتجريم في التشريع المقارن منها جريمة حيازة أو صنع برنامج لإعداد توقيع الكتروني، وجريمة كشف وفض مفاتيح التشفير الالكتروني.

أولا: جريمة حيازة أو صنع برنامج لإعداد توقيع الكتروني

تقوم جريمة حيازة أو صنع برنامج لإعداد توقيع الكتروني على ركنين مادي ومعنوي، الركن المادي فيها يتمثل في صناعة نظام معلوماتي أو برنامج لإعداد توقيع الكتروني أو حيازة النظام أو البرنامج المذكورين أو الحصول على أي منهما، وذلك بغرض إعداد ذلك التوقيع دون موافقة صاحبه، وهذا السلوك الإجرامي المتمثل في الاصطناع يقترب إلى فعل الاصطناع والتقليد في تزوير التوقيع الالكتروني، إلا أن الاختلاف بينهما أنه في التزوير يكون على جزء فقط من المحرر الالكتروني سواء وقع على التوقيع الالكتروني في حد ذاته أو في إحدى بياناته أما في جريمة صنع برنامج لإعداد توقيع الكتروني فإنه يكون بصنع برنامج جديد لم يكن موجود بغرض الإعداد لتوقيع الكتروني [1].

ويشترط أن ترتكب الجريمة من شخص أو جهة غير مرخص لها قانونا بإعداد توقيع الكتروني ويستوي في هذا الغرض أن يكون الجاني من الأشخاص الطبيعية أو الاعتبارية المرخص لهم بالعمل في هذا المجال أو غير المرخص لهم، طالما أنه في النهاية لا توجد موافقة لدوي الشأن من أجل استخراج هذا التوقيع الالكتروني من صاحبه، فمناط التجريم هنا أن التوقيع يتم عمله رغما عن إرادة صاحبه ولو من شخص مرخص له للعمل في هدا المجال، كما يتعين أن تكون تقنية البرنامج أو النظام المعلوماتي الذي يتم صناعته قادرا على عمل توقيع الكتروني، ولذلك لا تقوم الجريمة متى كان البرنامج أو النظام ليس له المقدرة الفنية على

[1]– عبد الفتاح بيومي حجازي ، التجارة الالكترونية في القانون النموذجي العربي ، المرجع السابق، ص 161 .

عمل توقيع الكتروني، وإنما عمل أشياء أخرى لا علاقة لها بذلك التوقيع وتنحصر هذه الأعمال في صناعة برنامج أو نظام معلوماتي، له القدرة على عمل توقيع الكتروني، وأن يكون ذلك رغما عن إرادة صاحب التوقيع، فإذا ما توافرت هذه الشروط في حق الفاعل توافر عنصر الركن المادي بغض النظر عن تمام استخراج التوقيع الالكتروني، لأن العبرة بصناعة البرنامج أو النظام المعلوماتي [1].

وفي الصورة الثانية المتمثلة في حيازة برنامج أو نظام معلوماتي لإعداد توقيع الكتروني دون موافقة صاحبه، فإن الحيازة المشروعة غير معاقب عليها طالما أن الشخص مرخص له بالحيازة من الجهة المختصة، أما إذا كانت رغما عن إرادة صاحب الشأن فهناك تقوم جريمة حيازة برنامج أو نظام معلوماتي لإعداد توقيع الكتروني، وللركن المادي أيضا صورة ثالثة وهي الحصول على نظام معلوماتي أو برنامج لإعداد توقيع الكتروني دون موافقة صاحب الشأن بمعنى أن الجاني ليس له الحق في الحصول على النظام أو البرنامج بصرف النظر عن تمام إعداد توقيع الكتروني أم لا، لأن ذلك من قبيل النتيجة الإجرامية غير المطلوبة للعقاب على الفعل لأن المشرع يعاقب على الفعل بمجرد تمام الحصول على البرنامج أو النظام المعلوماتي[2].

أما بالنسبة للركن المعنوي فإن جريمة حيازة أو صنع برنامج لإعداد توقيع الكتروني تقوم على عنصري العلم والإرادة، أي علم الجاني بأن الفعل معاقب عليه، مع اتجاه إرادته إلى ارتكاب الركن المادي للجريمة، كما تتطلب الجريمة بالإضافة إلى القصد العام، قصدا جنائيا خاصا وهو أن يكون بنية وغرض إعداد توقيع الكتروني.

---

[1]– عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون النموذجي العربي، المرجع السابق، ص 163 .

[2]– المرجع نفسه، ص ص 164 – 165 .

ثانيا: جريمة كشف وفض مفاتيح التشفير الالكتروني

تقوم جريمة فض مفاتيح التشفير على ركنين مادي ومعنوي، فالركن المادي فيها يتحقق بكشف مفاتيح الشفرة أو فض معلومات وبيانات التوقيع الالكتروني في غير الأحوال المصرح بها قانونا، عن طريق تسليم برنامج الشفرة ذاته لمن ليس له الحق في ذلك، والذي يعتبر برنامج من برامج الحماية تعتمد عليها عمليات حسابية معقدة حتى لو كان المستلم لا يستطيع فض الشفرة إلا بواسطة شخص ثالث، وعلى سبيل المثال يتم تشفير التوقيع الالكتروني بنظامين أحدهما يسمى النظام السيمتري وهو نوع من البرامج يعتمد على الرموز الهندسية المعقدة، والأخر يسمى النظام البيومتري وهو يعتمد على مواصفات شخصية تتعلق بصاحب التوقيع ذاته ولو قام الجاني بتسليم أيا من برامج فض الشفرة المذكورة لشخص لا صفة له تقوم في حقه الجريمة حتى ولو لم يستعملها الشخص المستلم، أما الصورة الثانية للركن المادي فهي فض مفاتيح التشفير عن طريق إعلانها وإذاعتها في غير الأحوال المصرح بها قانونا [1]، والباحث ليس من هذا الرأي لأن من منظورنا أنه يقصد بفض مفاتيح تشفير التوقيع الالكتروني هو فك رموزه السرية، مما ينجم عنه الكشف عن البيانات السرية لصاحب التوقيع، لأن مصطلح فض لا يعني الإيداع والإعلان، ومن جهة أخرى فقد جرم إيداع و إعلان بيانات التوقيع ضمن جريمة إفشاء بيانات التوقيع الالكتروني، ومثال عن فض مفاتيح تشفير التوقيع الالكتروني هو فك تشفير التوقيع السري في البطاقات الائتمانية.

أما بالنسبة للركن المعنوي فإن جريمة فض وكشف مفاتيح التشفير من الجرائم العمدية التي تتطلب علم الجاني بسلوك الكشف والفض لمفاتيح التوقيع الالكتروني مع اتجاه إرادته لفعل ذلك، في غير الأحوال المصرح بها قانونا، وينتفي القصد الجنائي إذا كان الجاني قد قام بفعل الكشف أو الفض في الأحوال المصرح بها قانونا.

[1]– عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون النموذجي العربي، المرجع السابق، ص 176 .

المطلب الثاني: الحماية الجزائية للتوقيع الالكتروني في مرحلة خدمات التصديق الالكتروني

الجهة المخولة قانونا للمصادقة على التوقيع الالكتروني هم مؤدي خدمات التصديق الالكتروني، والتوقيع الالكتروني كفل له القانون 15 – 04 حماية جزائية في مرحلة التصديق الالكتروني كون المصلحة المحمية في الجرائم الواقعة على التصديق الالكتروني هي في حد ذاتها حماية للتوقيع الالكتروني، لذلك سنتناول في هذا المطلب صور الحماية الجزائية للتصديق الالكتروني، نتطرق من خلاله إلى جريمة الإدلاء بقرارات كاذبة للحصول على شهادة تصديق إلكتروني، ثم إلى جريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف، ثم جريمة إفشاء بيانات التصديق الالكتروني، ثم إلى جريمة إصدار شهادة تصديق الكترونية دون ترخيص أو سحبه.

الفرع الأول: جريمة إفشاء بيانات التصديق الإلكتروني

جهة التصديق مهمتها إعطاء مصداقية لبيانات التوقيع الالكتروني، فبعدما يتم تصديقها، قد تكون بيانات التصديق الالكتروني عرضة للاعتداء بإفشائها، فقام المشرع الجزائري بتجريمها في نص المادة 70 من قانون التوقيع الالكتروني، وهذا ما يدعونا للتطرق إلى العلة من تجريم إفشاء بيانات التصديق الالكتروني، ثم أركانها، وعقوبتها.

أولا: العلة من التجريم

يهدف المشرع من خلالها حماية التوقيعات الإلكترونية من حيث الحفاظ على مضمونها وعدم استعمالها ونشرها وإيداعها بدون مبرر شرعي من قبل أحد الأمناء على التوقيع الإلكتروني بمقتضى وظيفته[1]، كما تضمنت المادة 42 من قانون التوقيع الالكتروني 15 – 04 أنه يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الالكتروني الممنوحة.

(1) – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 590.

ثانيا: أركانها

تقوم جريمة إفشاء بيانات التصديق الالكتروني على ركن مفترض متصل بصفة الجاني، مع ركن مادي ومعنوي .

أ.صفة الجاني

جريمة إفشاء بيانات التصديق الالكتروني المعاقب عليها بنص المادة 70 من قانون التوقيع والتصديق الالكترونيين 15 – 04 من الجرائم دوي الصفة التي تتطلب صفة معينة في الجاني وهي أن يكون أحد موظفي جهات التصديق الالكتروني، على عكس الإفشاء المعاقب عليه بنص المادة 68 من قانون التوقيع الالكتروني 15 – 04 فإن المشرع لم يتطلب صفة معينة في الجاني.

ب.الركن المادي

ويتم عن طريق إفشاء هذه المعلومات أو الأسرار، أي يعني إذاعتها أو نقلها وإطلاع الغير عليها وإعلانها للناس وخروجها من حيز الكتمان والسرية بعد أن كان العلم بها مقتصرا فقط على مقدمي خدمات التصديق والذين ائتمنوا عليها بحكم وظيفتهم والذين يقومون بدون علم ورضا صاحبها بإفشاء سرها، ويستوي في المعلومات التي يتم إفشاؤها أن تكون مكتوبة في أوراق أو مسجلة على دعامة إلكترونية على شريط مرن أو قرص ممغنط أو تكون مخزنة ضمن برنامج معلوماتي في جهاز حاسب آلي اطلع عليها مزود الخدمة بمناسبة معالجة هذه البيانات أو عند منح شهادة تصديق إلكتروني[1].

(1) – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص ص 551–552. وكذلك ما سبق ذكره عند تطرقنا لجريمة إفشاء بيانات التوقيع الالكتروني، وكذا إفشاء بيانات التوقيع الالكتروني في إطار التجارة الالكترونية .

ج.الركن المعنوي

من الجرائم العمدية التي تتطلب عنصري العلم و الإرادة، أي علم الجاني بأنه يطلع الغير على سرية البيانات المتعلقة بالتجارة الالكترونية مع اتجاه إرادته إلى إفشائها .

ثالثا:العقوبة

تعاقب المادة 70 من قانون التوقيع الالكتروني بالحبس من ثلاث 03 أشهر إلى سنتين 02 وبغرامة من مائتي ألف 200.000 دج إلى مليون 1000.000 دج أو بإحدى هاتين العقوبتين، كل مؤدي خدمات التصديق أخل بأحكام السرية المنصوص عليها في المادة 42 من قانون التوقيع الالكتروني .

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

الفرع الثاني: جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني

جهات التصديق الالكتروني تستقبل البيانات والإقرارات من صاحب التوقيع الالكتروني التي ممكن أن تكون غير صحيحة، ما أدى بالمشرع إلى تجريم الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق الالكتروني في نص المادة 66 من قانون التوقيع الالكتروني، لذلك سنتناول بالدراسة تعريفها والعلة من تجريمها، ثم أركانها. ثم ارتباطها بجريمة نشر البيانات الخاطئة لغرض احتيالي، ثم عقوبتها.

أولا: تعريفها

نعرفها بأنها إخبار جهة التصديق الالكتروني بمعلومات خاطئة بقصد الحصول على شهادة تصديق الكتروني.

ثانيا: العلة من التجريم

الهدف من التجريم هو حماية المتعاملين في نطاق المعاملات الإلكترونية بالبيانات وزيادة الثقة فيما بينهم والحفاظ على حقوقهم[1].

ثالثا: أركانها

تقوم على ركنين مادي ومعنوي .

أ. الركن المادي

يقوم الركن المادي فيها بفعل الإدلاء بإقرارات كاذبة لدى جهات التصديق الالكتروني، ويشترط في البيانات المدلى بها أن تكون غير صحيحة، فبغير صحتها لا تقوم جنحة الإدلاء بإقرارات كاذبة، كما أن لا يشترط بأن تكون جميع البيانات المدلى بها خاطئة فيكفي لقيام الجريمة الإدلاء بأحد البيانات الغير صحيحة فقط حتى ولو كانت البيانات الأخرى صحيحة.

وسواء أكانت هذه البيانات الخاطئة قد أدلى بها صاحبها شفاهيا أو تم تقديمها في أوراق مكتوبة أو في دعامة إلكترونية تتضمن بيانات خاطئة، إذ أن نص المادة 66 لم يتضمن طريقة الإدلاء بالبيانات الخاطئة.

على أن يتم الإدلاء بهذه البيانات وجوبا إلى جهة تصديق الكتروني حاصلة على رخصة لممارسة وظيفة تصديق التوقيع الالكتروني.

وعدم صحة البيانات المدلى بها قانونا هي أحد العناصر القانونية لجريمة الإدلاء بإقرارات كاذبة، تفصل فيها المحكمة التي تنظر في الخصومة الجزائية لجريمة الإدلاء بإقرارات كاذبة، وبما أن تكييفها القانوني وهو جنحة، فالمحكمة المختصة هي محكمة الجنح.

(1) – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 496.

ب. الركن المعنوي

الركن المعنوي فيها يتطلب قصدا جنائيا عاما، يتحقق بعلم الجاني وأنه يدلي بإقرارات كاذبة للحصول على شهادة تصديق الكتروني، وأن تنصرف إرادته إلى ارتكاب الركن المادي في الجريمة.

كما أنها تتطلب إلى جانب القصد الجنائي العام، قصدا جنائيا خاصا يتعين توافره لدى الجاني، وهو أن تتجه نيته إلى الحصول على شهادة تصديق الكتروني.

رابعا: ارتباط جريمة الإدلاء بإقرارات كاذبة بجريمة نشر هذه البيانات لغرض احتيالي

من الجرائم التي ترتبط بجنحة الإدلاء بإقرارات كاذبة للحصول على شهادة التصديق الإلكتروني المنصوص عليها في المادة 66 من قانون التوقيع الالكتروني 15-04 [1]، هي جريمة نشر هذه البيانات الغير صحيحة بغرض احتيالي أو غرض غير مشروع، وجرمتها بعض التشريعات بنص خاص كالتشريع البحريني والإماراتي في نص المادة 29 والتي تجرم إفشاء أو نشر شهادة بيانات غير صحيحة لغرض احتيالي أو غرض غير مشروع.

ويتحقق الركن المادي فيها بنشر شهادة التصديق الإلكتروني المتعارضة مع الحقيقة ويستوي في النشر أن الجاني الذي أنشأها بنفسه أو شخص آخر غيره[2].

ومحل الجريمة هو أن تكون بيانات خاطئة ناتجة عن إقرارات كاذبة، فالفرق بين جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني وجريمة نشرها هو أن الإدلاء يكون دائما من الشخص الطبيعي الطالب الحصول على شهادة تصديق الكتروني، أما النشر فيمكن أن يرتكب من الشخص الطبيعي العادي أو من مقدمي خدمات التصديق الإلكتروني.

(1) – المادة 66 من قانون التوقيع والتصديق الالكترونيين 15-04 .

(2) – ياسر محمد الكومي، المرجع السابق ، ص 44.

خامسا: عقوبتها

الحبس من ثلاثة 03 أشهر إلى ثلاث 03 سنوات وبغرامة من عشرين ألف دينار 20.000 دج إلى مائتي ألف دينار 200.000 دج أو بإحدى هاتين العقوبتين فقط كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة وفقا للمادة 66 من قانون التوقيع الالكتروني.

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

الفرع الثالث: جريمة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها

حماية لخصوصية المعلومات في الحالات التي يجوز فيها جمعها ومعالجتها دفع النظم القانونية المختلفة إلى وضع مجموعة من القواعد الشكلية لتنظيم وجمع المعلومات ذات الطابع الشخصي كالحصول على ترخيص يسمح بجمعها[1]، والاستعمال غير المشروع للبيانات الشخصية من الأفعال التي تنطوي على المساس بالحقوق الجوهرية للحياة الخاصة وهو ما يشكل جريمة في عدد قليل من التشريعات[2]، ومن هذه البلدان القليلة جرم المشرع الجزائري

* جمع بيانات التوقيع الإلكتروني من مؤدي خدمات التصديق تتطلب ترخيص.

ومن أشهر القضايا التي انطوت على مخالفة القواعد الشكلية لانتهاك المعالجة الآلية للمعلومات الشخصية تلك المتعلقة بإحدى شركات التأمين الفرنسية بالاشتراك مع بعض العاملين في شركة كهرباء فرنسا « EDF » وتتلخص وقائعها استلام عدد من الأشخاص كانوا قد انتقلوا إلى منازلهم للسكن في منازل جديدة خطابات وبعد تحري هؤلاء الأشخاص عن المصدر الذي توصلت به شركة التأمين من خلاله إلى البيانات الخاصة به تبين لهم وأن هذا المصدر لا بد وأن يكون شركة الكهرباء خاصة أن بعد الأخطاء الإملائية في الأسماء التي انطوت عليها العقود المبرمة بين هؤلاء وشركة الكهرباء قد ظهرت في الخطابات التي أرسلت إليهم وبناء عليه تقدموا هؤلاء الأشخاص بشكوى إلى اللجنة الوطنية للمعلومات والحريات واتي قامت بدورها للانتقال إلى شركة التأمين بالتحري تمشيا مع ما تخوله إياها المادة 21 من قانون رقم 87 –17 لسنة 1987 مما أصفر اكتشاف اللجنة أن شركة التأمين تدير أعمالها من خلال نظام معالجة آلية للمعطيات حصلت عليه من خلال شركة الكهرباء بمقابل مالي. نائلة قورة، المرجع السابق، ص 239.

(2) – نائلة قورة، المرجع نفسه، ص 240 .

الاستعمال غير المشروع للبيانات الشخصية للموقع التي ترتكب من مقدمي خدمات التصديق الإلكتروني في نص المادة 71 من قانون التوقيع الالكتروني 15-04.

وبإعتبار التوقيع الالكتروني عبارة عن ملف رقمي يحمل العديد من البيانات من بينها البيانات الشخصية للموقع، فأثناء عملية جمعها لمعالجتها آليا، قد تصبح عرضة لاستخدامها لغير غرضها المشروع، لذلك سنتناول بالدراسة أركانها، ثم عقوبتها.

أولا: أركانها

تتطلب الجريمة صفة معينة في مرتكبها، وشروط في محلها، ناهيك عن ركنها المادي والمعنوي.

أ. صفة الجاني ومحل الجريمة

من الجرائم ذوي الصفة التي تشترط صفة معينة في مرتكبيها، وهي أن يكون من مقدمي خدمات التصديق الإلكتروني[1].

أما فيما تعلق بمحل الجريمة فقد أوضحت المادة 03 من القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي 18-07 المقصود من المعطيات ذات الطابع الشخصي "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف بصفة مباشرة أو غير مباشرة لاسيما الرجوع إلى إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الاجتماعية" .

* وما يمكن أن يعاب على نص المادة 71 من قانون التوقيع الالكتروني 15-04 أنها تستثني الأشخاص العاديين من العقاب وتحصرها إلا في الأشخاص الطبيعية والمعنوية لمقدمي خدمات التصديق الإلكتروني.

ب.الركن المادي والمعنوي

تقوم الجريمة على ركنين مادي ومعنوي

1.الركن المادي

يقوم على فعلين أولهما وهو تجميع البيانات الشخصية للموقع، وثانيهما وهو استخدامه في غير غرضه.

- **تجميع البيانات الشخصية للموقع دون موافقة منه**

مقدم خدمات التصديق يقوم بجمع بيانات صاحب التوقيع لأجل التأكد من صحتها ومطابقتها لصاحبها تمهيدا لمنحه الملف الرقمي الشخصي له المصادق عليه، ومن البيانات الشخصية للموقع اسمه، تاريخ ميلاده، عنوانه، وغيرها، ولقيام الركن المادي حسب المادة 43 من قانون التوقيع الالكتروني فلابد من جمع البيانات الشخصية للموقع دون موافقة منه، بمعنى أن الموافقة الصريحة من صاحب التوقيع الالكتروني غير موجودة، وحتى وإن وافق صاحب التوقيع الالكتروني على جمع البيانات الشخصية، فلا يحق لجهة التصديق الالكتروني إلا جممع البيانات الشخصية الضرورية حسب المادة 43 فقرة 02 [1].

- **استخدام البيانات الشخصية في غير غرضها**

جمع بيانات التوقيع الالكتروني لوحدها لا يكفي لقيام الركن المادي، فلابد من استخدامها في غير غرضها المشروع ولم تبين المادة 43 أين يتم استخدامها وتوظيفها، لذلك إذا فيجب أن يتم استخدامها في غير غرضها المشروع، كجمع البيانات الشخصية للموقع ومنحها لغيره، كما أكدت أيضا المادة 42 من قانون المعطيات الشخصية في الفصل الثاني من الباب الخامس المتعلق بمعالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التوقيع والتصديق

* كما ألزمت أيضا المادة 26 من قانون التجارة الالكتروني المورد الالكتروني الذي يقوم بجمع المعطيات الشخصية ويشكل ملفات الزبائن والزبائن المحتملين ، ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية كما يجب الحصول على موافقة المستهلكين الالكترونيين قبل جمع البيانات .

الالكترونيين على أن يتم جمعها لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الالكتروني من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها.

بالإضافة إلى أن قانون 15-03 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 المتعلق بعصرنة العدالة قد تضمن في المادة 17[1] منه، فعل الاستعمال بطريقة غير قانونية للعناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر .

2.الركن المعنوي

تتطلب الجريمة لقيام ركنها المعنوي قصدا جنائيا عاما، أي علم الجاني بأنه يجمع البيانات الشخصية للموقع دون موافقة منه، مع اتجاه إرادته إلى ارتكاب الركن المادي للجريمة.

كما تتطلب الجريمة أيضا قصدا خاصا، والمتمثل في نية استخدام البيانات الشخصية لأغراض غير مشروعة.

ثانيا: العقوبة

تعاقب المادة 71 من قانون التوقيع الالكتروني على جمع البيانات الشخصية للموقع واستعمالها لغير غرضها وفق نص المادة 43 من قانون التوقيع الالكتروني بالحبس من ستة أشهر 06 إلى ثلاث 03 سنوات وبغرامة من مائتي ألف 200.000 دج إلى مليون 1000.000 دج، أو بإحدى هاتين العقوبتين فقط.

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

* وهذا الفعل أي الاستعمال الغير قانوني للعناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر يعتبر جريمة مستقلة بذاتها تعاقب عليها المادة 17 من قانون عصرنة العدالة لسنة 2015 التي تنص "على أن يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة تتراوح بين 100.000 إلى 500.000دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر .

الفرع الرابع: جريمة إصدار شهادة تصديق إلكتروني دون ترخيص أو سحبه

تنظيم المهن من صلاحيات السلطة العامة للدولة، ونظرا لأهمية التصديق الالكتروني في المعاملات الالكترونية فإن ممارسته يتطلب ترخيص من الجهات المعنية بمنحه، وهو ما أدى بالمشرع الجزائري إلى تجريم إصدار شهادة تصديق الكتروني دون ترخيص أو سحبه في نص المادة 72 من قانون التوقيع الالكتروني [1]، لذلك سنتطرق بدراسة العلة من التجريم، ثم أركانها، وعقوبتها.

أولا: سبب التجريم

السبب من التجريم هو الآثار الخطيرة التي تترتب على شهادة التصديق الإلكتروني في حق الغير الذي يطمئن بمضمون سلامة وصحة بيانات التوقيع الالكتروني أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها وهو ما يدفع الغير للوقوع في الخطأ وتضيع حقوقه، كما أن هذا السلوك يقضي على الثقة التي يجب توافرها في المعاملات الالكترونية فضلا عن أنه يجهض جهود الدولة نحو الاستفادة من تطبيقات التقنيات الحديثة كالتجارة الالكترونية والحكومة لالكترونية[2]، وحفاظا أيضا على الثقة التي تتمتع بها جهات التصديق الالكتروني مع المتعاملين معها.

ثانيا : أركانها

تقوم الجريمة على ركنين مادي ومعنوي.

* وتقابلها نص المادة 46 من القانون التونسي التي تنص على انه "يعاقب على كل من يمارس نشاط مزود خدمات التصديق الالكتروني بدون الحصول على ترخيص مسبق بالحبس لمدة تتراوح بين شهرين و 3 سنوات وبخطية تتراوح بين 1000 و 10000 دينار أو إحدى هاتين العقوبتين ".

[2]– عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 540.

أ.الركن المادي

الركن الذي يتحقق بمجرد التعامل في بيانات التوقيع الإلكتروني دون ترخيص من الجهة المختصة، أي بمعنى أن ينتحل صفة مزود خدمات التصديق مرخص له على غير الحقيقة ويصدر شهادات تصديق إلكتروني دون ترخيص من الجهات المعنية بمنح الترخيص لممارسة التصديق الالكتروني[1].

أما الصورة الثانية للركن المادي وهي فعل إصدار شهادة تصديق الكتروني بعد سحب الرخصة من الجهات المعينة بمنح الترخيص.

فإذا قام مزود خدمات التصديق الإلكتروني بالتعامل عن طريق منح شهادة تصديق إلكتروني دون ترخيص من الجهة المختصة، أو عن طريق سحبها منحه يكون مرتكبا لجريمة إصدار شهادة تصديق الكتروني بدون ترخيص أو سحبه المعاقب عليها بنص المادة 72 من قانون التوقيع الالكتروني، والفرق بين الصورة الأولى وهي الإصدار والثانية وهي السحب، يكمن في أن الجاني أثناء ارتكابه لفعل الإصدار يكون لم يمارس من قبل وظيفة التصديق الالكتروني، بينما في السلوك الإجرامي المتعلق بسحب رخصة التصديق إلكتروني يكون الجاني قد مارس من قيل وظيفة التصديق الالكتروني، وهناك فرق آخر وهو أن شخص الجاني قد يكون شخصا طبيعيا أو معنويا في جريمة إصدار شهادة تصديق الكتروني دون ترخيص، أما سحب رخصة شهادة التصديق الالكتروني فيكون مرتكبها شخصا معنويا لأنه يفترض بالضرورة قد مارس وظيفة التصديق الالكتروني.

ب.الركن المعنوي

جريمة عمدية تقوم على القصد الجنائي العام، فيجب أن يعلم الجاني أنه يمارس نشاطا بإصدار شهادات التصديق الالكتروني في غير الأحوال المصرح بها قانونا، أو أنه أصدر

[1]– عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، المرجع السابق، ص 540.

شهادة تصديق الكتروني بعد سحب الرخصة منه، مع اتجاه إرادته إلى ارتكاب الركن المادي المتمثل في إصدار شهادة تصديق الكتروني دون ترخيص أو بعد سحبها منه .

ثالثا :العقوبة

تعاقب المادة 72 من قانون التوقيع الالكتروني على جريمة إصدار شهادة تصديق الكتروني دون ترخيص أو سحبه بعقوبة أصلية، وعقوبة المصادرة كعقوبة تكميلية.

أ.العقوبات الأصلية

العقوبة الأصلية هي الحبس من 01 سنة إلى 03 ثلاث سنوات وبغرامة من مائتي ألف 200.000 إلى مليوني 2000.000 دج.

وللقاضي السلطة التقديرية في تقدير العقوبة المناسبة للجاني، بين حد أدنى وأقصى للعقوبة السالبة للحرية والغرامة، وله أيضا السلطة التقديرية في الاختيار بين الحبس و الغرامة .

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

ب.المصادرة كعقوبة تكملية

العقوبات التكميلية حددها المشرع في نص المادة 09 مكرر من قانون العقوبات[1]، من هذه العقوبات التكميلية حسب الفقرة 02 من المادة 72 من قانون التوقيع الالكتروني، هي عقوبة

* حددت المادة 9 العقوبة التكميلية على سبيل الحصر وهي:

- الحجز القانوني
- الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية.
- تحديد الإقامة.
- المصادرة الجزائية للأموال.
- المنع المؤقت من ممارسة مهنة أو نشاط.
- إغلاق المؤسسة.
- الإقصاء من الصفقات العمومية.=

مصادرة التجهيزات المستعملة في ارتكاب جريمة إصدار شهادة تصديق الكتروني دون ترخيص[1].

وقد عرفت المادة 15 من قانون العقوبات المصادرة بأنها "الأيلولة النهائية للدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء".

فالمصادرة إذا عقوبة مادية أو عينية من شان الحكم بها أن ينتقل إلى جانب الدولة ملكية الأشياء التي تحصلت من الجريمة أو التي استعملت أو كان من شانها أن تستعمل فيها ويترتب على ذلك أن المصادرة لا تختلط بعقوبة الغرامة، وإن اتفقا في كونهما من العقوبات المالية، فالمصادرة تتمثل في نقل ملكية شيء من المحكوم عليه إلى الدولة، بينما تتمثل الغرامة في تحميل ذمة المحكوم عليه بدين لها [2].

والمصادرة قد تكون جوازية أو وجوبية، فهل مصادرة التجهيزات المستعملة لارتكاب جريمة إصدار شهادة تصديق الكتروني دون ترخيص أو سحبه جوازيا أو وجوبيا ؟.

تجيبنا المادة 15 فقرة 02 من قانون العقوبات على هذا التساؤل التي تنص بأن تكون مصادرة الأشياء وجوبا إذا كان القانون ينص صراحة على عقوبة المصادرة، وبالرجوع إلى الفقرة 02 من المادة 72 من قانون التوقيع الالكتروني فإنها تنص صراحة على مصادرة

– الحضر من إصدار الشيكات أو استعمال بطاقات الدفع.

– تعليق أو سحب رخصة السياقة أو إلغائها مع المنع من استصدار رخصة جديدة.

– سحب جواز السفر.

– نشر أو تعليق حكم أو قرار الإدانة.

* ومن العقوبات التكملية لجريمة إصدار شهادة تصديق الكتروني دون ترخيص تضمنها المشرع المصري في نص المادة 23 من قانون التوقيع هي: نشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار وعلى شبكات المعلومات الالكترونية المفنوحة على نفقة المحكوم عليه. محمد على سويلم، الحماية الجنائية للمعاملات الالكترونية بين الجوانب الإجرائية والأحكام الموضوعية لقانون تنظيم التوقيع الالكتروني وتكنولوجيا المعلومات–دراسة مقارنة، ط1 ، دار المطبوعات الجامعية، الإسكندرية، 2018 ، ص 170 .

[2]– سليمان عبد المنعم، علم الإجرام والجزاء، المرجع السابق، ص 470 .

التجهيزات المستعملة لارتكاب جريمة إصدار شهادة تصديق الكتروني دون ترخيص أو سحبه، لذلك فالقاضي ملزم وجوبا في حالة الإدانة أن يحكم بالمصادرة.

وما يمكن أن نستشفه من المادة 72 فقرة 02 من قانون التوقيع الالكتروني والمادة 15 مكرر فقرة 01 و 02 من قانون العقوبات فإنه يجب أن تأمر المحكمة في حالة الإدانة بمصادرة التجهيزات المستعملة أو التي ستستعمل لارتكاب جريمة إصدار شهادة تصديق إلكتروني دون ترخيص أو سحبه، أو التي تحصلت منها، وكذلك الهبات والمنافع الأخرى التي استعملت لمكافأة مرتكبها، مع مراعاة حقوق الغير حسن النية.

وعلة حماية حقوق الغير حسن النية نابعة عن الطبيعة القانونية للمصادرة وكونها عقوبة ، مما ينبغي عليه أن تكون ذات صفة شخصية ، فلا تنال غير من يستحقون العقوبة من اجل الجريمة، وفي ضوء هذه العلة يراد بالغير حسن النية كل من لا يسأل جنائيا عن الجريمة أي كل من لا يعد فاعلا لها أو شريكا فيها فهو من الغير من الوجهة الجنائية للجريمة، وحسن نيته تعني أن لا تتوافر لديه قصد أو خطأ بالنسبة لها، وهو على هذا النحو لا يستحق عقوبة هذه الجريمة، ولو كانت مجرد عقوبة تكميلية، فمجرد علم شخص بان شيئه يستخدم في الجريمة لا ينفي عنه أن يكون من الغير ذي النية الحسنة طالما لم يصدر عنه ما يجعله طبقا للقانون أحد المساهمين فيها [1].

وقد استعمل المشرع لفظ حقوق في نص المادة 15 من قانون العقوبات دون تقييدها لتشمل الحقوق العينية على اختلافها التي لا تقتصر فقط على حق الملكية، ولكن لا تمتد إلى الحقوق الشخصية، وأن يكون حق الغير ثابتا على الشيء، على وقت سابق على ارتكاب الجريمة حتى يمثل وضعا قانونيا مستقرا سابقا لها، ولكن حماية القانون تمتد إلى من نشأ حقه على الشيء في الفترة المنحصرة بين ارتكاب الجريمة واتخاذ الإجراءات الجنائية في حقها إذا كان غير عالم باستعمال الشيء في الجريمة أو تحصله منها، ولا تعني حماية حقوق الغير حسن النية عدم

[1]– محمود نجيب حسني، قانون العقوبات– القسم العام، المرجع السابق، ص 967 .

جواز المصادرة إطلاقا، وإنما تعني أن ملكية الشيء الذي توافرت فيه شروط المصادرة تنتقل إلى الدولة محملة بحقوق الغير، فإذا كان المتهم شريك في ملكية الشيء حلت الدولة محل المتهم في نصيبه، وإذا كان للغير حق انتفاع على الشيء حلت الدولة محل المتهم في ملكية رقبته [1].

الفرع الخامس: جريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف

بداية نشاط ممارسة التصديق يكون عن طريق الحصول على رخصة من الجهات المعنية بمنحها، وعند التوقف عن النشاط فيجب إعلام السلطة الاقتصادية عن التوقف، الذي يرتب عن عدم إعلامها جريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف المنصوص عنها في المادة 67 من قانون التوقيع الالكتروني، لذلك سنتطرق إلى العلة من تجريمها، ثم أركانها، وعقوبتها.

أولا: علة التجريم

المساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة عن الاستخدام غير المشروع للحاسبات الآلية والشبكات المعلوماتية، وحماية الاقتصاد الوطني[2].

ثانيا : أركانها

تقوم الجريمة على ركنين مادي ومعنوي.

أ.الركن المادي

الركن المادي في الجريمة قد يكون بفعل ايجابي أي القيام بفعل، أو سلبي بالامتناع عن القيام بفعل، وغالبية الجرائم تكون بفعل ايجابي كالقتل والسرقة وغيرها، وفي حالات أخرى تأخذ الجريمة الطابع السلبي بالامتناع التي يجرمها القانون بنص خاص، كجريمة عدم التبليغ عن

[1]– محمود نجيب حسني، قانون العقوبات– القسم العام، المرجع السابق، ص ص967– 977 .

[2]– محمد علي سويلم، المرجع السابق، ص 163.

جناية[1]، وجريمة الإخلال بإخبار السلطة الاقتصادية في نص المادة 67 من قانون التوقيع الالكتروني 15 – 04، التي يتمثل الركن المادي فيها باتخاذ الجاني موقفا سلبيا بعدم إخبار السلطة الاقتصادية عن التوقف، أي عدم قيامه بما يجب أن يقوم به وهو الإخبار بالتوقف.

ويشترط لقيام جريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف أن يكون الجاني مقدم خدمات التصديق سبق له وأن مارس وظيفة التصديق الالكتروني مرخص له بذلك بطريقة قانونية، فإذا لم يكن الجاني سبق وأن مارس وظيفة التصديق برخصة قانونية ثم توقف عن النشاط، فإنه لا تقوم في حقه جريمة إخبار السلطة الاقتصادية عن التوقف، ولكن يمكن متابعته على جزائيا على أساس ارتكابه لجريمة إصدار شهادات التصديق الالكتروني دون ترخيص المعاقب عليه بنص المادة 72 من قانون التوقيع الالكتروني 15 – 04 .

كما أن السلوك الإجرامي السلبي لفعل عدم الإخبار لابد أن يكون بعد التوقف عن ممارسة خدمة التصديق الالكتروني، فلا تقوم الجريمة إذا كان التوقف جزئيا ثم بعدها سيستأنف النشاط كوجود خلل تقني مثلا بسببه يوقفه عن العمل لبضعة أيام، لذلك فالجريمة تشترط التوقف النهائي لمقدم خدمات التصديق الالكتروني.

وفيما تعلق بالآجال الواجب احترامها لإعلام السلطة الاقتصادية عن التوقف، فيجب إعلامها فورا [2]، لتقوم بإلغاء شهادة التصديق الالكتروني الموصوفة بعد تقديم الأسباب المقدمة حسب نص المواد 58 و59 من قانون التوقيع الالكتروني 15-04.

والفعل المادي لعدم الإخبار من جرائم الخطر لأنها لا تتطلب نتيجة إجرامية فمجرد الامتناع عن الإخبار بالتوقف يقوم الركن المادي، وبغض النظر عن أنه وقع ضررا للمتعاملين مع مقدم خدمات التصديق أم لا.

---

[1]- Bernard bouloc,haritini mastopolou, op-cit , p87.

* كان من الأجدر على المشرع في قانون التوقيع الالكتروني أن يحدد المدة القانونية الواجب فيها إعلام السلطة الاقتصادية عن التوقف.

ب.الركن المعنوي

جريمة عمدية تقوم على القصد الجنائي العام، فيجب أن يعلم الجاني أنه امتنع عن إخبار السلطة الاقتصادية عن التوقف، مع اتجاه إرادته إلى ارتكاب الركن المادي في الجريمة، ولا عبرة أيضا بالباعث مهما كان نبيلا على عدم إخبار وإعلام السلطة الاقتصادية عن التوقف.

ثانيا: العقوبة

يعاقب الشخص الطبيعي بالحبس من 02 شهرين إلى 01 سنة واحدة، وبغرامة من مائتي ألف 200.000 دج إلى مليون 1000.000 دج، أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بالتزام إعلام السلطة الاقتصادية عن التوقف وفقا لنص المادة 67 من قانون التوقيع الالكتروني.

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

مع إمكانية تطبيق عقوبة العمل من أجل النفع العام .

ويبقى للقاضي السلطة التقديرية في تقدير العقوبة المناسبة للجاني حسب مبدأ تفريد العقوبة، أي أن لكل مجرم تفرد له العقوبة المناسبة له.

الفرع السادس: جريمة كشف معلومات التوقيع الالكتروني أثناء التدقيق

تعاقب المادة 73 من قانون التوقيع الالكتروني كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق، لذلك سنتطرق إلى المصلحة المحمية من تجريم كشف معلومات التوقيع الالكتروني أثناء التدقيق، ثم إلى صفة الجاني، ثم أركانها، و أخيرا عقوبتها.

أولا: المصلحة المحمية

المصلحة المحمية قانونا من التجريم هو حماية السرية والخصوصية والثقة في بيانات التوقيع الالكتروني.

ثانيا: صفة الجاني

الشخص المكلف بالتدقيق وهو عادة يكون من أحد أشخاص السلطة الاقتصادية للتصديق الالكتروني لأنها هي من لها صلاحية التدقيق والرقابة لجهات التصديق الالكتروني وهو ما نستشفه من خلال نص المادتين 51 و 52 من قانون التوقيع الالكتروني.

ثالثا: أركانها

تقوم جريمة الكشف عن بيانات التوقيع الالكتروني أثناء التدقيق على ركنين مادي ومعنوي.

أ.الركن المادي

يتحقق الركن المادي فيها بكشف المكلف بالتدقيق واطلاع الغير بأي وسيلة كانت شفهيا أو كتابيا أو الكترونيا عن معلومات سرية، ولم يبين المشرع هنا طبيعة المعلومات المكشوف عنها عكس المادة 68 التي حصرتها في بيانات التوقيع الالكتروني، فقد تكون بيانات توقيع الكتروني موصوف خاصة بالغير، أو أي معلومات سرية أخرى سواء معلومات متعلقة بصاحب التوقيع الالكتروني أو الجهة مقدم خدمات التصديق الالكتروني، أو معلومات سرية خاصة بالسلطة الاقتصادية للتصديق الالكتروني.

ب.الركن المعنوي

جريمة عمدية تتطلب قصد جنائي عام وهو توافر عنصري العلم والإرادة، أي أن تتصرف إلى علم الجاني بأنه يقوم بالكشف عن بيانات سرية متعلقة بالتوقيع الالكتروني أثناء قيامه بالتدقيق، وإلى نتيجة إجرامية هي خروج بيانات التوقيع الالكتروني من دائرة السرية، مع اتجاه

إرادة الجاني إلى ارتكاب الركن المادي في الجريمة، ولا تشترط قصدا خاصا لقيام الركن المعنوي فيها فيكفى فقط كشفها بغض النظر عن القصد والباعث.

رابعا:العقوبة

يعاقب الشخص الطبيعي بالحبس من 03 أشهر إلى سنتين ، وبغرامة من 20.000 دج عشرين ألف إلى مائتي ألف 200.000 دج، أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق، وفقا لنص المادة 73 من قانون التوقيع الالكتروني.

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع الالكتروني.

مع إمكانية تطبيق عقوبة العمل من أجل النفع العام .

ويبقى للقاضي السلطة التقديرية في تقدير العقوبة المناسبة للجاني حسب مبدأ تفريد العقوبة، أي أن لكل مجرم تفرد له العقوبة المناسبة له.

الفرع السابع: جريمة استعمال شهادة التصديق الالكتروني الموصوفة بطريقة غير شرعية

استعمال شهادة التصديق الالكتروني الموصوف الخاص بالغير فعل مجرم في المادة 74 من قانون التوقيع الالكتروني، وهذا ما يدعونا للتطرق إلى أركانها، ثم عقوبتها.

أولا: أركانها

تقوم جريمة استعمال شهادة التصديق الالكتروني الموصوف الخاص بالغير على ركنين مادي ومعنوي.

أ.الركن المادي

شهادة التصديق الالكتروني تستخدم في المجالات المرخص لها قانونا باستعمالها، فإذا ما استعملت في غير هذه الحالات نكون بصدد جريمة استعمال بطريقة غير شرعية، كاستعمال شهادة تصديق الكتروني في معاملات الكترونية محظورة قانونا، كمعاملة مثلا لشراء مخدرات أو بطاقات ائتمان مزورة أو القمار عبر الانترنت.

وتعتبر هذه الجريمة من جرائم الخطر فبمجرد الاستعمال الغير الشرعي لشهادة التصديق الالكتروني تقوم الجريمة، بغض النظر عن نتيجتها الضارة أم لا.

ب.الركن المعنوي

الاستعمال الغير شرعي لشهادة التصديق الالكتروني جريمة عمدية تتطلب قصدا جنائيا عاما، والمتمثل في توافر عنصري العلم و الإرادة، أي علم الجاني بأنه استعمل شهادة تصديق الكتروني بطريقة غير شرعية، مع اتجاه إرادته إلى ارتكاب الركن المادي في الجريمة.

ولا تشترط المادة 74 من قانون التوقيع الالكتروني قصدا خاصا، أو نية خاصة بقصد الإضرار بالغير، وإن كان قد ينتج عنه من الناحية الواقعية أضرار نتيجة النشاط الإجرامي، كما لا عبرة أيضا من الباعث أو الدافع من وراء الاستعمال الغير شرعي لشهادة التصديق الالكتروني .

ثانيا: العقوبة

يعاقب الشخص الطبيعي بغرامة من ألفي دينار 2000 دج إلى مائتي ألف 200.000 دج كل شخص يستعمل شهادته للتصديق الالكتروني الموصوفة لغير الأغراض التي منحت من أجلها وفقا لنص المادة 74 من قانون التوقيع الالكتروني، وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب جنحة الاستعمال الغير الشرعي لشهادة التصديق الالكتروني الموصوفة هو شخص معنوي، وفقا لنص المادة 75 من قانون التوقيع

الالكتروني، ويبقى للقاضي السلطة التقديرية في تقدير العقوبة المناسبة للجاني حسب مبدأ تفريد العقوبة، أي أن لكل مجرم تفرد له العقوبة المناسبة له.

خلاصة الباب الأول

نخلص من دراستنا في الباب الأول للحماية الجزائية الموضوعية للتوقيع الالكتروني، أنه بالرجوع إلى النصوص التقليدية لجرائم الأموال كالسرقة والنصب وخيانة الأمانة والإتلاف نجد بأن البيانات الالكترونية للتوقيع الالكتروني قد حصل فيها اختلاف فقهي وقضائي بشأن حمايتها جزائيا، فهناك من يري بأنه لا تتمتع بالحماية الجزائية لافتقارها لطبيعتها المادية، وهناك جانب آخر يرى بأنها تقع محلا لهذه الجرائم، وهناك اتجاه آخر ينادي بتجريم خاص للجرائم المرتكبة بالوسائل الالكترونية، ومنها الاعتداء على بيانات التوقيع الالكتروني المعالجة آليا ضمن نظام معلوماتي، وهو ما انتهجه المشرع الجزائري في تعديل قانون العقوبات لسنة 2004، لتفادي هذه الاختلافات وعدم الخروج عن مبدأ الشرعية الجنائية وتفسير النصوص، كما أنه تطبق النصوص التقليدية لجرائم التزوير المنصوص عنها في قانون العقوبات الجزائري في حالة تزوير بيانات التوقيع الالكتروني في التشريع الجزائري، عكس المشرع الفرنسي الذي جرم بنص خاص التزوير المعلوماتي والالكتروني .

وأول قانون ينظم عملية التوقيع الالكتروني بما فيه حمايته الجزائية الموضوعية هو قانون التوقيع والتصديق الالكترونيين 15-04، وتشمل هذه الحماية الجزائية للتوقيع الالكتروني في المادة 68 التي تجرم أفعال الاستعمال، الحيازة، الإفشاء لبيانات التوقيع الالكتروني، ولأن التوقيع الالكتروني يتم استخدامه في العديد من المجالات كان لإفشاء بيانات التوقيع الالكتروني علاقة وارتباط بجرائم أخرى كإفشاء البيانات الشخصية المعالجة آليا، وإفشاء البيانات الالكترونية في التجارة الالكترونية، وإفشاء البيانات الالكترونية الماسة بالحياة الخاصة، كما تشمل أيضا الحماية الجزائية للتوقيع الالكتروني في مرحلة التصديق عليه أو ما يسمى بجرائم التصديق الالكتروني كجريمة استعمال شهادة التصديق الالكتروني الموصوفة بطريقة غير

شرعية، وجريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني، وجريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف، وجميع جرائم التصديق الالكتروني تعطي حماية جزائية للتوقيع الالكتروني، لأن شهادة التصديق الالكتروني هي وثيقة في شكل الكتروني تبين وتتحقق من العلاقة بين التوقيع الالكتروني والموقع، ورأينا أن كل جرائم التوقيع الالكتروني وصفها القانوني من الجنح، التي لا يكون الشروع فيها إلا بنص خاص، وهو ما لم ينص عليه المشرع في قانون التوقيع والتصديق الالكترونيين، بحيث يفلت من العقاب كل من يحاول ارتكاب جرائم التوقيع الالكتروني، كما أن عقوبة المصادرة كعقوبة تكميلية لا تطبق إلا في جريمة واحدة من دون الجرائم الأخرى وهي جريمة ممارسة نشاط التصديق الالكتروني دون ترخيص أو سحبه المعاقب عليها بنص المادة 72 من قانون التوقيع والتصديق الالكترونيين.

الباب الثاني:
الحماية الجزائية الإجرائية للتوقيع الالكتروني

الباب الثاني: الحماية الجزائية الإجرائية للتوقيع الالكتروني

كما يقول الفقيه الفرنسي قارو Garaud أن الهدف دائما من الإجراءات هو الوصول إلى الحقيقة[1]، ولا يمكننا بلوغها وفق الأحكام الموضوعية التي تبقى ساكنة إذا لم يتم تحريكها وفق أحكام إجرائية، وقد نظم المشرع الجزائري أحكام الحماية الجزائية الإجرائية للتوقيع الالكتروني في موضعين، الأول هي إجراءات التحري الخاصة في تعديل قانون الإجراءات الجزائية لسنة 2006، إذا ما كنا بصدد جريمة اعتداء على منظومة للتوقيع الالكتروني، أما الموضع الثاني هي الإجراءات الخاصة بالجرائم المرتكبة في بيئة الكترونية على التوقيع الالكتروني، وليس الواقعة على الأنظمة المعلوماتية فقط المنصوص عليها في قانون الوقاية من جرائم تكنولوجيات الإعلام والاتصال لسنة 2009.

ومما لاشك فيه أن مصير أي متابعة جزائية بجريمة ما سواء واقعة في بيئة الكترونية أم تقليدية هو الوصول إلى إدانة أو تبرئة مرتكبها قضائيا عبر مراحل إجرائية ينضمها قانون الإجراءات الجزائية والقوانين المكملة والمساعدة له، لتبدأ المرحلة الأولى بمرحلة جمع الاستدلالات أو البحث والتحري بعد وقوع الجريمة مباشرة يمارسها رجال الضبطية القضائية تحت إشراف وإدارة وكيل الجمهورية، ثم تأتي المرحلة الثانية وهي مرحلة التحقيق القضائي يختص بها قاضي التحقيق وغرفة الاتهام تتولى التنقيب والبحث والترجيح بين أدلة النفي أو الاتهام، لتأتي بعدها المرحلة الثالثة وهي المحاكمة أو مرحلة التحقيق النهائي التي يختص بها قاضي الحكم وفيها تتم محاكمة المتهم عن جريمة الاعتداء على التوقيع الالكتروني، وللإلمام بالجوانب الإجرائية الجزائية الكفيلة بحماية التوقيع الالكتروني، سنتطرق في هذا الباب بدراسة مرحلة ما قبل المحاكمة للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني في الفصل الأول، ثم مرحلة المحاكمة في الفصل الثاني.

(1) - Coralie Ambroise Castérot,la procédure pénal, 2 eme édition, gualino l'extenso, paris, 2009, p 133.

الفصل الأول: مرحلة ما قبل المحاكمة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

تعتبر مرحلة ما قبل المحاكمة الجزائية أهم مراحل الخصومة الجزائية لأن فيها تجمع الأدلة التي يتم عرضها في مرحلة المحاكمة، فبقدر ما يكون التحقيق الابتدائي ملما بحقيقة الجريمة كلما كان الحكم يعبر عن الحقيقة القضائية والقانونية، وتخضع جرائم الاعتداء على التوقيع الالكتروني للأحكام الإجرائية التقليدية المنصوص عليها في قانون الإجراءات الجزائية إذا ما ارتكبت خارج البيئة الالكترونية، لكن ووفق لما سبق بيانه في الباب الأول من أن جرائم التوقيع الالكتروني ترتكب أيضا ضمن بيئة الكترونية سترتكز دراستنا على إضفاء الخصوصية في إجراءات التحقيق الابتدائي للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، سواء في مرحلة جمع الاستدلالات أو البحث والتحري أمام الضبطية القضائية، أو أمام جهات التحقيق القضائي، لذلك سنتطرق في هذا الفصل إلى مرحلة جمع الاستدلالات للجرائم الالكترونية الواقعة على التوقيع الالكتروني في المبحث الأول، ثم نمر لمرحلة التحقيق الابتدائي القضائي في المبحث الثاني.

المبحث الأول: مرحلة البحث والتحري أو جمع الاستدلالات في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

مرحلة جمع الاستدلالات أو ما يطلق عليها أيضا مرحلة البحث والتحري تختص بها الشرطة القضائية في إطار صلاحياتهم المنصوص عليها في قانون الإجراءات الجزائية وتكتسي هذه المرحلة أهمية بالغة في الإجراءات بعد وقوع الجريمة لاتصالها المباشر وأقربها إلى ميدان ومسرح الجريمة، ولأن جرائم التوقيع الالكتروني تقع ضمن بيئة الكترونية فمرحلة البحث والتحري فيها سيكون يتميز بطبيعة خاصة تبدأ من ضبطية قضائية متخصصة في مجال الجرائم المرتكبة بالوسائل الالكترونية واختصاصاتها في مجال الضبط والتحري، وأساليب تحري

خاصة بها سنتطرق لها في المطلب الأول، ثم سنتطرق إلى الآليات والأجهزة التي تساعد الضبطية القضائية في البحث والتحري في المطلب الثاني.

المطلب الأول: إجراءات البحث و التحري للضبطية القضائية في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

الضبطية القضائية لها صلاحية البحث والتحري عن كافة الجرائم بواسطة أجهزتها، لكن طبيعة الإجرام الالكتروني وجريمة الاعتداء على التوقيع الالكتروني اتجهت غالبية التشريعات إلى منح التحري فيها إلى ضبطية مختصة في الجرائم المرتكبة بالوسائل الالكترونية وهو ما سنتطرق له في الفرع الأول، بالإضافة إلى أنه يناط بها العديد من الاختصاصات والإجراءات العادية والخاصة المسندة لها في قانون الإجراءات الجزائية والقوانين المساعدة له، التي منحها لها المشرع الإجرائي الجزائري في تعديل قانون الإجراءات الجزائية لسنة 2006، وقانون الوقاية من جرائم تكنولوجيات الإعلام و الاتصال لسنة 2009، وهو ما سنتناوله من خلال إجراءات التحري العادية والخاصة في الفرعين الثاني والثالث.

الفرع الأول: ضرورة ضبطية قضائية مختصة في الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني

إن عدم قدرة الضبطية القضائية في مجال مكافحة جرائم الحاسب سيعين مرتكبي هذه الجرائم، وقد أثبت الواقع أن هنالك جرائم متعلقة بالحاسب الآلي ارتكبت على مرأى ومسمع من رجال الأمن، خاصة في المجتمعات العربية التي نجد فيها من يعطيك بطاقته الائتمانية ويملي عليك رقمه السري لتساعده على سحب مبلغ من المال عبر جهاز الصراف الآلي[1].

كما أن الضبطية القضائية في الجرائم المرتكبة بالوسائل الالكترونية تختلف تماما عن تلك التي تقوم بالكشف عن الجرائم التقليدية لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التي يتلقاها رجال الشرطة للوصول إلى هذه المرتبة وإنما تعتمد على قوة وتكوين البناء العلمي

[1]– محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1 ، دار الحامد، الأردن، 2014 ، ص 107 .

والتكنولوجي لأفرادها، وهي تتولى بذلك مهمة جمع الاستدلالات والتحري في العالم الافتراضي من أجل كشف النقاب عن هذا النوع المتميز من الإجرام كما يمكنها أن تطارد الهكرة ومخترقي الأنظمة على كافة المستويات[1]، سواء قبل ارتكاب الجريمة كما في حالة التبليغ عنها قبل وقوعها أو بعدها، هذا ما يجعل لأكثر من ضرورة لضبطية قضائية مختصة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني بصفة خاصة، لذلك سنتطرق إلى صعوبات الضبطية القضائية المختصة في الجرائم المرتكبة بالوسائل الالكترونية، وبعض من نماذجها في كلا من الجزائر، والولايات المتحدة الأمريكية.

أولا: صعوبات الضبطية القضائية في الجرائم المرتكبة بوسائل الكترونية على التوقيع الالكتروني

لقد بدأت بعض الأجهزة الأمنية والقضائية في استيعاب المختصين في الحاسب الآلي ضمن أجهزتها، كما يجري تدريب رجال الشرطة على استخدام الحاسب الآلي، إلا أن كل ذلك لم يجعل في القريب العاجل تلك الأجهزة قادرة على مواكبة التطور السريع في مجال الحاسب الآلي للأسباب التالية:

– الميزانيات المرصودة للجانب البشري في الأجهزة الحكومية لا تكفي لاستقطاب النخبة المتميزة في مجال الحاسب الآلي والذين تستقطبهم عادة شركات ومؤسسات القطاع الخاص.

– أجهزة الشرطة لها مجالات متنوعة ينبغي تغطيتها بالدعم والعناية وهي ليست متفرغة لجرائم الحاسب الآلي وحده مما يؤثر على قدرة تلك الأجهزة في المواكبة.

– حداثة تجربة أجهزة الشرطة والنيابة بجرائم الحاسب وقلة الجرائم المكتشفة لم تسمح لتلك الأجهزة لاكتساب الخبرة الكافية للعمل في هذا المجال.

---

[1] – نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات– دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013 ، ص100 .

– انتشار الحاسب الآلي على نطاق واسع وتنوع أنظمته وبرامجه يجعل من الصعب حصر أساليب الجريمة وصورها وأنماطها وبالتالي يتعذر تدريب المحققين على مواجهة حالات محددة[1].

وإزاء هذه الصعوبات هناك من يرى منح صفة الضبطية القضائية لأولئك العاملين في مجال المعلومات الأمنية سواء كانوا من أفراد الشرطة أو في القطاعات ذات العلاقة بجهاز الحاسب الآلي سواء كانوا مفتشين أو خبراء وذلك حتى يتمكنوا من ضبط الجرائم المرتكبة بالوسائل الإلكترونية، سيما أن قانون الإجراءات الجزائية في بعض الدول تخول صفة الضبط القضائي لبعض الموظفين بالنسبة للجرائم التي تدخل في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم [2]، والباحث ليس من هذا الرأي لسببين، الأول يتمثل في منح صفة الضبطية القضائية للعاملين في مجال المعلوماتية فيه مساس بخصوصيات الأفراد وحرياتهم لأنها تكون غير مراقبة قضائيا كأعمال السلطة القضائية، ومن جهة ثانية إن المشرع الإجرائي في قانون الإجراءات الجزائية لما منح صفة الضبطية القضائية لبعض الموظفين كانت في مجالات محددة ومضبوطة على عكس الجرائم باستعمال الوسائل الالكترونية التي تتسم بتعقدها وكثرتها، لذا نرى أنه من الأفضل العمل على تطوير ضبطية قضائية مختصة في مجال الإجرام الإلكتروني.

ثانيا: بعض نماذج الدول عن الضبطية المختصة بالجرائم المرتكبة بالوسائل الالكترونية

تتجه غالبية الدول إلى منح اختصاص البحث في الجرائم المرتكبة بوسائل الكترونية، إلى ضبطية مختصة بذلك، لطبيعة الإجرام الالكتروني المتميز بالتعقد، وهو ما انتهجه التشريع الجزائري، وسبقه في ذلك التشريع في الولايات المتحدة الأمريكية.

---

[1] – محمد الأمين البشري، المرجع السابق، ص 161 .

[2]– عبد الفتاح بيومي حجاري، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط1، منشأة المعارف الإسكندرية، 2009 ، ص 204 .

أ. الضبطية القضائية المختصة بالجرائم المرتكبة بالوسائل الالكترونية في الجزائر

لقد ساير المشرع هذا التطور باستحداث ضبطية قضائية مختصة بمكافحة الجرائم المرتكبة بالوسائل الالكترونية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 2009، وأصبح هناك جهاز متخصص بمكافحة الجرائم المرتكبة بالوسائل الالكترونية ومنها جرائم الاعتداء على التوقيع الالكتروني، بسبب الطبيعة الخاصة لهذه الجرائم التي يكون مرتكبيها يتمتعون بقدرات ذهنية عالية ومتمكنين من المعلوماتية، ما يجعل الضبطية القضائية الغير متخصصة في هذا النوع المستحدث من الجرائم لا تستطيع مواجهته بالطرق التقليدية لوحدها كسماع الشهود والمعاينات الميدانية ورفع البصمات وغيرها، فلابد من إجراءات مستحدثة لمواجهتها تمارسها ضبطية قضائية لها القدرة على استعمالها.

ب. الضبطية القضائية في الولايات المتحدة الأمريكية

تعد الولايات المتحدة الأمريكية من أولى الدول التي واجهت الجرائم الالكترونية بإنشاء إدارة مختصة لمتابعة الجرائم الالكترونية بمكتب التحقيقات الفيدرالي وتضم مجموعة من الأشخاص المدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أدلة، ففي سنة 1991 تأسست وحدة لمكافحة جرائم الحاسوب وحقوق الملكية الفكرية التابعة لوزارة العدل الأمريكية، ثم تم تطويرها سنة 1977 لتصبح قسما لمكافحة جرائم الحاسوب، ليتم بعدها إنشاء وحدة جرائم الانترنيت تختص بالتحقيق في الجرائم المرتبطة بالتقنية العالية، وفي نوفمبر 2000 تم افتتاح المعمل الإقليمي الشرعي للحاسوب، مقره سان ديجو وهو أحد فروع المباحث الفدرالية الأمريكية ليكون هدفه مواجهة التصعيد الخطير في الجريمة الالكترونية عبر الانترنت، وذلك بتحليل وتصنيف الدليل الرقمي، ووسيلة تعاون لمختلف جهات

التحقيق القضائي التي تتعامل مع المعمل الشرعي بهدف مكافحة الجرائم المرتكبة بالوسائل الالكترونية [1].

الفرع الثاني: إجراءات التحري العادية الأولية في الجرائم الواقعة على التوقيع الالكتروني

الجرائم المرتكبة بالوسائل الالكترونية تشترك مع الجرائم التقليدية في بعض المهام والاختصاصات للضبطية القضائية في مرحلة جمع الاستدلالات مع اختلاف في أسلوب تنفيذها نذكر منها إجراء تلقى الشكاوى والبلاغات، والانتقال إلى مسرح الجريمة، وكذا الكشف عن مرتكب الجريمة الواقعة على التوقيع الالكتروني عبر الانترنت.

أولا: تلقي الشكاوى والبلاغات

منحت المادة 17 من قانون الإجراءات الجزائية للشرطة القضائية صلاحية تلقى الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية، والشكاوى والبلاغات كما هو معروف في الجرائم التقليدية يكون كتابيا أو شفهيا، غير أن في الجرائم في الوسط الالكتروني لما تتسم به من خطورة فقد أورد المشرع الجزائري و التشريعات المقارنة طرق جديدة للتبليغ أو الشكوى كالتي تتم عبر الانترنيت بالبريد الالكتروني، لذلك سنتطرق إلى مفهوم الشكوى والتبليغ، ثم سنتطرق إلى طرق الشكوى أو التبليغ في جرائم الاعتداء على التوقيع الالكتروني، ثم إلى أوجه الشبه والاختلاف بين البلاغ في الجرائم الالكترونية والتقليدية.

أ. مفهوم الشكوى والبلاغ

الشكوى هي إجراء يعبر به المجني عليه في جرائم معينة عن إرادته في رفع العقبة الإجرائية التي تحول دون ممارسة السلطات المختصة لحريتها في المطالبة بتطبيق القانون[2]، أما البلاغ

---

[1] – محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي– دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2018 ، ص138 .

[2] – محمد زكي أبو عامر، الإجراءات الجنائية– مرحلة جمع الاستدلالات–سير الدعوى الجنائية والدعوى المدنية المرتبطة بها– التحقيق والحكم والطعن في الحكم الصادر في الدعوى الجنائية ، ط1 ، منشورات الحلبي الحقوقية، لبنان، 2010 ، ص 386 .

فهو إخبار السلطات بوقوع جريمة حتى ولو كان الشخص المبلغ ليس من وقع عليه الاعتداء، والفرق بينها وبين الشكوى أن البلاغ يكون من الضحية أو الغير، في حين أن الشكوى لا تكون إلا من الضحية.

وهذا ما يجعل النيابة ليست دائما لها الحرية في تحريك الدعوى العمومية قد تكون مقيدة بشكوى من الضحية في الجرائم التي يشترط فيهم القانون الشكوى، لكن بالرجوع إلى جرائم التوقيع الالكتروني سوء الواقعة على النظام المعلوماتي للتوقيع الالكتروني، أو الجرائم المعاقب عنها في قانون التوقيع والتصديق الالكترونيين، فإنه لا يشترط فيهم شكوى مسبقة من الضحية، وهذا ما يعطي للنيابة العامة الحرية في تحريك الدعوى العمومية من دون التقيد بشكوى الضحية.

ب.أوجه التشابه والاختلاف بين البلاغ في الجرائم الالكترونية والجرائم التقليدية

يتشابه البلاغ في الجرائم الالكترونية مع نظيره في الجرائم التقليدية من حيث الهدف والمبلغ، فمن حيث الهدف نجد أن هدف كلا منهم هو اتصال علم السلطات بالجريمة، ومن حيث المبلغ يجوز لأي شخص سواء أصابه ضرر أم لا، أما عن وجه الاختلاف، فإذا كان من الممكن في الجرائم التقليدية قبول البلاغ سواء بواسطة الانترنت أو الطرق العادية لإمكان إثبات الجريمة والتوصل إلى الجاني [1].

إلا أن الأمر يبدو أكثر اختلافا في الجرائم الالكترونية التي تظل في معظم أحوالها مستترة بل قد لا يعلمها المجني عليه نفسه إلا عن طريق الصدفة، فهي ترتكب بطريقة لا يشعر بها المجني عليه، فهنا لا يتم البلاغ إلا عند اكتشافها وبعد فترة من ارتكابها، مما يعد أمر البلاغ بالنسبة لغير المجني عليه أمرا صعبا، فضلا عن أنه قد لا يلجأ إلى البلاغ لخشية اهتزاز الثقة كما لو كان المجني عليه أحد البنوك أو المؤسسات المالية الكبرى، لدى فإن نسبة البلاغ في

[1] – محمد كمال شاهين، المرجع السابق، ص 246 .

الجرائم الالكترونية أقل بكثير من الجرائم التقليدية مما يجعل هناك تفاوت بين نسبة الإجرام الحقيقي ونسبة الجرائم المبلغ عنها وهو ما يعبر عنه علماء الإجرام بالرقم الأسود[1]، والمجني عليه في الجرائم المعلوماتية لا يقوم بالإبلاغ عنها ويرجع ذلك لأسباب تتعلق بسمعة المؤسسة التي يمثلها والتي قد تتأثر إذا ما نما إلى علم المتعاملين معها تعرض المعلومات الخاصة بها إلى التلاعب[2]، لذلك ينبغي تشجيع المجني عليهم في جرائم الحاسب بصفة عامة والجرائم والتي تقع على بيانات التوقيع الالكتروني على وجه الخصوص بالإبلاغ عن هذه الجرائم مع تقرير عقوبات رادعة للأشخاص الذين يعملون على نشر هذه الجرائم بغرض هز الثقة في الجهات المجني عليها، سيما وأن من الصعوبات التي تواجه رجال الضبط القضائي والتحقيق هو عدم التبليغ [3]، كما يجب العمل على ضمان استفاء حقوق المجني عليه من دون المساس بسمعته وزبائنه، وإعطاء المؤسسات وخاصة المالية منها وسائل لتبليغ حديثة وسريعة مع الجهات الإدارية التي تتعامل مع الضبطية القضائية، كتسهيل تبليغ الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال الماسة بالتوقيع الالكتروني.

ج.طرق التبليغ والشكوى المستحدثة في الجرائم المرتكبة بالوسائل الالكترونية

التبليغ والشكوى كما هو سائد في غالبية النظم القانونية لفترة كبيرة من الزمن يكون إما كتابيا أو شفهيا، لكن التطور التكنولوجي مكن من ظهور آليات جديدة للتبليغ والشكوى عن طريق الانترنت بواسطة البريد الالكتروني للضبطية القضائية والنيابة المختصة ، وهو ما سنتطرق له من خلال طريقة التبليغ أو الشكوى في كلا من الجزائر، فرنسا، دبي.

---

[1]– محمد كمال شاهين، المرجع السابق، ص 246 .

[2]– نائلة قورة، المرجع السابق، ص 51.

[3] – عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 277 .

1. طريقة التبليغ والشكوى عن الجريمة المرتكبة بالوسائل الالكترونية في الجزائر

بعد صدور قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال لسنة 2009 تم إنشاء مصالح شرطة قضائية متخصصة في الجريمة المرتكبة بالوسائل الالكترونية، سواء على مستوى الشرطة أو الدرك الوطني، ويتم التبليغ عن طريق هاتف الشرطة رقم 1548[1] والدرك الوطني رقم هاتف 1055، أو الولوج إلى البريد الالكتروني ppng.mdn .dz لتجذ أحد الخيارين سواء شكوى مسبقة أو معلومات أي إرسال معلومات أو التبليغ عن أي جريمة مهما كان نوعها بغرض المساهمة في حفظ النظام والأمن العمومي عن طريق ملئ معلومات متعلقة بالهوية، ففي حالة الشكوى يحدد موعد للشاكي أمام الفرقة ويرسل إليه عن طريق البريد الالكتروني، وإذا لم يتقدم لتأكيد الشكوى خلال ثلاثين يوما بعد الموعد المحدد، تلغى الشكوى تلقائيا[2].

وقد سايرت وزارة العدل استخدام التكنولوجيا في تسيير قطاع العدالة وعصرنته، عبر إطلاق خدمة الأرضية الرقمية للنيابة الالكترونية e–nyaba بتاريخ 28 جويلية 2020 يستطيع من خلالها الأفراد تقديم الشكوى الكترونيا بإتباع الخطوات التالية:

1.الولوج إلى أرضية النيابة الالكترونية المخصصة لهذا الغرض والمتاحة عبر البوابة الالكترونية للوزارة .e-nyaba. mjustice

2 . النقر على خانة تسجيل شكوى .

3. ملئ استمارة تسجيل شكوى عن بعد ، بإدخال البيانات الشخصية الخاصة بهويته كاملة، وعنوان إقامته ، وكذا عنوان بريده الالكتروني ، إن وجد .

4. النقر على الزر "التالي" .

---

[1]- http://algeriepolice.dz
اطلع على الموقع في: 11 ماي 2020 على الساعة 11:15
[2]- htp ://ppgn.mdn.dz
اطلع على الموقع في: 05 سبتمبر 2020 على الساعة 13:10

5.النقر على الزر "ok "، الذي يظهر في نافدة تأكيد المعلومات المدخلة عندئذ تظهر مباشرة نافدة تبين إرسال رمز التأكيد عبر هاتفه المحمول ، وكذا عبر بريده الالكتروني .

6. فور تلقيه التأكيد المذكور، يصبح بإمكانه إدراج البيانات المتعلقة بالشكوى ، وذلك بإتباعه الآتي :

– إدراج رمز التأكيد المرسل .

– النقر على الزر "التالي" ، لإدخال البيانات الخاصة بالشكوى والمتمثلة في : إختيار الجهة القضائية الموجه إليها الشكوى، تحديد نوع الشكوى وإدخال مضمونها ، تحميل المرفقات، أي وثائق الإثبات المدعمة للشكوى إن وجدت ، وبعدها النقر على الزر" تسجيل " .

– النقر على الزر"ok" ، الذي يظهر في نافدة تأكيد المعلومات ليتم تحويل هذه الشكوى، بطريقة آلية إلى ممثل نيابة الجهة القضائية الموجه إليها الشكوى (وكيل الجمهورية بالمحكمة أو النائب العام بالمجلس القضائي) ، لاتخاذ الإجراء المناسب والتصرف فيها .

بعد ذلك تظهر للمعني نافدة تؤكد تسجيل الشكوى بنجاح ، وتبين ضرورة الاحتفاظ باسم المستخدم وكلمة المرور اللذان سيزود بها في ذاته لتمكينه من الاطلاع على مآل شكواه عن بعد .

مع الإشارة فإن إعلام المعني بمآل شكواه يتم أيضا عبر رسالة نصية قصيرة sms أو عبر بريده الالكتروني [1].

وبإطلاق خدمة تقديم الشكوى الكترونيا سيخفف من عناء تنقل المشتكين إلى مكاتب وكلاء الجمهورية، والنواب العامين، كما أنه أيضا سيقلص من جهد ووقت وكلاء الجمهورية في استقبالهم، ويخفف من الأعباء المالية لوزارة العدل من أوراق وطباعة وغيرها، وسيزيد في

[1] – دليل مستخدم خدمة النيابة الالكترونية e-nyaba، متاح للتحميل من موقع وزارة العدل: www.mjustice. Dz
اطلع على الموقع في: 10 نوفمبر 2020 على الساعة 18:30 .

سرعة الرد عن مآل شكواهم، وطرق التبليغ المستحدثة في الجزائر لا تمس جرائم محددة بعينها وإنما يجوز استخدامها على كل الأنماط الإجرامية التقليدية والمستحدثة.

2. طريقة التبليغ والشكوى عن الجريمة المرتكبة بالوسائل الالكترونية في فرنسا

يتخذ البلاغ في الجريمة المرتكبة بالوسائل الالكترونية بصور عديدة فقد يتم كتابيا أو شفويا بمعرفة المجني عليه أو غيره ممن شاهد ووقوع الجريمة أو وصل إليهم خبر وقوعها شانه في ذلك شأن البلاغ في الجرائم التقليدية، وقد يتم عن طريق الانترنيت أي ما يسمى بالبلاغ الرقمي عن طريق إرسال رسالة الكترونية إلى عنوان البريد الالكتروني للجهات المختصة بالتحري والتحقيق كالعنوان البريدي للدرك الوطني judiciair@ gendarmeriedefense.fr باعتباره الجهة المختصة بالتحري والتحقيق في الجرائم الالكترونية [1]، أو عن طريق ملئ استمارات رقمية موجودة للمواقع المخصصة لتلقى الشكاوى والبلاغات على أن يستوجب ملئها التوضيح والتدقيق في المعلومات المتحصل عليها لتسهيل عملية التأكد منها من قبل الجهات المختصة، وإلى جانب التبليغ عن طريق الانترنيت فإنه يمكن التبليغ بالطرق التقليدية إما عن طريق بلاغ مادي يتوجه به المبلغ نفسه إلى أقرب جهة مختصة للإدلاء ببلاغه كتابيا أو شفويا أو بالبريد العادي أو مكالمة هاتفية وللمبلغ في كل الحالات الحرية في الاختيار بين الإفصاح عن هويته أو إبقائها مجهولة [2].

3.طريقة التبليغ والشكوى عن الجريمة المرتكبة بالوسائل الالكترونية في دبي

يتم التبليغ عن الجريمة المرتكبة بالوسائل الالكترونية في دبي عن طريق الولوج إلى موقع شرطة دبي https:// dubaipolice@ gov. ae تجد عنوان باسم الجريمة الالكترونية، ثم بعدها تضغط على خدمات الدخول لتجيب بنعم أو لا عن السؤال التالي "هل الشكوى المقدمة تتعلق بالشبكة العكنبوتبة أو الخدمات المقدمة عبر الانترنيت (بريد الكتروني ، وسائل التواصل

---

[1] – محمد كمال شاهين، المرجع السابق، ص 246 .

[2] – نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت، المرجع السابق، ص ص 183 – 184 .

الاجتماعي، مكالمات الانترنت، الاحتيال الالكتروني، الاختراقات التقنية، الابتزاز والتهديد عن طريق الانترنيت) "، ثم بعدها الخطوة الثانية للإجابة عن سؤال الجهة المقدمة للشكوى بالضغط على خيار من هذه الخيارات: مؤسسة خاصة– دائرة حكومية محلية– هيئة اتحادية، ثم الخطوة الثالثة والتي تتمثل في ملئ البيانات الشخصية لمقدم الشكوى من بطاقة الهوية والعنوان، ورقم هاتفه أو عنوان بريده الالكتروني للتواصل معه عن فحوى الشكوى[1]، وبهذه الخطوات الثلاثة البسيطة تكون قد قدمت شكوى عن إحدى الجرائم الالكترونية.

ثانيا: الانتقال والمعاينة لمسرح الجريمة المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني

ويقصد بذلك انتقال الضبطية القضائية إلى مكان وقوع الجريمة وإثبات الحالة وضبط الأشياء المختلفة عن الجريمة أو التي استعملت في ارتكابها، وبصفة عامة كل ماله صلة بالجريمة، ويقتضي واجب إثبات الحالة أن تقوم الضبطية القضائية برصد ووصف كل ما يتعلق بمكان وقوع الجريمة وما يحيط بها وزمانها و الأشياء الناجمة عنها، والأسلحة أو الأدوات التي استخدمت في تنفيذها، والانتقال والمعاينة يشترط فيهما أن يتما في الطريق و الأماكن العامة، فلا يجوز للضبطية إجراء المعاينة في منزل مسكون إلا برضا حائزة لأن القول بهذا يجعل من المعاينة تفتيشا، والتفتيش عمل من أعمال التحقيق لا يجوز إجراؤه إلا بخصوص إذن عن سلطة التحقيق[2] .

والمعاينة إجراء يستهدف أمرين، الأول جمع الأدلة التي تخلفت من الجريمة كرفع البصمات وتحليل الدم، وحصر ما بجسم الجريمة كالجثة من أثار كآثار المقاومة والطعنات والإكراه، وبالعموم جمع ما يفيد للكشف عن الحقيقة سواء لأنه استخدم في إحداث الجريمة أو تخلف

---

[1] – https:// dubaipolice@ gov. ae

اطلع على الموقع في: 05 ماي 2020 على الساعة 18:05

[2] – سليمان عبد المنعم، أصول الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2015 ، ص 608.

عنها، أما الثاني ففرصة للمحقق ليشاهد بنفسه على الطبيعة مسرح الجريمة حتى يتمكن من تمحيص مدى صدق الأقوال التي أبديت حول كيفية وقوع الجريمة وتقدير المسافات ومدى الرؤية وغيرها من فنون التحقيق والمعاينة بهذا الشكل تتطلب سرعة الانتقال إلى مكان الجريمة قبل أن تزول معالمها أو تمتد إلى أدلتها يد العبث ، إلا أنه ليس إجراء صالح لكل الجرائم[1].

إلا أن الانتقال إلى المعاينة في الجرائم المرتكبة بالوسائل الالكترونية، يعد من الموضوعات الجديدة، ذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي وإنما عبر العالم الافتراضي، وهناك عدة طرق يستطيع بواسطتها المحقق الوصول إلى عالم الفضاء الالكتروني من خلال مكتبه بالمحكمة بالكمبيوتر الخاص بالعمل أو من مزود خدمة الانترنيت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة [2].

وهناك بعض الإجراءات يحبذ إتباعها من الضبطية القضائية قبل الانتقال لمسرح الجريمة الالكتروني تتمثل في:

– توفير معلومات مسبقة عن مكان الجريمة، نوع و عدد الأجهزة المتوقع مداهمتها و شبكاتها .

– إعداد خريطة للموقع الذي تتم الهجوم عليه وتفاصيل المبنى أو الطابق من المبنى موضوع البلاغ أو الشكوى، وتحديد مواقع الأجهزة والخزائن والملفات، ويتم ذلك عبر مصادر المعلومات السرية .

– تحديد عدد و أنواع الأجهزة المحتمل تورطها في الجريمة لتحديد إمكانات التفاعل معها نفسيا من حيث الضبط و التأمين وحفظ المعلومات backup .

– الحصول على الاحتياجات الضرورية من أجهزة و برامج صعبة و لينة للاستعانة بها في الفحص و التشغيل.

---

[1] – محمد زكي أبو عامر، المرجع السابق، ص227 .

[2] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية– دراسة مقارنة، ط1 ، دار الفكر الجامعي، الإسكندرية، 2018 ، ص 106 .

– إعداد فريق التفتيش من المتخصصين وفق قائمة تحدد الأسماء و الاختصاصات و المهام الموكلة لهم بكل دقة [1].

وعلى خلاف الجرائم التقليدية التي يوجد فيها مسرحا جرت عليه الأحداث وتركت أثارها المادية ومنه تنبثق الأدلة والذي يتيح مثل هذا المسرح للمحقق معاينة الآثار المادية التي خلفتها الجريمة والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها، بينما لا يوجد مسرح مماثل لذلك في الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، وأقرب تشبيه لمسرحها قد يكون الموقع أو المكتب الذي توجد فيه الأجهزة والأنظمة المعلوماتية التي كانت محلا للجريمة أو أدلتها، ومسرح الجريمة أثقل إلى حد كبير فرص عن الحقائق المستهدف التوصل إليها من وراء معاينته لسببين رئيسين أولهما أن الجرائم الالكترونية قلما تخلف عن ارتكابها أثارا مادية، والثانية أن عدد كبير من الأشخاص يكون قد تردد على مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا التي تنقضي عادة بين ارتكاب الجريمة واكتشافها مما يفسح المجال إلى حدوث تغيير أو إتلاف أو تلفيق أو عبث بالآثار المادية[2] ، كما أن حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة التقليدي إلى مسرح الجريمة الالكتروني ذلك أن التطبيقات والبرامج والبيانات المرقمة عنصران أساسيان يتحتم على أجهزة الشرطة والعدالة وخبراء الأدلة الجنائية جمعها واستخلاصها[3]، لأن الآثار المعلوماتية الالكترونية أو الرقمية المستخلصة من أجهزة الحاسب من الممكن أن تكون ثرية جدا فيما تحويه من معلومات، مثل المواقع، والبريد الالكتروني، والفيديو الرقمي، الصوت الرقمي، غرف الدردشة والمحادثة المخزنة في الكمبيوتر

[1]– محمد الأمين البشري، المرجع السابق، ص 112 .

[2] – هشام رستم، المرجع السابق، ص 484 .

[3] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، المرجع السابق، ص145 .

الشخصي، الصور المرئية، الدخول للخدمة والاتصال بالأنترنت أو الشبكة عن طريق مزود الخدمات، لذلك فالآثار الرقمية تشمل رؤية لمسرح الجريمة الحقيقي[1].

وهذا ما يدعو الشرطة القضائية أثناء المعاينة الأولية للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني التقيد بالإجراءات التالية :

– أثناء المعاينة يجب التحفظ على مستندات الإدخال و الإخراج الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد بها من بصمات.

– قصر مباشرة المعاينة على الذين تتوافر لديهم الكفاءة العلمية والخبرة العلمية في مجال الحاسبات والشبكات واسترجاع المعلومات، ويتلقون تدريبا كافيا للتعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم الالكترونية الواقعة على التوقيع الالكتروني [2].

كما يجب على القائم بالمعاينة تسجيل كل شيء عن الوسط الالكتروني في محضر معد لذلك باستخدام الوسائل المناسبة لذلك مثل تسجيل ملاحظات أو عمل رسومات تخطيطية للشبكات في الوسط الالكتروني أو صور تسجيلات فيديو، وتسجيل الاتصالات التي تتم من خلال المسرح أو الوسط الالكتروني والتي تصدر من وإلى أي موقع الكتروني آخر، من خلال مجموعة من الإجراءات مثل تصوير شاشة النظام الحاسوبي للكمبيوتر مثلا، وتسجيل كافة المعلومات المتاحة عليها، وتوضيح هل كانت الشاشة على صورة أم برنامج أم بريد الكتروني[3].

---

[1] – ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون ، المجلد الخامس، جامعة الإمارات العربية المتحدة، ص 2238.

[2] – هشام رستم، المرجع السابق، 487 .

[3]– David w hagy, électronique crime scène investigation a guide for first responders , national institu of justice p 7-8.

Krik paul , crime scène investigation a guide for law enfoncement , septembre 2013, p12.

نقلا عن : محمود عبد الغني جاد المولى، دور الدليل الالكتروني في الإثبات الجنائي–دراسة مقارنة، ط1 ، دار الفكر الجامعي، الإسكندرية، 2019 ص 116 .

ثالثا: الكشف عن هوية مرتكب جريمة التوقيع الالكتروني عبر الانترنت بطريق العنوان الالكتروني ip

العنوان الالكتروني internet Protocol IP هو رقم يسمح بالتعرف على الحاسب في شبكة الانترنت أو العنوان الالكتروني للحاسب المتصل بشبكة الانترنيت [1]، ومن خلاله يتم التعرف على هوية مستعمل الحاسب في ارتكاب جريمة التوقيع الالكتروني باستخدام شبكة الانترنيت .

ولكن خط الانترنيت قد يصادفه العديد من الهويات التي يمكن أن تكون محلا للتغاير بين أعضاء الانترنيت المشتركين في مزود انترنيت واحد، فعلى سبيل المثال إذا تواجد شخص على الانترنيت فإنه يملك هوية رقمية محددة حال تواجده على الشبكة، وفي هذه الحالة نكون أمام فرضيين، الأول وهو يحدث عند تواجد الشخص على الشبكة ولكن ينقطع الإرسال ثم عاد هذا الشخص من جديد إلى الاتصال بالأنترنت فسوف يكون له هوية رقمية مغايرة للأولى وتكون الهوية السابقة لغيره ويترتب على ذلك عدم إمكانية الوصول إلى صاحب الهوية بسهولة، أما الافتراض الثاني وهو إذا استمر الشخص بنفس الهوية ولكن اتصاله عبر مقاهي الانترنيت، وهنا تثور إشكالية أخرى ألا وهي أن القائمين على إدارة هذه المقاهي عدم إمساك سجلات يدون فيها أسماء المترددين على المقهى الذين استخدموا الانترنيت من خلال أجهزتهم ، كذلك عدم إثبات أرقم تلك الأجهزة وتوقيت الدخول والخروج ورقم ip الخاص بالجهاز الذي استعمله المستخدم أثناء فترة وجوده في المقهى، وبالتالي إذا تم تحديد مكان الجهاز ففى مثل هذا

(1) - Romain boss ,la lutte contre la cybercriminalité au regard de l action des états, thèse doctorat université de lorraine faculté de droit de Nancy , 2017 , p10.

الفرض فإنه يصعب تحديد شخص مرتكب الجريمة ما لم يتم إمساك مثل هذه السجلات وإحكام المراقبة عليها ومتابعتها بصفة دورية ومستمرة [1].

ويترتب على هذه الفرضيات أن ما يتم تحصيله وجمعه من تحريات ومعلومات حول مرتكب الجريمة الالكترونية الواقعة على التوقيع الالكتروني عبر الانترنت يحوله الكثير من الشكوك حول الفاعل، مما يصعب معه عمل سلطات الضبط والتحري التي تتخذ تلك المعلومات كمصادر أولية لمباشرة إجراءات أخرى تفيد التحقيق، مما يستدعى معه ضرورة تطوير الأساليب التقنية التي تعتمد عليها الضبطية القضائية المختصة بالجريمة الالكترونية [2].

وتختلف طريقة الحصول على ip تبعا لنوع الجريمة والموقع الذي تم ارتكاب الجريمة باسمه فإذا كانت الواقعة تمت بالبريد الالكتروني فهنا لا يوجد مشكلة فيتم بفحص البريد الذي تم به التهديد أي IP مرسل البريد، من خلال ما يعرف بـ : full headers للبريد الإلكتروني و بهذه الطريقة يتم معرفة ip المرسل، ويتم مخاطبة الشركة مقدمة الخدمة التي يتبعها هذا المستخدم و يتم الحصول على بيانات كاملة، أما إذا كانت الواقعة تمت على أحد المواقع وأنظمة البنوك العالمية كفيزا كارط، كحالة تزوير توقيع الكتروني لبطاقة فيزا ، فهنا يتم مخاطبة الموقع أو البنك عن طريق ملفات logfilles المتواجدة على الموقع، وأغلب المواقع المشهورة كالـ yahoo، google facebook، تطلب من جهات التحقيق ما يسمى بالإنابة القضائية الدولية لكي تسمح لها بالحصول على البيانات الخاصة بها[3]، نظرا لما تتمتع به هذه المواقع العالمية من ثقة لدى عملائها ومرتادي شبكة الانترنت وسمعتها العالمية، وتجدر الإشارة إلى أغلبية المواقع العالمية الإلكترونية يتم إدارتها من الولايات المتحدة الأمريكية لذا يصعب على جهات التحقيق من خارج الولايات المتحدة الأمريكية الحصول على معلومات وبيانات عن مرتكب الجريمة وتعقد

---

[1] – محمد كمال شاهين ، المرجع السابق، ص 104.

[2] – المرجع نفسه، ص 105 .

[3]– حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط1 ، دار النهضة العربية، القاهرة، 2017 ، ص 90.

الإجراءات التي لا تتم إلا بواسطة وزارة الخارجية الأمريكية، ومكتب المباحث الفيدرالي الأمريكي FBI.

الفرع الثالث: إجراءات التحري الخاصة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

نص قانون الإجراءات الجزائية المعدل سنة 2006 على مجموعة من إجراءات التحري الخاصة ببعض الجرائم الخطرة منها الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني، كاعتراض الاتصالات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر05 ، كما نصت أيضا في المادة 65 مكرر12 على إجراء أسلوب التسرب، ومع تطور خطورة الجرائم المرتكبة في وسط الكتروني، نص المشرع في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 على إجراء المراقبة الالكترونية كأحد أساليب البحث والتحري الخاصة، لذلك سنتطرق إلى أهم هذه الأساليب المستحدثة وهي اعتراض المراسلات السلكية و اللاسلكية، المراقبة التليفونية أو التصنت، المراقبة الالكترونية، التسرب.

أولا: اعتراض الاتصالات السلكية و اللاسلكية

هذا الإجراء نصت عليه المادة 65 مكرر05 من قانون الإجراءات الجزائية بنصها "أنه إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جريمة المساس بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية، ووضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وتسجيل الكلام، أو التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص".

واعتراض الاتصالات عرفه القانون الأمريكي بأنه اكتساب سماعي أو غيره لمحتوى أيه أي اتصالات سلكية أو الكترونية أو شفهية وذلك من خلال استماع أي جهاز سواء ا كان الجهاز آليا أو الكترونيا أو غير ذلك [1].

وتجيز بعض التشريعات كالقانون الأمريكي بوضع أجهزة لتسجيل الاتصالات الالكترونية في حالة الضرورة بدون إذن من النيابة العامة إذا توافر خطر حال على الحياة أو خطر جسيم على السلامة الجسمية للأشخاص في حالة التآمر، إذا كان ذلك يقتضي وضع أجهزة تسجيل أو تتبع الأثر قبل الحصول على الإذن اللازم لذلك، وما دام قد توافر من الأسباب ما يدعو للاعتقاد بأن هذا الإذن سوف يصدر، فإذا لم يصدر فيجوز لمزود خدمات الانترنيت أن يطلع على المواقع التي يقوم المشترك قد وافق عند اشتراكه في تلك الخدمة على وضع وسائل فنية للمتابعة تسمح بمعرفة تلك المواقع، ويعتبر ذلك أن الرضا يجيز الاطلاع على المعلومات الشخصية [2] .

وانطلاقا من أهمية حماية الحياة الخاصة نجد أن الدستور والمشرع العادي قد كفل حماية خاصة بالمراسلات السلكية واللاسلكية، وإذا كانت شبكات الحاسب الآلي تستخدم خطوط التيليفون وتستعين في ذلك بجهاز معدل الموجات والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب إلى موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط التيليفون، وبذلك فإنه يتبين وجود علاقة بين المراسلات التي تتم بطرق تقليدية وتلك التي تتم بالوسائل الإلكترونية بحيث يمكن القول أن هناك تصنتا ومراقبة إلكترونية تتم على شبكات الحاسب الآلي، ولقد أجازت بعض التشريعات هذا التصنت الإلكتروني، كالمشرع الفرنسي الذي أجاز بقانون 10 جويلية1991 الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات، وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كان

---

[1] – شيماء عبد الغني، المرجع السابق ، ص 205 .

[2] – خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الالكترونية، المرجع السابق، ص 302 .

الغرض لضبط جرائم خطيرة، ويمكن أن تتم المراقبة أيضا على التليكس والفاكس ونقل البيانات[1].

وقد تفادى التشريع الفرنسي هذا النقص بأن نصَ على حرمة المراسلات التي يتم نقلها عن طريق الهاتف أو غيره بأي وسيلة من وسائل الاتصال، وبانتهاء الحديث عن إجراءات الحصول على الأدلة من الوسائل الإلكترونية وتحديد الأدلة التي ستتحصل من هذه الطرق كالمخرجات الإلكترونية والمستندات الإلكترونية والكيانات المادية والمعنوية وأنواع الغش والتزوير والإتلاف والتلاعب الذي قد تكشف عنه هذه الطرق، فإن الباب ينفتح عن تقدير هذه الأدلة في إطار نظرية الإثبات الجنائي[2].

ثانيا: مراقبة المحادثات التليفونية

مراقبة المحادثات التليفونية أو ما يسمى بالتصنت والأشكال الأخرى للمراقبة الالكترونية رغم أنها تثير الكثير من الجدل إلا أنها مسموح بها تحت ظروف معينة في جميع الدول تقريبا، في التشريع الجزائري تجيزه نص المادة 65 من قانون الإجراءات الجزائية، وفي فرنسا مثلا يجيز قانون 10 جويلية 1991 اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات، وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وفي فنلندا يجوز للشرطة التصنت على المكالمات التليفونية الخاصة بشبكات الحاسب بمقتضى إذن يقدم على كل حالة على حدة، وفي كندا فإن القوانين العادية التي تهيمن على المراقبة الالكترونية يمكن أن تطبق على أنواع عديدة من شبكات اتصالات الحاسب الآلي، وفي أمريكا يجوز اعتراض الاتصالات الالكترونية، بما فيها شبكات الحاسب بشرط الحصول على إذن

[1]– أشرف عبد القادر قنديل، الإثبات في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2015 ، ص69 .

[2]– المرجع نفسه، ص 70 .

تفتيش صادر من القاضي، وفي اليابان أقرت محكمة مقاطعة kofu سنة 1991 في غياب وجود نصوص تشريعية شرعية التصنت على شبكات الحاسب للبحث عن الدليل [1].

وفي التشريع الفرنسي لا يجوز لضباط الشرطة القضائية أثناء التحري في التحقيق الابتدائي أو الجرائم المتلبس بها القيام بإجراء التصنت التليفوني ولو حتى بموافقة الأجهزة المسئولة عن جهاز التصنت، ولا يحق إلا للسلطة القضائية المتمثلة في قاضي التحقق أو قاضي الحريات الإذن بإجراء وضع المتهم أو المشتبه فيه تحت المراقبة التليفونية[2]، وهو نفس النهج المتبع من المشرع الجزائري إذ لا يحق إلا للسلطة القضائية الإذن به، مع اختلاف أن الإذن بإجراء التصنت التليفوني من صلاحيات وكيل الجمهورية أيضا حسب المادة 65 مكرر 05.

ولقد اختلف الفقه في تكييف إجراء المراقبة للمحادثات السلكية واللاسلكية، فذهب رأي إلى أنها تعد تفتيشا وبالتالي تخضع لقيوده، واستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف من البحث في وعاء للسر توصلا إلى السر ذاته وإزاحة ستار الكتمان عنه بغرض ضبط ما يفيد في الوصول إلى الحقيقة، ولا أهمية هنا لوجود كيان مادي للسر فيصبح أن يكون ماديا يمكن ضبطه بوضع اليد عليه استقلالا، ويمكن أن يكون معنويا يتعذر ضبطه إلا إذا اندمج في كيان مادي، فالغاية من مراقبة المحادثات التيليفونية هي البحث عن دليل معين وهي ذات الغاية من مراقبة المحادثات التيليفونية من التفتيش[3].

في حين ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة واعتبر الأول إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها وحبسها لمصلحة العدالة وأما الثانية فليس لها كيان مادي ملموس وأنها قد تؤدي إلى سماع سر للمتحدث ولكنه قولي يسمعه المتحدث ولا يلمس له كيانا، والقول بأن هذا الحديث يندمج في كيان مادي هو أسلاك التيليفون أوشريط

---

[1] – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي– دراسة مقارنة، ط2 ، دار النهضة العربية، القاهرة، 2008 ، ص 80 .

[2]- Coralie Ambroise Castérot, op- cit , p 176.

[3]– أشرف قنديل، المرجع السابق، ص 68 .

التسجيل لا يصح أن يفهم منه إلا الحديث له كيان مادي يمكن ضبطه، فأسلاك التيليفون أو التسجيل ليست هي الدليل ذاته وما هي إلا وسيلة أو أداة لسماع الحديث أو إعادته ويبقى الدليل المستمد منها حديثا غير مادي حيث لا تتأثر طبيعته بوسيلة أو أداة للحصول عليه، وهذا الرأي الأخير هو الصواب لأن المشرع الإجرائي قد أفاد أحكاما خاصة لكل من التفتيش والمراقبة على المراسلات السلكية واللاسلكية نظرا لاختلاف المحل الذي قد يقع على كل منهما، فالأخير يقع على حرمة الحياة الخاصة لمطلق القول أما الأول فقد يمس بالمصادفة هذه الحياة الخاصة حتى ولو تمَ على كيانات معنوية، لذلك نجد أن المشرع قد أحاط المراقبة بضمانات تزيد عن تلك المقررة للتفتيش، فليس معنى أنه يتصور التفتيش على كيان معنوي وأن المراقبة دائما تتم على كيانات معنوية أن نسوى بينهما من حيث تأثيرهما على حرمة الحياة الخاصة والذي لا شك فيه أن المراقبة تكون أشد وطأة في مساسها بحرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش[1].

ثالثا: المراقبة الالكترونية

منح المشرع الإجرائي الجزائري في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الصادر سنة 2009 العديد من السلطات والصلاحيات للضبطية القضائية تحت إشراف السلطة القضائية في اختيار أسلوب إجراء التحري وبالطريقة التي يراها مناسبة لإتمام العملية بصورة إيجابية ودون المساس بحرمة الحياة الخاصة للحصول على أكبر عدد من المعلومات حول الواقعة محل المتابعة الجزائية، لذلك قد يتخذ البحث والتحري عن الجريمة المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني أسلوب المراقبة الالكترونية والتي تعتبر أحد الركائز الأساسية التي يستند عليها رجال البحث والتحري لجمع المعلومات حول الجرائم الواقعة على التوقيع الالكتروني.

[1]– أشرف قنديل ، المرجع السابق، ص 69 .

أ.تعريف المراقبة الالكترونية

يقصد بها كل عمل أمني له نظام معلوماتي إلكتروني يعتمد على التقنية الالكترونية، حيث يتولى المراقبة عن طريق الأجهزة الالكترونية وعبر شبكة الانترنت باستخدام البرمجيات الالكترونية وذلك لتحقيق غرض معين، ولكي تحقق المراقبة الالكترونية أهدافها يجب أن يتوافر أمران، الأول التعاون والتنسيق بين الشخص المناط به كشف الجريمة والبحث عنها وبين فريق المراقبة الذي يتولى التأهيل الفني للقائم بها ولفريق المراقبة [1].

ب. الجرائم التي يجوز فيها اللجوء إلى المراقبة الالكترونية

أجازت المادة 04 فقرة ب من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لسنة 2009 القيام بعمليات المراقبة الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، لذلك فإجراء المراقبة الالكترونية في جرائم التوقيع الالكتروني يتم اللجوء إليه في حالة احتمال الاعتداء على منظومة معلوماتية متعلقة بالتوقيع الالكتروني بشرط أن يكون هذا الاعتداء يهدد ويمس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، والتي تخضع للسلطة التقديرية للآمر بالإجراء.

ج.صور المراقبة الالكترونية

المراقبة الالكترونية من أجل البحث والتحري عبر الانترنت ممكن أن تتخذ صورتين، الأولى هي الإرشاد الجنائي عبر الانترنت، والصورة الثانية هي المراقبة عبر التقنيات الالكترونية الحديثة [2] .

---

[1] – محمد كمال شاهين، المرجع السابق، ص 251 .

[2]– المرجع نفسه، الصفحة نفسها .

1.نظام الإرشاد الجنائي عبر الانترنت

يعد نظام المرشد الجنائي في مجال جمع التحريات من أقدم الوسائل المستخدمة في البحث، وأكثرها فاعلية وهي محل اهتمام رجل البحث الجنائي في كافة النظم القانونية اللاتينية و الأنجلوساكسونية، ويعرف المرشد بأنه ذلك الشخص الذي يتصل بالضبطية القضائية سرا للحصول منه على معلومات معينة تفيد في منع الجريمة وكشف غموضها والوصول إلى الجناة، ويتلقى في بعض الأحيان منفعة مقابل هذه المهمات وأحيانا تدفعه الغيرة على مصلحة ما للإدلاء بهذه المعلومات[1].

كما يعد نظام الإرشاد الجنائي المتعارف عليه عند البحث في الجرائم المرتكبة في العالم المادي مختلف عما عليه الحال في العالم الافتراضي، فلا يتطلب الإرشاد الجنائي في جرائم التوقيع الالكتروني عبر الانترنت إلى الانتقال ومراقبة وتتبع المجرم أو المشتبه فيه من مكان لآخر، إذ يتم الإرشاد الجنائي عبر الانترنت عن طريق الولوج داخل صفحات الانترنت سعيا وراء الكشف عن الجريمة الواقعة على التوقيع الالكتروني عبر الانترنت ومرتكبيها، وفق آليات مختلفة والدخول إلى قاعات الدردشة أو حلقات النقاش العامة والتنكر باستخدام أسماء مستعارة وتبادل أطراف الأحاديث المختلفة مع مستخدمي الانترنت وبشكل عام الظهور بمظهر طبيعي كأنه أحد مستخدمي الشبكة، لأجل جمع المعلومات والتعرف عن مستخدمي الشبكات ذي النزعة الإجرامية، ومن ثمَ ليس للمرشد الجنائي عبر الانترنت، دفع الغير أو التحريض إلى ارتكاب جريمة عبر الانترنت [2].

ولكي يكون الإرشاد الجنائي مشروعا وقانونيا في جرائم التوقيع الالكتروني عبر الانترنت لابد من توافر مجموعة شروط يمكن إجمالها في [3] :

- يجب أن لا يكره الشخص المرشد على عملية الإرشاد.

---

[1]– حسام محمد نبيل الشنراقي، المرجع السابق، ص 381.

[2]– كمال شاهين، المرجع السابق، ص 252 .

[3]– المرجع نفسه، ص 383.

- أن يكون الإرشاد مرتبط بمنع وقوع الجريمة أو متصلة بتغطية معلومات مطلوبة من جهة إدارية أو قضائية في غير مجال الجريمة.
- أن يتيقن رجل الضبط القضائي عند حصوله على معلومات من المرشدين السريين أنهم حصلوا عليها بطرق مشروعة لعدم تعرضها للإبطال ولعدم المشروعية.
- يجب ألا ينصب الإرشاد الجنائي على التحريض على الجريمة أو استعمال الغش أو التحايل.
- أن يكون الهدف من الإرشاد هو الصالح العام ولا يخدم أي مصلحة شخصية.

2.المراقبة الالكترونية عن طريق التقنيات الالكترونية الحديثة

تتم المراقبة الالكترونية في هذه الصورة عن طريق إرسال برمجية إلى خوادم مختلفة بقصد التوصل إلى مرتكبي الجرائم المرتكبة بالوسائل الإلكترونية الواقعة على التوقيع الالكتروني، ويكون للبرمجيات دور رئيسي في إطار المراقبة أو الإرشاد الجنائي البرمجي، ويتعين التفرقة ما إذا كانت المراقبة الالكترونية بصورتيها تتم في الصفحات العامة عبر شبكات الانترنت أو تتم عبر الصفحات والمواقع الخاصة للأفراد، فإذا كانت المراقبة الالكترونية والإرشاد الجنائي يتم داخل المواقع والصفحات العامة والمتاحة للكافة، فلا يعد عمل المراقب انتهاك للحق في الخصوصية المعلوماتية للأفراد، أما إذا تم الولوج واختراق المواقع والصفحات الخاصة والتي يتطلب الاطلاع عليها ضرورة الحصول على إذن قضائي بذلك، فهنا تعد المراقبة انتهاك للحق في الخصوصية المعلوماتية [1].

ويتبين من ذلك أن نظام المراقبة الإلكترونية على درجة كبيرة من الأهمية لاتصالها المباشر للحق في الخصوصية، كما يعد عمل المراقب أمرا لا يمكن إهماله وخاصة إذا كانت الدول تسعى إلى نسج حماية جنائية إجرامية سليمة للمعلومات التي يتم فيها محاصرة الجريمة

[1]– محمد كمال شاهين، المرجع السابق، ص 253–254 .

الالكترونية من ناحية، وحماية المعلومة من ناحية أخرى، بهدف المحافظة على الحق في الخصوصية المعلوماتية للأفراد[1].

د.أشكال المراقبة الالكترونية

تتلخص أشكال المراقبة الالكترونية في استخدام وسائل تقنية من خلال ما يسمى بقلم التسجيل أو ما يسمى بالفخ والمتابعة وفي هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أو مع بريده الالكتروني أو ما يقوم بمحادثات ودردشات، أو عن طريق استخدام وسائل للتصنت على محتوى الرسالة الالكترونية أو المحادثة الفورية بوسائل للاعتراض والتصنت والضبطية تواجه مشكلة تشفير المراسلات الالكترونية في حال ارتكاب جريمة من فاعلها عن طريق برامج تشفير تباع بأثمان رخيصة في السوق، ما يثير مشكلات بالنسبة للضبطية القضائية بعد ضبط هذه الرسائل هو عدم القدرة على الاطلاع على محتواها لأنها مشفرة[2] .

وقد أسفر التقدم التقني عن ابتكار برامج لمكافحة ما يلجأ إليه المجرمون من تشفير رسائلهم الإجرامية وذلك باستعمال جهاز يقال له key logger ، وتسمح بتلك الوسيلة بتسجيل ضربات الجهاز على لوحة المفاتيح بعد استعمال الجهاز وبالتالي تسمح بمعرفة كلمة السر، كما ظهر برنامج آخر يقال له magic lantern ، في الجهاز الأول يتم تثبيت قطعة معينة على جهاز الكمبيوتر الخاص بالمتهم، الأمر الذي يستلزم دخول مسكن المتهم لإتمام هذه العملية، أما البرنامج الثاني فإنه لا يستلزم سوى إرسال برنامج معين مختفيا في إعلان مثلا إلى المتهم كما لو أرسلت له رسالة تقول " اضغط هنا " وعند الضغط تفتح الرسالة ويتم زرع برنامج magic lautern في جهاز المتهم دون أن يدري ، وفي كلا الحالتين بالوسيلة الأولى والثانية تسمحان بمعرفة كلمة السر لجهاز المتهم والدخول إليه لمعرفة الشفرة التي يستعملها المتهم في رسائله، كما أنه يجب التمييز بين الوسائل التقنية التي من شانها الاطلاع على الجهاز وهو مغلق لا

---

[1]– محمد كمال شاهين، المرجع السابق، ص 254 .

[2] – شيماء عبد الغني، المرجع السابق، ص ص257 – 258 .

يستخدمه المتهم في المراسلة كالوضع بالنسبة لوسيلة key logger system وبين الحالة التي يتم فيها التصنت على رسائل المتهم عند إرساله لها كما في حالة استعمال برنامج يسمى المفترس carnivore والذي يتيح التقاط الرسائل عند تداولها [1]، ونرى بأن هذين البرنامجين key logger system ، و magic lautern ، وسيلتان تلعبان دورا كبيرا في البحث والتحري عن مرتكبي الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، نظرا لما يقدمان من سهولة للحصول على دليل الكتروني تتمثل في رسائل الكترونية صادرة من المتهم نفسه، كل ذلك لا يتم إلا بالشروط المحددة قانونا والطرق المشروعة للوصول إلى الدليل الالكتروني.

رابعا: التسرب

يقصد بالتسرب وفقا للمادة 65 مكرر12 قيام ضابط الشرطة القضائية أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنحة أو جناية بإيهامهم بأنه فاعل معهم أو شريك أو خاف .

ويمكن تجسيد عملية تسرب في جريمة اعتداء على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، بقيام عون أو ضابط شرطة قضائية بإيهام المشتبه فيهم بأنه يريد الحصول على ما توصلوا إليه من إجرام، كإيهام من يحوز على توقيع الكتروني خاص بالغير تحصل عليه عن طريق اختراق نظام معلوماتي للتوقيع الالكتروني، أنه يريد شراءه مقابل مبلغ مالي مغري، أو يكون شريك معهم بأن يخلق معهم علاقات ومحادثات الكترونية وأن له قدرات في مجال المعلوماتية تساعدهم على الاختراق والدخول لنظام معلوماتي متعلق بالتوقيع الالكتروني.

---

[1]-Amitai etzioni implicztion of select new technologies for individual rights and public sagety , havard journal of law technology , 2002 , p 274 .

نقلا عن: شيماء عبد الغني، المرجع السابق، ص 258 .

أ.شروط صحة التسرب

شروط صحة التسرب حددتهما المواد 65 مكرر 11و 15 و 17 من قانون الإجراءات الجزائية والتي يمكن إجمالها في:

أن يكون إذن مكتوب من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية، مع ذكرهما للأسباب التي دفعتهما للجوء إلى إجراء التسرب وذلك تحت طائلة البطلان.

ويذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ونخص بالذكر هنا أن تكون جريمة اعتداء على نظام معالجة آلية لمعطيات للتوقيع الالكتروني.

مع التحديد في الإذن المدة الزمنية للتسرب التي لا يمكن أن تتجاوز أربعة 04 أشهر، على أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة [1]، مع أنه يمكن للعون المتسرب بعد وقف عملية التسرب مواصلة النشاطات المبررة قانونا في التسرب للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف آمنة دون أن يكون مسئولا جزائيا، على ألا تتجاوز مدة أربعة 04 أشهر، يمكن تمديدها مرة واحدة على الأكثر في حالة عدم تمكن العون المتسرب مواصلة نشاط المراقبة في ظروف تضمن أمنه.

ونرى من وجهة نظرنا أن يسند الإذن بالتسرب لقاضي التحقيق وحده دون وكيل الجمهورية نظرا لما يخلفه هذا الإجراء من أثار ومساس بالحياة الخاصة للأفراد من جهة، ومن جهة ثانية أن الوقائع الإجرامية لما تكون أمام قاضي التحقيق يكون هذا الأخير أكثر إلماما بتفاصيل القضية لما له من صلاحيات واسعة بالنسبة للتحقيق مع الأشخاص والوقائع.

* عدم تحديد مرات التجديد للتسرب قد يطيل المدة، لذلك نرى أنه من الضروي تحديدها بإعطاء القاضي مصدر الإذن الحق في التجديد مرتين، ولغرفة الاتهام مرة واحدة .

ب.الشروط الواجب توافرها في القائم بالتسرب وكيفية تنفيذه

للقائم بالتسرب في جرائم التوقيع الالكتروني لابد أن تكون له ثقافة في الحاسب، فوجود هذه الثقافة في رجال الضبطية القضائية وربطها بالثقافة العلمية بوجه عام سيكفل لها نجاحا في مواكبة ظاهرة جرائم الحاسب الآلي، فالقدرة على الملاحظة وقراءة تصرفات الأشخاص العاملين في مجال الحاسب الآلي والمهتمين بالبرامج وهواة صناعة الأنظمة وتقليدها هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي جرائم الحاسب، وإن الفئات التي يجب وضعها تحت المراقبة والملاحظة الدائمة هم في الغالب من أصحاب الياقات البيضاء والذين تدل مظاهرهم على الوقار، والمكانة الاجتماعية، ويعني التعامل مع هذه الفئات الانتقال بالحس الأمني لرجل البحث الجنائي من اهتمامه التقليدي بالعطالة والمتشردين والطبقات الفقيرة إلى مراقبة طبقات اجتماعية حديثة تتسلح بالعلم والخبرة والذكاء والثقافات المتنوعة، لذلك فإن معايشة وتسرب رجل الشرطة لهذه الفئات الجديدة والاتصال بهم تحتم عليه أن يرتقي إلى درجاتهم شكلا ومضمونا، ولا بد من الظهور بمظهر أصحاب الياقات البيضاء، ويتحدث لغتهم العصرية، وأن يكون قادرا على فهم عبارات ومفردات لغة الحاسب الآلي التي تمكنه من جمع المعلومات المناسبة ومتابعتها [1]، لكي يستطيع عون أو ضابط الشرطة القضائية التنسيق مع المشتبه فيهم بارتكاب جرائم الاعتداء على التوقيع الالكتروني هذا من جهة، ومن جهة أخرى حتى لا يتبادر إلى أدهان المشتبه فيهم بأن المتسرب هو من أحد أفراد الشرطة.

أما عن طريقة تنفيذ التسرب في الجرائم الواقعة على نظم المعالجة الآلية لمعطيات التوقيع الالكتروني فيتم بدخول عون أو ضابط الشرطة القضائية بآليات مختلفة لمتابعة الجريمة وتحديد هوية الجناة من خلال الولوج لقاعات الدردشة واستخدام برمجيات الاتصال المباشر المستقلة والتنكر على الانترنت واستخدام أسماء وصفات مستعارة والدخول إلى موقع ترويج البرمجيات المسروقة والبيانات والمعلومات المستولى عليها بطرق غير مشروعة من النظم المعلوماتية،

[1]– محمد الأمين البشري، المرجع السابق، ص 106 .

حيث يتم عرضها للبيع عن طريق هذه المواقع التي تكون معروفة لمعتادي شراء هذه المسروقات بأثمان بخسة كأرقام بطاقات ائتمان مسروقة أو برامج إعداد توقيعات إلكترونية مسروقة، وهنا يقوم القائم بالتسرب بتقصي المعلومات كأن يسأل المخترق عن كيفية الاختراق[1]، أو يقوم بعرض مبالغ مالية لشراء التوقيعات الالكترونية المخترقة والمسروقة، أو شراء البرامج التي يستعملها المجرمون لأجل الدخول إلى أنظمة التوقيع الالكتروني.

ومن التطبيقات الواقعية على التسرب في الجرائم المرتكبة عبر الانترنت قيام المباحث الفيدرالية الأمريكية بدس عضو ضبطية قضائية عن طريق أسلوب التسرب بين جماعة إجرامية مختصة بقرصنة البرمجيات وتحميلها على مواقع هكرة عبر الانترنت، وبالفعل تمَ ضبط هذه الجماعة الإجرامية [2].

ج.الأفعال المبررة في التسرب

الأفعال المبررة في التسرب حددتها المادة 65 مكرر 14 التي لا ترتب مسؤولية جزائية لعون أو ضابط الشرطة القضائية أو المرخص لهم بإجراء عمليات التسرب والأشخاص الذين يسخرونهم لهذا الفرض ، وهي على التوالي:

– اقتناء أو حيازة أو نقل أو تسليم أو إعطاء أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

– استعمال أو وضع تحت التصرف مرتكب هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

---

[1]– حسام محمد نبيل الشنراقي، المرجع السابق، ص 382.

[2]– محمد كمال شاهين، المرجع السابق، ص 252 .

د.الحماية الجزائية للقائم بالتسرب

عملية التسرب لابد وأن تتم في سرية تامة لأن المجرمين لا يعلمون وأنه من سلك الشرطة ولو علموا سيكون هو وأقربائه في خطر، لذا فالمشرع كفل حماية جنائية موضوعية للقائمين على التسرب بجريمة مستقلة، إذا يعاقب جزائيا كل شخص يقوم بإظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات[1] .

المطلب الثاني: الأجهزة والآليات المساعدة للضبطية القضائية في البحث والتحري عن جرائم التوقيع الالكتروني

الضبطية القضائية ولأجل التنقيب والتحري الناجع في جرائم التوقيع الالكتروني، تستعين بالعديد من الأجهزة والهيئات على المستوى الوطني إذا ما ارتكبت في نطاق وطني، وكذلك بآليات دولية إذا ما كان كانت عابرة للحدود الوطنية ودولية، لذلك سنتطرق إلى التعاون الأمني الدولي، ثم سنتطرق إلى التعاون الأمني الوطني .

الفرع الأول: دور التعاون الأمني الدولي في مرحلة جمع الاستدلالات

يمثل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم المعلوماتية في الدول أحد الوسائل الهامة التي يمكن من خلالها مكافحتها والإقلال منها، وتؤكد التحقيقات في المجال التعاوني الأمني الدولي أنه يستحيل على الدولة بمفردها القضاء على هذه الجرائم العابرة للحدود، لأن جهاز الأمن في هذه الدول وغيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدول التابعة لها، فملاحقة مرتكبي هذه الجرائم يتطلب القيام بإجراءات

* عقوبة من يكشف هوية القائم بالتسرب الحبس من 02 سنتين إلى 05 خمس سنوات وبغرامة من 50,000 إلى 200,000 دج ، وتشدد العقوبة إذا تسبب عن كشف الهوية أعمال عنف أو ضرب وجرح على أحد هؤلاء الاشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من 05 خمس إلى 10 عشر سنوات والغرامة من 200,000 إلى 500,000 دج ، وإذا تسبب عن هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر 10 سنوات إلى 20 عشرين سنة والغرامة من 500.000 إلى 100.000 دج .

التحري ومنها معاينة مواقع الانترنيت في الخارج وضبط الأقراص الصلبة أو تفتيش نظام الحاسب الآلي[1]، فما هي الصعوبات التي يثيرها التعاون الأمني الدولي؟ ودور المنظمة الدولية للشرطة الجنائية Interpol ؟ وما هو دور الأنظمة والشبكات التقنية في التعاون الأمني الدولي ؟ .

أولا: صعوبات التعاون الإجرائي الدولي

هناك العديد من الصعوبات منها تنوع واختلاف النظم القانونية الإجرائية التي تثبت فاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أوقد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية والتسليم المراقب والعمليات المستترة وغيرها من الإجراءات المشابهة فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، لذلك فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطاتها على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرقا غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع [2].

وعدم وجود معاهدات ثنائية أو جماعية بين الدول سيؤثر على التعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة على تحقيق الحماية المطلوبة في

[1]– فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية ، رسالة دكتوراه جامعة عين الشمس، ص 514 . نقلا عن : عادل عبد العال إبراهيم خراشي ، إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015 ، ص 21 .

[2] – عادل عبد العال إبراهيم خراشي، المرجع نفسه، ص ص 58 59 .

ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت، وتطور جرائم التوقيع الالكتروني بذات السرعة على نحو يؤدي إلى إرباك المشرع والشرطة القضائية والتعاون الأمني بين الدول[1] .

ثانيا: دور المنظمة الدولية للشرطة الجنائية Interpol

يصعب على الدولة بمفردها القضاء على جرائم المعلومات العابرة للحدود، لذلك فإن الحاجة ملحة إلى تعاون دولي بين أجهزة الشرطة بين الدول وتنسيق العمل فيما بينهم لضبط المجرمين ومكافحة نشاط الإجرام المعلوماتي الذي يتجاوز الحدود الدولية وقد تبلور هدا النوع من التعاون الدولي إنشاء المنظمة الدولية للشرطة الجنائية الأنتربول[2] .

ويعد التعاون الدولي بين سلطات الضبطية القضائية في مختلف الدول من أجل البحث والتحري والقبض بشأن المجرمين أحد أبرز مظاهر التعاون الأمني الدولي لتزداد أهميته أكثر في مكافحة الجرائم الالكترونية الواقعة على التوقيع الالكتروني العابرة للحدود الذي لا يمكن أن يتحقق إلا بتعاون أمني دولي يسمح بالاتصال المباشر بين أجهزة الشرطة بين مختلف دول العالم .

لذا أصبح هناك ضرورة ملحة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة لذلك، تم إنشاء المنظمة الدولية للشرطة الجنائية وتهدف هذه المنظمة إلى [3] :

– تأكيد وتشجيع التعاون بين سلطات الشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وتحقيق المشاركة الفعلية للدول الأعضاء في تقديم مساعدة فعالة إلى الشرطة الوطنية في مكافحة الجريمة، ويتم هذا التواصل والمشاركة عن طريق مكاتب وطنية توجد في كل دولة من الدول الأعضاء في

---

[1]– عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 106 .

[2]– طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 594 .

[3] – محمد كمال شاهين، المرجع السابق، ص ص 216 – 217 .

الأنتربول وتعد تلك المكاتب المركزية الوطنية هي نقطة الاتصال مع الإدارات الأجنبية التي تجرى تحقيقات خارج حدودها .

– تبادل المعلومات البيانات والمعلومات فما بين الدول الأعضاء والتعاون على ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها، أي أن عضو الانتربول لا يقوم بنفسه بإجراء القبض على المجرمين بل يناط هذا العمل لأجهزة الشرطة الوطنية في الدولة التي يتواجد على إقليمها المجرمين، وهو ما يؤكد احترام سيادة الدول على أراضيها.

ثالثا: دور الأنظمة التقنية في البحث والتحري على المستوى الدولي

تساعد الشبكات والبرامج الالكترونية في التعاون الأمني الدولي نذكر منها شبكة الطوارئ الدائمة لتفعيل المواجهة التقنية، وبرامج التتبع.

أ. شبكة طوارئ دائمة لتفعيل المواجهة التقنية للجرائم المعلوماتية

تناولت مادة وحيدة هي المادة 35 من اتفاقية بودابست بخصوص إنشاء شبكة طوارئ لتفعيل المواجهة التقنية للجرائم المعلوماتية، وتعمل هذه الشركة على مدار 24 ساعة يوميا وبمعدل 7 أيام في الأسبوع بغرض التأكد من توفير المساعدة الفورية لإجراء التحقيقات المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لتجميع أدلة ذات شكل إلكتروني لجريمة جنائية، وهذه المساعدة يجب أن تكون مشتملة على تسهيل مسموح وفقا للقانون الداخلي أو التطبيق العملي للقيام المباشر بالإجراءات التالية:

– تقديم المشورات التقنية.

– التحفظ على البيانات.

– تجميع أدلة وتقديم معلومات ذات طابع قانوني، وتحديد أماكن المشتبه فيها.

كما يجب أن تكون نقطة الاتصال الخاصة بكل طرف لديها قدرة على إجراء اتصالات مع نقطة اتصال لطرف آخر على وجه السرعة.

وإذا كانت نقطة الاتصال المحددة بواسطة طرف ما لا تعتمد على سلطة أو سلطات هذا الطرف المسؤولة عن المساعدة الدولية أو تبادل تسليم المجرمين، فإنه يجب عليها أن تكون قادرة على التعامل مع هذه السلطات على وجه السرعة، كما يجب على كل طرف أن يكون له طاقم مدرب ومزود بالأجهزة التي تسهل عملية تشغيل الشبكة[1].

وتستهدف نقطة الاتصال إما تسهيل الممارسة السريعة لوظائف الشبكة وإما التطبيق المباشر لعدد من التدابير من بينها توفير الإرشادات التقنية، التحفظ عن البيانات، جمع الأدلة، إعطاء معلومات ذات طابع قانوني، تحديد أماكن المشتبه فيهم، وبالنسبة لمصطلح المعلومات ذات الطابع القانوني الواردة في الفقرة 01 من اتفاقية بودابست فإنه يمتد ليشمل كل الحالات السابقة بخصوص التعاون الرسمي والغير رسمي، ولكل دولة الحرية في تحديد وموقع نقطة الاتصال بالنسبة لتنظيمه من السلطات المكلفة بتنفيذ القانون، فبعض الأطراف قد يضع نقطة الاتصال داخل هيكل السلطة المركزية المسؤولة عن المساعدة المتبادلة، في حين قد يرى البعض الآخر ربطها بجهاز الشرطة المخصص لمكافحة الإجرام المعلوماتي، وقد يذهب فريق ثالث إلى تبني اختيارات أخرى كأن يتم ربط نقطة الاتصال بجهاز إداري أو بنظام أو كيان قانوني، ولا يوجد حتى الآن حل وحيد يجمع عليه كل الأطراف، بيد أن القاسم المشترك بين هذه الاتجاهات هو قيام نقطة الاتصال بتوفير الإرشادات أو النصائح التقنية من أجل صد أي هجوم معلوماتي أو تحديد مصدره، وكذلك القيام بواجبات التعاون الدولي وتحديد أماكن المشتبه فيهم، وينتظر أن يتم تطوير بنية الشبكة مع مرور الوقت[2].

---

[1] – هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة، المرجع السابق، ص ص 240 -241 .

[2]– المرجع نفسه، ص 243 .

ب. برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه والعنوان التي تمت من خلاله عملية الاختراق واسم الشركة المزودة لخدمة الانترنت، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى [1] .

الفرع الثاني: دور الأجهزة و الهيئات الوطنية في البحث والتحري

الضبطية القضائية في حاجة ماسة لأجهزة وهيئات تساعدها في الكشف والتنقيب عن جرائم التوقيع الالكتروني، لأنه يتم معالجة بيانات التوقيع الالكتروني ضمن هذه الأجهزة، كخدمة المصادقة على التوقيع الالكتروني التي تمر عبر جهات التصديق الالكتروني لذا تلعب جهات التصديق الالكتروني دور هام في الكشف عن جرائم التوقيع الالكتروني، بالإضافة إلى الجرائم المرتكبة على التوقيع الالكتروني باستعمال شبكة الانترنت يجعل من مزودي خدمات الانترنيت أيضا من الأهمية البالغة في الكشف عن جرائم التوقيع الالكتروني ، لذلك سنتطرق إلى دور جهات التصديق الالكتروني و دور مزود خدمات الانترنت، وما لها أيضا من معلومات و صلاحيات تفيد البحث والتحري كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

أولا: دور مزود الخدمة في البحث والتحري

نظرا لأهمية الدور الذي يلعبه مزود الخدمة في نطاق جرائم التوقيع الالكتروني، فقد حرصت الفقرة ج من المادة الأولى من اتفاقية بودابست على إيراد تعريف له بقولها مزود الخدمة يشير إلى، كل جهة عامة أو خاصة تقدم لمستخدمي خدماتها إمكانية الاتصال عن طريق النظام المعلوماتي، أو كل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلا من خدمة الاتصال أو نيابة عن مستخدمي هذه الخدمة.

[1] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، المرجع السابق، ص 306 .

وقد حرصت هذه المذكرة التفسيرية على أن توضح أن تعريف مزود الخدمة ينطبق على كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو تخزينها، ويستوي في ذلك أن تكون الجهة التي تقدم الخدمة جهة عامة أو خاصة، كما يستوي أن تكون الخدمة مقدمة لمجموعة من المستخدمين يشكلون جماعة مغلقة أو أنها مقدمة للجمهور، وهذه الخدمة قد تكون بمقابل أو بدونه، ويشمل الأشخاص الذين يعرضون خدمة الاستضافة أو التخزين المؤقت أي خدمات الإخفاء أو الربط بالشبكة[1].

وتتجه العديد من التشريعات المقارنة إلى إلزام مزودي الخدمات بالتعاون مع سلطة التحقيق وسلطات الضبط القضائي، وفي ذلك يجيز المشرع الأمريكي لجهات التحقيق أن تصدر أمر بإلزام مزودي الخدمات بتقديم ما لديهم من معلومات تخص المشتركين لديها، إذا كان هناك مبررات معقولة تدعو إلى الاعتقاد بأن محتويات الاتصالات السلكية أو الالكترونية أو السجلات أو أي معلومات أخرى تفيد في كشف الحقيقة في تحقيق جنائي قائم ، وهو ما أقرته المادة 68 من قانون الإجراءات الجزائية من أن لقاضي التحقيق أن يتخذ جميع الإجراءات الضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام والنفي[2].

كما نصت المادة 20 فقرة 01 من اتفاقية بودابست 2001 على أن يلزم مقدم الخدمة في نطاق قدرته التقنية على جمع أو تسجيل البيانات من خلال تطبيق الوسائل الفنية، بالتعاون مع السلطات المختصة ومساعدتها بشكل فوري في جمع خط سير البيانات المرتبطة باتصالات معينة أو تسجيل خط سير تلك البيانات التي تم نقلها بواسطة نظام معلوماتي[3].

---

[1]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنيت بين التجريم الجنائي واليات المواجهة، المرجع السابق، ص239 .

[2] – محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة– دراسة مقارنة في التشريع الفرنسي والأمريكي والاتفاقيات الدولية و الإقليمية، المكتب الجامعي الحديث، الإسكندرية، 2018 ، ص 61 .

[3] – المرجع نفسه، ص 63 .

وعموما يمكن القول على وجه التحديد أن هناك طوائف من البيانات المتعلقة بالمرور والتي تخضع لنظام قانوني معين تكون متاحة عن طريق مزود ومقدم الخدمة وذلك لضرورات التحري والتنقيب الجنائي وهي:

– منشأ أصل الاتصال ويعني رقم التيليفون، وعنوان بروتوكول الانترنت، أو بطريقة مماثلة تحديد هوية جهاز الاتصال الذي يقوم مزود أو مقدم الخدمة بتقديم خدماته من خلاله.

– مكان الوصول، أي مكان الوصول إلى جهاز الاتصال التي تتجه إليه الاتصالات المرسلة.

– خط السير.

– وقت أو ساعة الاتصال، التاريخ، الطول أو حجم الاتصال، المدة أو الفترة.

– نوع الخدمة المؤذاة داخل الشبكة مثل نقل الملف، بريد إلكتروني بريد آني أو لحظي[1].

كما تبين المذكرة الإيضاحية أهمية بيانات المرور في حالة وقوع جريمة بقولها أنه في حالة التنقيب بخصوص الجريمة الجنائية ارتكبت في نظام معلوماتي، فإن بيانات المرور تكون ضرورية من أجل تحديد مصدر الاتصال وذلك كنقطة بداية تسمح لتجميع أدلة أخرى أو جزء من دليل جريمة، وبيانات المرور يمكن أن تكون سريعة الزوال لذلك يكون من الضروري العمل على حفظها فورا وبالتالي فإنه قد يكون من الضروري الكشف السريع عنها لمعرفة خط سير الاتصال وتجميع الأدلة قبل أن تمحى[2].

هذا وقد أوردت بعض التشريعات المقارنة استثناءات على التزام مزودي الخدمات بالتعاون مع الضبطية القضائية من ذلك الاستثناء الوارد في الفقرة من المادة 31 من القانون رقم 17 لسنة 1978 المتعلق بالمعلومات والحريات في فرنسا حيث تنص على عدم جواز مراقبة المعلومات التي تجمعها الكنائس أو تجمعات دينية أو فلسفية أو سياسية أو نقابية والتي تتعلق بأعضائها والمتراسلين معها، وما ورد في المادة 60 فقرة 02 من قانون الإجراءات الجزائية

[1]– هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة، المرجع السابق، ص 237 .

[2]– المرجع نفسه، ص 238 .

الفرنسي بخصوص المعلومات التي يغطيها سر المهنة حيث تنص على أنه باستثناء المعلومات التي تعتبر من أسرار المهنة التي أوردها القانون والمتواجدة في الأنظمة المعلوماتية أو أي أجهزة للمعالجة الآلية [1].

ثانيا: دور جهات التصديق الالكتروني

يجب على مزود خدمة تصديق التوقيع الالكتروني التعاون مع الضبطية القضائية و جهات التحقيق للبحث والتحري لأجل الكشف عن جرائم التوقيع الالكتروني، وتعتبر جهة التصديق الالكتروني هي الجهة الأكثر التي من الممكن أن تساعد كثيرا الضبطية القضائية وجهات التحقيق وبخاصة جرائم التوقيع الالكتروني الواقعة أثناء وبعد مرحلة التصديق الالكتروني المعاقب عليها بنص المواد 69 –70 –71 –72 من قانون التوقيع والتصديق الالكترونيين، لما تحوزه من معلومات حول التوقيع الالكتروني محل الحماية الجزائية والمعلومات المتعلقة بالشخص صاحب التوقيع، والتي تفيد الضبطية القضائية وجهة التحقيق كمعلومات مبدئية للوصول إلى مرتكب جريمة الاعتداء على التوقيع الالكتروني .

ثالثا: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في البحث والتحري عن جرائم التوقيع الالكتروني

الهيئة هي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، وفقا لما نصت عليه المادة 02 [2] من المرسوم الرئاسي رقم 15–261 المؤرخ في 24 ذي الحجة عام 1436 الموافق ل 08 أكتوبر سنة 2015 الذي يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1] – محمود محمد جابر، المرجع السابق، ص 48 .

[2] - الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 53 ، ص 16 .

ومن المهام الأساسية للهيئة أنها حسب المادة 04 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هي مساعدة السلطات القضائية ومصالح الشرطة القضائية في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

وهذه المعلومات يتم الوصول إليها بما منحه القانون في المادة 30 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من أنه يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول ولاسيما قانون الإجراءات الجزائية بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية .

ومن مهام الهيئة أيضا مساعدة للضبطية القضائية هو تسليمها لتسجيلات الاتصالات الالكترونية والمحررات إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وفقا لما نصت عليه المادة 20 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

كما أنشأت على مستوى الهيئة حسب المادة 11 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ما يسمى بمديرية المراقبة الوقائية واليقظة الالكترونية والتي من مهامها على الخصوص وفقا للفقرة 02 و 07:

إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة.

تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناءا على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومنها الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني.

المبحث الثاني: إجراءات التحقيق الابتدائي في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

التحقيق الابتدائي في الدعوى الجزائية هو عمل إجرائي يضم في ثناياه مجموعة من الإجراءات التي تتخذها سلطة معينة هي سلطة التحقيق وموضوعه هو الجريمة الواردة في محضر الاستدلالات، والهدف منه كشف الحقيقة بصدد هذه الجريمة والتحقق من مدى نسبتها إلى المتهم المذكور بغية إحالة الدعوى إلى المحكمة المختصة في حالة رجحان أدلة الإدانة، أو إصدار أمر بانتفاء وجه الدعوى إذا رجحت أدلة البراءة [1].

ولقاضي التحقيق أعمال عديدة ومتنوعة يحق لقاضي التحقيق اتخاذها وليس ملزما بمباشرة كافة هذه الأعمال بطبيعة الحال، ولا يتسنى من ذلك إلا الاستجواب فذلك عمل تحقيقي لا غنى عنه حتى بالنسبة إلى المتهم، إذ قد ينجح هذا الأخير أن يفند أدلة الإدانة الموجهة ضده وفيما عدا الاستجواب فلقاضي التحقيق أن يتخير ما يشاء من عمل تحقيقي أو يأمر بذلك وهناك نوعين من أعمال التحقيق الهادفة إلى الكشف عن الحقيقة ويطلق عليها إجراءات جمع الأدلة كالانتقال للمعاينة وندب الخبراء وسماع الشهود وضبط الأشياء والتفتيش والاستجواب، أما الثانية فهي أوامر التحقيق الهادفة إلى تأمين الأدلة ويطلق عليها إجراءات التحقيق الاحتياطية ومثالها أوامر الضبط والإحضار والحبس المؤقت[2]، والتي تخرج من نطاق دراستنا، ولا تكفي إجراءات جمع الأدلة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

---

[1]– جلال ثروت، سليمان عبد المنعم، أصول المحاكمات الجزائية، ط1 ، المؤسسة الجامعية للدراسات، بيروت، 1997 ص460 .

[2]– المرجع نفسه ، ص 491 .

على المستوى الوطني لوحدها بل لابد من آليات دولية للتحقيق لمجابهة الجرائم المرتكبة بالوسائل الالكترونية لعابرة للحدود، لذلك سنتطرق إلى إجراءات التحقيق الهادفة إلى الكشف عن الحقيقة أو إجراءات جمع الأدلة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني في المطلب الأول، ثم آليات التحقيق الابتدائي الدولي في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني في المطلب الثاني.

المطلب الأول: إجراءات جمع الأدلة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

على جهات التحقيق التعامل بحذر في جمع الأدلة الواقعة على نظام التوقيع الالكتروني كمخرجات الحاسب وقوائم التشغيل، وكما هو الحال أحيانا في الجرائم الأخرى قد يدمر المحقق الدليل بمحوه الأسطوانة الصلبة عن خطأ أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة، أو الخطأ والتسرع في جمع الأدلة [1]، وللوصول إلى الحقيقة وجمع أدلة مترابطة ومتماسكة لابد من مجموعة إجراءات يقوم بها قاضي التحقيق للترجيح بين أدلة النفي أو الإدانة في جرائم التوقيع الالكتروني، نذكر أهمها والتي تتمثل في التفتيش، الضبط، نذب الخبراء، سماع الشهود، الاستجواب.

الفرع الأول: الاستجواب

لقد نظم المشرع الجزائري أحكام الاستجواب في المواد من 100 إلى 108 من قانون الإجراءات الجزائية، والذي يكون عبر مراحل فهناك الاستجواب عند مثول المتهم لأول مرة أمامه ولكنه سماع أكثر منه استجواب، يتحقق فيه قاضي التحقيق عن هوية المتهم وإحاطته بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر في عدم الإدلاء بأي إقرار، أما إذا أراد ذلك تلقاها قاضي التحقيق منه ، وينبهه أيضا بأن له الحق في اختيار محام عنه حسب المادة 100 من قانون الإجراءات الجزائية، ثم في مرحلة أخرى استجواب المتهم في الموضوع ومواجهته

[1] – هشام رستم، المرجع السابق، ص 439 .

بحضور محاميه ووكيل الجمهورية الذي يجوز له أن يوجه مباشرة ما يراه لازما من أسئلة، على عكس محامي المتهم والمدعى المدني اللذان لا يجوز لهما الكلام ما عدا توجيه أسئلة بعد إذن قاضي التحقيق، وفقا لمقتضيات المواد 105 106 107 من قانون الإجراءات الجزائية.

وإجراء استجواب المتهم عمل تحقيقي لا يجوز لغير سلطة التحقيق مباشرته فليس لرجال الضبطية القضائية حق استجواب المتهم سواء فما تعلق بالجريمة المتلبس بها أو في حالة الندب من جهة التحقيق ذاتها.

ويقصد بالاستجواب مجابهة المتهم بالأدلة المحشودة ضده ومناقشته فيها مناقشة تفصيلية بهدف استجلاء ظروف وملابسات الجريمة وكشف الحقيقة فيما تعلق بالجرم الواقع والأدلة التي أمكن لرجال الضبطية القضائية التوصل إليها، والاستجواب على هذا النحو قد يفضي بالمتهم إلى الاعتراف بجرمه، وقد يحدو به على العكس إلى إنكار الجرم المنسوب إليه [1].

واستجواب المتهم في جرائم التوقيع الالكتروني تحكمه ذات القواعد العامة للاستجواب في أي جريمة تقليدية، لكن الفرق يكمن في ضرورة تأهيل وتكوين قضاة تحقيق في جرائم الحاسب الآلي والانترنت حتى يمكن لهم استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة و مصطلحاتها، سيما وأن المجرم الذي يتولى التحقيق معه ليس مجرما عاديا، ذلك أن المجرم الالكتروني له طبيعة خاصة في استخدام تقنيات الحاسب الآلي [2]، وهو يعطي مشكلة للمحقق حين استجواب المجرم الالكتروني أو في محاولة الحصول على اعتراف منه ، ذلك أن المجرم الالكتروني على عكس المجرم التقليدي يتميز بالذكاء ومتمرس بتفاصيل الحاسب والشبكات والبرمجيات، وتشير المعلومات إلى أن أعلب مرتكبي الجرائم المرتكبة بالوسائل الالكترونية يقيمون في دول العلم الثالث المتخلفة في كل شيء إلا في مجرميها الالكترونيين الأذكياء [3]،

---

[1] – جلال ثروت، سليمان عبد المنعم، المرجع السابق، 502 .

[2] – عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 681 .

[3] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، المرجع السابق، ص 240 .

وهذا ما يدعو لصعوبة الاستجواب مع مرتكبي جرائم التوقيع الالكتروني لقدرتهم من التهرب من المسؤولية الجزائية، لذا يتطلب من قاضي التحقيق أن يكون ملما بملف التحقيق في مواجهة المتهم، ويتمتع بقدرات فنية للتحقيق، والأكثر من ذلك إلمامه بتقنيات الحاسب لكي يستطيع انتزاع اعتراف منه .

وإجراء الاستجواب في الموضوع لجرائم التوقيع الالكتروني يتطلب من قاضي التحقيق الحنكة والتبصر فيه من خلال مواجهة المتهم بالدلائل القائمة ضده، ومواجهته أيضا بالشهود وأي شخص يراه في مواجهته لإظهار الحقيقة، وما يمكن أن يساعد قاضي التحقيق ويعطي له إضافة في الاستجواب مواجهته بالخبرة الالكترونية والخبراء في مجال الحاسب الآلي والجرائم الالكترونية .

الفرع الثاني: التفتيش

يعد التفتيش أحد أهم الآليات الإجرائية للبحث عن الدليل في الجرائم الالكترونية والتقليدية، الذي قد يكون في حيازة شخص المتهم أو مسكنه، كالبحث في الشخص الذي يحمل مواد مخدرة في جيبه، أو في المسكن المخبئة فيه، أما إذا ارتكبت الجريمة في وسط الكتروني فيكون محل التفتيش الوسائل الالكترونية الحديثة المادية منها أو المعنوية كالنظام المعلوماتي، لذلك سنتطرق إلى مفهوم التفتيش، ثم التفتيش في نظم الحاسب الآلي.

أولا: مفهوم التفتيش

المشرع الإجرائي الجزائري لم يعرف التفتيش، ولا يمكن لقاضي التحقيق اللجوء إليه أو انتداب الضبطية القضائية إلا في حالة توافر شروط موضوعية، وهذا ما سنتطرق له من خلال تعريف التفتيش التفتيش، وشروطه، وبيان أنواعه.

أ.تعريف التفتيش

التفتيش هو عمل من أعمال التحقيق التي تستهدف كشف الحقيقة بشأن الجرم الواقع ومدى ثبوته في مواجهة المتهم، ولقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، وإما أن يأذن بذلك للضبطية القضائية من خلال الندب[1]، أو هو إجراء من إجراءات التحقيق يهدف إلى البحث عن دلائل أو أشياء موجودة في مكان مغلق تفيد في كشف الحقيقة عن الجريمة، وهو ليس من إجراءات كشف الجرائم قبل وقوعها، بل هو من إجراءات تحقيقها بعد ارتكابها [2].

ب.الشروط الموضوعية للتفتيش

يشترط لمباشرة إجراء التفتيش للأشخاص والأماكن أو الإذن به باعتباره إجراء من إجراءات التحقيق توافر عدة شروط [3]:

– أن يكون إجراء التفتيش متعلقا بجريمة وقعت فعلا وتشكل في القانون إما جناية أو جنحة أيا كانت جسامتها أو طبيعتها أو أيَ ما كانت العقوبة المقررة لها ولو كانت الغرامة، كما لا يجوز التفتيش لضبط جريمة مستقبلية ولو ترجح وقوعها بالفعل أو قامت الدلائل أو التحريات على أنها ستقع لا محالة، لأن التفتيش إجراء من إجراءات التحقيق، وليس وسيلة لاكتشاف الجرائم وضبط مرتكبيها.

– أن يكون هناك اتهام موجه إلى الشخص المراد تفتيشه أو تفتيش مسكنه، أو أن توجد قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، فلا يكفي أن تكون هناك جناية أو جنحة قد وقعت، بل يلزم لإجراء التفتيش أو الإذن به أن تتوافر لدى المحقق دلائل كافية لاتهام أو حيازته لأشياء تتعلق بها حتى يمكن تفتيشه.

– أن يكون الغرض من التفتيش هو ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة.

---

[1] – جلال ثروت ، سليمان عبد المنعم، المرجع السابق، ص 499 .

[2] – أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، 1985 ، ص 946 .

[3] – محمد زكي أبو عامر، المرجع السابق، ص ص 634–635.

ج.أنواع التفتيش

التفتيش هو البحث عن الحقيقة الذي يكون محله سواء شخصا أو مكانا، لذا فإن التفتيش ينقسم إلى نوعين: تفتيش الأشخاص والأماكن:

تفتيش الشخص يكون بالبحث في كيانه المادي الذي يشمل أعضاءه الخارجية و الداخلية، ويتصل بهذا الكيان ما يرتدي من ملابس أو يحمله من أمتعة أو أشياء منقولة سواء في يديه أو في جيبه، أو ما يستعمله مثل مكتبه الخاص وسيارته الخاصة.

أما تفتيش المساكن فهو كل مكان خاص يقيم فيه الشخص بصفة دائمة أو مؤقتة، وينصرف المسكن إلى توابعه كالحديقة وحظيرة الدواجن والمخزن، ويمتد إلى الأماكن الخاصة التي يقيم فيها ولو لفترة محدودة من اليوم [1]، وهذان النوعان من التفتيش يكون غالبا في الجرائم التقليدية، أما في الجرائم الماسة بالنظام المعلوماتي للتوقيع الالكتروني فيكون التفتيش ضمن النظام المعلوماتي بحثا عن دليل يتناسب وطبيعة الجرم المرتكب، فهل يمكن تصنيف تفتيش النظام المعلوماتي ضمن تفتيش الأشخاص أو المساكن ؟ وهذا ما سنحاول الإجابة عليه في العنوان الموالي.

ثانيا:التفتيش في نظم الحاسب الآلي

أدرج التشريع الإجرائي الجزائري تفتيش نظام الحاسب الآلي في نص المادة 05 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 09- 04 "أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 ، الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكدا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية".

---

[1] – أحمد فتحي سرور، المرجع السابق ، ص 965 .

وقد شعرت العديد من الدول الأوربية التي سبقت المشرع الجزائري إلى إعادة النظر في قانون الإجراءات الجزائية ليتماشى مع التطور السريع في مجال تكنولوجيا الحاسب والانترنت فأصدر المجلس الأوروبي التوصية رقم 95 الصادرة في 11 سبتمبر 1995 في شأن مشاكل الإجراءات الجزائية الوطنية لتلاءم التطور في هذا المجال وأهم ما ورد في التوصية أن توضح القوانين إجراءات تفتيش أجهزة الحاسب وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها وتسمح الإجراءات الجنائية لجهات التفتيش بضبط برامج الحاسب والمعلومات الموجودة والأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بان النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها، كما يسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش وأن يسمح أثناء عملية تنفيذ التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الحاسب الأخرى في دائرة اختصاصه والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات بشرط أن يكون هذا الإجراء ضروريا[1]، ومن التشريعات الداخلية تجيز المادة 60 فقرة 02 من قانون الإجراءات الجزائية الفرنسي في حالة وجود تحقيق ابتدائي للمحقق البحث عن المعلومات داخل النظام المعلوماتي بناء على أمر صادر من قاضي الحريات والحبس، مع الاحتفاظ بالاتصالات الالكترونية وذلك خلال مدة سنة[2]، وهو ما يدعونا للتطرق إلى مدى خضوع النظام المعلوماتي للتفتيش، والضمانات الشكلية المقررة لتفتيشه.

أ.مدى خضوع النظام المعلوماتي للتفتيش

الحاسب الآلي يتكون من مكونات مادية ومعنوية منطقية، يجعلنا نتطرق إلى مدى خضوع المكونات المادية، وكذلك المعنوية المنطقية للتفتيش.

(1) – مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، المرجع السابق، ص 80 .

(2) - Jean nicolas robin, la matière pénal a l épreuve du numérique, thèse doctorat, université du rennes1 , 2017 , p305.

1.مدى خضوع مكونات الحاسب المادية للتفتيش

الواقع أن الولوج إلى المكونات المادية للحاسب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت على التوقيع الالكتروني ويفيد في كشف الحقيقة عنها وعن مرتكبها يدخل ضمن نطاق التفتيش العادي وفقا لقواعد قانون الإجراءات الجزائية و ما نصت عليه 81 من قانون الإجراءات الجزائية من أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، ويجوز أن يشمل التفتيش على المكونات المادية للحاسب مثل وحدة الإدخال –لوحة المفاتيح– شاشات اللمس– الإدخال المرئي– الإدخال الصوتي– الفأرة– القلم الضوئي– القراءة الضوئية– القراءة المغناطيسية– إدخال الأشكال والرسوم– وحدة الذاكرة الرئيسية(ذاكرة القراءة والكتابة)، وحدة الحاسب والمنطق والتحكم– وحدة الإخراج (الشاشة، الطابعة، الرسم، المايكرو فيلم، أجهزة تلقي الرسائل كالفاكس والتيلكس) – وحدة التخزين الثانوية (الأقراص الممغنطة ، القرص المرن القرص الصلب الأشرطة الممغنطة) [1].

إلا أن قواعد تفتيش الحاسب تختلف بحسب نوع الوسيلة المراد إجراء التفتيش عليها إذا كان الحاسب ثابتا أو محمولا.

- **تفتيش المكونات المادية للحاسب الثابت**

المكونات المادية للحاسب المكتبي تخضع لقواعد تفتيش الأماكن وهو ما يتوقف على طبيعة المكان الموجود فيه أكان خاصا أم عاما ، فإذا كان موجود في مكان خاص lieux privé كان لها حكم هذا المكان وهنا يجب التفرقة بين ما إذا كان هذا المكان الخاص هو منزل المتهم أو أحد ملحقاته حيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم وبنفس الضمانات المقررة قانونا للتفتيش في هذا المكان، وبين ما إذا كان هذا المكان الخاص

[1]– هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 73 . وكذلك: بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط1، دار الفكر الجامعي، الإسكندرية ، 2011، ص 68 .

منزل شخص آخر غير المتهم حيث لا يجوز تفتيشها إلا في حالات تفتيش مسكن غير المتهم، وفي داخل المكان الخاص يجب التفرقة بين ما إذا كانت مكونات الحاسب منعزلة عن غير ها من الحواسيب الأخرى أو أنها متصلة بحاسب أو نهاية طرفية في مكان أخر كمسكن غير مسكن المتهم ، فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخر من شانها إماطة اللثام عن وجه الحقيقة، تعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن[1] .

وبالنسبة للأماكن العامة، سواء أكانت من الأماكن العامة بطبيعتها كالطرق والشوارع والمنتزهات، أم كانت من الأماكن العامة بالتخصيص كالمطاعم والمقاهي والسيارات العامة، فإذا وجد شخص في هذه الأماكن وهو يحمل مكونات الحاسب أو حائزا أو مسيطرا عليها، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات المقررة لتفتيش الأماكن [2].

- **المكونات المادية للأجهزة التقنية المحمولة كالحاسب المحمول**

تخضع لقواعد تفتيش الأشخاص، مع مراعاة إذا كان هذا الشخص هو شخص المتهم أو شخص غير المتهم، إذ يجب مراعاة كل حالة مع مراعاة أحكام المواد 45 و 47 من قانون الإجراءات الجزائية، كما يجب التفرقة أيضا ما إذا كانت المكونات المادية لهذه الأجهزة متصلة بنهاية طرفية موجودة مع شخص أخر حيث تخضع لقواعد تفتيش شخص غير المتهم بالنسبة لهذه النهاية الطرفية، وبين ما إذا كانت متصلة بنهاية طرفية موجودة في مكان أخر حيث تخضع لقواعد تفتيش الأماكن بالنسبة لهذه النهاية الطرفية [3]، ويخضع تفتيش الأشخاص كإجراء تحقيق لذات أحكام تفتيش الأماكن، فهو في الحالتين بحث عن الحقيقة ، ولكنهما يختلفان من حيث الهدف إذ يرى كل من ميرل وفيثو أن هدف التفتيش باعتباره إجراء من

---

[1]– هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي، المرجع السابق، ص 73 .

[2] – المرجع نفسه، ص 74 .

[3]– بكري يوسف بكرى، المرجع السابق، ص 70 .

إجراءات التحقيق إلى جمع الأدلة عن جريمة ونسبتها إلى المتهم، وبذلك يختلف عن تفتيش الشخص الذي يتم لتجريده مما يحمل من أسلحة أو أدوات قد يعتدي بها على نفسه أو على الآخرين أو يستخدمها للفرار بعد القبض عليه، وهو ما يكون عند القبض على الشخص بناء على أمر إحضار أو عند إيداعه السجن تنفيذا لحكم جزائي أو تنفيذ لأمر إيداع، ويعد هذا التفتيش مجرد إجراء وقائي وليس إجراء تحقيق ، لذلك فان تفتيش الشخص يتميز عن تفتيش المسكن بأنه قد يكون وقائيا [1].

2.مدى خضوع المكونات المعنوية للتفتيش (نظام الحاسب)

اختلف الفقه بشأن التفتيش عن البيانات الموجودة في إطار غير مادي، كالتي يتم استدعائها بواسطة شبكة الانترنت أو البريد الالكتروني والمواقع الالكترونية.

فلقد ذهب البعض إلى أن التفتيش يشمل جميع الأدلة المادية الضرورية للتحقيق فلا يمتد إلى للبيانات والمعلومات الموجودة في حاملات بيانات مادية كالملفات والحقول وبرامج النظام وبرامج التطبيقات أو في الذاكرة الداخلية، لكن الصعوبة تثور في حالة البيانات غير المحسوسة كتلك المخزنة في وحدة معالجة مركزية يرتبط بها الحاسب لا يجوز لسلطة التحقيق التفتيش عن المعلومات في هذا النظام لما فيه من مساس بحقوق الغير في النظام الأخر محل التفتيش ويتم التغلب على هذه الصعوبة بمطالبة حائز البيانات المطلوب الإطلاع عليها بتقديمها إلى جهات التحقيق عند طلبها، وفي حالة رفضه يكون قد أخل بالتزام التعاون مع سلطة التحقيق.

بينما ذهب جانب آخر من الفقه إلى أن التفتيش يمتد ليشمل كل البيانات المحسوسة وغير المحسوسة كالسجلات الإلكترومغناطيسية التي تتميز بطبيعتها غير المرئية le caractère invisible، التي ينبغي تحويلها إلى سجلات مرئية عن طريق وحدات الإخراج الخاصة بالحاسب أو غيره من الوسائل الحديثة التي تتميز بهذه الميزة حتى يمكن تفتيشها، وقد أخذ الفقه

[1]– أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2 ، ط5 ، ديوان المطبوعات الجامعية ، الجزائر، 2010 ، ص 242 .

في كل من فرنسا وانجلترا وأمريكا واليابان بهذا الرأي [1]، والباحث من هذا الرأي لأن سرعة انتقال البيانات والمعلومات المطلوب التفتيش عنها من جهاز المتهم إلى نظام أخر تستدعى تتبعها لأجل ضبطها في أنظمة أخرى بنفس السرعة التي تمت انتقالها من حاسب المتهم إلى نهاية طرفية في مكان أخر.

وفي هذه الصورة يمكن التفرقة بين الفروض الثلاثة التالية:

- **الفرض الأول: اتصال حاسب المتهم بحساب أو نهاية طرفية موجودة في مكان آخر داخل الدولة**

وهذه الحالة تطرق إليها المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 09- 04 ضمن المادة 05 فقرة 01 في الحالة المنصوص عليها في الفقرة أ من المادة المتعلقة بتفتيش نظام الحاسب إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، والمقابلة لنص المادة 75 فقرة 01 من قانون الإجراءات الجزائية الفرنسي المضافة بالقانون 02 – 239، الذي أجاز للضبطية القضائية التفتيش عن المعلومات في الأماكن التي يجرى فيها التحقيق التي كانت مخزنة في نظام معلوماتي أخر طالما أن هذه المعلومات قد توصل إليها من النظام الأساسي أو متاح الوصول إليها بواسطة هذا النظام [2].

ومن التشريعات أيضا التي تبنت امتداد التفتيش صراحة قانون جرائم الحاسب في هولندا الذي ينص على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة في موقع آخر شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة، كما أثير تساؤل في ألمانيا

[1]– بكري يوسف بكري، المرجع السابق، ص ص 71 – 72 .

[2]– المرجع نفسه، ص 72 .

يتعلق بمدى إمكانية تمديد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، ويرى الفقه هناك أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر، استنادا لمقتضيات المادة 104، وذلك عندما يكون مكان التخزين الفعلي خارج المكان الذي يتم فيه التفتيش[1].

- **الفرض الثاني: اتصال حاسب المتهم بحساب أو نهاية طرفية موجودة في مكان آخر داخل الدولة**

وهذه الحالة نص عليها المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 09 – 04 ضمن المادة 05 فقرة 02 بنصها "إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

ونصت في الفقرة 03 من نفس المادة أنه" يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

ولقد أثار الفقيه الألماني Sieber Ulrich في تقريره المقدم لمؤتمر aidp قيام مرتكبي الجرائم بتخزين بياناتهم في تقنية أنظمة المعلومات خارج الدولة، عن طريق شبكة الاتصالات البعدية بهدف عرقلة التحقيقات، ولمواجهة ذلك ذهبت بعض النظم القانونية ومنها التشريع الجزائري في نص المادة 05 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقانون

---

(1) - mohrenshlager manfred , computer crimes and other crimes against in formation technologie in Germany , ridp, 1993 , p 351.

نقلا عن: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص77 .

جريمة الحاسب الهولندي التي أجازت لجهات التحقيق بإجراء التفتيش داخل الأماكن بما يضمن تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دولة أخرى [1].

ويتحفظ بعض الفقه منهم الفقيه الألماني Mohrenshlager Manfred على التفتيش نظام الحاسب الموجود في دولة أجنبية، مسببا ذلك بأن السماح باسترجاع البيانات التي تم تخزينها بالخارج وخاصة عندما يكون الاسترجاع مرتبطا بالوضع القائم لحساب في بنك مشكوك فيه، وأنه في غياب الاتفاق الخاص بالدول المعنية قد يعتبر ذلك خرقا لسيادة الدولة الأجنبية، وخرقا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية [2]، وهذا ما تداركه المشرع الجزائري في المادة 05 فقرة 02 من قانون الوقاية من تكنولوجيات الإعلام والاتصال 09 – 04، التي نصت "بأنه من أجل الحصول على المعلومات والبيانات في دولة أجنبية فإنه يكون ذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

د. الضوابط الشكلية لتفتيش نظم الحاسب الآلي

نظرا لخطورة إجراء التفتيش وما يمكن أن يترتب عنه من بطلان الإجراءات في حالة عدم احترام الضوابط الشكلية، ومساسه بالحياة الخاصة للأفراد، فقد كفله المشرع الإجرائي بمجموعة من الضمانات الشكلية واجب إتباعها من القائم بالتفتيش، أولها الإذن بالتفتيش، توقيت التفتيش والحضور الحضوري لبعض الأشخاص، تحرير محضر التفتيش، أسلوب تنفيذ التفتيش.

1. الإذن بالتفتيش في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

لايجوز لضابط الشرطة القضائية حسب المادة 44 الفقرة 01 من قانون الإجراءات الجزائية مباشرة التفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب

---

(1) -Sieber Ulrich, computer crimes and other crimes against in formation technology in germany, commentary and preparatory questions for the colloquim of the aidp in wurzburg ridp 1993 p77.
نقلا عن: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 78 .

(2) – هلالي عبد اللاه أحمد، المرجع نفسه ، ص 79 .

الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش، ولقد اشترطت نفس المادة أن يتضمن الإذن بالتفتيش مجموعة من الشروط وهي:

– أن يتضمن الإذن بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها وذلك تحت طائلة البطلان.

– تنجز هذه العمليات تحت الإشراف المباشر للقاضي التي أذن بها، وإذا اكتشفت أثنائها جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا في بطلان الإجراءات العارضة.

هذا فيما تعلق بالإذن بتفتيش المساكن في الجرائم بوجه عام، أما في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني فلقد ناقش الفقه في الولايات المتحدة الأمريكية المشاكل العملية المتعلقة بجرائم الحاسب والإجراءات الجزائية وخصوصا أن قيام القاضي بالتفتيش يفترض أن يكون ملما ببعض الجوانب التقنية للحاسب الآلي واستخداماته وحتى لا يكون قراره مشوبا بالبطلان وحتى لا تكون القرارات القضائية وسيلة للتسلط والاستبداد، لذا يفترض عند إصدار ادن بالتفتيش أن يكون الهدف منه محددا تحديدا دقيقا وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية بحيث لا يترك أي شيء للسلطة التقديرية للشرطة الذين يقومون بتنفيذ الأمر، وينبغي أن يكون القاضي ملما بالظروف المحيطة بطلب التفتيش ومدى مصداقية مخبر الشرطة الذي أمدها بالمعلومات، وقد جرى القضاء الأمريكي على استبعاد الأدلة الناتجة عن تفتيش باطل نتيجة لأخطاء متعلقة بالمعلومات الموجودة على قواعد بيانات أجهزة الحاسب والتي تم الاستناد عليها لإصدار أمر التفتيش[1].

2.التوقيت و الحضور الضروري لبعض الأشخاص أثناء إجراء تفتيش نظم الحاسب

تستوجب التشريعات الجزائية حضور بعض الأشخاص عند مباشرة التفتيش، وهو ما سار عليه التشريع الإجرائي الجزائري، فإذا حصل التفتيش في مسكن المتهم فقد نصت المادة 82

[1] – مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، المرجع السابق، ص 73 .

من قانون الإجراءات الجزائية على قاضي التحقيق أن يلتزم في الجنح بأحكام المواد 45 إلى 47 من قانون الإجراءات الجزائية، بحيث وضحت المادة 45 فقرة 01 و 02 بأنه إذا وقع التفتيش في مسكن شخص يشتبه في أنه يساهم في ارتكاب الجناية فيجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثلا له وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته، أما إذا وقع التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش وإن تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة.

أما إذا كان التفتيش في غير مسكن المتهم أستدعى صاحب المنزل الذي يجرى تفتيشه ليكون حاضرا وقت التفتيش فإذا كان ذلك الشخص غائبا أو رفض الحضور أجري التفتيش بحضور اثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش فإن لم يوجد أحد منهم فبحضور شاهدين لا يكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية، مع مراعاة أحكام المادتين 45 و 47 من قانون الإجراءات الجزائية.

وفيما تعلق بميقات التفتيش فوضحت المادة 47 من قانون الإجراءات الجزائية بأنه لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا إلا إذا طلب صاحب المنزل ذلك أو وجدت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا.

مع أنه لا تطبق أحكام المادة 45 و 47 من قانون الإجراءات الجزائية إذا كان المتهم متابع بجريمة المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني، وذلك حسب الفقرة 07 من المادة 45 ، والمادة 47 فقرة 03 من قانون الإجراءات الجزائية.

3.محضر تفتيش نظم الحاسب الآلي

التفتيش عمل من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاضا في محضر التفتيش سوى ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره، وتوقيع محرره، وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها، أما فيما تعلق بمحضر تفتيش نظم الحاسب الآلي فإنه يتطلب بالإضافة إلى الشكليات السابقة إحاطة قاضي التحقيق بتقنية المعلومات، وينبغي أن يكون هناك شخص متخصص في الحاسب يرافقه للاستعانة به في مجال الخبرة الفنية الضرورية، لأنه سوف يساعده في صياغة محضر التفتيش بتغطية كل الجوانب التقنية في عملية التفتيش والضبط، مع المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح [1].

4.أسلوب تنفيذ التفتيش

أسلوب تنفيذ التفتيش يخضع للسلطة التقديرية للقائم به، إلا أن يرد عليها قيدا هاما يتعلق بتفتيش الأنثى، التي تقتضي أن يكون تفتيش الأنثى بواسطة أنثى كونها قاعدة يقتضيها الحياء العام وتمليها ضرورة حماية الآداب العامة، ولذا فهي قاعدة من النظام العام، ولا يتحقق لهذه القاعدة موجبها إلا عندما يكون محل التفتيش من المواضيع الجسمانية للمرأة التي لا يجوز لضباط الشرطة القضائية وقاضي التحقيق الاطلاع عليها ومشاهدتها وهي عورائها التي تخدش حياءها إذا مست، وتعترف الكثير من القوانين بقاعدة تفتيش الأنثى كالقانون الأمريكي بل إن إدارات الشرطة تستخدم عددا من النساء يصاحبن رجال الشرطة في حالات تفتيش النساء وقت القبض عليهن [2]، أما في التشريع الجزائري فإنه لم ينص قانون الإجراءات الجزائية على تفتيش الأنثى إلا أنه من الناحية العملية فيتم تفتيش الأنثى بواسطة أنثى حماية للآداب العامة.

---

[1] – هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص ص 169 – 170 .

[2] – المرجع نفسه، ص173 .

الفرع الثالث: ضبط الأدلة الالكترونية

لكي يحقق التفتيش غايته في جمع الأدلة على الجريمة التي ارتكبت فلابد من وسيلة بموجبها يتم وضع اليد على شيء يتصل بها ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهذه الوسيلة تتمثل في الضبط والتي عن طريقها يتم الوصول إلى الأدلة التي تهدف إليها إجراءات الإثبات الجنائي، لذلك سنتطرق إلى مفهوم الضبط في جرائم التوقيع الالكتروني، ثم أنواع الضبط في جرائم التوقيع الالكتروني .

أولا: مفهوم الضبط في جرائم التوقيع الالكتروني

يقصد بضبط الأشياء بوجه عام أن تقوم سلطة التحقيق بوضع يدها على كافة الأشياء المتعلقة بالجريمة والتي تفيد في كشف حقيقة الجرم الواقع أو في إثبات أو نفي التهمة في مواجهة المتهم، ويستوي أن تكون الأشياء المضبوطة مملوكة للمتهم أو لغيره، كما لا يهم طبيعتها أو نوعها سواء أكانت منقولا أو عقارا، وسواء كانت من وسائل الجريمة أو متحصل عنها [1] .

والضبط بالنسبة لجرائم التوقيع الالكتروني التي تقع على الوسائل الإلكترونية أو عن طريقها يشتمل على كل ما استعمل في ارتكابها أو أعد لهذا الغرض كأجهزة نسخ وتسجيل برامج الحاسب الآلي، أجهزة الربط مع الشبكات الإلكترونية، أجهزة اختراق الاتصالات وتحليل الشفرات وكلمات السر، كافة البرامج المقلدة والمنسوخة، المحررات الإلكترونية، التوقيعات الإلكترونية المزورة والملفات المعنوية التي تعد وسيلة لارتكاب الجريمة، والضبط هنا يقصد به الضبط القضائي والذي يستهدف الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة، والضبط قد يقع على مكونات الوسائل الإلكترونية، وقد يكون محله أيضا المراسلات الإلكترونية[2].

---

[1] – جلال ثروت، سليمان عبد المنعم، المرجع السابق، ص497 .

[2]– أشرف قنديل ، المرجع السابق، ص ص 60 – 61 .

والمواد المراد ضبطها قد لا تكون على الأجهزة المضبوطة، فقد تكون على جهاز غير موجود بمكان مسرح الجريمة، ويقوم العاملون بتشغيله فقط من المكان محل التفتيش، وقد تكون البيانات على ذات الأجهزة ولكنها مشفرة ولا يعرف فك الشفرة سوى شخص أو أكثر من العاملين فيثور التساؤل عن مدى مشروعية إجباره على فك الشفرة، أو قد تكون المعلومات مشفرة ولكن يتمكن أحد العاملين من محو البيانات الموجودة على الجهاز أو الأجهزة بمجرد العلم بإجراء التفتيش[1].

ثانيا: محل الضبط في الوسائل الالكترونية الحديثة

يتنوع ضبط الوسائل الالكترونية بحسب الوسيلة المراد ضبطها إذا ما كانت من الوسائل المادية أو المعنوية، وهناك أيضا بما يسمى بضبط المراسلات الالكترونية والبريد الالكتروني.

أ. ضبط الكيانات المادية والمعنوية في الوسائل الإلكترونية

المكونات المادية للحاسب الآلي لا يثير ضبطها أي إشكال فيمكن ضبط الوحدات المعلوماتية الآتية، مثل وحدة المدخلات بما تشمله من المفردات كلوحة المفاتيح وشاشة اللمس، نظم الإدخال المرئي، نظام الإدخال الصوتي، نظام الفأرة، نظام القلم الضوئي، نظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات، ويمكن أيضا ضبط وحدة الذاكرة المركزية سواء أكانت ذاكرة للقراءة فقط والكتابة معا، وضبط وحدة الحساب والمنطق بما تشمله من دائرة إلكترونية ومسجلات، وضبط وحدة التحكم وضبط وحدة المخرجات وما تشمل عليه من وسائل كالشاشة الطابعة والرسم والمصغرات الفيلمية وضبط وحدات التخزين الثانوية بما تشمل عليه من أقراص مغناطيسية بنوعيها المرن والصلب والأشرطة المغناطيسية [2].

---

[1] – مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، المرجع السابق، ص 71 .

[2] – هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 198 .

ويلاحظ كذلك أنه يمكن ضبط كافة الأدوات والمستندات التي تكون قد استعملت أو تحصلت من الجرائم التي تقع على العمليات الإلكترونية، فيمكن ضبط الأوراق المالية المزورة وقد تضبط هذه الأوراق بداخل الحاسبات الآلية أو تضبط أدواتها بداخل نظم الحاسب، ويمكن أيضا ضبط التوقيعات الالكترونية في المحررات الإلكترونية المزورة كمخرجات أو بيانات داخل ذاكرة الحاسب أو داخل أنظمة الصراف الآلي طبقا لما هو مسجل من بيانات داخل هذه الأنظمة[1].

أما بالنسبة للكيانات المعنوية فيمكن ضبطها وحجزها حسب نص المادة 06 من قانون الوقاية من تكنولوجيات الإعلام والاتصال لسنة 2009 التي نصت على أنه" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، إذ يتم نسخ المعطيات محل البحث، وكذا اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع تحت أحراز".

وقد أثير ضبط الكيانات المعنوية للحاسب خلافا بين الفقه، فهناك من يرى بأنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البيانات الالكترونية، بمشتملاتها من ملفات وسجلات وحقول سواء اتخذت برامج نظام أو برامج تطبيقات[2].

فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي تستهدف الوصول إليها فإن المعالجة التي تجرى عليها لجعلها مرئية للإطلاع عليها وإثباتها أو بإخراجها من الحاسب بصورة مستندات مطبوعة لا تعد تفتيشا عن أدلة الجريمة ولكنها تمثل وصولا إلى هذه الأدلة، ومن ثَمَ تعد ضبطا لها، وتجدر الإشارة إلى أن ضبط الأدلة المتحصلة من الوسائل الإلكترونية قد تكتنفه الصعوبة البالغة عندما يكون متعلقا بنظام آلي بأكمله إذ أن هذا الأمر يحتاج إلى

---

[1]– أشرف قنديل، المرجع السابق، ص 63 .

[2] – هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص ص 199 – 200 .

تعاون دولي لأجل إتمام هذا الضبط دون إعاقة سير النظام المعلوماتي[1]، لذلك قد يصادف ضبط الأنظمة المعلوماتية صعوبتان، الأولى وهي أن الضبط سيؤدي إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر مما قد يتسبب عنه أضرار بالجهة مستخدمة النظام، أما الثانية فهي عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق مما يعني لها الضبط بأنه مساس بحقوق الغير [2].

ومن التشريعات التي تجيز ضبط أي شيء منها المكونات المعنوية للوسائل الالكترونية نجد التشريع اليوناني الذي يجيز في المادة 201 من قانون الإجراءات الجزائية التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، ويفسر الفقه اليوناني عبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة الكترونيا، لذلك فإن ضبط البيانات المخزنة في حاملات البيانات المادية أو في الذاكرة الداخلية لا تسبب أي مشكلة في اليونان، إذ يجوز للمحقق أن يعطي أمرا للخبير بجمع البيانات التي تكون مقبولة كدليل في المحاكمة الجزائية، كما تجيز أيضا المادة 260 من قانون الإجراءات الجزائية استخدام القوة القسرية أثناء ضبط المستندات المتعلقة بالجريمة في حالات البنوك أو المؤسسات الخاصة والعامة، ولهذا فإن المحققين بمقدورهم أن يأخذوا البيانات المخزنة في حاملات البيانات، وفي كندا تجيز المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط "أي شيء" طالما تتوافر أسس معقولة للاعتقاد بأن الجرم ارتكب أو يشتبه في ارتكابه أو أنه سينتج دليلا على وقوع الجرم [3].

وبالتالي نلاحظ أن هناك تشريعات نصت صراحة على جواز ضبط وتفتيش نظم الحاسب الآلي والبيانات الالكترونية كالتشريع الجزائري، وهناك تشريعات توسعت في مفهوم ضبط

---

[1]– أشرف قنديل، المرجع السابق، ص ص 62 – 63 .

[2] – عفيفي كامل عفيفي، فتوح عبد الله الشادلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون– دراسة مقارنة، منشورات الحلبي الحقوقية ،بيروت، 2007، ص 354 .

[3] – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 200 .

الأشياء لتشمل أيضا أنظمة الحاسب الآلي والبيانات المخزنة الكترونيا، ونؤيد من وجهة نظرنا جواز ضبط الكيانات المعنوية للحاسب الآلي.

ب.ضبط المراسلات الإلكترونية

الحماية التي يكفلها المشرع للمراسلات العادية لا يقتصر نطاقها على الصور المختلفة لهذه المراسلات، وإنما منطق القول يحتم امتداد هذه الحماية إلى المراسلات الإلكترونية من باب أولى بحسبان أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، وهذه الأسرار الشخصية تكون أكثر انتهاكا إذا ما استخدمت الوسائل الإلكترونية في الوصول إليها، ومن ثمَ فإنها تكون في حاجة إلى حماية أكثر من تلك التي تحتاجها المراسلات في صورتها التقليدية[1] .

فالمراسلات الالكترونية ما هي إلا مراسلات ذات صبغة تقليدية من ناحية المضمون، ولا تختلف عن المراسلات العادية إلا من حيث الوسيلة التي تستخدم لنقلها، في حين أن المراسلات التقليدية تتم عبر البريد العادي فإن المراسلات الالكترونية تتم عبر الهاتف المحمول أو الحاسب الآلي المربوط بشبكة الانترنيت حيث يخصص لكل شخص موقع الكتروني le courrier box électronique وهذا الموقع عبارة عن ملف يستخدم لاستقبال الرسائل les messages بواسطة معالج الرسائل le messagerie وعندما يريد أي مستخدم الحصول على الرسائل الخاصة به فإنه يستدعيها باستخدام أي وصلة طرفية بالانترنيت أو بإرسال رسائل إلى أي مكان في العالم باستخدام خطوط التيلفون أو الموجات اللاسلكية أو الأقمار الصناعية [2].

لذلك على المشرع أن يضمن ضبط المراسلات الالكترونية بالضمانات المقررة في الدستور وفي قانون العقوبات والإجراءات الجزائية، لمساسها بالخصوصية الفردية وبالحياة الخاصة

[1] – أشرف قنديل، المرجع السابق، ص 65 .

[2] – بكري يوسف بكري، المرجع السابق، ص 138 .

للأفراد التي لا يجوز الاطلاع عليها إلا بإذن من السلطات القضائية وبالضمانات المقررة قانونا.

ج. ضبط مراسلات البريد الإلكتروني

يعد البريد الالكتروني من الخدمات المهمة التي تقدمها شبكات المعلومات حتى أنه أصبح واحدا من أكثر وسائل الاتصال شيوعا وهو شكل من أشكال الاتصال الالكتروني يسمح للأفراد بتبادل الرسائل بشكل فوري من خلال شبكات المعلومات التي تعرف مجتمعة بالانترنت[1]، أو بمعنى آخر يقصد بالبريد الإلكتروني استخدام شبكات الانترنت لنقل الرسائل بدلا من الوسائل التقليدية وبالنظر إلى سهولة استخدامه فقد أصبح من أكثر وسائل الانترنت شيوعا واستخداما في الوقت الحالي.

وقد عرف القانون الأمريكي بشأن خصوصية الاتصالات الالكترونية الصادر سنة 1986 البريد الالكتروني بأنه " وسيلة اتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية خاصة أو عامة، وغالبا يتم كتابة الرسالة يتم إرسالها الكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه حيث يتم إرسالها عبر نظام خطوط التليفون إلى كمبيوتر المرسل إليه.

وعرفه القانون الفرنسي بشأن الثقة في الاقتصاد الرقمي الصادر في 22 جويلية 2004 بأنه " كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صوت أو أصوات ويتم ارسالها عبر شبكة اتصالات عامة، وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها " [2].

ولعل من المسائل الهامة التي تتعلق بالبريد الإلكتروني وجوب المحافظة على سريته، وهو ما حدا بالمبتكرين لبرامجه بابتكار برامج تشفير خاصة به بحيث لا يمكن الاطلاع الرسالة إلا

---

[1] – نائلة قورة، المرجع السابق، ص 44 ,

[2] – هذه التعاريف واردة في : خالد ممدوح ابراهيم، حجية البريد الالكتروني في الاثبات، المرجع السابق، ص 43 .

لمن يعرف هذه الشفرة، ويمكن حفظ البريد الإلكتروني في صناديق بريد خاصة أو في ملف أو نسخ الرسالة والاحتفاظ بها، ولقد ساعد ظهور التوقيع الإلكتروني في تسيير عملية التراسل عبر البريد الإلكتروني، فالبرنامج يقوم بتخزين توقيع المستخدم كرمز أو شفرة ويضعه تلقائيا على كل رسالة، وأشهر هذه البرامج التشفيرية البرنامج المعروف باسم البريد بالغ السرية privacy enhaned mail (pem) ، وبرنامج سري جدا pretty good privacy ، وهي أكثر برامج تشفير البريد شيوعا في الولايات المتحدة الأمريكية وأروبا [1].

وإذا كان مفهوم المحررات قد تغير اليوم فقد حلت المحررات الالكترونية أو الرقمية محل الكثير من الوثاق المطبوعة على الورق، فإن الرسائل الإلكترونية تعد محررات، فالمحرر أصبح مفهومه يتفق مع ثورة الاتصالات عن بعد و أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو إلكترونية، فالعالم يعيش اليوم عصر الثورة الرقمية حيث صارت الكلمة والصوت والأشعة والصورة والمعلومات رقمية، ولقد تمَ الاعتراف بها من قبل الكثير من التشريعات وبحجيتها في الإثبات وأنها تصلح من أن تكون محلا يقع عليه التزوير، فإذا كان محتوى المحرر قد أصبح يعبر عنه بلغة رقمية، فإن هذه اللغة هي التي حلَت محل الكتابة، ومن ثمَ يصلح هذا المحرر الرقمي لتقوم به جريمة التزوير، وطالما أيضا المحرر الالكتروني يعبر على فكرة وكان بالإمكان قراءتها وإدراك معناها وفهم مضمونها فإنه يعد محررا ومن ثمَ فإنه يحوز الحجية وفقا لطبيعة الشخص المنسوب إليه الإصدار ولمن وضع عليه توقيعه الإلكتروني[2].

ويترتب على اعتبار الرسائل الإلكترونية التي تتم عن طريق البريد الإلكتروني بمثابة رسائل شخصية أنه يجب حمايتها بذات الحماية التي تتمتع بها المراسلات الورقية ومن ثمَ فلا يجوز التصنت عليها أو الإطلاع على الأسرار التي تحويها إلا بذات الطرق التي تنص عليها قوانين الإجراءات الجزائية فلا يستطيع المحقق اختراق صندوق البريد الإلكتروني أو الدخول إلى أنظمة

---

[1] – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص 213 .

[2]– أشرف قنديل، المرجع السابق، ص ص 66 – 67 .

الحاسب الآلي المخزنة بها الرسائل البريدية الالكترونية وضبطها إلا عن طريق إتباع الإجراءات المنصوص عليها في القوانين الإجرائية [1].

وفيما تعلق بحفظ البريد الالكتروني فهي تماثل بطريقة حفظ البريد العادي بأحد الطرق التالية:

- الحفظ في صناديق بريد خاصة .
- الحفظ في ملفات .
- طباعة الرسائل وحفظها في ملفات خاصة مع البريد الورقي التقليدي.

وأسهل هذه الطرق عادة هي حفظ الرسائل في أحد صناديق البريد الذي هو عبارة عن ملف مليء بالرسائل التي يفصل بين كل منها حاجز خاص ، والمصنفة وفقا للموضوع أو المرسل، ليقوم برنامج البريد الالكتروني عادة بمساعدة المستخدم في تصنيف الرسائل على أساس المرسل وعنوانه [2].

أما عن طريقة ضبط البريد الالكتروني، فعلى قاضي التحقيق الدخول إلى صندوق البريد الخاص بالمتهم في جريمة التوقيع الالكتروني بطريقتين، تتمثل الأولى في أن المتهم يعطي عنوان بريده الالكتروني ورقمه السري لقاضي التحقيق لأجل الدخول، أما الطريقة الثانية فهي الولوج إلى بريده الالكتروني عن طريق تشفير رقمه السري، ثم يذهب إلى قائمة البرنامج الرئيسية للبريد الالكتروني، فتظهر القائمة بها خيارات الصادر، الوارد، الحفظ، المهملات، فيدخل للرسائل الواردة التي استقبلها المتهم، أو اختياره للرسائل الصادرة والتي أرسلها المتهم، أو مجموعة الرسائل التي كتبها المتهم ثم قام بحفظها، أو باسترجاع الرسائل التي قام المتهم بمحوها من قائمة سلة المهملات [3].

---

[1]– أشرف قنديل، المرجع السابق، ص 67 .

[2] – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 214 .

[3] – المرجع نفسه، ص 216 .

وتحرص غالبية الدساتير ومنها الدستور الجزائري على كفالة ضمانة سرية المراسلات بوجه عام، لتشمل أيضا سرية المراسلات الالكترونية ومراسلات البريد الالكتروني التي تعد من المسائل الشخصية للفرد التي لا يجوز للغير الاطلاع عليها إلا بإرادته، نتيجة لما أفرزته التكنولوجيا الحديثة من انتشار واسع في المعاملات التي تقع في وسط إلكتروني، كالرسائل المتبادلة عبر البريد الالكتروني عبر شبكة الانترنت ما يقتضي حمايتها في الدستور، وبضمانات أثناء ضبطها من السلطات القضائية تنص عليها سواء في قانون العقوبات أو قانون الإجراءات الجزائية.

الفرع الرابع : الخبرة في الجرائم الواقعة على التوقيع الالكتروني

أصحاب الجبة السوداء (القضاة)، بحاجة إلى أصحاب الزى الأبيض (الخبراء في المسائل العلمية والتقنية)، لاستكمال مهامهم القضائية[1]، فقاضي التحقيق عندما يحقق في جريمة واقعة على التوقيع الالكتروني أجازت له المادة 143 من قانون الإجراءات الجزائية أن يأمر بندب خبير بناء على طلب النيابة العامة وإما من تلقاء نفسه أو من الخصوم في المسائل العلمية والتقنية التي لا يكون القاضي ملما أو على دراية بها، لذلك سنتطرق إلى تعريف الخبرة في الجرائم الالكترونية الواقعة على التوقيع الالكتروني، ثم إلى شروط الخبير، مجالات الخبرة، أساليب تنفيذها، الهدف منها، دور الخبير في حفظ الدليل الالكتروني.

أولا: تعريف الخبرة

الخبرة هي وسيلة لكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو الأدلة أو تحديد قيمتها الثبوتية في الإثبات ومن هنا كانت الخبرة وقفا على الأخصائيين من أهل العلم والتكنولوجيا فهم يدلون بخبرتهم من واقع معلوماتهم العلمية لا بناء على مجرد مشاهداتهم أو سماعهم، ولدا جاز استبدال الخبير في

[1]- Carolie ambroise, casterot, op – cit, p 251.

الدعوى بغيره من الخبراء وهو أمر غير متصور للشاهد لأن دوره في الدعوى قاصر عليه وحده[1]، أو هي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى لإثبات كفحص بصمات عثر عليها بمكان الحادث أو مدى نسبة توقيع معين إلى شخص بعينه أو تحديث سبب الوفاة في جريمة القتل، ولأجل الوقوف على الحقيقة في مثل هذه المشاكل العلمية والفنية فإن المحقق أجاز له القانون أن يستعين بخبير متخصص في المسألة موضوع الخبرة ويعد ندب المحقق للخبير إجراء من إجراءات التحقيق يقطع التقادم وذات الشأن بالنسبة لإيداع تقارير الخبرة، لكن أعمال الخبرة ذاتها لا أثر لها على التقادم لأنها أعمال مادية[2] .

وإذا ولينا وجهنا شطر ثورة الاتصالات عن بعد نجد أنها قد أتت بتقنيات علمية ذات طبيعة فنية متقدمة، وقد أفرزت هذه التقنيات جرائم ذات طبيعة علمية وفنية معقدة كالجرائم الالكترونية الواقعة على التوقيع الالكتروني، يحتاج جمع الدليل بالنسبة لها إلى بحث مسائل علمية وفنية، فالأدلة قد تكون غير مرئية ويلزم تحويلها إلى أدلة مقروءة، وقد تكون نتيجة تلاعب في حسابات معينة أو في نظم التوقيع الالكتروني بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب، وقد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة استخدام الشفرات و التوقيعات الالكترونية السرية، وبالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية الواقعة على التوقيع الالكتروني فإن إماطة اللثام عنها قد يحتاج في أغلب الحالات إلى خبرة فنية تظهر الحاجة إليها منذ بدأ مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[3].

---

[1]– أحمد فتحي سرور، المرجع السابق، ص 385 .

[2]– أشرف قنديل، المرجع السابق، ص 58 .

[3]– المرجع نفسه، الصفحة نفسها .

ثانيا: شروط الخبير في مجال الجرائم المرتكبة بالوسائل الإلكترونية

إذا كانت الوسائل الإلكترونية وشبكات الاتصال متنوعة، فإن طبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة، ما يستوجب من جهات التحقيق والمحاكمة أن تراعي ذلك عند اختيارها للخبير، فيجب أن تتيقن أنه تتوفر لديه الإمكانات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة وإنما يجب أن تتوفر لديه أيضا الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية، وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية [1]:

– الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر أو كود التشفير.

– طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عامل المعالجة الآلية وتحديد أماكن التخزين المستخدمة في ذلك.

– قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك عطب أو تدمير للأدلة المتحصلة من الوسائل الإلكترونية.

– التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

ثالثا: مجالات الخبرة في الجرائم الالكترونية الواقعة على التوقيع الالكتروني

تتنوع العمليات الإلكترونية باستخدام الوسائل الإلكترونية، فنجد أمثلة لها في الأعمال المصرفية وفي الإدارة الإلكترونية وفي التجارة الإلكترونية، ولذلك فإنه يتصور تنوع الجرائم التي

[1]– أشرف قنديل ، المرجع السابق، ص ص 59 – 60 .

تقع على هذه العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها وأمثلتها تزوير التوقيع الالكتروني في المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة عن بعد المعالجة، التلاعب في بيانات التوقيع الالكتروني، الغش أثناء نقل وبث بيانات التوقيع الالكتروني[1]، وقد يكون التزوير أو التلاعب في التوقيع الالكتروني الخاص ببطاقة الائتمان، أو في التوقيع الالكتروني المستعمل إذا ما كنا أمام جريمة استعمال التوقيع الالكتروني من قبل الغير، أو في أجهزة وتطبيقات وبرامج صناعة التوقيع الالكتروني.

رابعا: أساليب عمل الخبير

الخبير التقني في سبيل التحري عن الحقيقة في جرائم التوقيع الالكتروني يستخدم الأساليب العلمية التي يقوم عليها تخصصه، وهناك أسلوبان لعمل الخبير التقني:

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة الكترونية في ذاتها، كجريمة الدخول لقاعدة بيانات متعلقة بالتوقيع الالكتروني ، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسباها إلى مسارها التي أعدت فيه وتحديد عناصر حركتها وكيف التوصل إلى معرفتها ، ومعرفة برتوكول الانترنيت الذي ينسب إلى جهاز الحاسب الذي صدرت منه الجريمة.

الثاني: القيام بتجميع وتحصيل المواقع التي لا تشكل موضوعها جريمة في حد ذاتها، وإنما تؤدي حال موضوع تتبعها إلى مساعدة مرتكب الجريمة [2]، كالمواقع التي توضع كيفية اختراق برامج وتطبيقات ونظم التوقيع الالكتروني.

وهناك أسلوب أخر يتمثل في التنسيق مابين الخبير المعلوماتي وقاضي التحقيق قبل محاكمة الجاني في الجريمة المعلوماتية على أن يشمل ذلك كافة الخبراء الذين ساهموا مع سلطات الضبط القضائي في تلقي البلاغ أو إجراءات الضبط أو التفتيش وفحص البرامج وجمع

---

[1]– أشرف قنديل، المرجع السابق، ص 58 .

[2] – خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية ، المرجع السابق، ص 299 .

الأدلة الجنائية، على أن يتم اللقاء حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بينة أو قرينة، كما يجب على قاضي التحقيق أن يوضح لهؤلاء الخبراء المسائل القانونية لطبيعة عملهم[1] .

خامسا: الهدف من الخبرة

الخبرة في الجرائم المرتكبة بالوسائل الالكترونية تساعد على الوصول إلى الأهداف التالية [2]:

- الكشف عن الدليل الرقمي .

- إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة العدالة.

- تحديد الخصائص الفريدة للدليل الالكتروني .

- إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب .

- عمل نسخة أصلية من الدليل الالكتروني الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل .

- جمع الآثار المعلوماتية الرقمية التي قد تكون قد تبدلت خلال الشبكة المعلوماتية.

سادسا: دور الخبير في حفظ الأدلة الالكترونية

في إطار الجرائم الالكترونية فإنه يميز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الآلي وبين تلك التي يجب بقاؤها في العالم الافتراضي وبين أيضا تلك النوعية من الأدلة التي تنتمي إلى العالم الرقمي، ومع ذلك يمكن اللجوء إلى إخراجها من إطار الحاسوب

---

(1) – محمد الأمين البشري ، المرجع السابق ص ، وكذلك : عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق في الجرائم المعلوماتية، المرجع السابق، ص 603 .

(2) – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 302 .

والعالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة تساعد في الإدانة والبراءة لمرتكبي جرائم التوقيع الالكتروني[1].

كما أن التحفظ على الأدلة داخل جهاز الحاسب من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يجوي عليها الحاسب، ما يستلزم بالخبير التقني الكشف عن مدى صحة حركة الحاسب من حيث الخلل والعطب ويعطي العدوان الفيروسي مثالا حيويا لها ، إذ يكفي أن يكون فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستقاة منه، وقد ذهب التشريع الانجليزي في هذا الاتجاه [2].

الفرع الخامس: سماع الشهود

لقاضي التحقيق من أجل الوصول للحقيقة في جرائم التوقيع الالكتروني أجازت له المادة 88 من قانون الإجراءات الجزائية صلاحية استدعاء كل شخص يرى فائدة من سماع شهادته، وفي حالة معرفة الشاهد بوقوع اعتداء لبيانات التوقيع الالكتروني فهل هو ملزم بإعلام سلطات التحقق، هذا ما سنتطرق له من خلال فكرة الالتزام بالإعلام في الجرائم الالكترونية، وقبلها سنتناول بالدراسة مفهوم الشاهد في الجرائم الالكترونية.

أولا: مفهوم الشاهد في الجرائم المرتكبة بالوسائل الالكترونية

هناك اختلاف بين الشهود في الجرائم المرتكبة بالوسائل الالكترونية و التقليدية التي يشهد فيها الشخص عما رآه أو سمعه، أما في الجرائم الالكترونية فالشاهد قد يكون أحد الخبراء الفنيين في مجال الحاسب والمعلوماتية، فما هو الشاهد في الجرائم الالكترونية، وكيف تتم الشهادة أمام قاضي التحقيق.

---

[1]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص ص 308– 309 .

[2]– المرجع نفسه، ص 309 .

أ. تعريف الشاهد في الجرائم الالكترونية

يعرف الفقه الشهادة بأنها إدلاء الشخص أمام القضاء بعد أداء اليمين بما يكون قد رآه أو سمعه بنفسه[1]، أما الشاهد في الجرائم المعلوماتية فيقصد به الفني صاحب الخبرة في تقنية وعلوم الحاسب، والذي تكون له معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذا مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذه النوعية الجديدة من الشهود مصطلح الشاهد المعلوماتي le témoin informatique ، وذلك تمييزا له عن الشاهد التقليدي [2].

ب. طريقة تأدية الشهادة أمام قاضي التحقيق

يؤدي الشهود شهادتهم أمام قاضي التحقيق حسب المادة 90 من قانون الإجراءات الجزائية فرادى بغير حضور المتهم ويحرر محضر بأقوالهم ، ويطلب من الشهود قبل سماع شهادتهم عن الوقائع أن يذكر كل منهم اسمه ولقبه وعمره وحالته ومهنته وسكنه وتقرير ما إذا كان له قرابة أو نسب للخصوم أو ملحق بخدمتهم أو ما إذا كان فاقد للأهلية وينوه في المحضر عن هذه الأسئلة والأجوبة وفق ما نصت عليه المادة 93 من قانون الإجراءات الجزائية.

ويؤدي كل شاهد ويده اليمنى مرفوعة بالصيغة الآتية: " **أقسم بالله العظيم أن أتكلم بغير حقد ولا خوف وأن أقول كل الحق ولاشيء غير الحق**"، باستثناء تسمع شهادة القصر مادون السادسة عشر بغير حلف اليمين.

ثانيا: مفهوم فكرة التزام الشاهد بالإعلام في الجرائم المرتكبة بالوسائل الالكترونية

جوهر الالتزام بالإعلام في الجرائم المعلوماتية أنه متى كان الشاهد المعلوماتي حائزا لمعلومات جوهرية لازمة لاختراق نظم المعالجة الآلية للبيانات بحثا عن أدلة للجريمة داخله

---

[1]- Coralie Ambroise Castérot,op-cit , p 162.

[2] – هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية– دراسة مقارنة، ط2 ، دار النهضة العربية القاهرة، 2008 ، ص 23 .

تتطلبه مصلحة التحقيق فإنه يكون مطالبا بها بأن يعلم سلطات التحقيق والتحري على سبيل الالتزام، وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة، وقد طرحت الفكرة من قبل الفقيه الألماني Ulrich Sieber بتساؤله حول ما إذا كان هناك التزام قانوني على الشهود بطبع ملفات البيانات المخزنة في ذاكرة الحاسب، أو الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتفيذ البرنامج [1].

وتجدر الإشارة إلا أنه لم ينص التشريع الجزائي الجزائري على الالتزام بالإعلام في الجرائم المعلوماتية والالكترونية ولا يوجد نص يلزمه بذلك، لأن المشرع ألزم الإبلاغ عن وقوع الجنايات ورتب مسؤولية جزائية عن ذلك بالامتناع عن التبليغ عن جناية في نص المادة 181 من قانون العقوبات، كما ألزمت المادة 91 كل شخص علم بوجود مخططات أو أفعال لارتكاب الخيانة والتجسس وغيرها من الأنشطة الضارة بالدفاع الوطني وقت الحرب أو السلم ولم يبلغ عنها للسلطات الإدارية والقضائية فورا، وكذلك أيضا إلزامية التبليغ عن جرائم الفساد لكل شخص يعلم بها بحكم وظيفته أو مهنته حسب ما نصت عليه المادة 47 من قانون الوقاية من الفساد 06-01، أما في الجرائم الواقعة على التوقيع الالكتروني فكلها جنح ما يجعل عدم الإبلاغ عنها لا يشكل جريمة ولا أي التزام من الناحية القانونية في التشريع الجزائري.

وفيما تعلق بمضمون الالتزام بالإعلام الذي يجب على الشاهد المعلوماتي أن يسدي به إلى سلطات التحقيق، هو ما يحوزه من معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات تنقيبا عن أدلة الجريمة بداخله، كما يراعى الشاهد المعلوماتي في إعلامه أن يكون بسيطا، مفهوما، محددا، دقيقا، صادقا أمينا، ويحتوي على عناصر جوهرية تتمثل في:

العنصر الأول: طبع ملفات البيانات المخزنة في ذاكرة الحاسب أو حاملاتها ويقوم بتسليمها لسلطات التحقيق.

[1] – هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية– المرجع السابق، ص26 .

العنصر الثاني: الإفصاح عن كلمات المرور السرية، يستلزم هذا العنصر أن يعلم الشاهد المعلوماتي سلطات التحقيق بكلمة المرور السرية، والتي في حقيقة الأمر ما هي إلا وسيلة لتأمين نظام الحاسب بواسطة شخص غير مسئول قد يسبب في فقد بيانات مهمة، لأن كلمات المرور لاتقتصر معرفتها إلا على الأشخاص المسئولين، وفي نظم المعلومات الكبيرة يتم تصميم كلمات المرور لمستويات الإدارة المختلفة تمكن المدراء من التعامل مع بعض البيانات دون سواهم [1]، وفي جرائم التوقيع الالكتروني قد نكون أمام جريمة اعتداء على الرقم السري بذاته من خلال جريمة الاعتداء على التوقيع الالكتروني الكودي أو السري في بطاقات الائتمان بحيث تكون سلطات التحقيق في حاجة لمعرفة هذا الرقم السري، كما أن كشف الشاهد لسلطات التحقيق للرقم السري يفيد في رفع اللبس عن ملابسات جريمة الاعتداء على نظام المعالجة الآلية للتوقيع الالكتروني، وذلك بمساعدة المسئولين عن هذا النظام.

أما شروط التزام الشاهد بالإعلام في الجرائم المعلوماتية فهناك ثلاثة شروط أساسية هي [2]:

الشرط الأول: أن نكون بصدد جريمة معلوماتية ارتكبت بالفعل، فلا يجوز لضبط جريمة مستقبلا ولو قامت التحريات على الكشف عن جريمة معلوماتية ستقع في المستقبل، ولا يكفي وقوع الجريمة بالفعل بل لابد وأن يكون التكييف القانوني لها جناية أو جنحة .

الشرط الثاني: معرفة الشاهد المعلوماتي بمضمون المعلومات الجوهري المتصلة بالنظام المعلوماتي محل الواقعة تمثل شرطا هاما لنشأة وميلاد الالتزام بالإعلام في الجرائم المعلوماتية، ويتمثل مضمون هذه البيانات في ثلاث عناصر تتمثل في ملف البيانات والإفصاح عن كلمة السر والكشف عن مفاتيح الشفرات .

---

[1]– هلالي عبد اللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص ص 60 – 61 .

[2]– المرجع نفسه، ص 67 – 68 .

الشرط الثالث: أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية، ينبغي ضرورة أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية، خاصة إذا كان الأمر يتطلب اختراق نظام التوقيع الالكتروني بحثا عن أدلة للجريمة الكائنة بداخله.

المطلب الثاني: الآليات الدولية في مجال التحقيق الابتدائي القضائي

إن البعد الدولي للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني يستدعي ضرورة وجود تعاون دولي لتفادي العقبات الإجرائية، ومن أجل خلق هذا التعاون القضائي الدولي بين أجهزة التحقيق الابتدائي من مختلف الدول لابد من صيغة أو آلية تستند إليها الدولة أهمها الاتفاقيات الدولية، والمعاملة بالمثل، والإنابة القضائية الدولية.

الفرع الأول: الاتفاقيات الدولية

هناك العديد من الاتفاقيات الدولية المبرمة في مجال مكافحة الجريمة الالكترونية، من أهمها نذكر اتفاقية بودابست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أولا: اتفاقية بودابست

وضعت اتفاقية بودابست 2001 العديد من القواعد المنظمة للتعاون القضائي الدولي بين الدول الأعضاء في مجال مكافحة الإجرام الالكتروني من أهمها:

أولا: حث الدول الأطراف على التعاون فيما بينهم، وذلك من خلال تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والعمل على وضع تشريعات جنائية موحدة ومتماثلة لأقصى درجة ممكنة لأغراض إجراء التحقيقات التي تتعلق بجرائم نظم بيانات الحاسب أو من أجل تجميع أدلة الجريمة في شكلها الالكتروني.

ثانيا: تجيز أحكام الاتفاقية تسليم المجرمين في الجرائم الالكترونية المنصوص عليها في المواد 2 و 11 من الاتفاقية بشرط أن تكون هذه الجرائم معاقب عليها وفقا لقانون الدولتين المعنيتين بعقوبة مقيدة للحرية لمدة سنة على الأقل، أو بعقوبة أشد.

ثالثا: تجيز الاتفاقية في الظروف العاجلة أن تطلب الدول الأطراف من بعضها البعض تبادل المساعدة القضائية في مجال التحقيقات الجنائية باستعمال وسائل الاتصال الحديثة مثل البريد الالكتروني بشرط توفير وسائل الأمن وضمان سلامة المعلومات المتبادلة بين الطرفين، على أن يتم تعزيز ذلك بطلب رسمي لاحق [1].

رابعا: يمكن للدولة الطرف في الاتفاقية وبدون سبق الحصول على إذن من دولة طرف أخرى في الاتفاقية أن :

أن تحصل على البيانات المخزنة علنا المتاحة للجمهور والموجودة على شبكة الانترنيت ويغض النظر عن مكان تواجد تلك البيانات جغرافيا.

– أن تدخل أو تستقبل من خلال نظام الحاسب على إقليمها بيانات أو معلومات مخزنة في إقليم دولة أخرى وذلك في حالة حصول الموافقة القانونية أو التخلي عن تلك البيانات طواعية من الشخص الذي له الحق في الكشف عنها.

خامسا: تنظم الاتفاقية مسألة المساعدة المتبادلة بشأن البيانات المارة وذلك في الوقت الحقيقي لها، ففي الكثير من الحالات يتعذر على المحققين تعقب اتصال ما وصولا إلى مصدره وذلك عن طريق متابعة عمليات البحث السابق، إذ لا يستبعد إقدام مزود الخدمة على محو البيانات المارة الأساسية تلقائيا ضمن سلسلة البحث وقبل التمكن من حفظها.

سادسا: تنظم الاتفاقية المساعدة المتبادلة فيما يتعلق باعتراض البيانات الخاصة بالمحتوى عن طريق تجميع وتسجيل محتوى البيانات بصورة عاجلة التي تتعلق باتصالات الكترونية محدودة.

سابعا: تحث الاتفاقية أعضائها على ضرورة إنشاء نقطة اتصال في كل دولة طرف تكون متاحة طوال الأربع والعشرين ساعة يوميا ولمدة 07 سبعة أيام لضمان توفير المشورة الفنية

[1] – المواد 23 و 24 من اتفاقية بودابست للجريمة الالكترونية، : ص 67 . مشار إليهم في: محمد كمال شاهين، المرجع السابق، ص 67 .

وتقديم المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الالكترونية الواقعة على التوقيع الالكتروني [1].

ثانيا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

سيرا على خطى الاتجاه السائد لتعزيز التعاون الدولي في مكافحة الجرائم المرتكبة بالوسائل الالكترونية سارعت الدول العربية في عقد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010 بالقاهرة، المصادق عليها من قبل الجزائر بموجب المرسوم الرئاسي رقم 252 – 14 المؤرخ في 08 سبتمبر 2014 [2].

وقد تناولت التعاون بين الدول الأطراف في مجال التحقيق في الفصل الرابع المواد من 30 إلى 43 من الاتفاقية حيث أجازت الفقرة أ من المادة 31 تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد .

ودعت المادة 32 فقرة 01 إلى تبادل المساعدة بين الدول الأطراف بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

ونصت المادة 32 فقرة 03 على "أنه يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني، على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية بما في ذلك استخدام التشفير، وتأكيد الإرسال حسبما تطلب الدولة الطرف

[1] – المواد 25 ، 32 ، 33 ، 34 ، من اتفاقية بودابست للجريمة الالكترونية. مشار إليهم في : محمد كمال شاهين، المرجع السابق، ص ص 226 –227 .

[2] – الجريدة الرسمية للجمهورية الجزائرية ، العدد 57 ، الصادرة في 28 سبتمبر 2014 .

ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات"[1] .

الفرع الثاني: المعاملة بالمثل في الجرائم الالكترونية

ليس معنى عدم وجود اتفاقيات بين الدول من أجل مكافحة الجرائم الخطيرة ذات البعد الدولي غل يد الدول عن مثل هذا التعاون، فالعلاقات الدولية في إطار القانون الدولي العام تضمنت أشكالا أخرى من التعاون كنظام المعاملة بالمثل، فالدول لن تقف مكتوفة الأيدي حيال الجرائم الخطيرة العابرة للحدود كالجرائم الالكترونية الواقعة على التوقيع الالكتروني، نظرا لكونها تهدد السلم الدولي في ظل النظام العالمي الجديد القائم على الانفتاح والتكامل .

وقد عرفت المعاملة بالمثل فقهيا بأنها وضع ينشأ عندما تقوم دولة ما بالتعهد لدولة أخرى أو الوعد بأنها ستقوم بمعاملة ممثليها أو رعاياها أو تجارتها معاملة مماثلة ومتكافئة مع المعاملة التي تتعهد بها الدولة الثانية أو تعد بها [2]، ومن إجراءات التحقيق في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني التي نص عليها المشرع الجزائري بتطبيق المعاملة بالمثل، ما جاء به قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 في المادة 05 فقرة 05 عندما يتعلق الأمر بالتفتيش أو الدخول إلى منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

---

[1] – المواد 31 ، 32 فقرة 01 و 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات . مشار إليهم في: محمود محمد جابر، المرجع السابق، ص ص 73 – 74 .

[2]– شريف محمد عمر، التعاون الدولي في مجال مكافحة الجرائم– دراسة مقارنة (تسليم المتهمين والمحكوم عليهم، تسليم الأشياء والتسليم المراقب، الإثبات والمساعدات القضائية، تنفيذ الأحكام الأجنبية، نقل المحكوم عليهم، التحقيق الجنائي عن بعد ، إنشاء قواعد بيانات خاصة بالجرائم الإرهابية)، المكتب الجامعي الحديث، الإسكندرية ، 2019 ، ص ص 71 – 72 .

الفرع الثالث: الإنابة القضائية الدولية

يتطلب التحقيق في الجرائم الالكترونية الواقعة على التوقيع الالكتروني العابرة للحدود الوطنية والتي مست عدة أقاليم من دول أجنبية اللجوء إلى إنابة قضائية لممارسة بعض الإجراءات على إقليمها، لذلك سنتطرق إلى مفهوم الإنابة القضائية الدولية، ثم إلى تقنية التحقيق الجنائي عن بعد وعلاقتها بالإنابة القضائية الدولية.

أولا: مفهوم الإنابة القضائية الدولية

تعد الإنابة القضائية الدولية أحد الواجبات والالتزامات التي يفرضها القانون الدولي العام، والتي بموجبها يعهد للسلطات القضائية في دولة ما بالقيام بالتحقيق أو بالعديد من التحقيقات لمصلحة السلطة القضائية المختصة في دولة أخرى ، يراعى فيها احترام حقوق وحريات الإنسان المعترف بها عالميا، وفي المقابل من ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة.

وقد تعددت التعريفات التي تناولت مصطلح الإنابة القضائية إلا أنها تتحد من حيث المضمون منها أن الإنابة القضائية عبارة عن طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية تتقدم الدولة المنيبة إلى الدولة المنابة، لضرورة الفصل في مسألة معروضة على السلطة القضائية المختصة في الدولة المنيبة، ويتعذر عليها القيام به بنفسها، كما أن طلب تنفيذ الإنابة القضائية غير ملزم للدولة المنابة لأن أساسها اعتبارات المجاملة الدولية la courtoisie international ، أو هي قيام الدولة أو الجهة الطالبة بتفويض السلطة المختصة في الدولة المطلوب إليها لاتخاذ إجراء أو أكثر من إجراءات التحقيق التي تتعلق بالجريمة المطلوب التعاون بشأنها [1].

[1]– هذه التعاريف مشار إليها في : شريف محمد عمر، المرجع السابق، ص 128.

وأورد بعض الفقه مجموعة من الخصائص التي تظهر مضمون الإنابة القضائية الدولية وبيانها كالتالي [1]:

– أنها تعد بمثابة عملية دولية تنظيمية بين دولتين أو أكثر بموجب اتفاق أو معاهدة دائمة أو تتم باتفاق خاص بصدد عملية إجرامية محددة كجريمة الاعتداء على توقيع الكتروني، خاصة إذا كانت هذه العملية تمثل خطورة كبيرة وتمس بمصالح أساسية للدولة.

– تفترض الإنابة القضائية الدولية القيام بعمل إجرائي، وبالتحديد إجراء من إجراءات التحقيق في إحدى جرائم التوقيع الالكتروني، وبالتالي تخرج إجراءات الاستدلال من نطاق الإنابة القضائية .

– تفترض الإنابة اختصاص الدولة الطالبة بالجريمة الواقعة على التوقيع الالكتروني التي تقدمت بطلب الإنابة لأجلها، ويفترض كذلك عدم اختصاص الدولة المنفذة بها ، بشرط أن يكون هذا الطلب قد صدر من سلطة قضائية للدولة الطالبة، ولو تم ذلك بالطريق الدبلوماسي.

– تفترض الإنابة أيضا أن نكون بصدد جريمة واقعة على التوقيع الالكتروني، وليس بصدد فعل ضار أو مسألة من مسائل الأحوال الشخصية.

وقد تضمن قانون الوقاية من جرائم تكنولوجيات الإعلام والاتصال لسنة 2009، المساعدة القضائية الدولية للجزائر مع الدول الأجنبية في المادة 16 فقرة 01 التي نصت على أنه " في إطار التحريات والتحقيقات القضائية الجارية لمعاينة جرائم تكنولوجيات الإعلام والاتصال وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني ".

وذلك بتحفظ حسب المادة 17، وهي أن تكون "وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الثنائية الدولية ومبدأ المعاملة بالمثل ".

---

[1] – عمر سالم، الإنابة القضائية في المسائل الجنائية– دراية مقارنة، دار النهضة العربية، 2011 ، ص 17 . مشار إليه في: شريف محمد عمر، المرجع السابق، ص 130.

وبقيود تضمنتها المادتين 18 و 19 وهي على التوالي :

"رفض تنفيذ طلبات المساعدة إذا كان من شانها المساس بالسيادة الوطنية أو النظام العام".

"ويمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب".

ثانيا: تقنية التحقيق الجنائي عن بعد وعلاقتها بالإنابة القضائية الدولية

القاعدة العامة أن التحقيق أو المحاكمة لابد وان تتم في نطاق جغرافي واحد، بحيث يتواجه طرفا الخصومة الجنائية كل بأدواته ووسائله، بحيث يكون كل من الطرفين فاعلا ايجابيا يسمع ويرى ويتكلم ويساهم في كل ما يدور في جلسة التحقيق، ولكن باستخدام تقنية الاتصال السمعي والمرئي أصبح من الممكن أن يمتد نطاق جلسة التحقيق ليشمل أقاليم متعددة بحيث تكون سلطة التحقيق في دولة والمتهم الذي يتم التحقيق معه في دولة أخرى والشاهد أو الخبير في دولة ثالثة كل ذلك في نفس الوقت على نحو يسمح بالتفاعل والمواجهة بين الشهود أنفسهم وبين الشهود والمتهمين[1]، وقد أجاز المشرع الجزائري لجهات التحقيق والحكم استعمال تقنية المحادثة المرئية عن بعد لأول مرة في قانون عصرنة العدالة 15-03 في المادة 15، ثم عدلت بموجب الأمر رقم 20 -04 المؤرخ في 30 أوت سنة 2020، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية [2]، بحيث نصت المادة 441 مكرر 01 إلى 10 على أنه يمكن استجواب المتهم غير المحبوس أو سماعه أو إجراء مواجهة بينه وبين غيره في مرحلتي التحقيق القضائي أو المحاكمة، باستعمال تقنية المحادثة المرئية عن بعد، سواء من تلقاء نفسها أو بطلب من النيابة أو أحد الخصوم، كما يمكن أيضا أن تستعمل المحادثة المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء، والمترجمين.

---

[1] – عمر سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي– المراقبة الالكترونية والتحقيق الجنائي عن بعد، ط1 ، دار النهضة العربية، القاهرة، 2013 ، ص ص 184 185 .

[2] – الجريدة الرسمية للجمهورية الجزائرية، العدد 57 ، الصادر في 31 أوت 2020 .

وإذا أمر قاضي التحقيق وضع المتهم المسموع عن طريق تقنية المحادثة المرئية عن بعد رهم الحبس المؤقت، يقوم عن طريق نفس التقنية بتبليغه هذا الأمر شفاهة ويحيطه علما بحقوقه.

فكما يستخدمها قاضي التحقيق على المستوى الوطني فلا مانع أيضا من استخدامها على مستوى دولي، وإن كان تطبيقها على المستوى الوطني لا يثير أي إشكالية، فعلى المستوى الدولي تثير إشكالية سيادة الدولة الأجنبية، وإذا ما كانت تجيز أم لا في قانونها استخدام تقنية التحقيق الجنائي عن بعد، والاتفاقيات الدولية التي أبرمتها الجزائر مع الدولة المطلوب منها التنفيذ.

وتعد الولايات المتحدة الأمريكية من أكثر الدول استعمالا لتقنية التحقيق عن بعد سواء على المستوى الداخلي والدولي مند عام 1997، والقانون الأمريكي إن لم يضع تنظيما خاصا لهذه التقنية إلا أنه في نفس الوقت لا يضع عقبة أمام استخدامها، إذ لا يجوز اللجوء إليها حتى على المستوى الدولي، طالما لم يكن في ذلك تعارضا مع المبادئ الأساسية في القانون الأمريكي، وفي ذات السياق فإنه يجب احترام القواعد المنصوص عليها في اتفاقية المساعدة القضائية بين الولايات المتحدة الأمريكية والدول الطالبة أو المنفذة [1].

ولمعرفة شروط تطبيق تقنية الفيديو vidéo conférence على المستوى الدولي يمكننا الاستعانة بما نصت عليه الاتفاقية الأوربية للمساعدة القضائية في 08 نوفمبر 2001 بستراسبورغ التي أكدت على ثلاث شروط أساسية لتطبيقها [2]:

الشرط الأول: عدم تعارض استخدام تقنية الفيديو vidéo conférence مع المبادئ الأساسية لقانون الدولة المطلوب منها التنفيذ، ولما كان استخدام هذه التقنية في سماع شاهد أو خبير أو استجواب متهم يتواجد بإقليم الدولة المنفذة هو في الأصل مباشرة لاختصاص قضائي يدخل في اختصاصها لذلك يجب موافقة الدولة المنفذة التي يتواجد الشخص المطلوب منها الإدلاء بأقواله

[1] – عمر سالم، المرجع السابق، ص 187 .

[2] – شريف عمر، المرجع السابق، ص ص 224 إلى 226 .

على أرضها، ولهذه الدولة أن تقدر مدى تعارض أو عدم تعارض هذه الإجراءات مع المبادئ الأساسية لقانونها الداخلي.

الشرط الثاني: توافر الوسائل والإمكانيات التي تمكن الدولة المنفذة من استخدام هذه التقنية، وبالتالي ففي عدم توافر هذه الوسائل والإمكانات وعجز الدولة المطلوب منها التنفيذ عن توفيرها يحق لها أن ترفض استخدام هذه التقنية، وقد يكون استخدامها في بعض الأحيان مكلفا للدولة المطلوب منها التنفيذ ويحملها نفقات مالية باهظة، وقد أجازت الاتفاقية للدولة المطلوب منها التنفيذ أن تعرض عليها إعانات سواء على سبيل الإعارة أو الهبة لأجل توفير الإمكانيات التقنية اللازمة لاستخدام هذه الوسيلة.

الشرط الثالث: حصر استخدام هذه التقنية في مجال سماع الشهود والخبراء، فوفقا للمادة العاشرة من البرتوكول الإضافي للاتفاقية الأوروبية للمساعدة القضائية المتبادلة يقتصر استخدام تقنية vidéo conférence في مجال المسائل الجنائية على سماع شهادة الشهود وإفادات الخبراء، ما يمكن للسلطات القضائية لإحدى الدول المتعاقدة طلب سماع شخص يتواجد على إقليم دولة متعاقدة أخرى بصفته شاهدا أو خبيرا عبر هذه التقنية متى ثبت استحالة مثول هذا الشخص بنفسه.

لكن هناك شرط إضافي جدير بالاهتمام تضمنته الفقرة الأولى من المادة العاشرة مفادها أن اللجوء إلى تقنية vidéo conférence في التحقيق الجنائي يتم بصورة احتياطية وليس أصلية، فنص هذه المادة يحظر استخدامها إلا في الحالات التي يثبت فيها عدم استطاعة انتقال الشاهد أو الخبير إلى الدولة الطالبة للمثول أمام سلطاتها القضائية [1].

* ومن الحالات التي لا يستطيع فيها الخبير أو الشاهد الانتقال، غلق الخطوط الجوية لأغلب الدول بسبب استفحال مرض كورونا كوفيد 19 الذي استفحل في ديسمبر 2019.

الفصل الثاني: مرحلة المحاكمة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

المحاكمة هي المرحلة الثانية للدعوى الجزائية ويطلق عليها كذلك تعبير التحقيق النهائي، والمحاكمة هي مجموعة من الإجراءات تستهدف تمحيص أدلة الدعوى جميعا، ما كان منها مع أو ضد مصلحة المتهم، كما تهدف أيضا إلى تقصي كل الحقائق القانونية والواقعية في شان الدعوى، ثم الفصل في موضوعها، إما بالإدانة إن كانت الأدلة جازمة، وإما بالبراءة إذا لم تتوافر الأدلة الجازمة بالإدانة، وللمحاكمة أهمية كبيرة في تحديد مصير المتهم وتقدير الأدلة فيها نهائي، وتتميز بطابعها القضائي[1]، والأدلة المتحصل عليها في جرائم التوقيع الالكتروني المرتكبة في بيئة الكترونية تكون ذو طابع الكتروني خاص يميزها عن باقي الأدلة التقليدية وهو ما يسمى بالدليل الالكتروني أو الرقمي، كما أن إجراءات محاكمة المتهمين في جرائم التوقيع الالكتروني في التشريع الجزائري تخضع للقواعد العامة في قانون الإجراءات الجزائية من حيث الاختصاص النوعي وسير الجلسات، إلا أنها تثير بعض الإشكالات فيما تعلق بالاختصاص الإقليمي، وبعض الصعوبات في الاختصاص النوعي، وهذا ما يدعونا للتطرق إلى مسألة الاختصاص والجهة القضائية المختصة بمحاكمة المتهمين في جرائم التوقيع الالكتروني في المبحث الأول، ثم سنتطرق إلى أدلة إثبات جرائم التوقيع الالكتروني، والدليل الالكتروني وأثره على القناعة الشخصية للقاضي الجنائي في المبحث الثاني.

المبحث الأول: الجهة القضائية المختصة بالمحاكمة في جرائم التوقيع الالكتروني

الجرائم التي ترتكب على الإقليم الجزائري فقط من قبل جزائريين التي لا يثير فيها إشكال في الاختصاص الإقليمي والنوعي فيها والتي يختص بها القضاء الجزائري، لكن مع ما تأخذه الجرائم الالكترونية الواقعة على التوقيع الالكتروني من امتداد دولي، قد يكون هنالك تداخل في الاختصاص بين القضاء الجزائري والأجنبي، لذلك سنتطرق للاختصاص القضائي الوطني

[1]– محمود نجيب حسني، الموجز في شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، 1996، ص 02 .

والأجنبي بجرائم التوقيع الالكتروني، ثم سنتطرق للاختصاص القضائي الوطني بجرائم التوقيع الالكتروني.

المطلب الأول: الاختصاص القضائي الوطني والأجنبي في جرائم التوقيع الالكتروني والمبادئ المطبقة عليه

الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني تأخذ في أغلب حالاتها طابع دول دولي، في حين أن المعلومات في حد ذاتها هي معطيات نظمها القانون الوطني، ففي هذه الحالة تدفق المعلومات الحر والسريع يرجع إلى قدرة سلطات التحقيق والحكم المربوط أساسا بقدرتها على الإقليم الوطني وعلى مبدأ السيادة [1]، وتطبيق الاختصاص القضائي المكاني يحكمه أربع مبادئ وهم الإقليمية، الشخصية، العينية، العالمية.

الفرع الأول: مبدأ إقليمية النص الجنائي والاختصاص بجرائم التوقيع الالكتروني

الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني التي ترتكب في إقليم دولة وتكون نتيجتها في إقليم دولة أخرى تثير مشاكل وتنازع في الاختصاص على عكس الجرائم المرتكبة على إقليم واحد، وهو ما سنتطرق له من خلال بيان المقصود بمبدأ الإقليمية، وتحديد الجهة القضائية المختصة في حالة تنازع القوانين، وموقف الاتفاقيات الدولية من الجرائم الالكترونية الواقعة على التوقيع الالكتروني.

أولا: المقصود بمبدأ الإقليمية

يقصد بمبدأ الإقليمية تطبيق التشريع الجزائي الوطني على كافة الجرائم المرتكبة في إقليم الدولة بصرف النظر عن جنسية الجاني أو المجني عليه سواء كان وطنيا أم أجنبيا، وبصرف النظر أيضا عن المصلحة التي أهدرتها الجريمة ، ولو كانت مصلحة تخص دولة أجنبية[2] ، و يشمل إقليم الدولة أجزاء ثلاثة الإقليم الأرضي، المائي، الجوي، فالإقليم الأرضي هو المنطقة

---

[1]- Mohamed chawki, essai sur la notion de cyber criminalite ,pp 3-4. « https ://www.ie-ei-eu. اطلع على الموقع في: 04 أفريل 2020 على الساعة 20: 15

[2]– سليمان عبد المنعم، النظرية العامة لقانون العقوبات، المرجع السابق، ص 89 .

من الكرة الأرضية التي تعينها الحدود السياسية للدولة كذلك طبقات الأرض دون هذه المنطقة إلى مركز الكرة الأرضية، والإقليم المائي هو مساحات الماء التي تقع داخل حدود الدولة، وهو كذلك بحرها الإقليمي وتشمل مساحات الماء الداخلية الأنهار الوطنية والأجزاء التابعة للدولة من الأنهار الدولية، والبحيرات، والبحار المغلقة، والقنوات والمضايق والخلجان الداخلية والموانئ البحرية، أما البحر الإقليمي فهو الجزء من البحر العام الذي يلاصق شواطئ الدولة وعرضه وفقا للعرف الدولي ثلاث أميال بحرية تحسب من آخر نقطة ينحصر عنها البحر وقت الجزر والمقدر ب اثنا عشر ميلا، ويشمل الإقليم الجوي كل طبقات الهواء التي تعلو الإقليم الأرضي والمائي إلا ما لا نهاية في الارتفاع[1].

ويعد مبدأ الإقليمية القاعدة الأساسية في اختصاص قضاء الدولة الجزائرية طبقا للقاعدة العامة المنصوص عليها في المادة 03 من قانون العقوبات: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب على إقليمها، سواء أكان مرتكبها جزائريا أو أجنبيا".

وتطبيقا لذلك يطبق قانون العقوبات الجزائري على كافة جرائم التوقيع الالكتروني المرتكبة على الإقليم الجزائري بغض النظر عن جنسية مرتكبها سواء كان جزائريا أم أجنبيا.

ثانيا: تحديد مكان ارتكاب الجريمة وتنازع الاختصاص بين القضاء الوطني و الأجنبي

الإشكالية الرئيسية في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني هي كيف نحدد مكان ارتكابها، وهو ما سنتطرق له من خلال بيان موقف المشرع الجزائري، والتشريعات الأنجلوساكسونية.

أ. موقف المشرع الجزائري

إذا كانت الجريمة المرتكبة مكتملة أركانها داخل الإقليم فإن القضاء الوطني هو المختص تطبيقا لنص المادة 03 من قانون العقوبات، ولكن قد يكون أن يكون كل عنصر من عناصر جرائم التوقيع الالكتروني مرتكب داخل إقليم دولة تختلف عن الأخرى كمن يقوم في الجزائر

[1] – محمود نجيب حسني ، شرح قانون العقوبات– القسم العام، المرجع السابق، ص 146 .

بتزوير توقيع الكتروني ويتم استعماله في إنجلترا أو كندا، وفي هذه الحالة يختص القضاء الجزائري بها حسب المادة 586 من قانون الإجراءات الجزائية التي تعتبر أن الجريمة مرتكبة على الإقليم الجزائري إذا كان أحد الأعمال المميزة لها مرتكبا داخل الإقليم الجزائري .

كما أن القضاء الجزائري يختص بجرائم التوقيع الالكتروني المرتكبة في الخارج وفقا للمادة 585 قانون الإجراءات الجزائية إذا كان فاعلها شريكا في الإقليم الجزائري، بشرط أن تكون الواقعة معاقب عليها في الدولتين، وأنه قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية.

ب. موقف بعض التشريعات الأنجلوساكسونية من الاختصاص الإقليمي في الجرائم المرتكبة بالوسائل الالكترونية

أوصت لجنة تعديل القوانين في انجلترا بتحديد اختصاص المحكمة الجنائية ليكون على أساس مكان وجود مقدم الخدمات، أو مكان وجود جهاز الحاسب المستخدم في ارتكاب الجريمة، وقد نص المشرع الانجليزي على تحديد الاختصاص في الجريمة الالكترونية بمقتضى قانون 1990 في المادة الخامسة منه على أن يختص القضاء الانجليزي إذا تكون هناك علاقة بين مرتكب الجريمة والإقليم الانجليزي، حتى ولو لم تقع الجريمة على الإقليم الانجليزي، ويقصد بالعلاقة المنصوص عليها في المادة الخامسة أن يتواجد المتهم الذي نفد الجريمة على الإقليم الانجليزي وقام باستعمال الجهاز على إقليم انجلترا، أو أنه كان خارج إقليم انجلترا إلا أن الجريمة وقعت على الإقليم الانجليزي، لذلك فهذا الاتجاه يتماشى مع الاتجاه العالمي في تحديد الاختصاص في قضايا الحاسب والانترنيت، كما أنه يتفق مع اعتبارات التعاون الدولي في مكافحة هذا النوع من الجرائم [1].

ومن مزايا اختصاص محكمة الجهاز الخادم هو سهولة معرفة مكان تواجد الجهاز بينما يصعب أحيانا معرفة مرتكب الجريمة، أما الميزة الأخرى فهي أنه في حالة رفع الدعوى أمام

[1] – شيماء عبد الغني، المرجع السابق، ص 379 .

محكمة الجهاز الخادم يجيز التعويض عن سائر الأضرار التي تحققت في أماكن مختلفة من العالم، على خلاف الحال عند رفع تلك الدعوى أمام إحدى المحاكم التي تصل إليها شبكة الانترنيت ويمكن الدخول إلى الموقع فيها، حيث إن ذلك لا يجيز إلا التعويض عن الضرر الذي تحقق في هذا المكان وحده دون غيره [1].

وفي الولايات المتحدة الأمريكية اعتمد القانون الأمريكي مبدأ النتيجة الإجرامية كأساس لامتداد اختصاص القضاء الأمريكي بجرائم التوقيع الالكتروني عبر الانترنت التي ترتكب بالخارج إلا أن نتيجتها الإجرامية كأحد عناصر الركن المادي يمكن أن يمتد إلى الإقليم الأمريكي، وقد كانت الخطوة الرائدة في اعتماد مبدأ النتيجة الإجرامية عندما أطلق النائب العام في ولاية مينيسوتا بيانا بعنوان تحذير كل مستخدمي ومزودي خدمات الانترنت حول امتداد الاختصاص القضائي لولاية مينيسوتا إلى كل جريمة يمكن أن تصل نتائجها إلى الولاية ومن التطبيقات ما قضت به الدائرة الاستئنافية الخامسة في قضية قمار ومراهنات عبر الانترنت أنه بالرغم من أن عرض ألعاب القمار قد تم من خلال مكاتب في الكاريبي إلا أن قبول القمار والمراهنات قد تم في الولايات المتحدة الأمريكية، كما قضت محكمة ولاية misouri باختصاصها بنظر قضية تقليد علامة تجارية trademark مع أن المتهم فيها يقيم في ولاية كاليفورنيا استنادا إلى أن بث العلامة التجارية يصل إلى مستخدمي الانترنت في تلك الولاية[2] لذلك فإذا ارتكبت جريمة توقيع الكتروني كتزوير توقيع الكتروني في ولاية، ويتم استخدامه في ولاية ثانية، فوفقا لمبدأ النتيجة الإجرامية يكون الاختصاص القضائي في مثالنا هذا في الولاية الثانية.

ثالثا: مبدأ الإقليمية في الاتفاقيات الدولية للجرائم المرتكبة بالوسائل الالكترونية

أقرت اتفاقية بودابست للجرائم الالكترونية مبدأ الإقليمية ضمن نصوصها في المادة 22 فقرة 01 على أنه يعتمد كل طرف قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لإقرار

[1] – شيماء عبد الغني، المرجع السابق، ص 380 .

[2] – محمود محمد جابر، المرجع السابق، ص ص 84 – 85 .

الاختصاص القضائي بشأن الجرائم المنصوص عليها في هذه الاتفاقية وذلك عندما ترتكب الجريمة في إقليمه، أو على متن إحدى السفن التي ترفع علم ذلك الطرف، أو على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف .

كما جاءت المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010 لتؤكد على هذا المبدأ بقولها " تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في هذه الاتفاقية ، وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت:

أ. في إقليم الدولة الطرف .

ب. على متن سفينة تحمل علم الدولة الطرف.

ج. على متن طائرة مسجلة تحت قوانين الدولة الطرف[1].

الفرع الثاني: مبدأ الشخصية

يقصد بمبدأ الشخصية وجوب سريان القانون الجزائي لكل دولة على رعاياها المتمتعين بجنسيها أينما كانوا، ولمبدأ الشخصية جانبان: جانب ايجابي مؤداه تطبيق القانون الجزائي للدولة على مرتكبي الجرائم الذي ينتمون إلى جنسيتها بصرف النظر عن مكان وقوع جريمتهم، وأيا كانت جنسية المجني عليه في هذه الجريمة، ويعرف هذا بمبدأ الشخصية الايجابي principe de la personnalité active ، أما الجانب السلبي للمبدأ فيعني سريان القانون الجزائي للدولة على الجرائم التي يكون المجني عليه فيها متمتعا بجنسيتها، حتى ولو ارتكبت الجريمة خارج إقليم الدولة أو كان الجاني أجنبيا، ويعبر هذا الجانب عن مبدأ الشخصية السلبي principe de la personnalité passive [2].

[1] – محمود محمد جابر، المرجع السابق، ص 86 .

[2] – سليمان عبد المنعم، النظرية العامة لقانون العقوبات، المرجع السابق، ص 116 .

ولقد نظم المشرع الجزائري أحكام هذا المبدأ في المواد من 582 إلى 584 من قانون الإجراءات الجزائية التي تقضي بتطبيق النصوص الجزائية على الجزائريين الذين يرتكبون جرائم التوقيع الالكتروني ثم يفرون عائدين إلى الجزائر، وفقا للمادة 583 من قانون الإجراءات الجزائية إذا ارتكب جزائري جريمة توقيع الكتروني توصف بأنها جنحة في نظر القانون الجزائري أم في نظر تشريع القطر الذي ارتكبت فيه يجوز المتابعة من أجلها والحكم فيها في الجزائر إذا كان مرتكبها جزائريا، وذلك وفقا للشروط المنصوص عليها في الفقرة الثانية من المادة 582 والفقرة الثالثة من المادة 583 وهي أنه لا يجوز أن تجرى المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر ولم يبثت أنه حكم عليه نهائيا في الخارج وأن يبثت في حالة الحكم بالإدانة أنه قضي العقوبة أو سقطت منه بالتقادم أو حصل العفو عنها، ولا تجرى المتابعة في حالة ما إذا كانت جنحة التوقيع الالكتروني مرتكبة ضد أحد الأفراد إلا بناء على طلب النيابة العامة بعد إخطارها بشكوى من الشخص المضرور أو ببلاغ من سلطات القطر الذي ارتكبت جريمة التوقيع الالكتروني فيه.

وقد أخذت اتفاقية بودابست للجرائم الالكترونية بمبدأ الشخصية في الفقرة د من المادة 122 والتي تنص على أنه "يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الاختصاص القضائي بشأن الجرائم المنصوص عليها في هذه الاتفاقية، من جانب أحد مواطنيه إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي لمكان ارتكابها"، كما أخذت بالمبدأ أيضا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفرع الثالث: مبدأ العينية

يقصد بمبدأ العينية أو كما يقال له أحيانا الذاتية تطبيق قانون العقوبات الوطني للدولة على الجرائم التي تشكل إخلالا بمصالحها الأساسية أو الجوهرية ، وذلك بصرف النظر عن مكان وقوع الجريمة وأيا كان جنسية فاعلها، ولهذا المبدأ أهمية غير بالغة حيث تحرص الدول جميعها على بسط سلطانها التشريعي على الجرائم التي تمس بمصالحها الأساسية ، لاسيما

حين لا تلقى هذه الجرائم اهتماما من الدول التي وقعت على إقليمها ، فمن المتصور ألا يطبق قانون هذه الدول لسبب أو لأخر مما يندر بإفلات الجناة من العقاب، فكأن الدولة بتقريرها مبدأ العينية تمارس نوعا من الدفاع الشرعي عن مصالحها الأساسية [1].

ولقد نص المشرع على هذا المبدأ في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 2009 في المادة 15 منه بأن "تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"، لذلك إذا ارتكبت إحدى جرائم التوقيع الالكتروني كالدخول لنظام الحالة المدنية المتعلق بالتوقيع الالكتروني للجزائريين مستهدفا وزارة الداخلية، أو وزارة الدفاع، أو المساس بالمصالح الاستراتيجية للاقتصاد الجزائري من طرف شخص أجنبي أمريكي أو سعودي الجنسية مثلا، فالمحاكم الجزائرية هي المختصة بالنظر في هذه الجرائم، دفاعا عن المصالح الأساسية للدولة الجزائرية.

الفرع الرابع: مبدأ العالمية

تأخذ بعض التشريعات المقارنة بمبدأ العالمية في تحديد الاختصاص الوطني الجنائي مثل بلجيكا، ويقصد بهذا المبدأ أن المحاكم الوطنية تختص بمحاكمة مرتكبي بعض الجرائم على الرغم من وقوعها في خارج إقليم الدولة وأن المتهمين ليسوا من مواطني تلك الدولة أي تخل بقيمة من قيم المجتمع العالمي مثل جرائم المخدرات والإرهاب والقرصنة والجرائم الجنسية الواقعة على الأطفال، ومنها ما يتم بالوسائل الالكترونية .

ومن الدول العربية التي تأخذ بمبدأ عالمية النص الجنائي الإمارات العربية المتحدة في بعض الجرائم وهي:

– جريمة تخريب أو تعطيل وسائل الاتصال الدولية، ويقصد بذلك عادة جرائم خطف الطائرات

[1] – سليمان عبد المنعم، النظرية العامة لقانون العقوبات، المرجع السابق، ص 128 .

- جريمة الاتجار بالمخدرات

- جريمة الاتجار بالرقيق

- جرائم القرصنة

- جرائم الإرهاب الدولي .

ويكون سريان القوانين الجزائية الإماراتية واختصاص القضاء الإماراتي بتلك الطائفة من الجرائم ممتدا إلى الفاعل فيها والشريك أيا كان مكان وقوع الجريمة [1].

وطبيعي ألا يطبق هذا المبدأ على كل الجرائم، إذ يؤدي ذلك إلى تنازع خطير بين التشريعات الجنائية للدول المختلفة، وهو ما يقتصر تطبيقه على مجموعة من الجرائم تهم المجموعة الدولية كلها délit de droit des gens بحيث يعد مرتكبها معتديا على مصلحة مشتركة لكل الدول ومن بينها الدولة التي قبض على الجاني فيها.

وأهمية هذا المبدأ مستمدة من خطورة الإجرام الدولي الحديث، ذلك أن وسائل الاتصال قد أتاحت الفرصة لنشوء عصابات دولية مكونة من مجرمين ينتمون إلى جنسيات متعددة ويمتد نشاطهم إلى أقاليم دول عديدة، ولمكافحة هذه العصابات لابد أن تتعاون الدول فما بينها، وتتولى كل واحدة منها عقاب المجرم الذي يضبط في إقليمها دون اكتراث بجنسيته أو مكان جريمته، وتفعل الدولة ذلك باعتبارها نائبة عن المجتمع الدولي [2]، ونظرا للطابع العالمي التي تكتسبه الجرائم المرتكبة بالوسائل الالكترونية فكان من الأجدر بالدول التي تأخذ بمبدأ العالمية أن تدرج الجرائم الالكترونية منها الجرائم الواقعة على التوقيع الالكتروني ضمن الجرائم التي تخضع لمبدأ العالمية لسببين اثنين، يتمثل الأول في سهولة تكوين جماعة إجرامية منظمة عابرة للحدود من جنسيات مختلفة بواسطة الانترنت، يكون غرضها ارتكاب جرائم الكترونية، أما السبب الثاني هو أن الجرائم المرتكبة بالوسائل الالكترونية من أكثر الجرائم التي تكون أضرارها

[1]– شيماء عبد الغني، المرجع السابق، ص ص 368– 369 .

[2] – محمود نجيب حسني، قانون العقوبات– القسم العام، المرجع السابق، ص 167 .

تمس أكثر من دولة وعابرة للحدود الوطنية والدولية، ولا يوجد نص في قانون العقوبات الجزائري يتضمن مبدأ عالمية النص الجنائي.

المطلب الثاني : الاختصاص القضائي الوطني

لا يكفي لكي يستجمع الحكم سلامته القانونية أن يكون صادرا من محكمة مشكلة تشكيلا قانونيا وإنما يلزم فوق ذلك أن يكون الحكم صادرا من محكمة لها الاختصاص في إصداره بتوافر شرطين، يتمثل الأول في احترام قواعد الاختصاص النوعي والشخصي والإقليمي، أما الشرط الثاني فهو أن يكون الحكم صادرا من عدد القضاة الذين باشروا جميع إجراءات الدعوى وسمعوا المرافعة[1]، إذا فلكل جهة قضائية صلاحية الفصل في الجرائم التي تدخل ضمن نطاق اختصاصها، ولتحديد اختصاص الجهة القضائية للفصل في أحد جرائم التوقيع الالكتروني لابد أن تكون مختصة إقليميا ونوعيا.

الفرع الأول: الاختصاص الإقليمي بالمحاكمة في جرائم التوقيع الالكتروني

الأصل في الاختصاص الإقليمي للمحكمة حسب المادة 329 من قانون الإجراءات الجزائية أنه يتحدد إما بمكان إقامة أحد المتهمين أو شركائهم أو محل الجريمة أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

إلا أن التطور وخطورة بعض الجرائم والتي من الممكن أن ترتكب في عدة أقاليم قام المشرع بتعديل فيما بعد المادة 329 من قانون الإجراءات الجزائية بإضافة الفقرة 05 بقانون 04-14، والتي فيها يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تشمل نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، وجرائم المخدرات والجريمة المنظمة عبر الحدود، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

---

[1] – محمد زكي أبو عامر، المرجع السابق، ص 775 .

الفرع الثاني: الاختصاص النوعي بالمحاكمة في جرائم التوقيع الالكتروني

المحاكم العادية هي صاحبة الاختصاص الأصيل في نظر كافة الدعاوى الجزائية ولا يكفي لسلب ولايتها بالقضاء لبعض الأشخاص أو بعض الجرائم أن يقرر القانون اختصاص جهة خاصة ببعض الدعاوى وإنما يلزم أن يكون القانون صريحا في اختصاص تلك الجهة للفصل في تلك الدعاوى [1]، كاختصاص الأقطاب الجزائية المتخصصة في بعض الجرائم الخطرة بموجب تعديل قانون الإجراءات الجزائية لسنة 2004، على هذا الأساس فهناك محاكم عادية ومتخصصة في الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني.

أولا: المحاكم العادية

تتم محاكمة المتهمين في جرائم الاعتداء على التوقيع الالكتروني أمام المحاكم العادية، وبما أن جل هذه الجرائم من الجنح سواء بالنسبة لجريمة الاعتداء على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، أو في جريمة إفشاء أو استعمال أو حيازة بيانات توقيع الكتروني موصوف خاص بالغير، أو في جرائم التصديق الالكتروني، وبالتالي إذا لم ترتبط هذه الجرائم بجنايات فإن المحاكمة تكون أمام محكمة الجنح، وتكون محكمة الأحداث مختصة إذا كان المتهم مرتكب إحدى جرائم التوقيع الالكتروني حدث لم يبلغ سن الرشد الجزائي و هو ثماني عشر 18 سنة .

ومن الصعوبات التي تعترض المحاكمة تقديم المعلومات العلمية والمصطلحات التقنية العالية أمام المحاكم وشرحها للقضاة تشكل صعوبة بالغة لهم ولأعضاء النيابة العامة، وترك مهمة الشرح لخبراء الحاسب يفقد القضية الجنائية عناصرها القانونية ولا تتمكن المحكمة من الوقوف على العناصر المكونة لأركان الفعل الإجرامي .

وبالتالي يمكن لقاضي الحكم القيام بإجراءات تلخيص القضية وإعداد ورقة حصر التهم المتابع بها مرتكب الجريمة المرتكبة بوسائل الكترونية على التوقيع الالكتروني كما كشفتها

[1] – محمد زكي أبو عامر، المرجع السابق، ص 779 .

التحريات، والاجتماع بخبراء الحاسب الآلي الذين أسهموا في التحقيق الابتدائي في إجراءات الضبط والتفتيش وفحص البرامج والأدلة الجنائية وترتيبها وفق لأهمية كل دليل وذلك من أجل ربط الجوانب القانونية مع الخبرة العلمية للتأكد من عناصر وأركان الجريمة[1].

ثانيا: الأقطاب الجزائية المتخصصة

أولى البوادر لإنشاء الأقطاب الجزائية المتخصصة كانت بموجب تعديل قانون الإجراءات الجزائية 04-14 المؤرخ في 10 نوفمبر 2004، عندما وسع في الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة في المواد 37- 40 -329 من قانون الإجراءات الجزائية في الجرائم الخطرة منها جريمة المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني والتي تبقى خاضعة للتنظيم، ليأتي فيما بعد تنظيمها بالمرسوم التنفيذي رقم 06 – 384 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق، لمحكمة سيدي محمد الجزائر، محكمة قسنطينة، محكمة ورقلة، محكمة وهران، ثم عدل هذا المرسوم بالمرسوم التنفيذي رقم 267-16 المؤرخ في 17 أكتوبر 2016 [2]، وكمثال عن ذلك إذا ارتكبت جريمة مساس بالنظام المعلوماتي للتوقيع

---

[1] – محمد الأمين البشري، المرجع السابق، ص 1079 .

* نصت المواد 3 ، 4، 5 من المرسوم 267 – 16 على اختصاص المحاكم الجهوية كمايلي:

– يمتد الاختصاص المحلي لمحكمة قسنطينة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية ل: قسنطينة، أم البواقي، باتنة، وبجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، خنشلة، سوق أهراس، ميلة. =

– يمتد الاختصاص المحلي لورقلة ووكيل الجمهورية وقاضي التحقيق بها إلى المجالس القضائية ل: ورقلة، أدرار، تامنغست، إيليزي، بسكرة، الوادي، غرداية .

– يمتد الاختصاص المحلي لمحكمة وهران ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية ل: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت نعامة، عين تيموشنت ، غليزان. الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 62، الصادر بتاريخ 23 أكتوبر 2016 ، ص10.

الالكتروني الخاص بمصالح الحالة المدنية البيومترية لبلدية باتنة فالقطب الجزائي المختص محليا ونوعيا بمحاكمة مرتكب الجريمة هو القطب الجزائي بمحكمة قسنطينة .

المبحث الثاني: إثبات الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني

المحاكمة الجزائية هي في الأساس مشكلة إثبات[1]، ومما لا شك فيه أن الثورة العلمية في مجال نظم المعلومات الإلكترونية لم تؤثر فقط في نوعية الجرائم التي ترتبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم، وإنما أثرت تأثيرا كبيرا على الإثبات الجنائي، حيث يمكن القول أن الطرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع من الجرائم المستحدثة من ذلك ظهر نوع خاص من الأدلة يمكن الاعتماد عليها في إثبات الجريمة الإلكترونية ونسبتها إلى فاعلها، وهو ما يعرف بالدليل الإلكتروني أو الرقمي[2]، وكل صور الاعتداء على التوقيع الالكتروني كتزوير المحررات الالكترونية أو إتلافها أو استعمالها أو المساس بسرية البيانات الالكترونية التي تحويها لا يتصور إثباتها دون تقديم أدلة الكترونية مستمدة من أجهزة الحاسب[3]، فتثبت جرائم التوقيع الالكتروني بجميع طرق الإثبات في المواد الجزائية وفق ما نصت عليه المادة 212 من قانون الإجراءات الجزائية كالشهادة والاعتراف والقرائن والخبرة، إلا أن الجرائم الالكترونية الواقعة على التوقيع الالكتروني وبما أنها ترتكب في بيئة الكترونية فتعتمد أساسا على الدليل الالكتروني في إثباتها، وهو ما سنتطرق له من خلال مدى ملائمة أدلة الإثبات التقليدية في المطلب الأول، ثم إلى الدليل الالكتروني وأثره على الاقتناع الشخصي للقاضي الجنائي في المطلب الثاني.

---

(1) - Coralie Ambroise-Castérot,op-cite , p158.

(2) – بيل جيتس، المعلوماتية بعد الإنترنت، طريق المستقبل، ترجمة عبد السلام رضوان، المرجع السابق، ص 41.

(3) – محمود جاد المولى، المرجع السابق، ص 313 .

المطلب الأول: مدى ملائمة تطبيق أدلة الإثبات التقليدية في إثبات جرائم التوقيع الالكتروني المستحدثة

تتنوع أدلة الإثبات الجنائي بحسب كل واقعة إجرامية، فمنها ما يتم إثباته بالشهادة أو الاعتراف أو المعاينة أو الخبرة، ولكل دليل قوته الثبوتية وتأثيره على قناعة القاضي، وهو ما سنتطرق له من خلال بعض أدلة الإثبات كالاعتراف، والشهادة، والقرائن، والمعاينة، والخبرة، والذكاء الاصطناعي.

الفرع الأول: الاعتراف

الاعتراف هو إقرار المتهم بصحة الاتهامات المنسوبة إليه كلها أو بعضها، فهو إجراء يقوم على المتهم أثناء استجوابه غالبا، ودليل إثبات يأخذ به القاضي، إذ يدعوه إلى إدانة المتهم وهو مرتاح الضمير، لا يخالجه شك في ارتكابه للوقائع لمنسوبة إليه، والاعتراف الذي يتمتع بهذه الأهمية هو الاعتراف القضائي الذي يصدر أمام المحكمة، وقد يكون غير قضائي، كأن يصدر أمام الضبط القضائي أو حتى أمام سلطة التحقيق الابتدائي، أو تتضمنه ورقة رسمية أو عرفية، مثل هذا الاعتراف لا يكتسب أهمية الاعتراف القضائي، ولكن قيمته تتوقف على الثقة في السلطة التي حدث أمامها أو شهادة من صدر أمامهم أو قيمة الورقة التي دون بها[1].

وليس معنى اعتراف المتهم بالتهمة المنسوبة إليه أن تكون المحكمة ملزمة بالحكم بالإدانة[2]، والاعتراف في القانون الجزائري كجميع عناصر الإثبات متروك لحرية تقدير القاضي حسب

---

[1]– أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2، ط5، ديوان المطبوعات الجامعية، الجزائر، 2010، ص 445.

[2]– نقض جنائي مصري الصادر بتاريخ 21-01-1983، مشار إليه في– عبد الحميد الشواربي، التعليق الموضوعي على قانون العقوبات، منشأة المعارف، الإسكندرية، 2003، ص 514.

المادة 213 من قانون الإجراءات الجزائية[1]، كما أن تراجع صاحب الاعتراف لا يلغي وجوده لو عدل عنه، وللقاضي السلطة التقديرية في أن يعتد بالإنكار اللاحق لهذا الاعتراف[2].

ونرى بأن أدلة الإثبات التقليدية كالاعتراف أو الشهادة في الجرائم المرتكبة بالوسائل لالكترونية الواقعة على التوقيع الالكتروني تعزز قيمة الدليل الالكتروني المستمد من الوسائل الالكترونية، ومن تطبيقات القضاء الأمريكي في هذا الشأن قضية wiliams [3].

والاعتراف في جرائم التوقيع الالكتروني هو إقرار المتهم بأنه ارتكب أحد جرائم التوقيع الالكتروني، كأن يقر متهم في جريمة تزوير توقيع الكتروني بأنه هو من قام بتغيير الحقيقة في التوقيع.

الفرع الثاني: الشهادة

للشهادة أهمية ودور أساسي في الإثبات الجنائي، تعمل بها كل النظم القانونية، وبتطور وسائل الاتصال الحديثة ظهر معه ما يسمى بالشهادة الالكترونية عن بعد، لذلك سنتطرق إلى الشهادة العادية، ثم إلى الشهادة الالكترونية عن بعد.

أولا: الشهادة العادية الحضورية

تعد الشهادة من أدلة الإثبات الجنائي ذات الأهمية البالغة، إذ كثيرا ما تكون للشهادة وخاصة تلك التي يدلى بها فور وقوع الحادث أكبر الأثر في الحكم بالإدانة أو بالبراءة لما تقوم

---

[1]– المادة 213 من قانون الإجراءات الجزائية التي تنص على أن "الاعتراف شأنه كشأن عناصر الاثبات يترك لحرية تقدير القاضي ".

[2] – أحمد شوقي الشلقاني، المرجع السابق، ص 442 .

* التي تتلخص وقائعها في أن المسماة الضحية jennie التقت بالمتهم wiliams في صيف 2005 في كنيسة، كان المتهم حينها يعمل بمركز رعاية الطفولة، و عمره 27 سنة بينما الضحية قاصر عمرها 13 سنة، وقد تم التواصل بينهما عبر رسائل البريد الالكتروني، وفي لقاء أخر مارس المتهم مع الضحية الجنس، وكانت الدلائل المقدمة من والدة الضحية في= القضية هو رسائل البريد الالكتروني التي تبادلها المتهم مع الضحية مقنعا إياها بممارسة الجنس، وعند مواجهته بهذه الرسائل أقر المتهم واعترف بأنها صادرة عنه، فأدانته المحكمة بناء على تصريحات الشاهدة والدة الضحية، مع إقرار المتهم بأن الرسائل الالكترونية صادرة عنه. الوقائع المشار إليها في : محمود عبد الغني جاد المولى، المرجع السابق، ص 238 .

به بدور الدليل في الدعوى بمفردها ودون أن يؤازرها دليل آخر، من أجل ذلك عنى القانون المقارن بتنظيم أحكام الشهادة وإحاطتها بضمانات متعددة زخرت بها التشريعات الإجرائية المختلفة بغية البعد بها عن كل ما يحتمل التأثير عليها، ولما كانت شهادة الشهود من أهم الأدلة التي يكمن بواسطتها الوصول إلى الحقيقة ومعرفة الجناة، وجب على القاضي أن يخضع الشهادة إلى مناقشة دقيقة لمعرفة مدى صدق شهادة الشاهد ومطابقتها للواقع، بالإضافة إلى حرية القاضي بأخذه بشهادة الشاهد أو رفضها، ويمكن له أن يأخذ بجزء منها ويصرف النظر عن الجزء الآخر، لأن هناك عوامل طبيعية ونفسية واجتماعية تؤثر على الشاهد، فالعاطفة والانفعال والخجل والعداوة والنسب والقرابة والمزاج والعاهات الطبيعية، كل أولئك له تأثير فعال على الشاهد [1].

وينص على الشهادة كدليل إثبات في التشريع الإجرائي الجزائري في المواد 220 إلى 234 من قانون الإجراءات الجزائية، ومن بين أحكامها في جلسة المحاكمة وبعد أن يتحقق رئيس الجلسة من هوية المتهم والقيام باستجوابه عن الوقائع والأفعال المنسوبة إليه من جرائم التوقيع الالكتروني، وبعد أن يكون قد منح النيابة العامة والأطراف الآخرين فرصة توجيه الأسئلة التوضيحية إلى المتهم يقوم بالمناداة على الشهود إن وجدوا، فيتحقق من هوية كل شاهد، حيث يسأله عن اسمه ولقبه وعن عمره وعن قرابته وعن علاقته بكل من المتهم والضحية ثم بعد ذلك يطلب منه أن يحلف اليمين القانونية المنصوص عليها في المادة 93 من قانون الإجراءات الجزائية التي مفادها أن يؤدي الشاهد اليمين ويده اليمنى مرفوعة إلى الأعلى بأن "يقسم بالله العظيم أن يتكلم بغير خوف ولا حقد، وأن يقول كل الحق ولا شيء غير الحق".

وبعد حلف اليمين يطلب الرئيس من الشاهد أن يدلي بشهادته حول ما سمع وما رأى مما يتعلق بالوقائع المسندة إلى المتهم عن جريمة المساس بالتوقيع الالكتروني، طبقا لما ورد النص عليه في المادة 225 من قانون الإجراءات الجزائية الجزائرية.

[1]– هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص 34.

ويقوم الرئيس بحسب المادة 225 فقرة 01 بسماع شهود طالبي المتابعة كشهود النيابة العامة أو شهود الطرف المتضرر باعتبارهم شهود إثبات، ثم ينتقل إلى سماع شهود المتهم باعتبارهم شهود نفي، ما لم يرى الرئيس بما له من سلطة أن ينظم بنفسه ترتيب سماع الشهود، وإذا لم يكن المتهم سبق وأن استدعى شهوده إلى الجلسة وأنه اصطحبهم معه، ويرغب في أن تسمع المحكمة شهادتهم، فإنه يجوز له عند افتتاح جلسة المرافعات أن يطلب من رئيس الجلسة أن يصرح له بسماع شهادة أي شاهد لم يكن قد أستدعي قبل الجلسة لإدلاء شهادته مع مراعاة أن يؤدي الشهود شهادتهم بالجلسة متفرقين بحيث لا يسمع بعضهم شهادة البعض ويعزل الشهود في مكان خاص خارج قاعدة الجلسات إلى ما بعد أداء شهاداتهم.

وللحرص على قيمة الدليل المستمد من سماع أقوال الشهود في الجريمة المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني فإنه يمكن للقاضي إتباع ضوابط محددة تساعده في سماع شهادة الشاهد نذكر منها[1]:

- تحديد النقاط التي ينبغي إثباتها أمام المحكمة تحديد دقيقا.
- وضع أسئلة نموذجية.
- ترتيب الأسئلة وفقا للوقائع ترتيبا منطقيا.
- تحديد الشهود الذين توجه لهم الأسئلة.
- وضع بدائل للأسئلة لمزيد من الشرح في حالة فشل الشاهد في إعطاء إجابات مقنعة.

ثانيا : الشهادة الالكترونية عن بعد

أدرج المشرع الجزائري الشهادة الالكترونية عن بعد لأول مرة في قانون عصرنة العدالة 15-03، المتضمن تقنية المحادثة المرئية عن بعد في الإجراءات القضائية، ثم عدلت بموجب الأمر رقم 20 -04 المؤرخ في 30 أوت سنة 2020، المعدل والمتمم للأمر رقم 66-155

[1] – محمد الأمين البشري، المرجع السابق، ص 131 .

المتضمن قانون الإجراءات الجزائية[1]، الذي نص في المادة 441 مكرر01 على إمكانية استعمال المحادثة المرئية عن بعد لسماع الشهود في مرحلة المحاكمة، وهذا ما يدعونا للتطرق إلى تعريف الشهادة الالكترونية عن بعد، ثم ذكر أنواعها.

أ.تعريفها

هي الشهادة التي لا يكون فيها الشاهد حاضرا جلسة المحاكمة بذاته جسديا وماديا وإنما يتم عبر وسائل الكترونية أو رقمية من خلال شبكة الانترنت مثلا [2].

ومن جهتنا نعرف الشهادة الالكترونية بأنها: إدلاء الشاهد بما رأى أو سمع أو شاهد عن الجريمة، أمام القضاء، عن طريق الوسائل الالكترونية .

ب. أنواع الشهادة باستخدام الوسائل الالكترونية

يجب التمييز بين نوعين من أنواع استخدام الوسائل الالكترونية للقول بصحة الشهادة ، ومن ثم قبول ما ينتج عنها من أدلة .

1. حالات الشهادة المسجلة مسبقا

وهي الحالة التي تكون فيها الشهادة قد تم تسجيلها مسبقا بحيث يمكن عرضها فيما بعد على محكمة الموضوع في التحقيق النهائي الذي تجريه في الجلسة، ومواجهة الشاهد بما صرح به في المحاضر المكتوبة.

وتستخدم السلطات القضائية أحيانا أسلوب تسجيل الشهادة و الإدلاء بالأقوال عموما، لكونه يشكل ضمانة أساسية للمتهمين[3]، كاستعانة جهات الحكم بتسجيلات الكترونية لشهود أمام قاضي التحقيق تمت بطريق المحادثة المرئية عن بعد، بشرط أن يتم تسجيلها على دعامة الكترونية تضمن سلامتها .

---

[1] – الجريدة الرسمية للجمهورية الجزائرية، العدد 57 ، الصادر في 31 أوت 2020 .

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 260 .

[3] – المرجع نفسه، ص 261 .

2 . حالة الشهادة الاليكترونية المرئية عن بعد

وهي التي تكون في التحقيق النهائي أمام محكمة الموضوع حيث يمكن من خلالها الحصول على أقوال الشاهد بشكل سمعي مرئي، عن طريق استعمال تقنية المحادثة المرئية عن بعد، تطبيقا لنص المادة 441 مكرر 01 المعدلة بموجب تعديل قانون الإجراءات الجزائية 20 – 04.

والقضاء قبل ظهور وسائل الاتصال الحديثة يفرض الحضور الجسدي للشاهد، والتي تصل إلى حد توقيع الجزاء عليه لعدم الحضور، أما بعد ظهور الدوائر الاتصالية الالكترونية المتكاملة من مغلقه ومفتوحة، فقد أثير مدى إمكانية قبول الشهادة الفورية عبرها، والذي كان فيه قبولا ففهيا، سيما وأن الشاهد غالبا ما يبرز في هيئته الكاملة في هذا الإطار كما لو كان حاضرا، ولقد كانت بدايات الأخذ بنظام الشهادة الالكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلات إدلاء الشهادة من قبل أشخاص وضعوا في برامج لحماية الشهود فقررت المحكمة الفدرالية العليا قبولها لنظام الشهادة طالما كانت هناك أسباب في القانون تدعوا إليه، بشرط أن يكون حاضرا في الجلسة مرئيا له، وكما لو كان حاضرا فعليا للجلسة [1].

الفرع الثالث: القرائن

القرائن هي صلة ضرورية بين واقعتين، يكون ثبوت الأولى فيها دليلا على حدوث الثانية، أو الصلة بين واقعة ونتيجتها يكون ثبوت الواقعة فيها دليلا على حدوث نتيجتها، وهذه القرائن قد ينشأها القانون فتسمى حينئذ بالقرائن القانونية، وقد يقيمها القضاء، فتسمى عندئذ بالقرائن القضائية أو الدلائل، والقرائن بأنواعها هي من طرق الإثبات غير المباشر أي التي لا تنصب دلالتها على الواقعة المراد إثباتها وإنما على واقعة أخرى تسبقها أو تنتجها بمحض اللزوم العقلي[2].

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص ص 261 – 262 .

[2]– محمد زكي أبو عامر، المرجع السابق، ص 263.

فالقرائن القانونية نوعان مطلقة لا تقبل إثبات العكس كافتراض العلم بالقانون بمجرد نشره في الجريدة الرسمية وقرينة انعدام التمييز في المجنون والصغير غير المميز، وقرينة الاستفزاز في قتل الزوج زوجته وشريكها حال مفاجأته لها متلبسة بالزنا، وقرينة الصحة في الأحكام النهائية. وهذه القرائن محددة في القانون على سبيل الحصر، ولا يجوز إثبات عكسها على نحو يقيد القاضي والخصوم، ولكن القرينة القانونية قد تكون بسيطة يمكن إثبات عكسها، كقرينة ارتكاب شريك الزوجة جريمة الزنا إذا وجد في بيت مسلم في مكان مخصص للحريم، إذا يجوز في هذه الحالات أن يثبت بكافة طرق الإثبات عكس المستفاد من تلك القرينة، أما القرائن القضائية أو ما يسمى بقرائن الأحوال ويطلق عليها بعض الفقه لفظ الدلائل، فهي القرائن التي يستخلصها القاضي من الوقائع الثابتة أمامه بطريقة الاستنتاج وترتيب النتائج على المقدمات، وهي بهذا المعنى لا تدخل تحت حصر وتدخل في صميم عمل القاضي[1].

ومن القرائن في جرائم التوقيع الالكتروني المرتكبة عبر الانترنت استخلاص القاضي من واقعة ضبط مرتكبها بواسطة العنوان الالكتروني للانترنت المستعملة أثناء ارتكاب الجريمة قرينة بسيطة تقبل إثبات العكس على أنه هو من قام بجرم المساس بالتوقيع الالكتروني.

الفرع الرابع: المعاينة

المعاينة لغة هي إدراك الشيء بالعين، وفي الاصطلاح هي الانتقال إلى مكان معين لفحصه وإثبات حاله، وهي من الوسائل التي يصح للمحكمة أن تركن إليها إذا قدرت ضرورتها أوجدتها للكشف عن الحقيقة التي تسعى إلى معرفتها، وللمحكمة في هذا السبيل أن تنتقل إلى أي مكان بناءا على طلب الخصوم أو من تلقاء نفسها، وهي لا تلتزم بإجابة الخصوم إلى طلبهم إذا رأت الأمر واضح إليها أو إذا تبين لها أن المعاينة المطلوبة غير منتجة، أو أنها صارت عديمة الجدوى وتكون كذلك إذا كانت الغاية منها معاينة أمور غير جوهرية في

[1]– محمد زكي أبو عامر، المرجع السابق، ص 264.

الدعوى، أو أنه قد زالت المعالم، فلم يعد الحال كما كانت عليه وقت ارتكاب الجريمة أو وقت الكشف عنها[1].

وإذا رأت المحكمة الانتقال للمعاينة وجب أن يكون انتقالها بكامل هيئاتها أو تندب لذلك أحد أعضائها أو أي قاض آخر، وما تسفر عنه المعاينة يكون دليلا في الدعوى يحق للمحكمة أن تبني عليه حكمها، ولا يقال عندئذ أنها قد حكمت بعلمها، ذلك أنه لا يتصور أن تحكم المحكمة في أي دعوى إلا بناء على علمها، وإنما المحظور عليها أن يحكم بعلم لم تحصله من أوراق الدعوى، أو من التحقيق الذي تجريه أو تأمر بإجرائه بنفسها، فالحظر محله العلم الذي يتوافر لدى المحكمة من خارج الدعوى، ولا يعد العلم الذي تحصله المحكمة نتيجة المعاينة علما خارجا عن نطاقا الدعوى بل هو علم لا يختلف عما تحصله من سماع الشهود ومناقشة الخبراء[2].

وعلى المحكمة إذا انتقلت لمعاينة إحدى الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني أن تراعي السرعة في الانتقال إلى مسرح الجريمة الالكتروني، وأن تصطحب معها أحد خبراء الحاسب بهدف ضبط ومعاينة أدلة الجرم المرتكب، التي قد تكون أدلة مادية كجهاز الحاسب، أو الأقراص الممغنطة، أو الصلبة، أو ذاكرة تحزين البيانات، أو معاينة الكيانات المنطقية كبيانات التوقيع الالكتروني الواقع عليها الاعتداء الموجودة داخل نظام الحاسب.

الفرع الخامس: الخبرة

الخبرة هي أداة لتطبيق العدالة الجنائية في المستقبل فبعد أن كان القاضي يستعين بنظام الأدلة المقبولة، ثم تطورت إلى الاقتناع الشخصي ثم إلى الدليل عن طريق الخبرة العلمية [3].

---

[1]– عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، المبادئ العامة في قانون الإجراءات الجنائية، منشأة المعارف ، الإسكندرية ، 2002 ، ص704.

[2]– المرجع نفسه، ص705.

[3]- Jean larguier , op-cit , p 94 .

والقاضي الجزائي يستعين بأهل الخبرة في الجرائم الواقعة على التوقيع الالكتروني كدليل إثبات، من بينهم مخططو البرامج أي الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تصنيفهم إلى فئتين، وهم مصممو برامج النظم ومصممو برامج التطبيقات، الأولى وهم مصممو برامج التطبيقات الذين يقومون بالحصول على خصائص ومواصفات النظام المطلوب من محل النظم ليقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما الثاني فهم مخططوا برامج النظام فيقومون باختبار وتعديل وتصحيح برامج النظام الداخلي المعقد، أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، مع إمكانية إدخال تعديلات على هذه البرامج أو الأجزاء[1].

وهناك المحللون أي الأشخاص الدين يحللون الخطوات ويقومون بتجميع بيانات نظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن بواسطة الحاسب، وثالثا هناك مهندسو الصيانة والاتصالات وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به، وأخيرا مديرو النظم وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[2] .

وعندما يتم عرض الخبرة العلمية على قاضي الحكم في أحد جرائم التوقيع الالكتروني فهي تخضع لسلطته التقديرية، لأن القاضي دائما غير ملزم بنتائج الخبير وهي تخضع للاقتناع الشخصي[3].

---

[1]– عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي، المرجع السابق، ص 224 . وكذلك: هلالي احمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص23 .

[2] – هلالي عبد اللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص 24 .

[3] - Jean larguier , op-cit , p94.

الفرع السادس: الذكاء الاصطناعي ودوره في إثبات جرائم الاعتداء على التوقيع الالكتروني

أثبتت تقنيات الحاسب نجاحها في جمع الأدلة الجنائية و تحليلها واستنتاج الحقائق منها كما يمكن الاستعانة بالذكاء الاصطناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومنه استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب وفق برامج صممت خصيصا لهذا الغرض[1]، كما أن انتشار ظاهرة استخدام تقنيات الحاسب الآلي في ارتكاب الجريمة يصبح من الضروري الاستعانة بذات التقنيات في مواجهة جرائم الاعتداء على التوقيع الالكتروني، بواسطة الحاسب الآلي نفسه في جمع الأدلة وترتيبها وتحليل القرائن واستنتاج الحقائق، وكما هو معلوم أن تقنيات الحاسب الآلي استخدمت في فحص وتسجيل الآثار المادية والحيوية والبيانات السمعية والبصرية، إلا أن الجديد هو استخدام الحاسب الآلي في صناعة البينة وإثبات الحقائق بعمليات حسابية بحثة فيما يعرف بالذكاء الاصطناعي للاستعانة بها في كشف الجرائم التقليدية والالكترونية، والتي تقوم على أساس حصر الحقائق والاحتمالات والأسباب والفرضيات، ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج صممت لهذا الغرض، وتعتمد نظرية الذكاء الاصطناعي على الآثار الموجودة في مسرح الجريمة وأقوال الشهود والقرائن التي يتم تحليلها تحليلا منطقيا بالقدر الذي يتوافق مع الحقائق والأسباب، ويقوم البرنامج بكشف كافة أكثر الاحتمالات وصولا إلى حقيقة الجريمة[2]، وتبقى دائما السلطة التقديرية للقاضي الجنائي في تقدير الأدلة المطروحة أمامه، إلا أن التطور التكنولوجي كالذكاء الاصطناعي يساعده في تكوين عقيدته واقتناعه.

---

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 308 .

[2]-John. r . josephson and susan josephson , abductive inference computation , philosophie and technologie , combridge , 1994 . p 86.

نقلا عن : محمد الأمين البشري ، المرجع السابق، ص126 .

المطلب الثاني: الدليل الالكتروني وأثره على الاقتناع الشخصي للقاضي الجنائي

العلم والتقنيات الحديثة أحدثت ثورة في مجال البحث عن الحقيقة في المواد الجنائية[1]، ومن هذه التقنيات الدليل الالكتروني الذي يعد أحد أبرز الأدلة الحديثة المفرزة نتيجة التطور التكنولوجي، وغالبية الجرائم الالكترونية الواقعة على التوقيع الالكتروني يكون إثباتها بواسطة الدليل الالكتروني، لذلك سنتطرق إلى مفهومه، ثم إلى أثره على قناعة القاضي.

الفرع الأول: مفهوم الدليل الالكتروني

الدليل الالكتروني له ذاتية خاصة تميزه عن باقي الأدلة التقليدية، ما جعله يحمل في طياته العديد من الخصائص والتنوع وصعوبة في الحصول عليه، وقد عزفت العديد من التشريعات إعطاء تعريف له تاركة المجال للفقه، لذلك سنتطرق إلى بيان تعريفه، خصائصه، تمييزه عن الدليل المادي، أنواعه، صعوبة الوصول إليه.

أولا: تعريف الدليل الالكتروني

عرف Casey الدليل الالكتروني بأنه جمع البيانات الرقمية التي تثبت أن هناك جريمة قد ارتكبت، وعرف أيضا بأنه معلومة محررة مأخوذة في شكل رقمي، بحيث يستخدمها الحاسوب في انجاز مهمة معينة أو هو الدليل المأخوذ من الكمبيوتر وهو دائما في شكل مجالات كهربائية أو نبضات مغناطيسية يمكن جمعها وتحليلها من خلال برامج وتطبيقات تكنولوجية خاصة وذلك من أجل اعتماده أمام سلطات الاستدلال والتحقيق والمحاكمة ، وعرف أيضا بأنه الجزء الناتج عن الاستعانة بتقنية معالجة البيانات والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة معينة أو بمعنى آخر فإنه كلما كان هناك مزج بين المعلومات والمعالجة الآلية لها كلما كان هناك دليل الكتروني [2]، وعرف أيضا بأنه الدليل

---

[1] - Carolie ambroise casterot , op- cit, p 133.

[2] – هذه التعاريف مشار إليها في : محمود جاد المولى، المرجع السابق، ص ص 26 – 27 .

المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة [1].

وعرف بأنه الدليل دو الطابع الرقمي مأخوذ بواسطة البرمجيات تكنولوجية معينة من الأجهزة التي تعمل بنظم تشغيل حاسوبية سواء تمثل في نصوص مكتوبة أو صور أو أصوات أو مواد فيلمية بغرض إثبات جريمة معينة وتقرير الإدانة أو البراءة فيها [2]، وعرف أيضا بأنه الدليل الذي يحتاج إلى معالج رقمي لقراءته أو فهم محتواه[3].

وقد عرفت المنظمة الدولية للتعاون في مجال تقييم أدلة الحاسب الآلي في مارس 2000 بأنها المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها، ثم أعادت تعريفه في أكثوبر 2001 بأنها المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية [4].

وهناك ما يعرف بالبصمة الرقمية كدليل الكتروني وهو الدليل المأخوذ من أجهزة الكمبيوتر يكون في شكل مجالات مغناطيسية أو نبضات كهربائية ، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء[5].

ويمكننا تعريف الدليل الالكتروني بأنه: كل ما هو مخزن في وسط الكتروني، يمكن الاعتماد عليه أمام الجهات القضائية.

ثانيا : التمييز بين الدليل الالكتروني والمادي

يمتاز الدليل الرقمي عن الدليل المادي بما يلي:

يختلف الدليل الالكتروني عن الدليل المادي من حيث الطبيعة والمضمون، إذ يترك آثارا مادية كاعتراف مكتوب أو مال مضبوط في جريمة رشوة أو بصمة أصبع في مسرح الجريمة،

---

(1) – عبد الحميد عبد المطلب ، زبيدة محمد جاسم، عبد الله عبد العزيز، المرجع السابق، ص 2240 .

(2) – محمود جاد المولى، المرجع السابق ، ص 28 .

(3) – حازم محمد حنفي ، المرجع السابق، ص 09 .

(4) – المرجع نفسه، الصفحة نفسها.

(5) – عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، المرجع السابق، ص 2238.

أما الدليل الالكتروني فيترك نبضات رقمية تتعامل مع القطع الصلبة للحاسوب، كما أن طريقة نسخ الدليل الرقمي من أجهزة الحاسب تقلل أو تعدم تقريبا مخاطر إتلاف الدليل الأصلي بحيث تتطابق طريقة النسخ مع طريقة الإنشاء، زيادة على أنه إذا تم مسحه فإن الأصل يبقى على القرص الصلب للحاسوب فيمكن استرجاعه بوسائل تقنية معينة، على عكس الدليل المادي الذي هو عرضة للإزالة أو التلف بغير استرجاع كتمزيق المحرر الورقي [1]، فالصعوبة النسبية لتحطيم أو محو الدليل الالكتروني، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الحاسب يمكن للدليل الالكتروني الرقمي أن يعاد تظهيره من خلال الحاسب نفسه [2]، بالإضافة إلى أن التعامل مع الدليل الالكتروني أصعب من الدليل المادي لأن الأول يتطلب قدرات ذهنية فنية عالية لإزالته كإزالة التلاعب في التوقيع الالكتروني للرقم السري في بطاقات الائتمان، أما الدليل المادي فيمكن لأي شخص مثلا إزالته كمسح بقع الدم، أو تمزيق الورقة المزورة في جريمة التزوير، أو إخفاء الجثة في جريمة القتل، أو رمي المادة المخدرة في جرائم المخدرات.

ثالثا: خصائص الدليل الالكتروني

للدليل الالكتروني جملة من الخصائص منها:

– الاتساع العالمي لمسرح الدليل الالكتروني الرقمي يمكن من مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية وبمناطق مختلفة من العالم ، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبيا.

– امتيازه بالسعة التخزينية العالية فآلة الفيديو الرقمية يمكنها تخزين الآلاف من الصور.

– باستخدام التطبيقات والبرامج الصحيحة يكون من السهولة ما إذا كان الدليل الرقمي قد تم العبث فيه أو تعديله وذلك لإمكانية مقارنته بالأصل.

---

[1] – محمود جاد المولى، المرجع السابق، ص 31 .

[2] – عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، المرجع السابق، ص 2240 .

– يمكن من خلال الدليل الرقمي ترصد المعلومات عن الجاني وتحليلها في ذات الوقت ، فالدليل الرقمي يمكن أن يسجل تحركات الفرد كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه[1].

رابعا: صعوبات التعامل مع الدليل الالكتروني

يتسم الحصول على الدليل الالكتروني وملاحقة مرتكبي الجرائم الالكترونية الواقعة على التوقيع الالكتروني بصعوبة وتعقيد بالغين مردها جملة من الأسباب أبرزها ما يلي:

أ.إخفاء الجريمة

الجرائم التي تقع على الحاسبات وشبكات المعلومات أو بواسطتها مستترة خفية في أكثر صورها، لا يلحقها المجني عليه غالبا أو يدري حتى بوقوعها و الإمعان في حجب وإخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات أو الدبدبات الالكترونية التي تسجل البيانات عن طريقها، وذلك بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات غالبا لدى مرتكبيها [2].

ب.افتقار الآثار التقليدية

يكون من السهل ارتكاب العديد من الجرائم كاختلاس المال والتزوير بإدخال بيانات غير معتمدة في نظام الحاسب الآلي أو تعديل برامجه أو البيانات المخزنة داخله دون أن يتخلف على ما يشير حدوث هذا الإدخال أو التعديل، ما يؤدي إلى صعوبة الوصول إلى مرتكبي هذه الجرائم لأنه في سياق هذه العمليات وعدم ترك التغييرات في البرامج والبيانات أثار كتلك التي يخلفها التزوير المادي في المحررات التقليدية [3].

---

[1]– عبد الحميد عبد المطلب ، زبيدة محمد جاسم، عبد الله عبد العزيز ، المرجع السابق، ص ص 2240 – 2241 .

[2]– هشام رستم، المرجع السابق، ص 420 .

[3]– المرجع نفسه، ص 425 .

ج.إعاقة الوصول إلى الدليل بوسائل الحماية التقنية

هناك مجموعة أشياء كثيرة يقوم بها الفاعل قبل مغادرة مسرح الجريمة، في الأول هو إزالة أي ملف استخدمه كأداة للاعتداء به على الضحية، والثاني هو تعديل السجلات بهدف محو عمليات الدخول التي قام بها[1].

كما أن المجرم الالكتروني يقوم بإحاطة البيانات المحزنة الكترونيا بشبكات سياج من الحماية التقنية لإعاقة المحاولات الرامية للوصول غير المشروع للاطلاع عليها أو استنساخها كذلك يمكن للمجرم المعلوماتي زيادة صعوبة عملية التفتيش المتوقع عن الأدلة التي تدينه بحزام من التدابير الأمنية كاستخدام كلمات سر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها، ويشكل استخدام تقنيات التشفير لهذا الغرض أحد اكبر العقبات التي تعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، والتي تحد من قدرة جهات التحري والتحقيق على قراءتها، ما يجعل صون البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالإسرار التجارية العادية والالكترونية أو تدابير الأمن أو الدفاع أمر بالغ الصعوبة[2].

د, سهولة محو الدليل الالكتروني أو تدميره

من الصعوبات التي تعترض عملية الإثبات في الجرائم المعلوماتية سهولة محو الجاني أو تدميره لأدلة الإدانة في فترة زمنية قصيرة ، فضلا عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه حسبما تشهد بذلك عديدة سابقة علة خطأ في نظام الحاسب أو في الشبكة أو في الأجهزة، يسعى من خلالها الجاني لتدمير الأدلة على إدانته بطريقة آلية متطورة كقضية تهريب الأسلحة في النمسا [3]، وهذه الصعوبة تمس أيضا جهات التحقيق فالدليل الناشئ عن الوسائل

---

(1) -Peter stephenson, op- cit , p 34 .

(2)– هشام رستم ، المرجع السابق ، ص 467 .

* وتتلخص وقائع القضية في أن أحد مهربي الأسلحة أدخل تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر على الحاسب من خلال لوحة مفاتيحه=

الالكترونية لا يمكن التطبيق بشأنه الإجراءات التقليدية في مجال المعلومات ووسائل الاتصال الحديثة، وذلك نظرا لطبيعته فهو يتطلب خبرة فنية معينه لا تتوافر لدى جميع سلطات التحقيق فبعض الجرائم التي ترتكب بالوسائل الالكترونية تقتضى البحث في ذاكرة الأقراص الصلبة وغيرها من مستخرجات هذه الوسائل كما قد يستخدم المجرم المعلوماتي الوسائل الالكترونية في ارتكاب الجريمة، ما يتطلب الحرص والعناية الفائقة أثناء البحث عن الدليل الالكتروني حتى لا يصيبه التلف أو التشويه أو التحريف [1].

هـ. صعوبة الوصول إلى الدليل الالكتروني ومعرفة الفاعل

البيانات المحزنة الكترونيا أو المنقولة عبر شبكات الاتصال تتمتع بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها، كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو وضع تعليمات خفية بينها أو ترميزها لإعاقة أو منع الإطلاع عليها أو ضبطها لدا فاستخدام تقنيات التشفير لهذا الغرض يعد إحدى العقبات الكبرى التي تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تقلل من قدرة جهات التحري و التحقيق ما يجعل حرمة البيانات الشخصية

بالنسخ أو الطبع محو وتدمير البيانات كلها، ومع أن تعديل برمجة نظام الحاسب كان قد أجري خصيصا من قبل الفاعل للحيلولة دون نجاح أجهزة المتابعة في إجراءاتها المتوقعة للبحث عن الأدلة وضبطها على أن لم يفلح في تحقيق هذا الهدف نتيجة شعور أو إحساس المتخصصين في معالجة البيانات بالجهاز المركزي لمكافحة الغش المعلوماتي بالنمسا بأن شيئا ما في تشغيل نظام حاسب الفاعل قد جرى تغييره ، وقيامهم بناء على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسباتهم .

وفي حالة أخرى شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية للوصول لها من شانه محو هذه البيانات بأكملها بواسطة مجال كهربائي إذا ما تم اختراقه من قبل شخص غير مرخص له. الواقعتان مشار إليهما في: هشام رستم ، المرجع السابق، ص 430 .

[1] – محمد حسين على محمود، المرجع السابق، ص 208 .

للتوقيع الالكتروني المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية أو تدابير الأمن والدفاع أمر بالغ الصعوبة[1] .

وأكثر ما تتجه النظم المعلوماتية من أدلة لبيانات غير مرئية لا تفصح عن شخصية معينة مسجلة إلكترونيا محفوظا على دعائم أو وسائط التخزين ضوئية أو ممغنطة لا يمكن للإنسان قراءتها إلا عن طريق الآلة نفسها لا يترك التعديل أو التلاعب فيها أي أثر مما يقطع غالبا كل صلة بين المجرم والجريمة، ويكون عائقا يحول دون الكشف عن شخصية الفاعل[2].

خامسا: تقسيمات الدليل الالكتروني

قامت وزارة العدل الأمريكية بتقسيم الدليل الالكتروني عام 2002 إلى ثلاث مجموعات وهي: المجموعة الأولى السجلات المحفوظة في الحاسوب مثل البريد الالكتروني ورسائل غرف المحادثات وملفات برامج معالجة الكلمات، والثانية السجلات التي تعتبر مخرجات لبرامج الحاسوب ولم يتم في إعدادها العنصر البشري مثل سجلات الهاتف وفواتير أجهزة السحب الآلي atm ، والثالثة السجلات التي يتم تقديمها لبرامج الحاسوب ويتم معالجتها بإجراء حسابات عليها [3].

الفرع الثاني: حجية الدليل الالكتروني في الإثبات الجنائي

الإثبات الجنائي مر عبر مراحل متعددة منها الإثبات المقيد بدليل معين، ثم تطور لنظام الاقتناع الشخصي للقاضي الجنائي، ومع ظهور الإجرام الالكتروني كالجرائم الالكترونية الواقعة على التوقيع الالكتروني نتج عنه الدليل الالكتروني المثبت لها، لذلك سنتطرق إلى مدى قبول الدليل الالكتروني في أنظمة الإثبات الجنائي، ثم سنتطرق إلى مشكلات قبول الأدلة المحصلة من الوسائل الالكترونية.

---

[1] – أشرف قنديل ، المرجع السابق ، ص 104 .

[2]– هشام رشم، المرجع السابق، ص 424.

[3] – محمود جاد المولي، المرجع السابق، ص 39 .

أولا: مدى قبول الدليل الالكتروني في أنظمة الإثبات الجنائي

يتنازع قوة وسائل الإثبات المختلفة نظامان: نظام الأدلة القانونية ونظام الاقتناع الشخصي[1]:

ففي نظام الأدلة القانونية يحدد المشرع الأدلة المقبولة في الإثبات، كاستلزام الاعتراف في بعض الجرائم أو تعدد الشهود، أو توافر شروط خاصة فيهم كالذكورة أو السن أو المهنة. ومتى توافرت هذه الأدلة حكم القاضي بالإدانة وإلا قضى بالبراءة. وواضح أن دور القاضي يقف عند التحقق من توافر هذه الأدلة بشروطها القانونية دون اعتداد برأيه أو باقتناعه الشخصي، وقد نشأ هذا النظام في عهد الإمبراطورية الرومانية أثر العدول عن نظام المحلفين وتركيز السلطة القضائية في أيدي القضاة المحترفين، ثم ساد في التشريعات المختلفة في القرون الوسطى وما بعدها.

ومن تطبيقات هذا النظام، أن الشريعة الإسلامية تستلزم أربع شهود على جريمة الزنا، ورجلين في الشهادة على بقية الحدود، ورجلين أو رجل وامرأتين في الشهادة على حقوق العباد، كما تتطلب في الشاهد شروطا معينة تتعلق بالسن والسلامة البدنية والعدالة.

أما نظام الاقتناع الشخصي أو حرية تقدير الأدلة، فهو الوجه الآخر في مبدأ حرية الإثبات، وقد نشأ مع الثورة الفرنسية عندما أدخلت نظام المحلفين والإثبات الجزائي المبني على حرية القاضي في تكوين عقيدته وذلك في سنة 1791، ثم استقر نهائيا في تشريع التحقيق الجنائي الفرنسي الذي وضع سنة 1808، وقانون الإجراءات الجزائية الفرنسي المعمول به حاليا، ومنه انتقل إلى الشرائع التي نقلت عن القانون الفرنسي ومنها التشريع الجزائري الذي نص عليه في المادة 212 فقرة 01 بقولها:" وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، وكذلك في المادة 307 المتضمنة للتعليمات التي يتلوها رئيس محكمة الجنايات قبل مغادرة قاعة الجلسة، ومنها أن يقيموا حكمهم على أساس اقتناعهم الشخصي وحريتهم في تقدير الدليل.

[1]– أحمد شوقي الشلقاني، المرجع السابق، ص ص 440-441.

ويسيطر على الإثبات الجنائي في النظم اللاتينية مبدأ حرية القاضي في الاقتناع، فالقاضي الجنائي يستطيع أن يستمد عقيدته من أي دليل يرتاح إليه وجدانه، وهذه الحرية التي يتمتع بها القاضي الجنائي ليست مقررة لكي تتسع سلطته من حيث الإدانة والبراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية، فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على الحصول إلى الحقيقة، والقاضي على الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه يلتزم ببيان الأدلة التي استمد منها اقتناعه، فليس الحرية أن يطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر في استخلاص الحقيقة من أي مصدر مشروع، فهناك طرق للإثبات نص عليها قانون الإجراءات الجزائية وهي التي تعتبر مشروعة والتي يجوز له استخلاص الحقيقة منها[1] .

كما يلتزم القاضي بأن يبني اقتناعه على عملية عقلية منطقية تقوم على الاستقراء والاستنباط ينتهي في ختامها على نتيجة معينة فلا يجب أن يفهم القاضي من مبدأ حرية الاقتناع أن يتحلل من مراعاة القواعد اللازمة لقبول أدلة الإثبات فالقاضي حر في أن يعتقد أو لا يعتقد في قيمة الأدلة المطروحة، لكنه لا يملك التحكم في هذا الاعتقاد فاليقين المطلوب عند الاقتناع ليس هو اليقين الشخصي للقاضي، وإنما هو اليقين القضائي ، الذي يصل إليه القاضي بناء على العقل والمنطق [2].

وفيما تعلق بمسألة الأدلة الالكترونية في النظم اللاتينية منها التشريع الجزائري، فإنه يتعين قبول الدليل الالكتروني الرقمي في الإثبات أمام المحاكم الجنائية لما يمثله من قيمة إثباتيه في مجال الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني ، ففي الدول التي تأخذ بنظام حرية الإثبات كالتشريع الفرنسي الذي أخد بالأدلة الرقمية أو الناشئة عن الآلة مثل الرادارات والأجهزة السينمائية والتصوير وأشرطة التسجيل والتصنت، وتطبيقا لذلك قضت محكمة النقض أن أشرطة التسجيل الممغنطة التي يكون لها قيمة في الإثبات يمكن أن تكون

---

[1]– أشرف قنديل، المرجع السابق، ص ص 70 – 71 .

[2] – أحمد فتحي سرور، المرجع السابق، ص617 .

صالحة للتقديم أمام القضاء الجنائي، وعندما أصدر المشرع الفرنسي القانون رقم 230 – 2000 الصادر في 13 مارس 2000 بشأن الإثبات في مجال تكنولوجيا المعلومات والتوقيع الالكتروني الذي توسع فيه في مفهوم الكتابة التقليدية والالكترونية[1]، وفي التشريع الجزائري نصت المادة 323 مكرر من القانون المدني "أنه يعتبر الإثبات بالكتابة في الشكل الالكتروني، كالإثبات بالكتابة".

أما في التشريعات التي تأخذ بنظام الإثبات المقيد كالولايات المتحدة تضمنت قواعد الإثبات الفدرالي نصا صريحا يسمح بالاعتداد بالأدلة الالكترونية فتعرف المادة 1001 فقرة أ الكتابة بأنها تتكون من حروف أو كلمات أو أرقام أو ما يعادلها مسجلة بأي شكل من الأشكال، غير أنها مرهونة بحسب المادة 1002 من ذات القانون بتقديم الأصل إلا إذا نص على خلاف ذلك كنص الفقرة د من المادة 1001 التي تنص على قبول الدليل الالكتروني باعتباره مستندا أصليا مادام أن البيانات كانت مطبوعة أو مخرجة بأي شكل آخر مقروء بالعين المجردة وتعبر عن البيانات المخزنة الكترونيا بشكل دقيق[2].

كما أجاز القانون الفيدرالي الأمريكي الصادر في 30 جوان 2000 بشأن التجارة الالكترونية استخدام الأصوات في إجراء التوقيع الالكتروني، وتوسع في مفهوم المحرر ليشمل المحررات الالكترونية حيث منح الحجية القانونية للأصوات المسجلة على شرائط أو دعائم الكترونية وعلى مستوى الولايات فثمة قوانين عديدة تحوي نصوصا تعالج بوجه خاص مشكلات الأدلة الالكترونية كولاية كاليفورنيا تنص المادة 500 فقرة 05 من قانون الإثبات المعدل سنة 1983 على أن المعلومات والبرامج المسجلة الكترونيا أو نسخ أيهما لا يجب وصفها أو معاملتها على أنها غير مقبولة بمقتضى قاعدة أفضل الأدلة، وفي ولاية ايوا جاءت المادة 716 فقرة 16 من القانون الجديد لجريمة الحاسب لسنة 1984 بقاعدة إثبات جديدة تقضي بأنه في أحوال الاتهام

[1] – محمود محمد جابر، المرجع السابق، ص 127 .

[2] – المرجع نفسه، ص 130 .

تكون مخرجات الحاسب مقبولة كدليل على الكيان المنطقي أو البرنامج أو البيانات التي يحويها أو المأخوذة من الحاسب، بغض النظر عن تطبيق قاعدة إثبات تقضي بخلاف ذلك [1].

ثانيا : مشكلات قبول الأدلة المحصلة عن الوسائل الالكترونية

نظرا إلى الطبيعة الخاصة التي تتميز بها الأدلة المستخرجة من الوسائل الإلكترونية وصعوبة إجراءات تحصيلها، فإن قبولها في الإثبات قد يثير العديد من المشكلات، لأن مستودع هذه الأدلة هو الوسائل الإلكترونية، التي من الممكن التلاعب فيها وتغيير الحقيقة التي يجب أن تعبر عنها، والمشكلات التي تثيرها هذه الأدلة ليس لأن لها أولا حجية على القاضي الجنائي، وإنما المشكلة تتعلق بما تحدده كيفية ضمان مصداقية هذه الأدلة وأنها تعبر بالفعل عن الحقيقة التي تهدف إليها العدالة الجزائية، لذلك سنتطرق إلى مدى قبول مخرجات الوسائل الالكترونية في الأنظمة اللاتينية والأنجلوساكسونية، ولقبول هذه المخرجات في الإثبات الجنائي على قدر من الصعوبة في تحصيلها مما يتطلب شروط محددة نتطرق لها من خلال بيان شروط قبول الأدلة المحصلة من الوسائل الالكترونية.

أ.مدى قبول حجية مخرجات الوسائل الإلكترونية كأدلة في أنظمة الإثبات الجنائية

كما سبق بيانه للأنظمة الكبرى المنظمة للإثبات الجنائي وهي الأنظمة اللاتينية والتي تبانها التشريع الفرنسي والتشريعات التي أخذت منه كالتشريع الجزائري، أما النظام الثاني وهو النظام الأنجلوساكسوني كتشريع الولايات المتحدة الأمريكية وبريطانيا، لذلك سنتطرق إلى موقف كلا من النظامين من حجية مخرجات الوسائل الالكترونية في الإثبات الجزائي.

1. موقف الأنظمة اللاتينية

موقف الأنظمة اللاتينية كالفقه الفرنسي مثلا يدرس مخرجات الوسائل الالكترونية في المواد الجنائية، كالمستمدة من جرائم التوقيع الالكتروني، ضمن مسألة قبول الأدلة الناشئة عن الآلة والأدلة العلمية مثل أشرطة التسجيل وأجهزة التصنت والتي أخدها المشرع وقابلها القضاء في

[1] – محمود جابر، المرجع السابق، ص 130 .

إطار مجموعة من الشروط من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة وأن يتم مناقشتها حضوريا من طرف الأطراف، ولا يختلف الأمر بالنسبة لمخرجات الحاسب الآلي، ولكي يصل اقتناع القاضي الجزائي إلى حد الجزم واليقين والذي يكون نسبيا فقط لا مطلقا، فالمطلوب منه أن يبين عقيدته على أساس احتمالات درجة عالية من الثقة لا يهزها أو يناقضها احتمال آخر، فالإدانة لا يمكن إقامتها بأي شكل على مجرد ظنون وتخمينات، وعلى ذلك فالقاضي الجنائي حر في تقدير مخرجات الكمبيوتر، أما الحكم بالبراءة فهو تأكيد لمبدأ البراءة الذي يتمتع به الفرد من ميلاده [1].

ويصل القاضي إلى يقينية مخرجات الوسائل الالكترونية عن طريق نوعين من المعرفة أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينتها وتفحصها والثانية المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج عن طريق الربط بين هذه المخرجات والملابسات التي أحاطت بها لما ينته القاضي إلى الجزم بنسبة الفعل إلى المتهم المعلوماتي كان من المتعين عليه أن يقضي بالبراءة فالشك يجب أن يستفيد منه المجرم المعلوماتي[2].

وتذهب التشريعات المقارنة اللاتينية إلى قبول مصادر المعلومات الخاصة بالحاسب الآلي أو المتحصل عليها من أنظمته مثل مخرجات نظام المعالجة الآلية للبيانات المكتوبة على الشاشة، أو المسجلة على دعائم ممغنطة أو المخزنة داخل نظام المعالجة كأدلة يقوم عليها الإثبات الجنائي، وهذه الأدلة المحصلة من الوسائل الإلكترونية تخضع للسلطة التقديرية للقاضي الجنائي، فإن استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد اقتناعه ويعول عليها في الحكم الذي ينتهي إليه.

ولقد أثيرت في فرنسا مشكلات الإثبات بمحاضر المخالفة التي تتم عن طريق جهاز السنموتر، وانتهى القضاء هناك إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة بالوسائل الالكترونية حجة بذاتها في الإثبات، وإنما ذهب كل من الفقه والقضاء إلى أن أي محضر لا

---

[1]- هلالي أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص 85 .

[2]- المرجع نفسه، ص91.

تكن له قوة إثباتيه إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقق منها بنفسه، وبناء على ذلك فإن المحضر الذي يحرره عقب عملية المراقبة الإلكترونية للسيارات لا يصلح دليلا على ارتكاب الجريمة، حيث أن محرري المحضر لم يتحققوا بأنفسهم من ارتكاب المخالفة، فمخالفة القيادة بسرعة التي تزيد عن السرعة المقررة والتي يتم ضبطها عن طريق جهاز الرادار طبقا لقانون المرور، لا يكون قد شاهد بنفسه المخالفة وإنما قام بتسجيلها فقط عن طريق الإشارة اللاسلكية التي تكون قد وصلت إليه، ولذلك فإن تقدير مخالفة المرور عن هذه المخالفة لا يمكن أن يحل محل محضر جمع الاستدلالات ولا يصلح لأن يكون دليلا قائما بذاته لإثبات المخالفة[1]، ويشترط لقبول الأدلة الالكترونية الناتجة عن استخدام الرادار في رصد سرعة السيارات المتجاوزة للسرعة المحددة في القانون ثلاث شروط أولها أن يجرى فحص فني دوري لأجهزة الرادار، وثانيها أن يتم استخدامها بطريقة فنية سليمة، وثالثها أن يتم اختبار الرادار قبل تشغليه واستخدامه[2]، وهذه الشروط يمكن الاستعانة بها في حالة التعامل مع وسيلة الكترونية يستمد منها دليل الكتروني في أحد جرائم التوقيع الالكتروني، كالبرنامج المعلوماتي للتوقيع الالكتروني الذي بحوزة جهات التصديق الالكتروني، فالدليل الالكتروني المستمد منه يجب أن يحصل عليه بطريقة سليمة، مع إجراء فحوصات تقنية دورية له.

ولذلك فالمخرجات المحصلة من الوسائل الإلكترونية لا تمثل مشكلة في النظام اللاتيني حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع، فالفقه والقضاء الفرنسي يتناول حجية هذه المخرجات في المواد الجنائية ضمن مسألة قبول الأدلة المحصلة عن الآلة أو ما يسمى بالأدلة العلمية والتي يجب ألا تقبل كطرق إثبات إلا إذا توفرت الشروط المقررة بذلك، وما توصل إليه الفقه والقضاء الفرنسي يصدق الأخذ به في التشريع الجزائري [3].

---

[1]– أشرف قنديل، المرجع السابق، ص 72 .

[2] – محمود جاد المولى ، المرجع السابق، ص 314 .

[3] – أشرف قنديل، المرجع السابق، ص 72 .

2.موقف النظام الأنجلوساكسوني

يثير قبول الأدلة المحصلة من الوسائل الإلكترونية مشكلات عديدة في ظل قواعد الأنجلو أمريكية للإثبات الجنائي، والتي تعتنق كمبد أساسي الإثبات بالشهادة للواقعة محل الإثبات، ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية والتي هي عبارة عن إشارات إلكترونية ونبضات ممغنطة يمثل مشكلة أمام القضاء في هذا النظام قد لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتولدة منها ووضع أيديهم عليها، وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية [1].

ولقد نصت المادة 69 من قانون الإثبات الجنائي الانجليزي سنة 1948 على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعوا إلى الاعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة، ويجب كذلك أن يكون الحاسب الناتج منه المخرج الإلكتروني يعمل بكفاءة وصورة سليمة، ويلاحظ أن هذه التحفظات الأخيرة لا تطبق إلا إذا كانت مطبوعات الحاسب دليلا حقيقيا أو أصليا وليس مجرد نقل عن الغير، وتقبل مخرجات الوسائل الإلكترونية كوسائل إثبات في الولايات المتحدة الأمريكية بالنسبة للبرامج والبيانات المخزونة فيها وبالنسبة للنسخ المستخرجة من البيانات التي يحتويها الحاسب[2]، ومن تطبيقات القضاء الأمريكي قبول مخرجات الدليل الالكتروني واعتبرته دليلا أصليا في قضية frank whitaker ، والتي تتخلص وقائع القضية في أن frank whitaker اتهم بترويج وتوزيع مخدر الماريجوانا وذلك من خلال شبكات ووسائل التواصل الاجتماعي وبتفتيش حاسوب المتهم تم ضبط ما يفيد أنه يقوم بتوزيعها، وقامت بالاستعانة بسجلات الحاسب وطباعة صورة مطبوعة عنها كدليل مستخرج من الحاسب أدانته على أساسه، وعند استئناف الحكم طعن المتهم بتشكيكه في قبول الأدلة المستمدة من حاسوبه لأنها كانت في صورة مستخرج مطبوع وليس دليلا أصليا، كما شكك أيضا في طريقة طباعتها إلا أن المحكمة رفضت دفوعه واعتبرت

---

[1]–أشرف قنديل، المرجع السابق، ص 73 .

[2]– المرجع نفسه، ص 74 .

المستخرج دليلا أصليا بشهادة الخبير التقني الذي أكد سلامة عملية طباعة السجلات من الحاسوب [1].

كما اقترح بعض الفقهاء الانجليز في حالة ما إذا كان الحاسب موضوعا للاستخدام غير المصرح به فإن أي أدلة ناتجة عنه بخصوص أصل ومدة الاستعمال لن يكون مقبولا، لأن سوء استخدام الحاسب في حد ذاته أدى إلى أن الجهاز لا يعمل كما ينبغي، لذا فإن عدد من الفقهاء ناقش مسألة إلغاء المادة 69 بخصوص الدليل الناتج عن الحاسب الآلي [2]، وهذا ما تجنبه القضاء الأمريكي في أحكامه المختلفة من أن مخرجات الحاسب يجب أن تكون مقبولة كأدلة إثبات طالما كان الحاسب المتولد عنه يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الثقة والطمأنينة.

ويلخص الفقيه الأمريكي أدوار وايز Edward Wise الوضع بالنسبة لمدى قبول الأدلة الناتجة عن الحاسب بقوله إن الصعوبات الحقيقية في الولايات المتحدة الأمريكية نابعة من عدم الألفة مع تكنولوجيا الحاسب الآلي أكثر من كونها صعوبات قانونية، فمن غير المعتقد على الوجه العموم أن تكون هناك حاجة ماسة إلى سن تشريعات بخصوص التعامل مع مدى قبولية السجلات المعالجة بواسطة الحاسب[3].

ب:شروط قبول مخرجات الوسائل الإلكترونية في أنظمة الإثبات الجنائي

من أجل إضفاء شرعية ومصداقية للأدلة المحصلة عن الوسائل الالكترونية يأخذ بها القاضي وهو مطمئن لها، وجب توافرها على شروط كأن تكون هذه الأدلة يقينية، مشروعة، تمت مناقشتها في معرض المرافعات، لها مصداقية.

---

[1] – الوقائع مشار إليها في: محمود جاد المولى، المرجع السابق، ص 263 .

[2] – هلالي عبد اللاه أحمد، حجية مخرجات الكمبيوتر، المرجع السابق، ص 54 .

[3] – المرجع نفسه، ص 55 .

1.أن تكون هذه الأدلة يقينية

إذا كانت الأدلة المحصلة عن الوسائل الإلكترونية قد توجس منها كل من الفقه والقضاء خيفة من عدم تعبيرها عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف والتحريف والأخطاء المتعددة، فإنه ذلك قد تطلب وجوب توافر مجموعة من الشروط التي قد تضفي عليها المصداقية ومن ثمَ اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية، ولذلك فإنه لقبول هذه الأدلة كأساس تشيد عليه الحقيقة في الدعوى الجنائية سواء أكان الحكم الصادر فيها بالإدانة أو البراءة فإنه يلزم أن تتوافر فيه شروط اليقينية.

وهذا الشرط يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه، وهذا هو اليقين، ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال، والقاضي يمكنه أن يصل إلى يقينية المخرجات المتقدم ذكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها وعن طريق المعرفة العقلية بما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه استنادا إليها [1].

ويلخص الفقيه الألماني ميترماير mettermaier الوصول إلى اليقين بثلاث أساليب، تتمثل الأولى فيما يستخلص من الواقعة من ممكنات فالصور التي تنقلها الحواس للإنسان وتتفق مع الأفكار الممكنة ويزداد تأكيدها عن طريق الخبرة الإنسانية المكتسبة ففي هذه الحالة ينظر لها على أنها حقيقية، وعلى العكس إذا ما كانت تتعارض مع الحواس والمدارك الظاهرة غير المألوفة فإن الشك يدب في النفوس ولا يرى الإنسان سوى الغموض الذي يكتنفها، وثانيها

[1] – أشرف قنديل، المرجع السابق، ص ص 74 – 75 .

الاستدلال المستمد من تقييم الوقائع وهذا يتطلب أن يكون هناك قدرا من التشابه بين أمرين وعلى ضوء هذا التشابه أو الاختلاف يمكن الوصول إلى الأسباب الصحيحة المقنعة، وأخيرا ثالثها الاستنتاجات المستمدة من الظروف إذا كانت مرتبطة بالواقعة [1]، فمثلا إذا وقعت جريمة تزوير توقيع الكتروني على محرر الكتروني، ثم تبين أنه استعمل من طرف شخص مختص في المعلوماتية يحوز على وسائل الكترونية تستعمل في التزوير، فذلك يدعو للاعتقاد بأنه هو من قام بتزويره.

2.يتعين مناقشة مخرجات الوسائل الإلكترونية تطبيقا لمبدأ شفوية المرافعات

لا يجوز للقاضي بحسب المادة 212 فقرة 02 من قانون الإجراءات الجزائية أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات وحصلت المناقشة فيها حضوريا أمامه، فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات في الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم، ويترتب على ذلك أن هذه المخرجات سواء أكانت مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات فيلمية تكون محلا للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة، فإذا كان القاضي الجنائي يحكم باقتناعه وليس باقتناع غيره، فإنه يجب أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناع بقربه من الحقيقة والواقعية التي يصبوا إليها كل قاضي عادل ومجتهد، ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استنادا إلى علمه الشخصي، أو استنادا إلى رأي الغير، إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولدا من عقيدته وهو ليس بتقرير الخبير[2].

---

[1] – هلالي عبد اللاه أحمد، حجية مخرجات الكمبيوتر، المرجع السابق، ص 79 .

[2]– أشرف قنديل، المرجع السابق، ص 67 .

وحتى يكون للقاضي القدرة على مناقشة مخرجات الحاسب يجب أن يكون مسلحا بتقنيات وعلوم الحاسب وتدريبا فنيا خاصا للتعامل مع تقنية المعلومات وأنظمة معالجة البيانات المعقدة ومع الأدلة الناتجة عن الحاسب بشكل دقيق، فلا شك أن هذا التأهيل العلمي يضمن نجاح المهمة التي تناط بالقضاة وهم بصدد مناقشة مخرجات الحاسب على اختلاف عناصرها ومفرداتها [1].

3.يجب أن تكون الأدلة المحصلة من الوسائل الإلكترونية مشروعة

حتى يكون الدليل مشروعا لابد أن من الاستعانة بمعياران أساسيان أحدهما شكلي والأخر موضوعي، أما المعيار الشكلي فهو أن يتم البحث عن الدليل وتحصيله بطريقة يحظرها نص في اتفاقية ملزمة للدولة، أو نص دستوري، أو نص تشريعي أو ينص صراحة استبعاده كدليل إثبات أو يقرر بطلان الإجراء غير المستوفى لما يضعه من الشروط، أما المعيار الموضوعي، طبيعة القناة التي من خلالها استقاء الدليل، ومدى توافقها مع الحقوق والحريات الرئيسية للمواطنين، والمبادئ القانونية العامة، والقيم الأخلاقية والمعنوية السائدة لدى الجماعة ، ونزاهة الجهات القائمة على إدارة العدالة الجنائية، ونسبة الفائدة التي يحققها الدليل بكيفية معينة مقارنة بالأضرار الفردية والاجتماعية التي تنجم عن قبوله [2].

ومن المقرر أن الإدانة في أي جريمة التي قد تصلح لتبنى على دليل أخلاقي، وهذا يتطلب أن تكون الأدلة مشروعة أي أن الحصول عليها يكون قد تمَ وفق قواعد الأخلاق واحترام القانون، فمبدأ مشروعية الدليل الجنائي بالنسبة للوسائل الإلكترونية يتطلب ضرورة اتفاق الحصول على هذه الأدلة بما يتفق والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، ويترتب على ذلك أن إجراءات جمع الأدلة المحصلة من الوسائل الإلكترونية إذا

---

[1] – هلالي عبد اللاه أحمد ، حجية مخرجات الكمبيوتر، المرجع السابق، ص 115.

[2] – أحمد عوض بلال ، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، ط3 ، دار النهضة العربية، القاهرة، 2013 ، ص37 .

خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية [1].

فمشروعية الدليل تتطلب صدقه في مضمونه وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليها، ويجب الحيطة بالنسبة لشرط شرعية الأدلة المحصلة من الوسائل التكنولوجية في الحصول على الأدلة لأنها قد تحتوي على حقيقة علمية تخالف الحقيقة القضائية التي تتطلب لقبول هذه الحقيقة العلمية أن يكون الوصول إليها قد تم بطرق مشروعة، مثلما عملت إيطاليا عندما نصت في المادة 191 من قانون سنة 1989 على عدم صلاحية الدليل الباطل للاستعمال، وهذا يفيد رفض الدليل الغير مشروع سواء أكان هذا الدليل ينتمي إلى الأدلة التقليدية أم أنه ينتمي إلى الأدلة المحصلة من الحاسب الآلي أو الوسائل الالكترونية الحديثة[2].

ومن أمثلة الطرق الغير مشروعة التي قد يتم من خلالها الحصول على أدلة تتعلق بالوسائل الإلكترونية، استخدام التعذيب والإكراه المادي أو المعنوي في مواجهة الجاني الذي يرتكب جريمة واقعة على التوقيع الالكتروني لكي يفك شفرة أو يبوح بكلمة السر، ويعد من قبل هذه الطرق الغير مشروعة التدليس والغش والخديعة في الحصول على الأدلة المحصلة من الوسائل الإلكترونية.

4.مصداقية الدليل

صحة السجلات الالكترونية لقبولها كدليل الكتروني يخضع لنفس القواعد التي تتبعها المحكمة للتأكد من صحة أي دليل معروض عليها ولا حاجة لوضع قواعد جديدة للتأكد من صحة الأدلة الالكترونية، غير أنها أكثر صعوبة من الأدلة التقليدية بحيث على المحكمة أن تتأكد دائما من أن النظام الحاسوبي محل الدليل الالكتروني يعمل بطريقة منتظمة ودقيقة[3]،

[1]– أشرف قنديل، المرجع السابق، ص 76.

[2]– المرجع نفسه، ص 77 .

[3]– محمود جاد المولى، المرجع السابق، ص 220 .

لذلك تشترط المحاكم ذات النظام الأنجلوسكسوني أن يكون الدليل متعلقا بالقضية التي يجرى نظرها وأن يكون محل ثقة ومعتمد كشرط لقبول جميع الأدلة الفنية التي تقدم في جرائم التوقيع الالكتروني ويقوم القضاء بتحديد درجة مصداقية وفاعلية الدليل العلمي للوصول إلى النتيجة النهائية التي تم الحصول عليها باستخدام أحد الأدوات التناظرية الرقمية ، الذي يكون قبل إجراءات المحاكمة باستخدام موجات أو اختبارات " دوابورت "وهو أسلوب تتبناه المحاكم لقبول الدليل العلمي[1]، ويقوم القاضي وتحت مسؤوليته أثناء جلسة اختبار داوبورت في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في تحديد الدليل العلمي والقيام بذلك وفقا لدرجة التوثيق المتعمدة [2].

وللمحكمة أيضا الاستعانة بالبرامج للتأكد من مصداقية الدليل الالكتروني، كبرنامج hash values الذي يعتمد أساسا على نظام البصمة الرقمية بالدخول إلى القرص الصلب للحاسوب وفحص أصل الدليل الموجود عليه للتأكد من سلامته وصحته من خلال عمليات فنية ورياضية تجريها هذه البرامج.

وقد استخدم القضاء الأمريكي برنامج hash values في قضية finely التي تتلخص وقائعها في اتهام finely بحيازة صور إباحية للأطفال وتوزيعها، وتم اكتشاف الواقعة من خلال احتفاظ ولاية Wyoming بقاعدة بيانات للصور الإباحية للأطفال والمنشورة على شبكة الانترنيت، وبواسطة البرنامج اكتشفت الشرطة بأن الصور الإباحية المنشورة الموجودة داخل الحاسب هي

---

(1)– عبد الحميد عبد المطلب ، زبيدة محمد جاسم، عبد الله عبد العزيز، المرجع السابق ، ص 2248 .

* تحدد طريقة اختبار داوبورت أربع فئات يجب استخدامها كموجات عند تقييم الإجراءات أو المنهجية المتبعة وهي:
الأولى، هل سبق تجربة واختبار الطريقة المتبعة، الثانية، نسبة الخطأ: هل هناك نسبة خطأ محتملة ترافق استخدام هذه الطريقة، الثالثة، النشر: هل جرى نشر الطريقة المتبعة وخضع ذلك للمراجعة بين من قبل الآخرين، الرابعة القبول: هل الطريقة المتبعة مقبولة بصورة عامة في المجتمع العلمي المعني.عبد الحميد عبد المطب وآخرون، المرجع نفسه، ص 2249.

نفسها التي تمت ضبطها بحوزته، ما أدى إلى اقتناع هيئة المحلفين بصحة الدليل الالكتروني المقدم في الدعوى وإدانته بالتهم الموجهة إليه [1].

ونرى بأن للمحكمة الحرية في أن تختار ما تراه مناسبا من الوسائل التقنية الحديثة للتأكد من مصداقية وصحة الدليل الالكتروني المعروض أمامها حتى إذا قبلته أو رفضته تكون مطمأنة الضمير، وأن تتماشى وتراعي في ذلك التطور الحاصل في المجال التكنولوجي، وما تستعين به الأنظمة المقارنة من برامج نستطيع أن نستفيد منها بالاستعانة بها وتطبيقها في القضاء الجزائري في حالة ما إذا رأى القاضي الجزائي الجزائري أن المسألة المعروضة في أحد جرائم التوقيع الالكتروني تتطلب دليل الكتروني يتم فحصه بواسطة هذه البرامج.

خلاصة الباب الثاني

نخلص من دراستنا في الباب الثاني للحماية الجزائية الإجرائية للتوقيع الالكتروني، أن إجراءات جمع الأدلة في جرائم التوقيع الالكتروني في مرحلتي البحث والتحري والتحقيق القضائي، لها إجراءات خاصة، يمكن جمعها من خلال ما تضمنه قانون الإجراءات الجزائية المعدل سنة 2006 من إجراءات تحري خاصة في الجرائم الواقعة على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني وهي التسرب ، التقاط الصور، التصنت، اعتراض المراسلات، وما تضمنه أيضا قانون الوقاية من تكنولوجيات الإعلام والاتصال لسنة 2009 المطبق في الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، وفي الجرائم الماسة بنظام المعالجة الآلية لمعطيات التوقيع الالكتروني، وهي المراقبة الالكترونية داخل شبكة الانترنت، وكيفية وشروط تفتيش نظم الحاسب الآلي، وما تلعبه أيضا الجهات الغير قضائية في مد يد المساعدة إلى الضبطية القضائية، وجهات التحقيق القضائي وفي مقدمتها مقدمي خدمات التصديق الالكتروني على التوقيع الالكتروني، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي من مهامها حسب المرسوم الرئاسي الصادر سنة 2015، تزويد

[1]– محمود جاد المولى، المرجع السابق، ص 226 .

السلطات القضائية والضبطية القضائية، تلقائيا أو بناءا على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، من ضمنها الجرائم المرتكبة بوسائل الكترونية على التوقيع الالكتروني.

وعلى المستوى الدولي فتأخذ جرائم التوقيع الالكتروني طابعا دوليا، إذا ما ارتكبت في أكثر من إقليم دولة، وتتسم جرائم التوقيع الالكتروني المرتكبة بوسائل الكترونية بأنها من الجرائم العابرة للحدود والمنظمة، فقد يقوم الجاني بواسطة وسيلة الكترونية في الجزائر من اختراق عدة أنظمة للتوقيع الالكتروني متواجدة في أقاليم دول مختلفة في وقت وجيز، وهذا ما يجعل أهمية الاتفاقيات الدولية، والمساعدات القضائية الدولية بشأن تتبع المجرمين وجمع الأدلة في جرائم التوقيع الالكتروني في الشكل الالكتروني، كالمساعدة القضائية الدولية المتبادلة للجزائر مع دول أجنبية التي نص عليها المشرع في المواد 15 إلى 19 من قانون الوقاية من جرائم تكنولوجيات الإعلام والاتصال لسنة 2009، المتعلقة بمجال التحريات والتحقيقات القضائية، بشروطها التحفظية وقيودها، وهي أن تكون وفقا للاتفاقيات الدولية، كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 بالقاهرة، المصادق عليها من قبل الجزائر سنة 2014، والاتفاقات الثنائية، ومبدأ المعاملة بالمثل، وألا تمس بالسيادة الوطنية.

ورأينا أن الهدف الأسمى من الإجراءات هو أن يصيب القاضي الحقيقة في حكمه سواء بالإدانة أو البراءة، وهو ما لا يتحقق في محاكمة مرتكبي الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، إلا بواسطة قضاة حكم متمكنين في مجال الإجرام الالكتروني، لما يواجهونه من مسائل معقدة متعلقة بالجريمة المرتكبة ومرتكبيها، وما تثيره أيضا من مسائل متعلقة بالاختصاص القضائي الدولي والوطني كالمحكمة الفاصلة في الجريمة، وأفضل معيار إتباعه هو المحكمة الواقع في دائرة اختصاصها الوسيلة الالكترونية المستعملة من مرتكبها، وما يطرح على قضاة الحكم من أدلة طابع ذات الكتروني، التي تتطلب أن تعرض على خبراء

متخصصين في مجال التكنولوجيا الحديثة، وأن تكون مستمدة بطريقة مشروعة حتى يطمئن لها القاضي.

خاتمة

خاتمة

نخلص من هذه الدراسة أن التطور الحاصل في التكنولوجيا الحديثة، وانتقال العالم أكثر فأكثر إلى استخدام التقنيات الحديثة منها التوقيع الالكتروني الذي ساعد في المعاملات الالكترونية في مجال التجارة الالكترونية والحكومة الالكترونية، سيزيد ويضاعف من محاولات اختراقه والاعتداء عليه كأحد التهديدات الواقعة على الجريمة المرتكبة في بيئة الكترونية، منها جرائم الاعتداء على التوقيع الالكتروني، لنخرج من بحثنا بمجموعة من النتائج وهي:

1. تعد جرائم الاعتداء على التوقيع الالكتروني من أخطر الجرائم المرتكبة بالوسائل الالكترونية الحديثة لمساسها البالغ بالخصوصية الفردية للشخص الموقع، و اهتزاز الثقة في المعاملات الموقعة الكترونيا، وبالمستهلك الالكتروني.
2. التوقيع الالكتروني محل الحماية الجزائية في جرائم التوقيع الالكتروني يكون إما التوقيع الالكتروني في حد ذاته، أو إحدى بياناته التابعة والمرتبطة به منطقيا.
3. المشرع الجزائري قد أعطى حماية جزائية موضوعية للتوقيع الالكتروني في موضعين، الأول في قانون العقوبات من خلال التجريم الخاص بأنظمة المعالجة الآلية للمعطيات من ضمنها معطيات التوقيع الالكتروني في نص المادة 394 مكرر من قانون العقوبات، وأيضا تجريم تزوير التوقيع الالكتروني المطبق عليه النصوص التقليدية العامة المتعلقة بالتزوير التي نص عليها المشرع الجزائري في المواد من 214 إلى 229 من قانون العقوبات، أما الموضع الثاني فهو في قانون التوقيع والتصديق الالكترونيين لسنة 2015 من خلال الجرائم الواقعة على التوقيع الالكتروني في المواد من 66 إلى 74 .
4. نصنف جرائم الاعتداء على التوقيع الالكتروني إلى فئتين رئيستين، الأولى وهي الجرائم الواقعة على سلامة النظام الذي يحوي التوقيع الالكتروني، أما الثانية فهي الواقعة على سلامة وسرية وثقة بيانات التوقيع الالكتروني.

5. بسط المشرع الجزائري حماية جزائية موضوعية لسلامة وسرية وثقة بيانات التوقيع الالكتروني في قانون التوقيع والتصديق الالكترونيين لسنة 2015، حماية لمصلحة شرعية تداول البيانات وخصوصيتها وحماية للثقة في التوقيع الالكتروني مع حماية المستهلك الالكتروني من الغش والتحايل، وبذلك يكون المشرع قد سد الفراغ القانوني المتعلق بالتوقيع الالكتروني بتجريمه لإفشاء بيانات التوقيع الالكتروني في نص المادة 68 منه، حماية لمصلحة الخصوصية والسرية في المعاملات الموقعة الكترونيا، وجرم أيضا المساس بالتوقيع الالكتروني في مرحلة التصديق عليه في المواد من 66 إلى 75 من قانون التوقيع الالكتروني، وتشمل جرائم الإدلاء بقرارات كاذبة للحصول على شهادة تصديق إلكتروني، الإخلال بإخبار السلطة الاقتصادية عن التوقف، إفشاء بيانات التصديق الالكتروني، إصدار شهادة تصديق الكترونية دون ترخيص أو سحبه، حماية لمصلحة المتعاملين مع جهات التصديق الالكتروني.

6. كل جرائم التوقيع الالكتروني تتطلب لقيامها ركنا ماديا ومعنوي يختلف بحسب نوعية التجريم، مع ملاحظة بأن جرائم التوقيع الالكتروني لا يعاقب فيها على الشروع، لأنها من الجنح وفيها لا يعاقب على الشروع والمحاولة إلا بنص صريح، كما أنه يعاقب فيها الشخص الطبيعي والمعنوي أيضا بغرامة تعادل خمس مرات الحد الأقصى للغرامة المطبقة على الشخص الطبيعي، وفيما تعلق بالعقوبات التكميلية فهناك جريمة ممارسة نشاط التصديق الالكتروني دون ترخيص أو سحبه المعاقب عليها في نص المادة 72 من قانون التوقيع الالكتروني فقط من تطبق فيها مصادرة التجهيزات كعقوبة تكميلية، ما يجعل نظرة المشرع في أنها جريمة يفترض فيها تجهيزات ووسائل وبرامج تستعمل في ارتكابها يجب مصادرتها.

7. لم يكتفي المشرع بالحماية الجزائية الموضوعية فقط، بل بسط أيضا حماية جزائية إجرائية خاصة لمتابعة جرائم الاعتداء على التوقيع الالكتروني سواء في تعديل قانون الإجراءات لسنة 2006 من خلال إجراءات التحري الخاصة في جرائم المساس بأنظمة

المعالجة لمعطيات التوقيع الالكتروني وتشمل إجراءات التسرب التقاط الصور المراقبة التليفونية، ثم بعدها منح المشرع الإجرائي الجزائري في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الصادر سنة 2009 العديد من السلطات والصلاحيات للضبطية القضائية تحت إشراف السلطة القضائية باستحداث إجراءات تتلاءم وطبيعة الجرائم المرتكبة في نطاق الكتروني كتفتيش أنظمة الحاسب الآلي وامتداده على نطاق دولي، وإجراء المراقبة الالكترونية للاتصالات الالكترونية للجرائم الالكترونية الواقعة على التوقيع الالكتروني.

8. تلعب جهات التصديق الالكتروني دورا أساسيا في مد يد المساعدة للضبطية القضائية ولسلطات التحقيق والحكم، وبخاصة جرائم التوقيع الالكتروني المرتكبة في مرحلة التصديق الالكتروني.
9. غالبية القضايا المطروحة على القاضي الجزائي في جرائم التوقيع الالكتروني المرتكبة في بيئة الكترونية، يكون دليل إدانة أو تبرئة مرتكبها عبارة عن دليل الكتروني، والذي له أثر في تكوين القناعة الشخصية للقاضي.
10. من أجل حماية جزائية إجرائية فعالة من جرائم التوقيع الالكتروني لابد أن تتجه الدول نحو اتجاهين، الأول داخلي بحيث تتلاءم تشريعاتها مع تطور تجريم الجريمة المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، والثاني دولي بطريق الاتفاقيات الدولية والمساعدات القضائية الدولية حتى لا يفلت مرتكبيها من المتابعة الجزائية والتحقيق والمحاكمة.

وبما أن النصوص الجزائية التقليدية غير كافية لمواجهة الجرائم الواقعة على التوقيع الالكتروني، وعلى الرغم من الحماية الجزائية الموضوعية والإجرائية الخاصة التي كرسها المشرع الجزائري للتوقيع الالكتروني، إلا أنه ينتابها بعض القصور، ما يجعلنا نتقدم بمجموعة من الاقتراحات:

1. نقترح حذف المادة 17 من قانون عصرنة العدالة 15-03 التي تجرم الاستعمال بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني، لأنها تتعارض مع المادة 68 من قانون التوقيع الالكتروني 15-04، بحيث أصبح هناك مادتان تعاقبان على نفس الجرم وهو استعمال بيانات التوقيع الالكتروني بعقوبتين مختلفتين، ففي في المادة 17 من قانون عصرنة العدالة تعاقب عليها بالحبس من 01 سنة إلى 05 خمس سنوات أما في المادة 68 من قانون التوقيع الالكتروني فتعاقب عليها بالحبس من 03 ثلاثة أشهر إلى 03 ثلاث سنوات.
2. نقترح تجريم سرقة بيانات التوقيع الالكتروني.
3. نقترح تجريم إتلاف بيانات التوقيع الالكتروني.
4. نقترح تجريم تزوير التوقيع الالكتروني واستعماله بنص خاص، مع تجريم تزوير التوقيع الالكتروني في بطاقات الائتمان والدفع الالكترونية .
5. نقترح تجريم استعمال التوقيع الالكتروني أو الرقم السري في بطاقات الائتمان والدفع الالكترونية بنص خاص، لأنها من الجرائم التي ستكون أكثر انتشارا في السنوات القادمة مع اتجاه الجزائر نحو الدفع الالكتروني.
6. نقترح تجريم صنع توقيع الكتروني.
7. نقترح تجريم المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني بنص خاص، أي جريمة الاعتداء على قاعدة بيانات معلوماتية متعلقة بالتوقيع الالكتروني، وذلك بهدف إخراجها من إطارها العام المعاقب عليه بنص المواد 394 مكرر إلى 394

مكرر 07 من قانون العقوبات، أو بتجريم الدخول بطريق الغش إلى قاعدة بيانات بغرض التلاعب بالتوقيع الالكتروني.

8. نقترح تجريم الشروع أو المحاولة في جميع جرائم الاعتداء على التوقيع الالكتروني المعاقب عليها في قانون التوقيع والتصديق الالكترونيين 15-04 نظرا لخطورتها، ولأنها كلها جنح فلابد من العقاب على الشروع بنص خاص بإضافة عبارة" يعاقب على الشروع بالعقوبات ذاتها المقررة للجريمة التامة" لكل نص تجريمي.

9. نقترح تشديد العقوبات الأصلية في جرائم الاعتداء على التوقيع الالكتروني المنصوص عليها في قانون التوقيع والتصديق الالكترونيين 15-04 على النحو التالي:

- تشديد العقوبة الأصلية في جريمة إفشاء أو استعمال التوقيع الالكتروني لتصبح الحبس من 01 سنة إلى خمس سنوات 05 سنوات.

- تشديد العقوبات الأصلية لجرائم التوقيع الالكتروني في مرحلة التصديق التي يعاقب عليها المشرع في نص المواد من 66 إلى 73 من قانون التوقيع والتصديق الالكترونيين، لتصبح كلها من 01 سنة إلى خمس سنوات 05 سنوات.

- تشديد العقوبة الأصلية في نص المادة 74 من قانون التوقيع الالكتروني التي تجرم استعمال شهادة التصديق الالكتروني لغير الأغراض التي منحت لأجلها المعاقب عليها بالغرامة فقط بإضافة عقوبة الحبس مع رفع قيمة الغرامة لتصبح العقوبة كالآتي: الحبس من 03 ثلاثة أشهر إلى 03 ثلاث سنوات، والغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200.000 دج، أو بإحدى هاتين العقوبتين فقط.

10. نقترح إضافة ظروف التشديد في جرائم التوقيع الالكتروني المتمثلة في:
- إضافة ظرف تشديد العقوبة إذا كان مرتكبها من مزودي خدمات التصديق الالكتروني.
- إضافة ظرف تشديد جرائم التوقيع الالكتروني إذا ما ارتكبت من طرف جماعة إجرامية منظمة.

11. نقترح إضافة العقوبات التكميلية في جميع الجرائم الواقعة على التوقيع الالكتروني المتمثلة في:
- غلق المواقع الالكترونية المستعملة في جميع الجرائم الواقعة على التوقيع الالكتروني.
- مصادرة الأجهزة والبرامج والوسائل المستخدمة في جميع الجرائم الواقعة على التوقيع الالكتروني.

12. نقترح تسهيل إجراءات التبليغ والشكوى عن الجرائم المرتكبة بالوسائل الالكترونية على التوقيع الالكتروني، وذلك بالاستعانة بوسائل الاتصال الحديثة كالتبليغ والشكوى عن طريق الإيمايل، والمواقع الالكترونية .

13. نقترح تمكين قضاة النيابة، التحقيق والحكم، الاستعانة بخبراء في المجال الالكتروني لأجل المساعدة في التحري والتحقيق والحكم عن الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني.

14. نقترح إضافة نص مادة في قانون الإجراءات الجزائية تمنح الاختصاص القضائي الإقليمي في الجرائم المرتكبة بالوسائل الالكترونية إلى المحكمة الواقع في دائرة اختصاصها الجهاز الذي ارتكب الجرم بواسطته.

15. نقترح تشجيع انضمام الجزائر إلى المعاهدات والاتفاقيات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبدلها الدول في مجال مكافحة جرائم الاعتداء على التوقيع الالكتروني.

16. نقترح تمكين القاضي الجزائري من الوسائل و بالبرامج الحديثة للكشف عن صحة ومصداقية الأدلة الالكترونية ومخرجات الحاسب.
17. نقترح إضافة نص مادة في قانون الإجراءات الجزائية تجيز للقاضي في المواد الجزائية أن يبني حكمه بناءا على أدلة الكترونية، إذا ما اطمأن إلى سلامتها ومشروعيتها ومصداقيتها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: قائمة المصادر

أ. الاتفاقيات الدولية

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 بالقاهرة ، المصادق عليها من قبل الجزائر بموجب المرسوم الرئاسي 252 – 14 المؤرخ في 08 سبتمبر 2014 . الجريدة الرسمية للجمهورية الجزائرية، العدد 57 ، الصادرة في 28 سبتمبر 2014 .
2. اتفاقية بودابست للجرائم الالكترونية 2001 .

ب. القوانين

1. الأمر رقم 66 – 156 المتضمن قانون العقوبات المعدل والمتمم .
2. الأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم .
3. قانون التوقيع والتصديق الالكترونيين 15 -04، الجريدة الرسمية للجمهورية الجزائرية العدد06 الصادرة بتاريخ 10 -02 – 2015 .
4. قانون التجارة الالكترونية 18 – 05 . الجريدة الرسمية للجمهورية الجزائرية، العدد 28 ، الصادر في 13 ماي 2018 .
5. القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي18 – 07. الجريدة الرسمية للجمهورية الجزائرية، العدد 34 ، الصادرة في 10 جوان 2018 .
6. القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 09 – 04 . الجريدة الرسمية للجمهورية الجزائرية، العدد 47 ، الصادرة في 16 أوت 2009 .
7. قانون العقوبات الفرنسي.
8. قانون التوقيع الالكتروني الفرنسي الصادر في 13 مارس 2000 .
9. قانون المعاملات الالكترونية العماني .

10. قانون التجارة الالكترونية الإماراتي.
11. قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004 .

ثانيا: قائمة المراجع

أ. المراجع باللغة العربية

1 . الكتب

- **الكتب العامة**

1. أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2 ، ط5 ، ديوان المطبوعات الجامعية ، الجزائر، 2010.
2. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، 1985 .
3. بكري يوسف بكري محمد، قانون العقوبات– القسم العام، ط 1، مكتبة الوفاء القانونية، الإسكندرية، 2012.
4. جلال ثروت، سليمان عبد المنعم، أصول المحاكمات الجزائية، ط1 ، المؤسسة الجامعية للدراسات، بيروت، 1997 .
5. رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مكتبة الوفاء القانونية، الإسكندرية، 2015.
6. سامان عبد الله عزيز، المسؤولية الجنائية الناشئة عن إفشاء الأسرار المهنية والوظيفية– دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2017.
7. سليمان عبد المنعم ، علم الإجرام والجزاء، ط1 ، منشورات الحلبي الحقوقية، بيروت، 2005 .
8. سليمان عبد المنعم، أصول الإجراءات الجنائية ، دار المطبوعات الجامعية، 2015 .
9. سليمان عبد المنعم، النظرية العامة لقانون العقوبات–دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003 .
10. سليمان عبد المنعم، قانون العقوبات– القسم الخاص– الجرائم المضرة بالمصلحة العامة، دار الجامعة الجديدة، الإسكندرية، 2018.
11. عادل عبد العال إبراهيم خراشي ، إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديد، الإسكندرية ، 2015 .

12. عبد الحميد الشواربي، التعليق الموضوعي على قانون العقوبات، منشأة المعارف، الإسكندرية، 2003 .
13. عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، منشأة المعارف ، الإسكندرية ، 2002 .
14. كامل السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، ط1 ، دار الثقافة، عمان ، 2008 .
15. محمد زكي أبو عامر، الإجراءات الجنائية– مرحلة جمع الاستدلالات–سير الدعوى الجنائية والدعوى المدنية المرتبطة بها– التحقيق والحكم والطعن في الحكم الصادر في الدعوى الجنائية ، ط1 ، منشورات الحلبي الحقوقية، لبنان، 2010 .
16. محمد زكي أبو عامر، سليمان عبد المنعم – قانون العقوبات– القسم الخاص، منشورات الحلبي الحقوقية، بيروت ، 2009 .
17. محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، ج1، ط2، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1979.
18. محمود نجيب حسني ، النظرية العامة للقصد الجنائي– دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، ط3 ، دار النهضة العربية، القاهرة، 1988 .
19. محمود نجيب حسني، الموجز في شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، 1996 .
20. محمود نجيب حسني، شرح قانون العقوبات– القسم الخاص، دار النهضة العربية، القاهرة، 1988.
21. محمود نجيب حسني، شرح قانون العقوبات– القسم العام، ط8 ، دار النهضة العربية، القاهرة، 2018 .
22. مصطفى عبد اللطيف إبراهيم، جريمة الاتفاق الجنائي–دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2011 .

- **الكتب الخاصة**

23. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2005 .
24. أحمد عوض بلال ، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، ط3 ، دار النهضة العربية، القاهرة، 2013 .
25. أشرف عبد القادر قنديل، الإثبات في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2015 .
26. إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008 .

27. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط1، دار الفكر الجامعي، الإسكندرية ، 2011 .

28. ثروت عبد الحميد ، التوقيع الالكتروني- ماهيته مخاطره وكيفية مواجهتها مدى حجيته في الإثبات، دار الجامعة الجديدة ، الإسكندرية ، 2007.

29. جمال صالح عبد الحليم، الحماية الجنائية للحق في الحق الخصوصية في مواجهة نظم المعلومات ، ط1 ، دار النهضة العربية، 2018 .

30. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية-دراسة تطبيقية على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013 .

31. حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط1 ، دار النهضة العربية، القاهرة، 2017.

32. خالد حسن لطفي ، المستند الالكتروني ووسائل اثباته وحمايته ، دار الفكر الجامعي، الإسكندرية ، 2019 .

33. خالد ممدوح إبراهيم ، حجية البريد الالكتروني في الإثبات- دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2018 .

34. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2018 .

35. خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية-دراسة مقارنة، ط1 ، دار الفكر الجامعي، الإسكندرية، 2018 .

36. راشد بن حمد البلوشي ، التوقيع الالكتروني والحماية الجزائية المقررة له ، ط1 ، منشورات الحلبي الحقوقية، بيروت، 2018 .

37. السعيد قنديل، التوقيع الالكتروني- ماهيته صوره حجيته في الإثبات بين التداول والاقتباس، دار الجامعة الجديدة ، الإسكندرية، 2006 .

38. شريف محمد عمر، التعاون الدولي في مجال مكافحة الجرائم- دراسة مقارنة (تسليم المتهمين والمحكوم عليهم، تسليم الأشياء والتسليم المراقب، الإثبات والمساعدات القضائية، تنفيذ الأحكام الأجنبية، نقل المحكوم عليهم، التحقيق الجنائي عن بعد ، إنشاء قواعد بيانات خاصة بالجرائم الإرهابية)، المكتب الجامعي الحديث، الإسكندرية ، 2019.

39. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007 .

40. طارق الدسوقي إبراهيم عطية، الأمن المعلوماتي – النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة الإسكندرية ، 2009 .

41. عبد الحليم فؤاد الفقي ، جريمة تزوير التوقيع الالكتروني ، دار النهضة العربية، القاهرة، 2016.

42. عبد الفتاح بيومي حجازي ، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، ط1 ، دار الفكر الجامعي، الإسكندرية، 2007 .

43. عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، منشأة المعارف ، الاسكندرية، 2009 .

44. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، ط1 ، دار الفكر الجامعي الإسكندرية ، 2006.

45. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية ، دار الفكر الجامعي، الإسكندرية، 2004 .

46. عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي ، الإسكندرية، 2005.

47. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية– دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، ط1 ، منشأة المعارف، الإسكندرية، 2009 .

48. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2010 .

49. عفيفي كامل عفيفي، فتوح عبد الله الشادلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون–دراسة مقارنة، منشورات الحلبي الحقوقية ،بيروت، 2007 .

50. عمر سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي– المراقبة الالكترونية والتحقيق الجنائي عن بعد، ط1 ، دار النهضة العربية، القاهرة، 2013.

51. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1 ، دار الحامد، الأردن، 2014 .

52. محمد حسين على محمود ، التزوير باستخدام الوسائل الالكترونية ، دار النهضة العربية، القاهرة ، 2017 .

53. محمد حسين منصور، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، 2006 .
54. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007 .
55. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ، القاهرة، 2003 .
56. محمد على سويلم، الحماية الجنائية للمعاملات الالكترونية بين الجوانب الإجرائية والأحكام الموضوعية لقانون تنظيم التوقيع الالكتروني وتكنولوجيا المعلومات–دراسة مقارنة، ط1 ، دار المطبوعات الجامعية، الإسكندرية، 2018 .
57. محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي– دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2018 .
58. محمود عبد الغني جاد المولى، دور الدليل الالكتروني في الإثبات الجنائي–دراسة مقارنة، ط1 ، دار الفكر الجامعي، الإسكندرية، 2019 .
59. محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة– دراسة مقارنة في التشريع الفرنسي والأمريكي والاتفاقيات الدولية و الإقليمية، المكتب الجامعي الحديث، الإسكندرية، 2018 .
60. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية– دراسة مقارنة، دار النهضة العربية، القاهرة، دون ذكر سنة النشر.
61. مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000 .
62. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006 .
63. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات– دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013 .
64. هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000 .
65. هلالي عبد اللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية– دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2008 .

66. هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية– دراسة مقارنة، ط2 ، دار النهضة العربية القاهرة، 2008.

67. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي– دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 2008.

68. هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة، دار النهضة العربية، القاهرة، 2016 .

69. هلالي عبد اللاه أحمد، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، دار النهضة العربية، القاهرة، 2013 .

2. الملتقيات والمقالات

1. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، 2003

2. أورين كير، ترجمة عمر محمد بن يونس، نطاق الجريمة الافتراضية– تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، مجلة القانون، جامعة نيويورك، العدد78، نوفمبر، 2003 .

3. بيل جيتس، ترجمة عبد السلام رضوان، المعلوماتية بعد الانترنيت طريق المستقبل، مجلة الثقافة والفنون والآداب، الكويت، 1990.

4. رضوان قرواش، هيئات التصديق الالكتروني في ظل القانون 15 –04 المتعلق بالتوقيع والتصديق الالكترونيين، مجلة العلوم الاجتماعية، العدد 24 ، جوان ، 2017 .

5. عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن والتأمين في شبكة الانترنيت، مؤتمر القانون والكمبيوتر، جامعة الإمارات العربية المتحدة، 2003 .

6. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط3 ، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون ، 2003 .

7. عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات العربية، 2003 .

8. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط3 ، جامعة الإمارات العربية المتحدة، 2003 .

9. فارس خطابي، العمل من أجل النفع العام كعقوبة بديلة في التشريع الجزائري، الملتقى الوطني حول العقوبات البديلة في التشريع الجزائري، جامعة خميس مليانة، كلية الحقوق، 02 ماي 2018 ، مداخلة غير منشورة.

10. فارس خطابي، حجية التوقيع الالكتروني في الإثبات الجنائي، دفاتر السياسة والقانون، عدد خاص ، جوان ، 2018 .

11. محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 13 ، العدد01 ، جوان، 2018 .

12. ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون ، المجلد الخامس، جامعة الإمارات العربية المتحدة ، 2003 .

13. هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الالكتروني، مؤتمر القانون والكمبيوتر والانترنت، المجلد الثالث، ط3، جامعة الإمارات العربية المتحدة، 2003 .

14. هدى حامد قشقوش، الحماية الجنائية للتوقيع الالكتروني، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، 2003 .

15. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مؤتمر القانون والكمبيوتر و الانترنت، المجلد الثاني ، ط3 ، جامعة الإمارات العربية المتحدة ، 2003 .

3. رسائل الدكتوراه

1. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الالكتروني، رسالة دكتوراه، جامعة عين شمس، منشورة في دار النهضة العربية، القاهرة، 2011

2. دليلة مباركي، غسيل الأموال، رسالة دكتوراه، جامعة باتنة، كلية الحقوق، 2007 – 2008 .

3. شنين صالح، الحماية الجنائية للتجارة الالكترونية– دراسة مقارنة ، رسالة دكتوراه، كلية الحقوق ، جامعة تلمسان، 2012– 2013 .

4. محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية– دراسة مقارنة، كلية الحقوق ، جامعة عنابة ، 2010 – 2011 .

5. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية– دراسة نظرية وتطبيقية، ط1 ، رسالة دكتوراه منشورة في دار منشورات الحلبي الحقوقية، بيروت، 2005 .

6. هروال هبة نبيلة، جرائم الانترنت– دراسة مقارنة، رسالة دكتوراه، كلية الحقوق ، جامعة تلمسان، 2013 – 2014 .

7. ياسر محمد الكومي، الحماية الجنائية والأمنية للتوقيع الالكتروني–دراسة مقارنة، رسالة دكتوراه، جامعة حلوان، منشورة في منشأة المعارف، الإسكندرية، 2014 .

4. القرارات والأحكام القضائية

1. قرار المحكمة العليا رقم 559251 ، الصادر بتاريخ 22 –10 –2008 ، غرفة الجنح والمخالفات.

2. قرار المحكمة العليا رقم 522390 ، الصادر بتاريخ 07 –01 –2010 ، غرفة الجنح والمخالفات.

3. قرار المحكمة العليا رقم 572259 ، الصادر بتاريخ 18 –02 –2009 ، غرفة الجنح والمخالفات.

4. قرار المحكمة العليا رقم 27199، الصادر بتاريخ 26–10–1982، غرفة الجنح والمخالفات.

5. قرار المحكمة العليا رقم 39130 ، الصادر في 02–01 –1985، غرفة الجنح والمخالفات.

6. الحكم الصادر عن محكمة باتنة رقم 05272 –10 ، الصادر في 01 –06 – 2010 .

ب. المراجع باللغة الفرنسية

A. Ouvrage

1. Abdelmadjid zaalani, Eric mathias, la responsabilité pénal , Berti, Alger,2009.
2. Bernard bouloc,Haritini mastopolou, droit pénal général et procédure pénal, Dalloz, paris, 2009.
3. Coralie Ambroise Castérot, la procédure pénal, 2 eme édition, gualino l’extenso, paris, 2009.
4. Georges vermelle , le nouveau droit pénal, Dalloz, paris, 1994.
5. Jean larguier, droit pénal général et procédure pénal, Dalloz, paris, 1977.
6. Jean paul antona, Philippe colin, François lenglart, la responsabilité pénal des cadres et des dirigeants dans le monde des affaire, Dalloz paris, 1996.

7. Jean-Claude soyer, droit pénal et procédure pénale, 18^{ém} Edition, libraire générale de droit et de jurisprudence, paris, 2004.
8. Michèle laure rassat, droit pénal spécial - infraction contre les biens , les personnes, la famille, les mœurs et la paix public, 4eme édition, tome 1, dalloz , paris , 1976.

B. Thèses

1. Jean Nicolas robin, la matière pénal a l épreuve du numérique, thèse doctorat, université du rennes1 , 2017 .
2. Romain boss, la lutte contre la cybercriminalité au regard de l action des états, thèse doctorat université de lorraine faculté de droit de Nancy , 2017 .

C. Article

1. Alain bensousan , La signature numérique et électronique en procédure pénal.
2. Emilo c vino, société de l'information et le droit pénal , revue international de droit pénal , vol 84 , 2013 .
3. Jean Pradel, la mondialisation du droit pénal, revue juridique Thémis , édition Thémis, faculté de droit université de Montréal.
4. Jean Pradel, les infraction relative a l informatique, revue international de droit compare, vol 42, n 02, juin, 1990.
5. Mohamed chawki, essai sur la notion de cyber criminalité.

ج. المراجع باللغة الانجليزية

Books

Peter Stephenson, investigating computer – related crime , crc press , new York , 2000 .

د. مواقع الانترنت

1. https://whoint/ ar- news-room q-a-détail
2. https://ar.m.wikipidia.org
3. https :// www. De alain.bensoussan. com
4. https ://www.ie-ei-eu.
5. htp :// www.dalloz.fr
6. htp://algeriepolice.dz
7. htp ://ppgn.mdn.dz
8. htp ://www.mjustice. Dz
9. htp :// dubaipolice@ gov. ae

فهرس المحتويات

فهرس المحتويات

ملخص

انتشار المعاملات الالكترونية الموقعة الكترونيا عبر وسائل الاتصال الحديثة سيؤدى إلى كثرة الاعتداءات الواقعة على التوقيع الالكتروني، وكلما تطورت وسائل الحماية التقنية له كلما تطورت وسائل اختراقه، ما يقتضي ضرورة إضفاء حماية جزائية للتوقيع الالكتروني، التي نظم المشرع الجزائري أحكامها الموضوعية، بحمايته لنظام المعالجة الآلية الذي يحوي التوقيع الالكتروني في تعديل قانون العقوبات سنة 2004، وحمايته من صور جرائم الاعتداء على سلامة وخصوصية بيانات التوقيع الالكتروني في قانون التوقيع والتصديق الإلكترونيين 15 – 04، ولأن هذه الجرائم مرتكبة في بيئة إلكترونية، فلقد كفلها المشرع أيضا بحماية إجرائية خاصة في التحري والتحقيق والمحاكمة .

Abstract

The proliferation of electronic transactions electronically signed through modern means of communication will lead to a proliferation of attacks on electronic signature, and the more technical means of protection develop, the more the means of penetration, the need to provide penal protection for electronic signature, the substantive provisions of which were regulated by the Algerian legislature, by protecting the automated processing system that contains the electronic signature in an amendment The Penal Code of 2004, And protect it from images of offenses against the integrity and privacy of signature data Electronic signature and authentication law15-04, Because these crimes are committed in an electronic environment, the legislature has also ensured them special procedural protection in the Detective , investigation and trial.

Résumé

La multiplication des transactions électroniques signées électroniquement par les moyens modernes de communication va entraîner une multiplication des attaques contre la signature électronique, et plus les moyens techniques de protection se développent, plus les moyens de pénétration, la nécessité d'assurer une protection pénale de la signature électronique, dont les dispositions de fond ont été réglées par le législateur algérien, en protégeant le système de traitement automatisé qui contient la signature électronique dans un amendement au code pénal de 2004, et le protéger des images d'infractions contre l'intégrité et la confidentialité des données de signature. Loi sur la signature électronique et l'authentification15-04, Parce que ces infractions sont commis dans un environnement électronique, le législateur leur a également assuré une protection procédurale spéciale dans le cadre de l'enquête et du procès.