جـامعة العربي التبسي –تبسة– الجزائر

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر

تخصص: قانون جنائي وعلوم جنائية

بعنوان:

الحماية الجزائية للتوقيع الإلكتروني

إعداد الطالب:

❖ يوسف بوزيدة

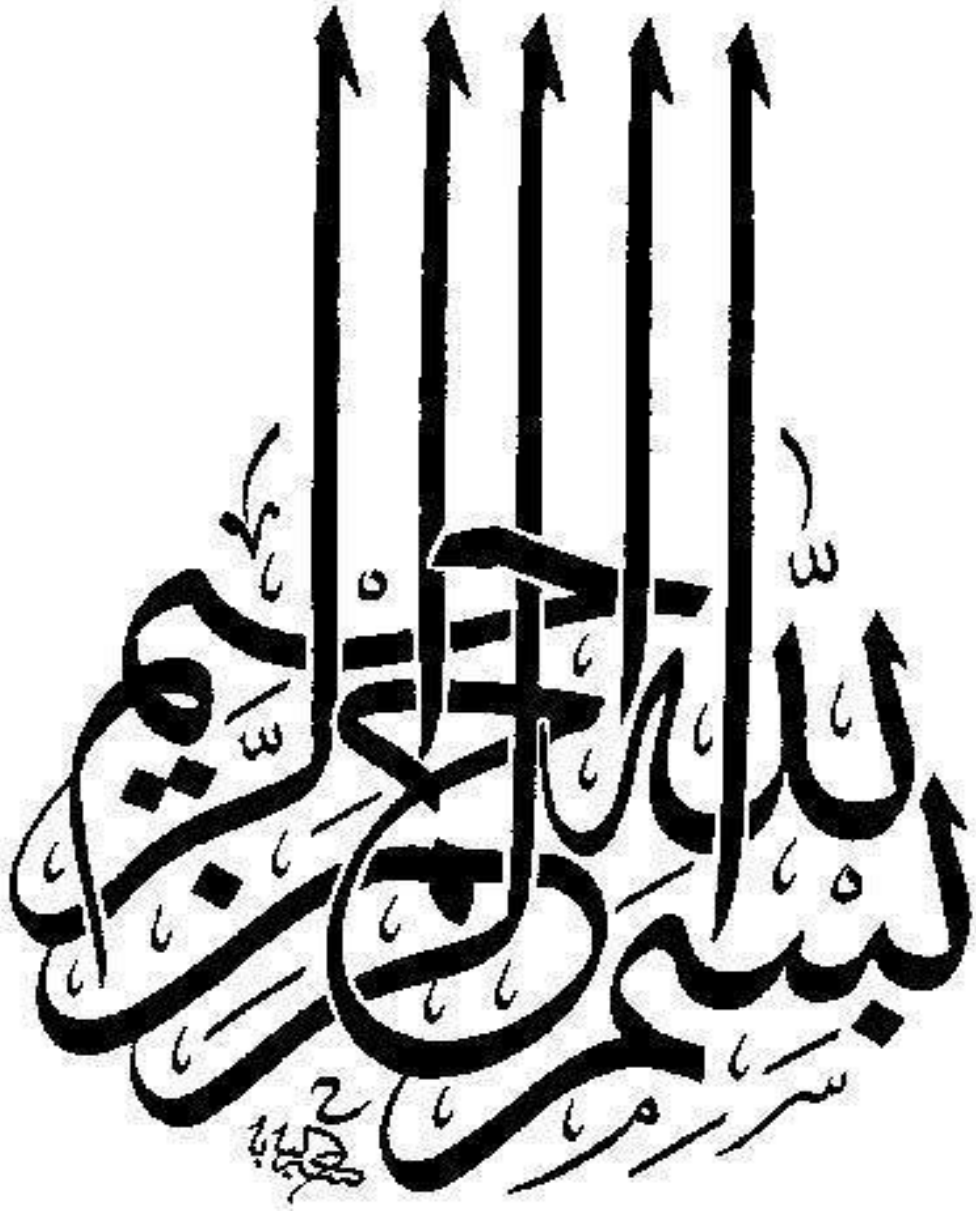
إشراف الدكتورة

ثابت دنيا زاد

أعضاء لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة في البحث
شعبان لاميـــة	أستاذ محاضر قسم –ب–	رئيسا
ثابت دنيا زاد	أستاذ محاضر قسم –أ–	مشرفا
خمايسية حفيظة	أستاذ مساعد قسم –أ–	ممتحنا ومقررا

السنة الجامعية 2021/2020


بسم الله الرحمن الرحيم

قال تعالى:

﴿وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ
وَالْبَحْرِ وَرَزَقْنَاهُم مِّنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ
عَلَى كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلاً﴾

سورة الإسراء -70-

شكر وتقدير

أولا شكري يكون لله عز وجل الذي أنعم علينا بنعمة العلم ويسر أمرنا طيلة مشوارنا الدراسي فالحمد له والشكر على كل نعمة تفضل بها علينا.

جزيل الشكر للأستاذة المشرفة: **الدكتورة ثابت دنيا زاد** على الجهد الذي بذلته معنا لإتمام هذا العمل، وعلى الإرشادات و النصائح والتي كانت توجهها لنا في كل خطوة من عملنا

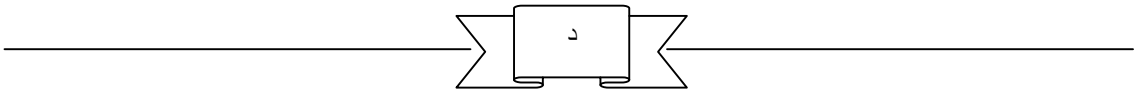
كما نتقدم بجزيل الشكر للجنة المناقشة لقبولهم مناقشة هذه المذكرة .

كما أتقدم بجزيل لكل أساتذة كلية الحقوق والعلوم السياسية على ما كل ما قدموه لنا

الشكر كذلك لكل من ساعدنا لإتمام هذا العمل سواء من قريب أو من بعيد.

قائمة المختصرات

قائمة المختصرات



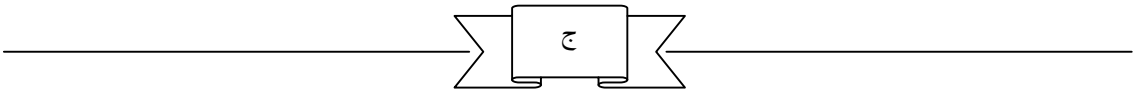
د.د.ن: دون دار نشر

د.ب.ن: دون بلد نشر

د.ط: دون طبعة

ص: صفحة

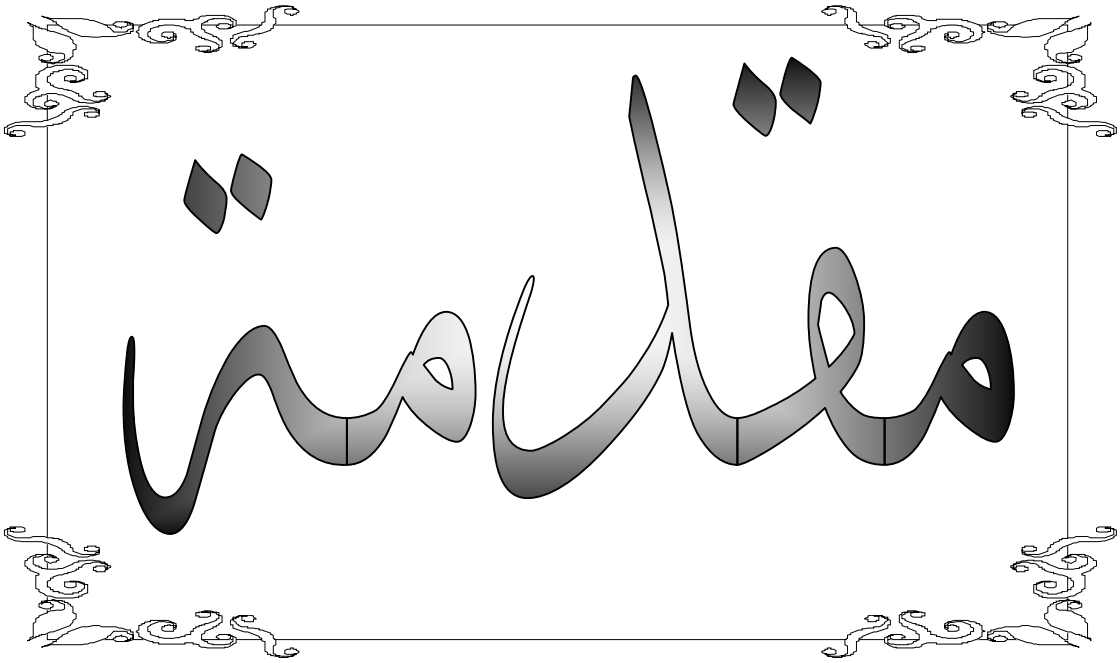
ف: فقرة



ج، ر،ع : الجريدة الرسمية عدد

ق .ع.ج: قانون العقوبات الجزائري

ق .إ.ج: قانون الإجراءات الجزائية


مقدمة

مقدمة

يشهد العالم في عصرنا هذا تطورا هائلا في كافة المجالات السياسية و الاقتصادية والتجارية وذلك باستخدام أنظمة معلوماتية وتطبيقات قوامها أجهزة الكومبيوتر والشبكات المتصلة به مما نتج عنه نسيج مترابط من العلاقات والمعاملات بين الأفراد تتعدد خطوطها، فألغيت بذلك الحدود الجغرافية بين الدول، وانعكس هذا التطور على الإدارة التي أصبحت تعتمد على المعاملات الالكترونية والوثائق ذات الطبيعة البيومترية مبتعدة بذلك شيئا فشيئا عن المعاملات الورقية.

فمن بين هذه المعاملات الالكترونية نجد التوقيع الالكتروني، الذي يعتبر من بين التطبيقات التي ظهرت وتوسع في استخدامه موازاة مع استخدام الحاسوب وتقدم تقنياته خاصة أنه يتميز بعدة خصائص لا تتوفر في التوقيع التقليدي فعمدت العديد من الدول بإدخال تعديلات في تشريعاتها خاصة المتعلقة بالتوقيع الالكتروني.

وفي ظل التحولات التي شهدها ميدان التكنولوجيا والاتصال والتجارة الالكترونية وتأثيره على التوقيع على المحررات الالكترونية، ظهرت الحاجة إلى طرف ثالث وظيفته خلق بيئة تعاملات الكترونية آمنة يلعب دور الوسيط المؤتمن بين المتعاملين في هذه البيئة الالكترونية، فيؤكد هوية الأطراف ويحدد أهليتهم للتعامل ويضمن حماية لبياناتهم الشخصية ويوفر الحماية المادية لهم من خلال إجراءات و جهات تعرف بمقدمي خدمات التصديق.

وعلى الرغم من الإيجابيات التي حملتها المعاملات الالكترونية إلا أنها لم تخلو من السلبيات في ظل تنامي ظواهر مثل القرصنة والجرائم الواقعة على التوقيع الالكتروني، أين عمدت العديد من الدول إلى إدخال تعديلات في تشريعاتها وإحداث تشريعات خاصة بالتوقيع الإلكتروني.

وفي إطار مسايرة هذه التعديلات واستحداث تشريعات خاصة بالتوقيع الالكتروني وأخرى لمحاربة الجرائم الواقعة عليه، أصدر المشرع الجزائري القانون رقم (15-04) الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، والقانون رقم(09-04) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والذي اتبعه بالمرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية

للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا إدراج تعديلات هامة في قانون العقوبات وقانون الإجراءات الجزائية.

1- أهمية موضوع الدراسة

تبرز أهمية موضوع الدراسة من خلال وحمايته الجزائية في:

- الوقوف على مفهوم التوقيع الالكتروني من حيث أنه أحد أهم المظاهر الحديثة في مجال المعاملات الالكترونية، وما يميزه من سرعة في الأداء وإنهاء للمعاملات الالكترونية وكذا صوره ونطاق الحماية الموضوعية له.

- محاولة الوقوف على توجهات المشرع الجزائري في تنظيمه للتوقيع الالكتروني ووسائل الحماية الجزائية التي اعتمدها لمواجهة الجرائم الماسة بالتوقيع الالكتروني.

2- أسباب اختيار الموضوع

- الأسباب الشخصية:

- الرغبة في البحث عن هذا الموضوع.

الأسباب الموضوعية:

- الحداثة القانونية والتشريعية للتوقيع الالكتروني وما يدفعنا نحو مقارنة مدى مسايرة هذه النصوص لهذه المنظومة القانونية الجديدة مع التطورات الحاصلة في مجال المعاملات الالكترونية وكذا أهمية المصادقة على التوقيع الالكتروني.

- وسائل الحماية الإجرائية للتوقيع الإلكتروني.

3- إشكالية البحث

انطلاقا مما سبق فإن إشكالية الموضوع تتمثل في:

ما مدى مواكبة النصوص التشريعية المقررة للحماية الجزائية للتوقيع الالكتروني في القانون الجزائري للجرائم الماسة به ؟

وترتيبا على ذلك تثور العديد من **التساؤلات** تتمحور حول:

- ما هو التوقيع الالكتروني وفي ما تتمثل صوره؟
- ما هو التصديق الالكتروني؟
- ما هو نطاق الحماية الموضوعية للتوقيع الالكتروني؟
- ما هي آليات الحماية الجزائية الإجرائية التي أقرها المشرع الجزائري؟

ولقد تم الاعتماد في جمع المعلومات على مجموعة من الدراسات السابقة والتي تراوحت بين أطروحات دكتوراه، مذكرات جامعية، مقالات علمية، تحدثت عن هذا الموضع على الرغم من اختلاف طريقة تناولها لموضوع التوقيع الإلكتروني والتي نورد منها:

1. صالح شنين، **الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، رسالة دكتوراه، جامعة تلمسان، 2013.

2. أمال قارة ، **الجريمة المعلوماتية**، مذكرة ماجستير، كلية الحقوق جامعة الجزائر،2001-2012.

1. رشيدة بوكر، **الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد السابع والعشرون، العدد 02، 2011.

وأثناء البحث في الموضع تم التعرض لبعض **الصعوبات** كما هو معهود عليه في المواضيع الحديثة أبرزها:

- وباء فيروس كورونا المتفشي في الجزائر والعالم بأكمله الذي حال بنا دون التنقل إلى جامعات الوطن للبحث عن المراجع و الدراسات السابقة في الموضوع.
- نقص المراجع المتخصصة المتعلقة بالموضوع رغم أهميته خاصة الجزائرية وشبه انعدامها في مكتبة جامعة الشيخ العربي التبسي- تبسة - ونظرا لتكرار المعلومات نفسها في المراجع المتوفرة.
- عدم وجود أحكام قضائية متعلقة بالموضوع يستأنس بها في التعرف على حقيقة تطبيق القواعد التشريعية الخاصة بالجرائم الواقعة على التوقيع الالكتروني.
- تشعب الموضوع وخصوصيته خاصة في جانب إثبات الجرائم الواقعة على التوقيع الالكتروني.

ونظرا لخصوصية التوقيع الالكتروني والجرائم الواقعة عليه تم الاعتماد على عدة **مناهج علمية** تتكامل فيما بينها بهدف محاولة الإلمام بمختلف جوانب الموضوع من خلال الاعتماد على ما يلي :

* **المنهج التحليلي** : ويتجلى ذلك في محاولة تحليل وشرح النصوص التشريعية المتعلقة بالتوقيع الالكتروني بجوانبها الموضوعية و الإجرائية خاصة أن المشرع لم ينص صراحة

على أساليب الحماية الإجرائية للجرائم الواقعة على التوقيع الالكتروني بل جاءت في شكل عام تحت عنوان الجرائم الالكترونية.

* **المنهج الوصفي** : لأن طبيعة الموضوع تتطلب ذلك والذي يعتبر طريقة لوصف موضوع الدراسة وسردها عن طريق جمع المعلومات وتصنيفها وإخضاعها للدراسات الدقيقة ، يتبين خاصة عند عرض خصائص التوقيع الالكتروني و أساليب الحماية الإجرائية للجرائم الواقعة عليه.

* **المنهج المقارن** : نظرا لحداثة موضوع الدراسة في الجزائر، كان إلزاما التعرض لبعض التشريعات العربية والأجنبية في بعض مراحل بحثنا هذا ، وذلك من خلال الإشارة إلى محاولاتهم في وضع تعريف للتوقيع الالكتروني، و الإشارة إلى الأحكام القانونية التي تم وضعها لحماية التوقيع الإلكتروني.

وفي سبيل التعرف على التوقيع الالكتروني و الآليات المقررة لحمايته و الإجابة على الإشكالية المطروحة سابقا ، وكذا الإجابة على التساؤلات المطروحة كذلك فقد تم البحث عن حقيقة التوقيع الالكتروني من خلال الحماية الجزائية الموضوعية للتوقيع الالكتروني في الفصل الأول من حيث التوقيع الالكتروني كمحل للحماية ، كما تم الوقوف على نطاق الحماية الموضوعية له.

ثم تناولنا في الفصل الثاني الحماية الجزائية الإجرائية للتوقيع الإلكتروني فتم التعرض إلى التحري والتحقيق في الجرائم الماسة بالتوقيع الالكتروني ثم الانتقال إلى سلطة القاضي في قبول وتقدير الدليل الجنائي.

الفصل الأول :

الحماية الجزائية الموضوعية للتوقيع الإلكتروني

تمهيد:

في القديم كان إبرام العقود يتم بطريقة تقليدية ورقية وكان التوقيع التقليدي هو الذي يكسب العقد الحجية و يعبر عن رضا الأطراف المتعاقدة عليه ، ونتيجة للثورة المعلوماتية في العصر الحديث تم ابتكار دعامات الكترونية يتعذر استعمال التوقيع التقليدي فيها نظرا لطبيعتها الغير مادية ، حيث ظهر بديل الكتروني يتماشى مع طبيعة هذه الدعامة وهو "التوقيع الالكتروني" حيث سهل مختلف التعاملات بين الأفراد خاصة في المجال التجاري والبنوك والاتصالات ، ونظرا لخصوصية هذه المعاملات التي تجرى في جانب افتراضي لا يقوم على أي دعامة ورقية ، انتشرت أساليب الغش والتحايل الذي يتعرض إليه المتعاملون.
وهو ما دفع أغلب التشريعات بوضع أطر قانونية بتحديد مدلول التوقيع الالكتروني وشروط صحته وكذا أنشاء هيئات لحمايته وحماية البيانات الشخصية للمتعامل الالكتروني وتحديد الجرائم الواقعة عليه و كذا وضع عقوبات ردعية للمعتدين عليه.
سنطرق في هذا الفصل إلى الحماية الجزائية الموضوعية للتوقيع الالكتروني في مبحثين المبحث الأول التوقيع الالكتروني كمحل للحماية أما المبحث الثاني نطاق الحماية الموضوعية للتوقيع الالكتروني.

المبحث الأول: التوقيع الالكتروني كمحل للحماية

كان التوقيع التقليدي الوسيلة المعتمدة الوحيدة المستعملة في القرون الماضية للمصادقة وإمضاء المحررات ، ومع تطور العالم في شتى المجالات الاقتصادية وبفضل الثورة المعلوماتية وابتكار شبكات وسائل التواصل عن بعد المحلية والعالمية ، زالت مختلف العوائق وأصبح العالم قرية صغيرة ، حيث أصبح من الضروري ابتكار بدائل للمحررات الورقية بمحررات الكترونية لتسهيل عملية بالتوقيع و التصديق عليها عبر وسائط الكترونية من خلال التوقيع الإلكتروني .

وسنتطرق في هذا المبحث إلى التكوين التقني للتوقيع الالكتروني (مطلب أول) مفهوم التصديق الالكتروني (مطلب ثاني).

المطلب الأول: التكوين التقني للتوقيع الالكتروني

إن حجية وصحة المحررات والعقود ونسبتها إلى مصدرها سواءا كان شخصيا أم عن طريق التفويض، تكون بتوقيع وإمضاء الأطراف المتعاقدة عليه وبالتطور التكنولوجي الحاصل في العالم ظهر التوقيع الالكتروني لمواكبة التطورات الحاصلة، وعليه سنتناول في هذا المطلب: الفرع الأول التوقيع التقليدي الفرع الثاني تعريف التوقيع الالكتروني الفرع الثالث صور التوقيع الالكتروني.

الفرع الأول: التوقيع التقليدي

أولا: تعريف التوقيع التقليدي

يعرف التوقيع بأنه "علامة أو إشارة تميّز شخصية الموقّع، وتعبّر عن إرادته في الالتزام بمضمون السند الموقع و إقراراه له[1]، ويتسم هذا التوقيع التقليدي بسهولة تمييز صاحبه، فهو غالبا ما يُدمج مع اسم الموقّع.

ولا يوجد تعريف قانوني عام للتوقيع ، لذلك فإن معظم القوانين الوطنية تتبنى المبدأ الواقعي بأن أي علامة أو إشارة ستكون كافية إذا ثبت بها اتجاه نية الموقّع إلى الالتزام بهذا المستند[2].

---

[1]– محمد المرسي زهرة، **الحاسوب والقانون**، ط1 ، مؤسسة الكويت للتقّدم العلمي، الكويت ،1995، ص114.

[2]– محمد سعيد أحمد إسماعيل، **أساليب الحماية القانونية لمعاملات التجارة الإلكترونية دراسة مقارنة**، ط1، منشورات الحلبي الحقوقية، لبنان،2009 ، ص242.

ثانيا: خصائص التوقيع التقليدي

من خلال ما سقناه من تعريفات للتوقيع التقليدي، يمكن الإشارة إلى خصائصه في النقاط الآتية:

– تحديد هوية الموقّع، حيث يساعد التوقيع المكتوب (الخطي) على تمييز الشخص صاحب التوقيع.

–نسبة المستند للموقّع، حيث تمتد وظيفة التوقيع الخطي إلى مجال أوسع من تمييز الشخص صاحب التوقيع إلى نسبة المستند الموقّع إلى شخص معيّن يؤكّد ارتباط هذا الأخير بالمستند الذي وقع عليه.

– الموافقة، حيث أن وجود التوقيع الخطي على مستند ما يدل على قبول الشخص صاحب التوقيع على المحتوى الذي تضمنه هذا المستند. [1]

الفرع الثاني: تعريف التوقيع الالكتروني

تعددت التعريفات التي مُنحت للتوقيع الإلكتروني بتعدد الجهات التي عرّفته، وهذا ما سنتناوله في الفرع الحالي من خلال تعريف التوقيع الإلكتروني وفقا للفقه القانوني، فتعريفه في ظل التشريعات الدولية، وصولا إلى تعريفه وفق التشريع الجزائري.

أولا: التعريف الفقهي للتوقيع الالكتروني

اختلف الفقهاء في إعطاء تعريف موحد للتوقيع الالكتروني وذلك حسب النظرة إليه فهناك من يعرفه بناءا على رسائل بيانات التي يتم بها ، أو بحسب الوظيفة أو الدور الذي يؤديه التوقيع ، أو بناءا على التطبيقات العملية للتوقيع ، وبالرغم من اختلاف هذه التعريفات إلا أننا نقسمها إلى طائفتين هما كالتالي :

1– الطائفة الأولى : ارتكزت في تعريفها على الكيفية و الطريقة التي ينشأ من خلالها ، حيث ركزت على أنه ينشأ من إجراءات غير تقليدية أو معادلات خوارزمية ، إضافة لعدم بيانها للدور أو الوظيفة التي يقوم بها التوقيع الالكتروني وهي تحديد هوية الشخص وبيان موافقته والتزامه بما جاء في مضمون المحرر ومن هذه التعريفات نذكر :" التوقيع الناتج عن

[1]– محمد سعيد أحمد إسماعيل، المرجع السابق، ص 243

إتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معينة معروفة مقدما ، فيكون مجموع هذه الإجراءات هو البديل للتوقيع التقليدي" [1].

كما عرف أيضا :" استخدام معادلات خوارزمية متناسقة يتم معالجتها من خلال الحاسب الآلي تنتج شكلا معينا يدل على شخصية صاحب الموقع".[2]

02- الطائفة الثانية : ركزت هذه الطائفة على كيفية إنشاء التوقيع الالكتروني ، على اعتبار أنه مجموعة من الإجراءات التقنية ، دون تحديد وظائف لهذه الإجراءات ، تاركا المجال لأي إجراء قد يستجد ويكون ذا كفاءة على تحقيق وظائف التوقيع ، إضافة إلى إبراز الوظيفة التي يقوم بها التوقيع وهي تحديد هوية الموقع والتعبير عن إرادته الموافقة على مضمون المحرر الالكتروني الذي تم وضع التوقيع عليه ومن هذه التعريفات نذكر:" مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع الالكتروني بمناسبته ".[3]

ثانيا: تعريف التوقيع الإلكتروني في التشريعات الدولية والإقليمية

سنتناول في العنصر الحالي تعريف هيئة الأمم المتحدة ممثلةً بلجنة التجارة الإلكترونية (الأونيسترال) ومن ثَم تعريف الاتحاد الأوروبي من خلال التوجيه الأوروبي للتوقيع الإلكتروني.

1- تعريف التوقيع الإلكتروني في قانون الأونيسترال النموذجي: أصدرت لجنة الأمم المتحدة للتجارة الالكترونية للتجارة الالكترونية "الأونيسترال" قانونا خاصا بالتوقيع الالكتروني بتاريخ : 05 يوليو 2001 ، تصدت من خلاله لتعريف هذا التوقيع وكيفية استخدامه والقواعد الخاصة به بمساعدة من لجنة للدول في وضع قواعد خاصة بالتوقيع الالكتروني ، حيث جاء في المادة (2/أ)[4] منه هو:" أن التوقيع الالكتروني بيانات في شكل الكتروني

---

[1] – لورنس محمد عبيدات ، **اثبات المحرر الالكتروني** ، دار الثقافة للنشر والتوزيع ، الأردن 2005 ص 127

[2] – حسن عبدالباسط جميعي ، **اثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت** ، دار النهضة العربية ، مصر 2000 ، ص35.

[3] – خالد مصطفى فهمي ، **النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات** الدولية ، دار الجامعة الجديدة ، مصر ، 2007 ، ص 37

4 – المادة 2 فقرة أ من قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية مع دليل الإشتراع 2001 ، منشورات الأمم المتحدة نيويورك ،2002 .

مدرجة في رسالة البيانات أو مضافة إليها، أو مرتبطة بها منطقيا يجوز ان تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".

ويظهر من خلال التعريف السابق الإشارة إليه أن القانون النموذجي قد اهتم بمسألتين هما تعيين هوية الشخص الموقع ، وبيان موافقته على المعلومات الواردة في المحرر ، وهو بذلك انسجم مع الأصل العام للتوقيع للدلالة على شخص الموقع ، و للتأكيد على أن إرادته قد اتجهت للالتزام بما وقع عليه.[1]

2- تعريف التوقيع الإلكتروني في توجيهات الإتحاد الأوروبي: لقد كان ازدهار التجارة الالكترونية في دول المجموعة الأوروبية الدافع وراء التنظيم التشريعي للتوقيع الالكتروني ، فقد أصدر مشرع المجموعة الأوروبية التوجيه رقم : 93-1999 الصادر في :13 فيفري 1999 والمتعلق بوضع إطار اتحادي للتوقيع الالكتروني ، ولقد عرف الإتحاد الأوروبي نوعين من التوقيع الالكتروني ووضع لكل منهما تعريفا محددا وهما [2] :

* **التوقيع الالكتروني** :" معلومات في شكل الكتروني متعلقة بمعلومات الكترونية أخرى ومرتبطة بها ارتباطا وثيقا ويستخدم أداة توثيق".

* **التوقيع الالكتروني المعزز** :" هو عبارة عن توقيع الكتروني يشترط فيه أن يكون :

- مرتبط ارتباطا فريدا من نوعه مع صاحب التوقيع.
- قادر على تحقيق (تحديد) صاحب التوقيع والتعرف عليه باستخدامه.
- تم إيجاده باستخدام وسائل يضمن فيها صاحبه السرية التامة.
- مرتبط مع المعلومات المحتواة في الرسالة حيث أنه يكشف أي تغيير في المعلومات.

[1] - لزهر بن سعيد ، **النظام القانوني لعقود التجارة الالكترونية** ، دار هومة للطباعة والنشر و التوزيع ، الجزائر ،2012 ص 153-154.

[2] - علاء محمد نصيرات، **حجية التوقيع الالكتروني في الإثبات (دراسة مقارنة)**،ط1، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص 154

ثالثا: تعريف التوقيع الإلكتروني في التشريع الجزائري

اعترف المشّرع الجزائري بالتوقيع الإلكتروني لأول مرة بنص المادة 2/327 من القانون المدني، ومن ثَم في القانون المتعلق بنظام الاستغلال المطّق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

وصولا إلى تعريف المشرع الجزائري للتوقيع الإلكتروني في قانون خاص بالتوقيع والتصديق الإلكترونيين حصار، متمثلا في القانون رقم (15 -04) المؤّرخ في: 01-02-2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1].

اعترف المشّرع الجزائري بالتوقيع الإلكتروني في القانون المدني في المواد: (323 مكرر1) و(327) و نصّت المادة : (323 مكرر1) المستحدثة بالقانون رقم 50-01 مؤّرخ في : 02-07-2005 على ما يلي: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها".

و نصّت المادة (323 مكرر1) من القانون نفسه على أنه:" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها". [2]

أما المرسوم التنفيذي رقم (07 -162) لسنة 2007 فقد عرف المشّرع الجزائري التوقيع الإلكتروني من خلاله بنص المادة الثالثة (03) منه.[3]

بالإضافة إلى الفقرة (02) من المادة (03) من المرسوم السابق الذكر، تضمنت التوقيع المؤّمن وعرّفته على أنه:" توقيع إلكتروني يفي بالمتطلبات الآتية:

---

[1]- القانون رقم (15-04) مؤرخ في 01 -02-2015، يحدّد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 60.

[2] - المواد (323 مكرر1) و(327) من الأمر 75-58 المؤرخ في : 26 سبتمبر 1975 ، المتضمن القانون المدني الجزائري ج،ر،ع 78 مؤرخة في 30سبتمبر 1975 ، معدل ومتمم .

[3]- المادة 03 المرسوم التنفيذي رقم (07-162) المؤّرخ في 30 ماي2007 ، المتعلق بنظام الاستغلال المطّق على كل أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية يعدل ويتمم المرسوم التنفيذي رقم : (01-123) مؤرخ في 09 جويلية 2001 ج، ر،ع 27 الصادرة في 13 جويلية 2001. ونصها:" التوقيع الإلكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر، و323 مكرر1 ".

– أن يكون خاصا بالموقع .

–يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقّع تحت رقابته الحصرية.

– يضمن مع الفعل المرتبط به صلة، بحيث يكون أي تعديل لاحق للفعل قابلا للكشف.

أما تعريف المشّرع الجزائري للتوقيع الإلكتروني من خلال القانون رقم (15 –04) لسنة 2015 فقد كان بنص المادة (02) التي جاء فيها أن التوقيع الإلكتروني هو:" بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".[1]

ويتضح من خلال هذه النصوص أن المشّرع الجزائري قد عرّف التوقيع الإلكتروني من خلال مجموعة عناصر قانونية وتقنية، إضافةً إلى تبنيه التوقيع الإلكتروني العام أو البسيط، والتوقيع الإلكتروني المؤّمن.[2]

الفرع الثالث: صور التوقيع الالكتروني وخصائصه

ان تحديد صور التوقيع الإلكتروني يتم من خلال الطريقة التي يتم بها هذا التوقيع ، كما تتباين الصور فيما بينها من حيث درجة الثقة ومستوى ما تقدمه من ضمان بحسب الإجراءات المتبعة في إصدارها وتأمينها والتقنيات التي تخرجها ، كما أن للتوقيع الالكتروني عدة خصائص تقنية تميزه على التوقيع التقليدي وسنتعرض لكل منها على حدى على النحو التالي :

أولا: صور التوقيع الالكتروني

1– التوقيع باستخدام الخواص الذاتية (البيومتري): signature biométrique

يقوم هذا النظام على اعتماد الصفات والخواص الفيزيائية والطبيعية والسلوكية للإنسان والتي من المفترض والطبيعي أن تختلف من شخص لأخر ، ومن هذه الخواص البصمة الشخصية ، ومسح العين أو ما يعرف ببصمات قزحية العين وهي الجزء الموجود خلف قرنية العين والذي يعطي للعين لونها ، وتختلف من شخص لأخر ، وخواص اليد البشرية ، وبصمات أو نبرة الصوت والشفاه ، ودرجة ضغط الدم وغير ذالك من الصفات الجسدية والسلوكية [3] ،

---

[1]– القانون رقم (15–04) ، المرجع السابق.

[2]– يمينة حوحو، **عقد البيع الإلكتروني دراسة مقارنة**، أطروحة دكتوراه، جامعة ابن عكنون، الجزائر 2012 ص177.

[3] – عيسى الصمادي ، **الإثبات في عقد نقل التكنولوجيا الالكتروني – عبر شبكة الانترنت** –، مجلة دراسات قانونية ، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية ، الجزائر ، ع 06، 2010 ص 68.

ويتم تخزين هذه الخواص على جهاز الحاسب الآلي وذلك بطريقة التشفير ، ويعاد فك هذا التشفير للتحقق من صحة التوقيع ، وذلك بمطابقة صفات وسمات العميل المستخدم للتوقيع مع الصفات التي تم تخزينها على جهاز الحاسب الآلي[1].

2- التوقيع بالقلم الالكتروني : Pen-op:

ويتمثل ذلك في نقل التوقيع المحرر بخط اليد على شاشة الحاسب الآلي عن طريق برنامج معين ، ويقوم البرنامج بوظيفيتين أساسيتين لهذا النوع من التوقيعات ، الأولى هي خدمة التقاط التوقيع ، والثانية هي خدمة التحقق من صحة التوقيع. ولكن يحتاج هذا النظام إلى جهاز الحاسب الآلي بمواصفات خاصة ، و يستخدم هذا بواسطة أجهزة الأمن ، والمخابرات كوسيلة للتحقق من الشخصية.

ويرى البعض أن هذه الطريقة من طرق التوقيع الالكتروني توفر مزايا لايمكن إنكارها لمرونتها ، وسهولة استعمالها حيث يتم من خلالها تحويل التوقيع التقليدي إلى الشكل الالكتروني عبر أنظمة معالجة المعلومات.

إلا انه يعاب على هذا الأسلوب من التوقيع الالكتروني انه يحتاج إلى جهاز حاسب إلي ذو مواصفات خاصة تمكنه من أداء مهمته من التقاط التوقيع من شاشته والتحقق من مطابقة التوقيع المحفوظ بذاكرته ، كما أنه يحتاج إلى جهة توثيق إضافية[2].

3- التوقيع الرقمي : Digitale ou numérique signature

هو استخدام أرقام حسابية مطبوعة عن طريق التشفير لتركيز وضغط محتوى المعاملة التي يتم التوقيع عليها، وتتم الكتابة الرقمية للتوقيع ولمحتوى المعاملة عن طريق التشفير وذلك باستخدام مفاتيح سرية وطرق حسابية معقدة ومعادلات رياضية (لوغارتميات) تتحول بواسطتها المعاملة من رسالة ذات كتابة عادية مقروءة ومفهومة إلى معادلة رياضية أو رسالة رقمية غير مقروءة وغير مفهومة ، ما لم يتم فك تشفيرها ممن يملك فك الشفرة وهو

---

[1] – فيصل سعيد الغريب ، **التوقيع الالكتروني وحجيته في الإثبات** ، المنظمة العربية للتنمية الإدارية ، مصر ، 2005 ص 231.

[2] – عبد العزيز سمية ، **التوقيع الالكتروني وسيلة حديثة للإثبات –دراسة مقارنة**– مجلة معارف (مجلة علمية محكمة) قسم العلوم القانونية ، السنة الثامنه – العدد 17/ ديسمبر 2014 ، ص 177.

المعادلة الخاصة بذلك والصورة الحديثة للتوقيع الرقمي هي استخدام تقنية شفرة المفتاحين العام والخاص.

أ- مفتاح الشفرة العام: هو أداة الكترونية متاحة للكافة تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر والتأكد من صحة وسلامة محتوى المحرر الأصلي الالكتروني.[1]

ب- مفتاح الشفرة خاص : هو أداة الكترونية خاصة بصاحبها تنشأ بواسطة عملية حسابية خاصة تستخدم في وضع التوقيع الالكتروني على المحررات الالكترونية ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة ، وتستخدم هذه البطاقة كوسيط الكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الالكتروني ، ويحتوي على شريحة الكترونية بها معالج الكتروني وعناصر تخزين برمجيات للتشغيل وتمكن المتعاقدين وضع المفتاح الشفري الخاص به على العقد و إعادة إرساله إلى المتعاقد الآخر حيث تكتسب حصانه عدم إمكانية التعديل أو التغيير في البيانات فيحقق أعلى درجات الثقة و الأمان للمحرر.

ويتميز التوقيع الرقمي المفتاحي بأنه يشكل درجة كبيرة من الأمان والثقة بين المتعاملين لكون المعادلات الخاصة به ومفاتيح الشفرة تتيح لصاحبها بشكل كبير التأكد من صحة مضمونها ويبدو أن الفقهاء يخشون تسلط القراصنة على المتخصصين في استنساخ المفاتيح الخاصة وإعادة صياغة المبادلات الرياضية التي تمكن من الوصول إليها ، ومن ثم يقترح البعض إنشاء أرشيف تتولاه هيئة متخصصة تكون مهمتها اعتماد رسالة البيانات ووضع توقيعها الخاص عليه وذلك من خلال مفتاح خاص بها ، بينما يذهب البعض إلى وجوب إنشاء أكثر من مفتاح خاص بالمعاملات الالكترونية إذا توصل القراصنة إلى احدهم لا يتمكنون من الوصول إلى الآخر[2] .

4- التوقيع الإلكتروني اليدوي أو الإمضاء الآلي: نعني به قيام الشخص بتخزين إمضائه اليدوي في الكمبيوتر بعد تصويره و إدخاله إليه بالماسح الضوئي ويتم حمايته برقم سري ليتم

[1] - عبد العزيز سمية ، المرجع السابق ، ص 177-178.

[2] - المرجع نفسه ،ص 178- 179.

استعماله عند الحاجة، وهذا النوع لا يتمتع بد رجة كبيرة من الأمان إذ أن المرسل إليه يستطيع أن يحتفظ بنسخة من صورة التوقيع ويعيد لصقها على أي وثيقة إلكترونية.[1]

5- التوقيع بواسطة البطاقة الممغنطة والرقم السري:

تعتبر هذه الصورة من صور التوقيع الإلكتروني شيوعا في مجال المعاملات البنكية، إذ تتطلب أن يكون لدى الشخص حاسب آلي،

أو أن يتصل جهازه بشبكة الأنترنيت، لذا فإنها تستخدم بهدف قيام العميل بسحب المبالغ النقدية، والتي تحدد بمبلغ معين، عن طريق أجهزة الصراف الآلي، أو بهدف سداد ثمن السلع والخدمات للمحال التجارية بإدخال البطاقة في جهاز مخصص لهذا الغرض، فهذه البطاقة يصد رها البنك أو المؤسسات الائتمانية لعملائها لغرض تخفيف الضغط عليها،إذ بدلا من ذهاب العميل إلى البنك لسحب المبالغ النقدية، فإنه يقوم بهذه العملية عن طريق الصراف الآلي بإتبا ع إجراءات معينة تتم الاتفاق عليها بينه وبين الجهة المصدرة للبطاقة.[2]

يتم ذلك عندما يقوم العميل بإدخال البطاقة في الجهاز الذي يتعرف على البطاقة ثم يطلب منه أن يقوم بإدخال الرقم السري الخاص ليتأكد من أن حامل البطاقة هو الشخص المخول لدخوله إلى الحساب البنكي وبالتالي يسمح له بالقيام بما يريد من عمليات سحب وإيدا ع وغيرها من العمليات.

إن دقة هذا النظام تكمن في أنه يشتمل على رقم سري متميز بصاحبه، وبالتالي لو عثر على البطاقة فلا يستطيع أي شخص استخدامها ما لم يكن على علم بالرقم السري، وهذا نادرا ما يحدث إلا بإهمال شديد من قبل حامل البطاقة الذي يمكنه تفادي ذلك عن طريق مخاطبة البنك بوقف العمل بهذه البطاقة.[3]

---

[1]- حابت آمال، **التجارة الإلكترونية في الجزائر**، رسالة لنيل شهادة دكتورة في العلوم، تخصص قانون، كلية الحقوق، جامعة .مولود معمري، تيزي وزو، 2015 ، ص106.

[2]- عاطف عبد الحميد حسن، **التوقيع الإلكتروني، (مفهومه، صوره، حجيته في الإثبات في نطاق المعاملات المدنية)** د ط، دار النهضة العربية، القاهرة،2009 ، ص70 .

[3]- علاء محمد عيد النصيرات، المرجع السابق، ص36 .

ثانيا: خصائص التوقيع الالكتروني

يتميز التوقيع الإلكتروني بعدة خصائص أهمها ما يلي:

-التوقيع الإلكتروني يتم عبر وسائل إلكترونية وعن طريق أجهزة الحاسب الآلي والإنترنت أو على أسطوانة،[1] حيث أصبح بإمكان أطراف العقد الاتصال ببعضهم البعض والاطلاع على وثائق العقد والتفاوض بشأن شروطه وكيفية إبرامه و ٍإفراغه في محررات إلكترونية وأخيرا إجراء التوقيع الإلكتروني عليه. [2]

- لم يشترط في التوقيع الإلكتروني صورة معينة حيث أنه يمكن أن يأتي عن شكل حرف أو رمز أو رقم أو إشارة أو حتى صوت، المهم فيه أن يكون ذو طابع منفرد يسمح بتمييز شخص صاحب لتوقيع وتحديد هويته و ٍإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه .[3]

– الوظيفة الرئيسية للتوقيع الإلكتروني هي الحفاظ على مضمون المحرر الإلكتروني وتأمينه من التعديل بالإضافة أو الحذف، وذلك عن طريق ربط المحرر الإلكتروني بالتوقيع الإلكتروني.[4]

– التوقيع الإلكتروني يحقق الأمان والخصوصية والسرية في نسبته للموقع، وبالنسبة للمتعاملين، وخاصة مستخدمي شبكة الإنترنت، وعقود التجارة الدولية، وذلك عن طريق إمكانية تحديد هوية الموقع، ومن ثم حماية المؤسسات من عمليات تزوير التوقيعات.

التوقيع الإلكتروني يحدد شخصية الموقع ويميزه عن غيره .[5]

المطلب الثاني: التصديق الإلكتروني

نظرا لحتمية حماية البيانات الشخصية والمعلومات الخاصة بالأطراف المتعاقدة في مجال العقود الالكترونية أصبح من الضروري التصديق عليها من طرف هيئات مختصة ذات كفاءة تقنية وعملية قانونية موثوق بها وطاقم بشري مؤهل نظرا لصعوبة وتعقيد المهام

---

[1]– العبودي عباس، **تحديات إثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها**، ط1 ، منشورات الحلبي الحقوقية، .لبنان، 2010 ، ص149.

[2]– بشار محمود دودين، **الإطار القانوني للعقد المبرم عبر شبكة الإنترنت**، ط2 ، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص247.

[3]– العبودي عباس، المرجع السابق، ص149 .

[4]– بشار محمود دودين، المرجع السابق، ص248 .

[5]– ثروت عبد الحميد، المرجع السابق، ص38

المنوطة بهم وهذا ما يمنح للمتعاملين والأطراف المتعاقدة الثقة والأمان من خلال وثيقة تثبت تصديق هذه العقود.

ونظرا للدور المهم الذي يلعبه التصديق الإلكتروني وجب التطرق إليه من خلال الفرع الأول تعريف التصديق الالكتروني وطبيعته الفرع الثاني جهات التصديق الالكتروني الفرع الثالث شهادات التصديق الفرع الرابع سلطات التصديق الالكتروني.

الفرع الأول: مفهوم التصديق الإلكتروني وطبيعته

أولا: تعريف التصديق الالكتروني

يعرّف التصديق بأنه:" مجموعة من الأشياء أو العناصر التي تعتمد على الغرض الذي يراد استخدام التوثيق لتحقيقه".

ومن بين التعريفات التي صيغت للتصديق الإلكتروني أنه:" عملية لتحقيق التأكد والموثوقية في هوية المستخدم باستخدام الأجهزة والكيانات الأخرى من خلال نظم المعلومات والاتصالات".[1]

ويسجل بهذا الصدد اختلاف المصطلحات العربية بشأن التصديق الإلكتروني، فهناك من يسميه بالمصادقة، ومن يسميه بالتصديق، وآخرون بالتوثيق.

ونجد أن المشّرع الجزائري أطلق عليه اسم التصديق مثلما جاءت به المادة 02 الفقرة 15 من القانون رقم (15-04) لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث عرّف سياسة التصديق الإلكتروني على أنها: "مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين". [2]

ثانيا: طبيعة التصديق الالكتروني

يقول البعض عن طبيعة عملية التصديق الإلكتروني، أن منح شخص ثالث سلطة توثيق التوقيع الإلكتروني يقّرب مهمة الجهات القائمة على هذا الأمر من مهمة الموثق في النظام الفرنسي، أي التأكد من شخص المتعاقد ومن مضمون التصرّف المراد توثيقه".[3]

---

[1]– – حسام محمد نبيل الشنراقي، **الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني**، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013 ، ص65 .

[2]– المادة 02 ف 15 ، من القانون رقم(15-04) ، السابق الذكر.

[3]– عابد فايد عبد الفتاح فايد، **الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني** :دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني، دار الجامعة الجديدة، الإسكندرية، 2004 ، ص71

انطلاقا من هذا القول "عالج بعض الفقهاء موضوع سلطات التصديق تحت اسم فكرة الموثّق الإلكتروني، ومع ذلك يبقى فرق جوهري بين سلطات التصديق الإلكتروني والموثّق، يتمثل في أن هذه السلطات لا تملك أو ليس من مهمتها أن تتدخل في إنشاء وتأريخ وحفظ المحررات القانونية طبقا للإجراءات المنصوص عليها في القانون" .

فمهمة جهة التصديق الإلكتروني تقتصر على فحص التصرفات القانونية الإلكترونية و إعطاء ذوي الشأن شهادة بهذا المعنى تسمى شهادة التصديق الإلكتروني، ومع ذلك تشترك جهات التصديق مع الموثّق في التحمل ببعض الالتزامات. [1]

الفرع الثاني: جهات التصديق الالكتروني

سنتناول هذا الفرع جهات التصديق الإلكتروني بالتعريف بدايةً ثّم، تحديد دور واختصاصات جهات التصديق، وصولا إلى الوقوف على التزامات هذه الجهات.

أولا: تعريف جهات التصديق

تعددت التعريفات الفقهية والقانونية دوليا و إقليميا لجهات التصديق على التوقيع الإلكتروني، ومن بين أهم هذه التعريفات نورد ما يلي:

عرف جانب من الفقه القانوني جهات التصديق بأنها:" هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق به، يقّدم خدمات أمنية في التجارة الإلكترونية، من خلال إصدار شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، لتوثيق هوية الأشخاص مستخدمي التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه".[2]

وعرف قانون الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة (2001) جهة التصديق أو مقّدم خدمات التصديق بنص المادة (2-e) بأنه: "الشخص الذي يـُصْدر الشهادات الإلكترونية، ويمكن أن يقّدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية".[3]

---

[1]– عابد فايد عبد الفتاح فايد، المرجع السابق، ص 72.

[2]– نادية ياس البياتي، **التوقيع الإلكتروني عبر الانترنيت ومدى حجيته في الإثبات**، ط1 ، دار البداية ناشرون وموزعون، الأردن، 2014 ، ص188 .

[3]– حسام محمد نبيل الشنراقي، المرجع السابق، ص89 .

Art 2-e: «certification service provider means: a person that Issus certificates and my provide other services related to electronic signatures.

أما التوجه الأوروبي للتوقيعات الإلكترونية فقد عرّف مقدّم خدمة التصديق بنص المادة الثانية الفقرة (11) منه، بأنه:" كل كيان أو شخص طبيعي أو معنوي يقدّم شهادات التصديق أو خدمات أخرى لها علاقة بالتوقيعات الإلكترونية".[1]

أما المشرّع الجزائري فقد تناولها بصفة عرضية في المادة (03) من المرسوم رقم : (07 -162) لسنة 2007 والتي نصها: "مؤدي خدمات التصديق هو كل شخص في مفهوم المادة 8-8 من قانون رقم 03-2000 المؤرّخ في 05 -08-2000، يسلّم شهادات إلكترونية أو يقدّم خدمات أخرى في مجال التوقيع الإلكتروني".[2]

و بالرجوع إلى نص المادة (8 فقرة 8) من القانون أعلاه فقد جاء فيها أن: "موفد الخدمة هو كل شخص معنوي أو طبيعي يقدّم خدمة مستعملا وسائل المواصلات السلكية واللاسلكية.[3]

كما تناول المشرّع الجزائري تعريف جهات التصديق الإلكتروني أو مؤدي خدمات التصديق في القانون رقم (15-04) لسنة 2015 في الفقرة (12) من المادة (02) والتي نصت على أن: ""مؤدي خدمات التصديق هو كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يقدّم شهادات أخرى في مجال التصديق الإلكتروني".[4]

ثانيا: دور واختصاصات جهات التصديق الالكتروني

1- دور جهات التصديق الالكتروني

تتلخص مهام جهات التصديق الالكتروني فيما يلي :

أ- تحديد هوية المتعاملين في التعاملات الالكترونية وتحديد أهليتهم القانونية للتعاقد والتعامل، والتحقق من مضمون هذا التعامل وصحته وكذا جديته وبعده عن الغش والاحتيال.

---

[1]- التوجيه الأوروبي الصادر في 1999/12/13 بشأن التوقيعات الالكترونية :

Art 2-11: «prestataire de service de certification toute entité ou personne physique ou morale

qui délivre des certificats ou fournit d'autre services liés aux signatures électronique.

[2]- المرسوم التنفيذي رقم (07-162) لسنة 2007، السابق الذكر.

[3]- يمينة حوحو، المرجع السابق، ص202 .

[4]- القانون رقم (15 -04) لسنة 2015، السابق الذكر.

ب- تعقب المواقع التجارية على شبكة الانترنت للتحري عنها وعن جديتها و مصدقيتها، وإذا تبين عدم امن احد هذه المواقع تقوم بإرسال رسالة تحذيرية إلى المتعاملين معها توضح فيها عدم مصداقية هذه المواقع.

ج- إمساك السجلات الخاصة بالتواقيع الالكترونية، توضح فيها من الذي قام بهذه التوقيعات وما تم إلغاؤه منها وما تم إبطاله، وكذا ما تم إيقافه، وتعليق العمل به.

د- تزويد المتعاقدين في مجال التجارة الالكترونية بشهادات التوثيق أو التصديق الالكتروني، وهي تلك الشهادات التي تثبت نسبة التوثيق الالكتروني إلى الشخص مصدره استنادا إلى إجراءات توثيق معتمدة، وتقدم هذه الشهادات الدليل على أن صاحب الشهادة هو الشخص صاحب المفتاح العام، وشهد بان التوقيع الالكتروني هو توقيع صحيح ينسب لمن أصدره، ويستوفي الشروط والضوابط أللمطلوبة فيه باعتباره دليل إثبات يعول عليه.[1]

2- اختصاصات جهات التصديق

إنأهم اختصاص يُسند لمؤدي خدمات التصديق الإلكتروني هي عملية التصديق الإلكتروني، التي تهدف إلى ضمان صحة البيانات الإلكترونية وسلامتها، وتغطي مجالات عدة مثل التجارة الإلكترونية والإدارة والخدمات البنكية، فيتم إصدار وتسليم شهادات التصديق الإلكتروني التي تضمن فيها السلامة وصحة تلك البيانات".[2]

ففي التشريع الجزائري، فإن دور مؤدي خدمات التصديق إلى جانب تسليمه لشهادات المصادقة الإلكترونية، يقوم بأداء خدمات أخرى مرتبطة بالتوقيع الإلكتروني، منها حفظ الوثائق الإلكترونية واتخاذ التدابير اللازمة لتوفير الحماية لها وفقا للشروط المنصوص عليها قانونا، وهو ما نصت عليه المادة (30) من المرسوم التنفيذي رقم (07 -162) لسنة 2007 بقولها أن: "مؤدي خدمات التصديق الإلكتروني يسلم شهادات إلكترونية أو يقّدم خدمات أخرى في مجال التوقيع الإلكتروني" .[3]

---

[1]- عبد العزيز سمية، **التوقيع الالكتروني وسيلة حديثة للإثبات – دراسة مقارنة**- مجلة علمية محكمة، قسم العلوم القانونية، السنة الثامنة، العدد 17/ديسمبر 2014، ص 198.

[2]- يمينة حوحو، المرجع السابق، ص208.

[3]- المادة 30 من المرسوم التنفيذي رقم (07 -162) المؤّرخ في 30 -05 -2007، السابق الذكر.

إذ تختص السلطة الاقتصادية بتقديم ترخيص للتصديق الإلكتروني من أجل القيام بنشاط تأدية خدمات التصديق الإلكتروني، وهو ما جاء في نص المادة (33) من الفصل الثالث، القسم الأول، الفرع الأول من القانون رقم (15-04) لسنة 2015، كما أضاف القانون نفسه وأشار بنص المادة (41) وما يليها إلى أن مؤدي خدمات التصديق الإلكتروني يكلف بتسجيل و إصدار ومنح و إلغاء ونشر وحفظ شهادات التصديق الإلكتروني. [1]

الفرع الثالث: شهادات التصديق الالكتروني

بعد التطرق لجهات التصديق الإلكتروني، خرجنا بمجموعة من الأدوار والالتزامات الملقاة على عاتق هذه الجهات، ويعد إصدار شهادات المصادقة من أبرزها، تحتاج هذه الأخيرة (شهادات التصديق) إلى الوقوف عليها من خلال تعريفها، أنواعها، وأهم بياناتها.

أولا: تعريف شهادات التصديق الالكتروني

ورد في التشريع الجزائري فقد نصت المادة (03 مكرر7) من المرسوم التنفيذي رقم (07-162) لسنة 2007 على تعريف شهادة المصادقة الإلكترونية بأنها:"وثيقة تصدرها جهة التصديق الإلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقّع...". [2]
كما عرّفها القانون رقم (15- 04) لسنة 2015 والمتعلق بالتوقيع والتصديق الإلكترونيين في المادة (02 الفقرة 07) بأنها:"وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقّع. [3]

ثانيا: أنواع شهادات التصديق الإلكتروني

01-شهادات التصديق الإلكتروني العادية

ففي القانون الجزائري، فقد أشار في المادة : (03 مكرر8) من المرسوم (07 -162) لسنة 2007 إلى شهادة التصديق الإلكتروني العادية حيث سمّاها الشهادة الإلكترونية، وجاء في نص هذه المادة أن: "الشهادة الإلكترونية هي وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقّع". [4]

---

[1]- المادة 33 ، المادة 41 من القانون رقم (15 -04) لسنة 2015 ، السابق الذكر.

[2]- المادة 03 مكرر 07 من المرسوم التنفيذي(07 - 162) لسنة 2007، السابق الذكر.

[3]- المادة 02 فقرة 07 من القانون رقم (15 -04) سنة 2015، السابق الذكر.

[4]- يمينة حوحو، المرجع السابق، ص215

وهو نفس ما جاء به القانون رقم : (15-04) لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين حيث عرّفها على أنها:" شهادة تصدر عن جهات التصديق الإلكتروني المتنوعة تثبت الصلة بين معطيات التوقيع الإلكتروني والموقّع، إذ تحدد هوية الشخص الموقّع وتثبت ارتباط معطيات التوقيع الإلكتروني به".

وفي حقيقة الأمر فإن شهادة التصديق الإلكتروني العادية هي شهادة لا تفي بالمتطلبات المستوجبة في شهادة المصادقة الموصوفة، إذ أنها تصدر من أي جهة مختصة في إثبات هوية الموقّع لا غير، في حين شهادة التصديق الموصوفة تصدر عن جهة التصديق الإلكتروني المختصة في هذا المجال والموثوق بها".[1]

02- شهادات التصديق الإلكتروني المعتمدة

في القانون الجزائري فقد تناولها في المادة (03 مكرر9) من المرسوم (07-162) لسنة 2007 وعرفها بأنها:" شهادة إلكترونية تستجيب لمتطلبات محددة"، وهو نفس ما جاء به القانون رقم (15 -04) لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، إلا أن هذا الأخير أضاف مجموعة من البيانات التي يجب أن تحتويها هذه الشهادة، وسنتطرق إليها ببيانات شهادة التصديق بتفصيل أكثر.

إلى جانب النوعين الأولين لشهادة التصديق الإلكتروني، نجد أنواعا أخرى من الشهادات التي تقوم هيئات التصديق الإلكتروني بإصدارها، إذ تتنوع بحسب الغرض منها، ونذكر منها على سبيل المثال:

1- شهادة توثيق التوقيع الرقمي وتعد من أكثر أنواع الشهادات انتشرا وأكثرها أهمية.

2- شهادة توثيق تاريخ إصدار التوقيع الإلكتروني وهي الشهادة التي توثّق وقت وتاريخ صدور التوقيع الرقمي، حيث يقوم صاحب الشهادة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها. [2]

3- شهادة الإذن، حيث تتولى تقديم بيانات عن صاحب التوقيع الإلكتروني كمؤهلاته، محل إقامته والتراخيص التي يملكها وعمله .

---

[1]- يمينة حوحو، المرجع السابق، ص216.

[2]- خالد ممدوح إبراهيم، **إبرام العقد الإلكتروني**، ط1، دار الفكر الجامعي، مصر،2006 ، ص197

4- شهادة البيان التي تتحقق من صحة واقعة أو حدث ما وقت وقوعه، ومن هنا تظهر أهمية هذه الشهادة ومدى خطورة المعلومات التي تتضمنها والتي يعتمد عليها الغير وعلى أساسها يحدد تعاملاته.[1]

الفرع الرابع: سلطات التصديق الالكتروني

نص المشّرع الجزائري في القانون رقم (15- 04) لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين على سلطات التصديق الإلكتروني وقسّمها إلى ثلاثة أقسام، نوردها فيما يلي:

أولا: السلطة الوطنية للتصديق الإلكتروني

حدد القانون المذكور أعلاه في مواده من (16) إلى (25) تشكيلة السلطة الوطنية للتصديق الإلكتروني ومهامها وسيرها، حيث تقوم هذه السلطة التابعة للوزير الأول، والتي تتخذ شكل سلطة إدارية مستقلة حسب المرسوم التنفيذي رقم (134 -61) لسنة 2016[2] بتحديد السياسة الوطنية للتصديق الإلكتروني، وهي مكلفة بترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما، إضافةً إلى ضمان ومراقبة صحة استخدامهما.

وفي هذا الإطار، تتولى السلطة الوطنية للتصديق الإلكتروني المهام الآتية:

- إعداد سياستها للتصديق الإلكتروني والسهر على تطبيقها بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة.
- الموافقة على سياسات التصديق الإلكتروني الصادر عن السلطتين الحكومية والاقتصادية 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 والاقتصادية للتصديق الإلكتروني عن طريق الهيئة الحكومية المكلفة بالتدقيق.[3]

---

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 197

[2]- المرسوم التنفيذي رقم(134-16) مؤرخ في 05-04-2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، الجريدة الرسمية للجمهورية الجزائرية، العدد 62.

[3]- المادة 05 المرسوم التنفيذي رقم (134-16) ، المحددة لخلية التدقيق والمهام المكلفة بها، السابق الذكر.

وحسب القانون رقم(15-04) لسنة 2015 بنص المادة (09) منه، فإنه: تتشكل السلطة الوطنية من مجلس ومصالح تقنية وإدارية، ويتشكل هذا المجلس من خمسة أعضاء من بينهم الرئيس، يعيّنهم رئيس الجمهورية على أساس كفاءتهم، لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيا الإعلام والاتصال، وفي مجال قانون تكنولوجيا الإعلام والاتصال، وفي اقتصاد تكنولوجيات الإعلام والاتصال.

ويتمتع المجلس بجميع الصلاحيات اللازمة لأداء مهام السلطة، وبهذه الصفة يمكنه أن يستعين بأي كفاءة من شأنها أن تساعده في أشغاله، وتحدد عهدة أعضائه بأربعة سنوات قابلة للتجديد مرة واحدة .[1]

ثانيا: السلطة الحكومية للتصديق الإلكتروني

وعرّفها المرسوم التنفيذي رقم (135-16) لسنة 2007 بأنها:"سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي".[2]

وحسب القانون رقم (15- 04) لسنة 2015 فإن السلطة الحكومية تتولى المهام الآتية:[3]

1- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها.

2-الموافقة على سياسات التصديق الصادرة عن الأطراف الثلاثة الموثوقة والسهر على تطبيقها.

3-الاحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق بغرض تسليمها إلى السلطات القضائية المختصة عند الاقتضاء طبقا للأحكام التشريعية والتنظيمية المعمول بها.

4-نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة.

5- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناءً على طلب منها.

---

[1]- المادة 20 من القانون رقم (15 -04)، السابق الذكر.

[2]- المادة 20 من المرسوم التنفيذي رقم (135 -16) مؤرّخ في 25-04 -2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلتها وتنظيمها وسيرها، السابق الذكر.

[3]- المادة 28 من القانون رقم (15 -04)، السابق الذكر.

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

وتشكل السلطة الحكومية حسب المرسوم التنفيذي رقم (135-16) ويتولى إدارتها مدير عام، وتزود بمجلس للتوجيه بهياكل تقنية و إدارية.

ثالثا: السلطة الاقتصادية للتصديق الإلكتروني

تمثّل السلطة الاقتصادية للتصديق الإلكتروني الفرع الثاني للسلطة الوطنية (بعد السلطة الحكومية) وهي مكلفة بتسيير الشهادات المستعملة في المبادلات الإلكترونية بين المؤسسات (العقود الإلكترونية بين المؤسسات، وبين المؤسسة والمواطن) مثل (التجارة الإلكترونية) وبين المواطنين مثل (تبادل البريد الإلكتروني الموقع والمصادق عليه).

ويضمن تسليم الشهادات في الفرع الاقتصادي مانحو خدمات التصديق الإلكتروني المستفيدين من ترخيص لتقديم خدمات التصديق الإلكتروني.[1]

مما سبق يمكن القول أن التوقيع الالكتروني هو عبارة عن بيانات في شكل الكتروني حيث تحتاج هذه البيانات إلى تأمين وكذا التحقق من شخصية المتعاقدين وتأمين سلامة عملية تداول البيانات لإتمام الصفقات التجارية يحتاج إلى وسيلة حماية فنية بالدرجة الأولى ، ظهرت الحاجة إلى وجود طرف ثالث محايد موثوق به ، يتأكد بطريقة خاصة من صحة وجدية صدور التواقيع الالكترونية ، وكذا الإرادة التعاقدية الالكترونية ممن تنسب إليهم ، وبعدها عن الغش والاحتيال ، ويتمثل هذا الطرف الثالث المحايد في أفراد أو شركات أو جهات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الالكترونية يطلق عليها جهات التصديق أو مقدمي خدمات التصديق.

و سعيا منه إلى تكريس امن وسرية المعلومات من خلال حماية البيانات الشخصية للمتعاملين و إضفاء الثقة و الأمان على مختلف المعاملات في المجال الالكتروني الأساسية أصدر المشرع الجزائري القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين كتشريع مستحدث معالجا بذلك ما استجد من وسائل وأساليب لإبرام العقود.

[1]- المادة 29، المادة 30 من القانون رقم (15 -04)، المرجع السابق.

المبحث الثاني: نطاق الحماية الموضوعية للتوقع الالكتروني في القانون الجزائي

يعد التوقيع الالكتروني مفهوما حديثا جديدا نظرا لحداثة القوانين الصادرة في شأنه ، وتباينت التعريفات بشأنه في هذه القوانين إلا أنها تنظر بنفس الأهمية إلى مسألة حماية هذه الوسيلة جنائيا لأن التوقيع الالكتروني يرتبط أساسا بالوسيلة التقنية المستعملة وبقدرتها على الحفاظ على سرية وأمن المعلومات من الأخطار المتمثلة الاختراق و السطو والتعديل و التزوير و كذلك لكونه يتميز بخصائص تميزه عن التوقيع التقليدي وعليه سوف نحاول توضيح ما سبق من خلال هذا المبحث حيث سنتطرق فيه إلى نطاق الحماية الموضوعية للتوقيع الالكتروني من خلال مطلبين المطلب الأول تجريم المساس بالتوقيع الالكتروني أما المطلب الثاني العقاب على الاعتداء الواقع على التوقيع الالكتروني.

المطلب الأول: تجريم المساس بالتوقيع الالكتروني

إن الجرائم الواقعة على التوقيع الالكتروني تتميز بخصائص تقنية صعبة الإثبات نظر للبيئة الموجودة فيها ذات الطابع المعلوماتي وكذا الوسائل المستعملة في الاعتداء على التوقيع الالكتروني من خلال الإختراق والسطو والتعديل و التزوير حيث سنتناول في هذا المطلب الفرع الأول خصائص الجرائم الواقعة على التوقيع الالكتروني أما الفرع الثاني صور الجرائم الواقعة على التوقيع الالكتروني.

الفرع الأول: خصائص الجرائم الواقعة على التوقيع الالكتروني

تتميز جريمة تزوير التوقيع الإلكتروني بخصائص تجعلها مختلفة عن جريمة تزوير التوقيع العادي بحكم البيئة الافتراضية التي تتم فيها، والوسائل التي ترتكب بها، مما يجعل هذه الجريمة تتميز بطبيعة مختلفة عن جريمة تزوير التوقيع العادي، إن هذه الخصائص تتمثل في ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الاختراق، وصعوبة الكشف عن التزوير، لاستخدام أساليب تقنية دقيقة مقارنة بالتزوير العادي.

أولا : ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الاختراق

إن التوقيع الإلكتروني هو منظومة مكونة من رموز وأرقام تميز صاحبها وتحدد هويته، ومن بين صور هذا التوقيع المعتمدة على فكرة الرموز نجد التوقيع الكودي أو السري الذي يرتبط غالبا بالبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية، ويتم تزويره بعد تعرضه للسرقة، ثم استخدام الرقم والبطاقة في السحب.

أما صورة التوقيع البيومتري فتعتمد على الخواص الذاتية للشخص كقزحية العين، بصمة الأصبع، نبرة الصوت وغيرها، حيث يتم التقاط صورة دقيقة لعين المستخدم أو بصمة يده أو صوته ثم تخزن بطريقة مشفرة في ذاكرة الحاسب الآلي والذي يقوم بمطابقة صفات المستخدم مع هذه الصفات المخزنة ولا يسمح له بالتعامل إلا في حال المطابقة، لكن قد تتعرض هذه الصورة من التوقيع للأختراق بفك تشفير هذه البيانات ونسخها. [1]

كما يمكن التقاط أرقام البطاقات عبر شبكة الإنترنيت بعد عملية اختراق واستخدامها باسم مالك البطاقة، ففي عام 2004 أعلن مكتب التحقيقات الفيدرالي (FBI) أنه يحقق في حادث اختراق أجهزة كمبيوتر تم خلاله سرقة أرقام ثمانية ملايين بطاقة وفاء من شركة " Data processors international "، وقد تستخدم تقنية تفجير الموقع التي تعتمد على ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز القرصان إلى الجهاز المستهدف للتأثير على السعة التخزينية مما يشكل ضغطا يؤدي إلى تفجير الموقع وتشتيت البيانات المخزنة فيه، لتنتقل بعد ذلك إلى جهاز القرصان، ليتجول في الموقع بسهولة، ويحصل على كل ما يحتاجه من أرقام وبيانات خاصة ببطاقات الوفاء. [2]

ثانيا : استخدام أساليب تقنية في تزوير التوقيع الإلكتروني وصعوبة الكشف عنها

لقد أصبح للتوقيع الإلكتروني دورا واسعا في مجال المعاملات والتوقيع على الوثائق نتيجة الثورة التكنولوجية و الاعتماد على المعلوماتية في إنجاز هذه المعاملات، ومنها تلك التي تتم في القطاع الحكومي، حيث اتجه الواقع إلى البحث عن بديل للتوقيع التقليدي يستطيع أن يؤدي ذات الوظيفة من ناحية ويتكيف مع وسائل الإدارة الحديثة من ناحية أخرى، وهذا البديل يمكن أن يكون رقما سريا أو رمزا محددا وهو ما يسمى بالتوقيع الإلكتروني أي التوقيع الناتج عن إتباع إجراءات محددة تكنولوجيا تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي وهو ما نسميه بالتوقيع الإجرائي. [3]

---

[1] – أمجد حمدان الجهني،"**جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنيت**"،موقع الكتروني، تم الاطلاع عليه بتاريخ 2021/05/24 على الساعة، 15:45 **http://www.cojss.com/article.php?a=219**

[2] – المرجع نفسه.

[3]– أحمد السيد كردي ،"**التوقيع الإلكتروني مفهومه التكنولوجي وحمايته**" ، 32 سبتمبر 2011 تم الاطلاع عليه بتاريخ 2021/05/24 على الساعة 20:20 **http://kenanaonline.com/users/ahmedkordy/posts/323677**

إن هذا الاختلاف في طبيعة التوقيع يجعل تزويره مختلفا، ويصبح اكتشافه صعبا بالنظر لسهولة اكتشاف تزوير التوقيع الخطي بمضاهاة الخطوط، فيما لا يترك تزوير التوقيع الإلكتروني أثرا ظاهرا باعتبار أن التوقيع الإلكتروني هو ختم الكتروني مشفر يملك مفاتحه صاحب التوقيع .[1]

ويتم تزويره باعتماد التوقيع نفسه عن طريق الحصول عليه، بينما تزوير التوقيع العادي يكون من خلال تقليد التوقيع بطريقة تشبه التوقيع الأصلي.

إن تزوير التوقيع الإلكتروني أمر صعب بالمقارنة مع تزوير التوقيع العادي، باعتبار أن التوقيع الإلكتروني عبارة عن منظومة رقمية مرتبطة بأنظمة أمان تقنية، حيث يعتمد التوقيع الرقمي وهو أهم صور التوقيع الإلكتروني على الدوال الرياضية واللوغاريتمات، كما أنه يعتمد على نظام المفاتيح العامة والخاصة، كما يؤمنه نظام التشفير.[2]

ولذلك يعرف التوقيع الإلكتروني بأنه نظام تشفير الكتروني يعتمد على مفتاح خاص ومفتاح عام، وتنشأ المفاتيح بواسطة عمليات حسابية خاصة تضمن السرية، حيث يستخدم المفتاح الخاص في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ به على بطاقة ذكية مؤمنة، أما المفتاح العام فيوضع لدى شخص مستقبل الرسالة، ويستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي.[3]

الفرع الثاني: صور الجرائم الواقعة على التوقيع الالكتروني

أولا: جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني

عند تناول هذه الجريمة،"لابد من التفرقة بين الدخول والبقاء غير المصرح به، فالأول يتحقق باختراق نظم معلومات التوقيع الإلكتروني، أما البقاء فقد يترتب على الدخول غير المصرح به أو أن يكون الدخول قد تم بشكل قانوني مصرح به إلا أن القائم بالدخول استمر

---

[1]– ياسر العدل، **التوقيع الإلكتروني**، 2009/09/29، تم الاطلاع عليه بتاريخ 2021/05/25 على الساعة 17:20 **=https://www.m.ahewar.org/index.asp?ry=5&r=50&cid=0&i=1005&u=&q**

[2]– محمد محروك، **خصوصيات التوقيع الإلكتروني وحجيته في الإثبات**"، 4 فيفري 2013، تم الاطلاع عليه بتاريخ 2021/05/25 على الساعة 19:10 **https://www.marocdroit.com**

[3]– ياسر العدل، المرجع السابق.

داخل النظام متجاوزا الحد المسموح به للبقاء داخله فأصبح بذلك مرتكبا لجريمة رغم أن الدخول في بداية الأمر كان مشروعا".

1- الركن المادي للجريمة:

يتكون الركن المادي لهذه الجريمة" من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح به"[1]، و"دائما ما يثار التساؤل بشأن هذا الفعل وكيف يمكن تحديد ما إذا كان الفعل الذي ارتكبه الجاني هو ذاته الفعل المؤثم قانونا؟".[2]

فجريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني فإنه" لقيام هذه الجريمة لابد وأن الركن المادي المتمثّل في الدخول غير المشروع قد وقع على أنظمة معلوماتية أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني"، كما أن هذه الجريمة تصّنف من جرائم الخطر، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه".[3]

2- الركن المعنوي:

إن جريمة الدخول غير المصرّح به في نظم معلومات التوقيع الإلكتروني "من الجرائم العمدية التي يتمثّل الركن المعنوي فيها في القصد الجنائي العام بركنيه العلم والإرادة، ولا تتطلب قصدا جنائيا خاصا وذلك لكونها من جرائم الخطر التي يعاقب المشّرع فيها على مجرد إتيان الفعل المجرم، وعلى ذلك يعاقب المشّرع بعقوبة الجريمة التامة على إتيان الفعل المادي مع توافر القصد الجنائي دون اشتراط تحقق النتيجة المتوخاة من الجريمة".[4]

وانطلاقا من أن الركن المعنوي لجريمة الدخول غير المصرّح به لقاعدة بيانات تتعلق بالتوقيع الإلكتروني يتخذ صورة القصد الجنائي،" وعليه فإن معظم التشريعات التي جرّمت هذا الدخول غير المصرّح به قد تطلبت القصد العام.[5]

---

[1]- صالح شنين، **الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، رسالة دكتوراه، جامعة تلمسان، 2013، ص47.

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص141.

[3]- المرجع نفسه، ص 142.

[4]- المرجع نفسه، ص167.

[5]- المرجع نفسه، ص168.

ثانيا: الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية

يعد "الاحتيال في مجال نظم معلومات التوقيع الإلكتروني من أهم الجرائم التي يمكن أن تقع على التوقيع الإلكتروني وتسبب خسائر اقتصادية فادحة، نظرا للتطور المذهل في مجال التعامل واختزان التوقيعات الإلكترونية في حاسبات آلية موصولة بشبكة الانترنيت".[1]

1- تعريف الاحتيال الإلكتروني:

عُرّف الاحتيال المعلوماتي بأنه "التلاعب العمدي بمعلومات وبيانات تمثّل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناءا على هذه الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع و إلحاق ضرر بالغير".[2]

2- الركن المادي:

يتمثّل الركن المادي لجريمة الاحتيال الإلكتروني في: "التلاعب في معلومات وبيانات لها قيمة مالية بطرق احتيالية، قد لا تكون محصورة تماشيا مع طبيعة الاحتيال المعلوماتي، فالجريمة المعلوماتية بصفة عامة جريمة متطورة ومتجددة لارتباطها بتكنولوجيا المعلومات".[3]

أ- الوسائل الاحتيالية:

هناك خلاف فقهي بشأن تطبيق النص التقليدي للاحتيال على الاحتيال في مجال المعلومات ومدى إمكانية تصور الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط، انطلاقا من أن السائد قانونا وفقها أن السلوك الاحتيالي ينبغي أن يقع على شخص طبيعي، وعلى أساس هذا الخلاف الفقهي، تنوعت الوسائل الاحتيالية المستخدمة من قبل مرتكبي الجرائم المعلوماتية بتطور استخدامات الحواسيب، وتضمنت الوسائل الاحتيالية في جريمة

---

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص175.

[2]- حنان براهمي، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه، كلية الحقوق ،جامعة بسكرة ،2015. ص 84.

[3]- المرجع نفسه، ص 85.

النصب التقليدية عدة وسائل اشترط المشرع توافرها لكي يبلغ الجرم المرتكب مبلغ الاحتيال وهي:

- الطرق الاحتيالية.
- التصرف في مال ثابت أو منقول ليس ملكا للجاني ولا له حق التصرّف فيه.
- اتخاذ اسم كاذب أو صفة غير صحيحة.

أما فيما يتعلق بالاحتيال الإلكتروني، فإن اقتصار الفعل المادي على تلك الوسائل في شكلها التقليدي المادي البحت لا يحقق المعالجة القانونية لهذه المسألة".[1]

ويتجه الفقه الفرنسي إلى أن "غش وخداع نظم المعلومات والحاسبات لسلب المال تتحقق به الطرق الاحتيالية وفقا لنص المادة 405 عقوبات، حيث تتوافر فيه بالإضافة للكذب مظهر خارجي وهو إبراز المحررات أو المعلومات المدخلة للحاسب ونظام معلوماته".

كما يمكن أن تقع جريمة الاحتيال في بيئة التوقيع الإلكتروني "باتخاذ اسم كاذب أو صفة غير صحيحة ومن ذلك الدخول إلى نظام معلومات التوقيع الإلكتروني باستخدام أسماء وشفرات مستخدميه الشرعيين بقصد الاستيلاء على التوقيعات، ومن ثم الأموال".[2]

ب- تسليم معلومات التوقيع الإلكتروني (النتيجة الجرمية):

في مجال المعلومات الإلكترونية "يقوم الحاسب الآلي بفعل التسليم بالمفهوم المادي للكلمة، كما أن التسليم يجب ألا يُنظر إليه في الشكل المادي فقط وإنما هو عمل قانوني عنصره الجوهري إرادة المجني عليه المعيبة بالخداع وليست المناولة المادية سوى مظهره المادي أو أثره".[3]

ج- علاقة السببية بين طرق الاحتيال وتسليم المعلومات:

"لا يكفي لقيام جريمة الاحتيال التامة أن يصدر من الجاني فعل الاحتيال، وأن يسلم المجني عليه الشيء المملوك له إلى هذا الجاني، بل يلزم أن تتوفر صلة ما بين فعل

---

[1]- محمد هشام صالح عبد الفتاح ،جريمة الاحتيال دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، لجامعة النجاح الوطنية، نابلس، فلسطين ،2008، ص 80.

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص167.

[3]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص85.

الاحتيال وتسليم الشيء المملوك وأن يكون الثاني ثمرة أو نتيجة للأول"[1]، بمعنى لابد من توافر علاقة سببية ما بين فعل الاحتيال وفعل التسليم.

هذا فيما يتعلق بجريمة الاحتيال بصفة عامة، أما فيما يتعلق بجريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، فإن توافر علاقة السببية لازم لتحقيق الركن المادي في هذه الجريمة ،"فقد ذهب الفقه الفرنسي إلى أن غش وخداع نظام المعلومات بسلب المال يتحقق باستعمال الوسائل الاحتيالية بالكذب الذي تدعمه مظاهر مادية أو خارجية تؤيده، كتقديم محررات مستخرجة من الحاسب الآلي بالتلاعب أو معلومات مدخلة إليه.[2]

3- الركن المعنوي

باعتبار الاحتيال في مجال التوقيع الإلكتروني جريمة عمدية فهو يستلزم توافر القصد الجنائي بنوعيه أي القصد العام والقصد الخاص.

أ- القصد الجنائي العام:

يقوم القصد الجنائي العام على عنصري العلم والإرادة ،"إذ ينبغي أن يعلم الجاني أن التوقيعات الإلكترونية التي يستولي عليها مملوكة للغير بأنها مملوكة للمجني عليه أو لغيره، كما ورد بالمذكرة التفسيرية للاتفاقية الأوروبية لمكافحة جرائم المعلوماتية بشأن المادة (8/ب) أن الجريمة يجب أن تُرتكب عمدا، ويتمثّل العنصر العام للقصد في التلاعب أو التدخل ألمعلوماتي الذي يسّبب ضرار ماديا للغير".[3]

1-القصد الجنائي الخاص:

يقوم القصد الخاص في جريمة الاحتيال "اتجاه نية الجاني إلى تملك الشيء الذي تسلمه من المجني عليه، ويباشر مظاهر السيطرة التي ينطوي عليها حق الملكية وأن يحرم المجني عليه من مباشرتها، ولنية التملك في الاحتيال ذات مدلولها في جريمة السرقة، فإذا لم تتوافر لدى الجاني نية تملك الشيء الذي تسلمه فإن القصد الخاص لا يتوافر لديه".[4]

---

[1]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص 85

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص214.

[3]- المرجع نفسه، ص 215.

[4]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص86.

أما الاحتيال على نظم معلومات التوقيع الإلكتروني فهي "جريمة عمدية تتطلب توافر إرادة ارتكابها مع العلم بكون الفعل المراد ارتكابه مؤثم قانونا ومع ذلك تتجه نية الجاني لارتكابه، إذ أن الجاني يجب أن يكون عالما بأن التلاعب الذي يرتكبه في النظام المعلوماتي للتوقيع الإلكتروني أو المعلومات التي يقوم بالتحايل على الحاسب الآلي بإدخالها إليه، فيجعله يستجيب لما يريده، ويسلمه المعلومات التي يرغب في الحصول عليها، هو فعل مجرّم قانونا". [1]

إذا في إطار معلومات التوقيع الإلكتروني، فإنه "يجب أن تتجه إرادة الجاني إلى تحقيق ربح غير مشروع له أو لغيره، وهو ما فسرته المذكرة التفسيرية لاتفاقية بودابست الموقعة في 23-11-2001 بأن جريمة الاحتيال في مجال المعلومات تتطلب بالإضافة للقصد العام قصدا خاصا يتمثل في نية الغش أو نية الغش خاصة، أو بتعبير آخر نية غير آمنة أو غير شريفة بغرض الحصول على منفعة اقتصادية لشخص الجاني أو لغيره".[2]

ثالثا: جريمة تزوير التوقيع الإلكتروني

سنتناول في هذا الجزء جريمة أخرى من جرائم الاعتداء على التوقيع الإلكتروني والمتمثلة في جريمة تزوير التوقيع الإلكتروني، من خلال تعريف التزوير التقليدي والإلكتروني ومن ثم الوقوف على الركن المادي والمعنوي للجريمة، وصولا إلى تحديد عقوبة هذه الجريمة في عدد من التشريعات.

01- تعريف جريمة تزوير التوقيع الإلكتروني

أ- **تعريف التزوير**: يعرف التزوير لغةً على أنه "إصلاح الكلام وتهيئته، وهي كلمة مشتقة من الزور ويعني الكذب والباطل فيقال كلام مزور ومموه بالكذب، أما في الفقه فيعرف على أنه كل وسيلة يستعملها شخص ليغش بها آخر".[3]

أما التزوير قانونا فهو:"عملية مادية وصورة من صور الكذب التي يقوم بها الشخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو رسمي بإحدى الطرق المحددة في

---

[1]- أسامة بن غانم لعبيدي،"**حجية التوقيع الإلكتروني في الإثبات**"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28 العدد 56، جامعة نايف للعلوم الأمنية، السعودية ،2012، ص166.

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص214.

[3]- المرجع نفسه، ص233.

القانون ، ومن شأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الإدعاء بالتزوير".[1]

والتزوير في مجال الأنظمة المعلوماتية، يعرف على أنه: "التلاعب في المعلومات المخزّنة في أجهزة الحاسب المرتبطة بالشبكة أو اعتراض المعلومات بقصد تحريفها وتزويرها".[2]

ب- التزوير الإلكتروني: عرف الفقه التزوير الإلكتروني (المعلوماتي) بأنه :" تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها"، كما عرفه بأنه:" تغيير الحقيقة بأي وسيلة كانت سواءًكان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة".[3]

02 - الركن المادي لجريمة تزوير التوقيع الإلكتروني:

يتمثل الركن المادي لجريمة تزوير التوقيعات الإلكترونية في سلوك الجاني والمتمثل في تغيير الحقيقة والتي تكون محل التوقيع الإلكتروني، ويحصل التزوير بأي وسيلة كانت كاستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك.

أ- تغيير الحقيقة (سلوك الجاني): "تغيير الحقيقة هو استبدالها بما يخالفها، أي هو إدخال تغيير على المحرّر المراد تزويره على نحو يغير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته".[4]

ويُقصد بتغيير الحقيقة أيضا: "ليس تغيير الحقيقة الواقعية المطلقة إنما الحقيقة النسبية كأن يثبت في المحرر المزور ما يخالف إرادة صاحب الشأن ويقوم بتزوير توقيع صاحب الشأن عليها حتى ولو صادف ذلك الواقع فعلا".[5]

ويكون التزوير في نطاق المعلومات "بتغيير الحقيقة في الشرائط أو المحررات التي تمثّل مخرجات الحاسب الآلي طالما حدث تغيير في بيانات الحاسب الآلي نفسه، وهو ما انتهجه قانون العقوبات الفرنسي الجديد، حيث نص على أن الركن المادي للتزوير هو

---

[1]- عباس حفصي، **جرائم التزوير الإلكتروني- دراسة مقارنة-**، رسالة دكتوراه، جامعة أحمد بن بلة، وهران1، 2015 ص61.

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص253.

[3]- حنان براهمي، المرجع السابق، ص189.

[4]- حسام محمد نبيل الشنراقي، المرجع السابق، ص249.

[5]- المرجع نفسه، ص 250.

التغيير ألتدليسي للحقيقة، وبذلك أصبح النص يتعامل مع حالات التزوير التقليدي للمحررات وكذا تزوير المحررات التقليدية والإلكترونية التي تكون مطبوعة على سند أو دعامة أو بأية وسيلة". [1]

ب- وسائل وطرق التزوير: من أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني "استخدام برامج حاسوبية أو أنظمة معلوماتية خاصة بذلك يتم تصميمها على غرار البرامج والنظم المشروعة أو محاولة بعض الأشخاص كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني والقيام بنسخها و اٍعادة استخدامها بعد ذلك". [2]

ولذلك فإن التوقيع الإلكتروني يتعرض للتزوير "ممن لديهم خبرة باستخدام الحاسب الآلي ومعرفة تقنية بالبرامج واستخدامها، إذ يستطيعون الدخول إلى منظومات التوقيع الإلكتروني باستخدام برامج خاصة والاحتيال على تلك النظم وفك شفرات التوقيع الإلكتروني ومن ثَم استخدامها في أغراض احتيالية عن طريق نسخها أو تزويرها ووضعها على محرر مزور". [3]

للإشارة فإن التزوير في المعلومات والتوقيعات الإلكترونية يمر بثلاثة مراحل أساسية وهي: [4]

مرحلة التلاعب بالبيانات والتوقيعات عند الإدخال في النظام ألمعلوماتي، إذ يقوم الجاني بالتلاعب في التوقيعات الإلكترونية التي يتم إدخالها للنظام دون المساس بالبرنامج، هذا الأخير الذي يؤدي عمله

- بشكل عادي مما يؤدي لإخراج بيانات مزورة وغير حقيقية ولا تطابق البيانات التي يجب حفظها داخل النظام المعلوماتي.

- مرحلة تزوير التوقيعات الإلكترونية والبيانات في مرحلة المعالجة الإلكترونية، إذ يترك الجاني البيانات والتوقيعات الإلكترونية كما هي دون تغيير، ويتدخل في البرنامج الخاص

---

[1]- أسامة بن غانم لعبيدي، المرجع السابق، ص 360.

[2]- صالح شنين، المرجع السابق، ص360.

[3]- حنان براهمي، المرجع السابق، ص248.

[4]- حسام محمد نبيل الشنراقي، المرجع السابق، ص ص269،270.

بالمعالجة الآلية لها سواءً بالتعديل في البرنامج نفسه أو بوضع برنامج آخر يحقق هدف الجاني.

- مرحلة التلاعب المعلوماتي في مخرجات النظام كالمحررات والتوقيعات الإلكترونية، حيث يقوم الجاني بالتغيير والتلاعب في المعلومات والتوقيعات رغم خروجها سليمة وصحيحة من نظام المعلومات.

وعليه "فالطرق المذكورة في التزوير ليست على سبيل الحصر في جريمة التزوير المعلوماتي (التوقيع الإلكتروني) لأن هذه التكنولوجيا متطورة وأشكالها متغيرة بشكل سريع، ولذلك لا يناسب الصيغة التشريعية في تجريم تزوير الوثيقة المعلوماتية أن تكون دالة على حصر طرق التزوير فيها".

03- الركن المعنوي:

لا تكتمل جريمة تزوير التوقيعات الإلكترونية أو الوثيقة المعلوماتية "إلا بتوافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وهذه الجريمة هي جريمة عمدية".

وصورة الركن المعنوي فيها هي القصد الجنائي بنوعيه، "القصد الجنائي العام والمتمثّل في علم الجاني أنه يغيّر الحقيقة، وأن هذا التغيير ينصب على محرر بإحدى الطرق المنصوص عليها قانونا، وأن من شأن فعله إحداث الضرر ،وعلمه بأن هذا الفعل هو فعل محظور ومعاقب عليه ومع ذلك يقبل القيام به، وتتجه إرادته إلى الفعل ويقبل النتائج المترتبة عليه، بمعنى أنه يجب أن تتجه إرادته إلى فعل تغيير الحقيقة والأثر المترتب عليه وهو أن يشتمل المحرر على البيانات المخالفة للحقيقة".[1]

هذا فضلا عن توافر القصد الجنائي الخاص، في جريمة تزوير التوقيع الإلكتروني، ؤالمتمثّل في اتجاه نية الجاني إلى تحقيق غاية معينة وهي استعمال التوقيع الإلكتروني فيما زّور من أجله".[2]

[1]- حنان براهمي، المرجع السابق، ص226.

[2]- المرجع نفسه، ص227.

رابعا : جريمة إتلاف و تعييب التوقيع الإلكتروني

01 – تعريف الإتلاف

أ – **الإتلاف التقليدي:** يعني الإتلاف تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كليا أو جزئيا. [1]

ب – الإتلاف الإلكتروني: يمكن تعريف الإتلاف الإلكتروني بأنه إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواءً استيلاء على أموال أو إطلاع على معلومات، ولكن إحداث الضرر بالنظام ألمعلوماتي وإعاقته عن أداء وظيفته.[2]

وعرف جانب من الفقه الإتلاف على أنه محو المعلومات أو البرامج كليةً أو تدميرها إلكترونيا أو أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال.

ويعرّف حسام محمد نبيل الشنراقي إتلاف التوقيع الإلكتروني بأنه استخدام أي من الوسائل التكنولوجية أو البرامج لإحداث تعديل أو محو أو تدمير لنظم معلومات التوقيع الإلكتروني أو أي من مكوناتها المنطقية للإضرار بالمؤسسة أو الشخص صاحب التوقيع الإلكتروني بقصد جعل النظام ألمعلوماتي غير صالح للاستخدام.[3]

02 – الركن المادي:

يتمثّل الركن المادي لهذه الجريمة في الأفعال المادية التي يتكون منها السلوك المجرّم، وهذه الأفعال تتمثّل في إتلاف أو تعييب التوقيع الإلكتروني ويتحقق فعل الإتلاف بإفقاد البرنامج ألمعلوماتي الخاص بالتوقيع الإلكتروني قدرته على العمل عن طريق نشر فيروس معلوماتي أو سكب سائل على الوسيط الإلكتروني المحفوظ عليه ،ويحدث تعييب التوقيع الإلكتروني كذلك بذات الوسيلة على نحو يفقده القدرة على العمل أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوها أو غير واضح.[4]

---

[1]– حنان براهمي، المرجع السابق ، ص 45.

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

[3]– المرجع نفسه، ص296.

[4]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2005، ص 542.

وقد يقع الإتلاف على المعلومات المنسوخة على شرائط أو دعامات، وقد يقع أيضا على المكّونات المادية والأجهزة المستخدمة في عمل التوقيع الإلكتروني مثل شاشات العرض والأشرطة والأسطوانات والكابلات والمفاتيح والأقراص الممغنطة، وغيرها من المكونات المادية سواءً كانت تحوي بيانات أو برامج أو مجرد أوعية فارغة، بشرط أن يؤدي الإتلاف أو التخريب إلى التقليل من قيمتها الاقتصادية أو يؤدي إلى تعطيلها أو عدم صلاحيتها للاستخدام.[1]

ويتطلب لقيام هذه الجريمة "ضرورة توافر الضرر، فالضرر هو النتيجة الإجرامية الناتجة عن الاعتداء وترتبط بالفعل برابطة سببية قانونية حال توافر أركان الجريمة، ويستوي أن يكون الضرر ضرار ماديا أو معنويا،[2]

ثالثا- الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصرْيه العلم والإرادة ،"يتمثل الأول في علم مرتكب الواقعة (الجاني) بأن فعل الإتلاف أو التعييب للتوقيع الإلكتروني محظور ومعاقب عليه قانونا، وأن تتجه إرادته للفعل المجرّم، أما إذا كان الإتلاف أو التعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه، فلا تقوم هذه الجريمة.[3]

مع الإشارة إلى أن "هذه الجريمة لا تتطلب قصدا جنائيا خاصا، و انما يكفي وجود القصد الجنائي العام بعنصريه الإرادة والعلم، فتقوم بذلك الجريمة بتوافر الركن المادي والقصد الجنائي العام.[4]

---

[1]- أسامة بن غانم لعبيدي، المرجع السابق، ص363.

[2]- صالح شنين، المرجع السابق، ص174.

[3]- المرجع نفسه، ص174.

[4]- المرجع نفسه، ص174.

المطلب الثاني: العقاب على الاعتداء على التوقيع الإلكتروني

نظرا لخطورة وخصوصية الجرائم الواقعة على التوقيع الالكتروني وما ينجر عنها من اعتداءات على البيانات الشخصية وكذا الخسائر المادية خاصة في مجال التجارة الالكترونية أصدرت أغلب التشريعات على المستوى الدولي والإقليمي الإطار القانوني لردع و حد هذه الاعتداءات ، حيث أصدر المشرع الجزائري عدة قوانين ومراسيم تمس هذه الجرائم سنتناولها في هذا المطلب الفرع الأول العقوبات المطبقة على الشخص الطبيعي أما الفرع الثاني العقوبات المطبقة على الشخص المعنوي.

الفرع الأول: العقوبات المطبقة على الشخص الطبيعي

لقد أورد المشرع الجزائري جملة من الجزاءات على الشخص الطبيعي والتي تختلف باختلاف الفعل المرتكب.

أولا: العقوبات الأصلية: إن الملاحظ من نصوص الخاصة بالجرائم الماسة بالأنظمة المعلوماتية والتي منها الجرائم الواقعة على التوقيع الالكتروني ، وجود تدرج داخل النظام العقابي، وهذا يؤكد الخطورة الإجرامية لهاته التصرفات، ويتجلى هذا التدرج الهرمي على حسب خطورة، الجزاء المقرر لجرائم الاعتداء على سير النظام سنتناول الجزاء المقرر لكل من جريمتي الدخول والبقاء غير المشروع سواء في صورها البسيطة أو المشددة.

01- بالنسبة لجريمة الدخول أو البقاء غير المشروع

نص المشرع الجزائري من خلال نص المادة 394 مكرر من ق. ع. ج على عقوبة هاته الجريمة سواء في صورتها البسيطة أو المشددة.

أ - في صورتها البسيطة: يعاقب المشرع الجزائري طبقا لنص المادة سالفة الذكر بالحبس من 3 أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج ، ونجد هنا أن المشرع الجزائري ترك للقاضي السلطة التقديرية بأن جعل له حد أدنى وحد أقصى في تقدير العقوبة بحسب الوقائع المعروضة أمامه، حيث يختلف الباعث من شخص لأخر، فليس باعث الفضول والاكتشاف كباعث الجوسسة والربح، وعلى هذا وجب اختلاف التقدير.[1]

[1]- حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، كلية الحقوق، جامعة أكلي محند أولحاج، العدد الثاني، 2016، ص 74.

ب – في صورتها المشددة: أن المشرع الجزائري في نص المادة 394 مكرر فقرة الثانية والثالثة ضاعف من عقوبة جريمة الدخول والبقاء غير المشروع إذا ترتب عن هذا الأخير إما حذف أو تغير المعطيات، سواء في حدها الأدنى الذي أصبح ستة أشهر بعدما كان ثلاثة أشهر، أو في حدها الأقصى إلى سنتين بعدما كانت سنة واحدة .

وبالنسبة للغرامة تكون من 50.000 دج إلى 150.000 دج.[1]

2- الجزاء المقرر لجرائم الاعتداء العمدي على المعطيات

سنتناول فيه العقوبات الأصلية إلى نص عليها المشرع الجزائري بالنسبة لجريمتي الاعتداء العمدي على المعطيات الموجودة داخل النظام ثم العقوبات الأصلية لجريمة التعامل غير المشروع في المعطيات.

أ- بالنسبة لجريمة الاعتداء العمدي على المعطيات: الموجودة داخل النظام نصت المادة 394 مكرر1 من على العقوبة الأصلية المرتكب جريمة الاعتداء العمدي على المعطيات بالحبس لمدة تمتد من 6 أشهر إلى ثلاث سنوات وغرامة من 500.000دج إلى 2.000.000 دج.

ب – بالنسبة لجريمة التعامل غير المشروع بالمعطيات: تكون العقوبة عن طريق تقرير عقوبتان أصليتان هما الحبس والغرامة.

ج – بالنسبة للعامل في معلومات صالحة لارتكاب الجريمة: نصت المادة 394 مكرر2 ف1 على أن التعامل في المعطيات ينطوي على العديد من الأفعال والأعمال والعمليات السابقة على استعمال المعلومات كبحثها وتجميعها، وصولا إلى توفيرها ونشرها أو الاتجار فيها حيث يعاقب المشرع على القيام العمدي أو عن طريق الغش بالأفعال السابقة الذكر بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج.[2]

د – بالنسبة لجريمة التعامل في معلومات متحصلة من الجريمة

أضاف المشرع الجزائري صورة ثانية من صور التعامل في معلومات غير المشروعة تتمثل في التعامل في معلومات متحصلة عن جريمة وذلك في حالة ارتكاب فعل من الأفعال

---

[1]- المادة 394 مكرر، ف2، ف3، الأمر66-156 المؤرخ في: 18صفر1386 الموافق 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات ، المعدل والمتمم بالأمر 20-01 المؤرخ في: 30 يوليو سنة 2020.

[2]- حمودي ناصر، المرجع السابق، ص75.

التي حصرتها الفقرة الثانية من المادة 394 مكرر2 ف2 [1]، هي الحيازة أو الإنشاء أو النشر أو الاستعمال والتي يعاقب عليها بنفس العقوبة المقررة في الصورة الأولى من جريمة التعامل غير المشروع في المعطيات.

هـ - بالنسبة لجريمة التزوير الالكتروني

فنجد أن القوانين الجنائية لم تفرض عقوبة الإعدام على مرتكبي هذا نوع من الجرائم ولكنها شملت في قوانينها عقوبات أخرى كالسجن والحب والغرامة وغيرها من العقوبات كما جاء في المواد: 214 ق ع، 215ق ع، و 216 ق ع، 217 ق ع، 218 ق ع، الخاصة بالتزوير التقليدي، وكذلك المواد 394 مكررا إلى مكررة الخاصة بالجرائم المعلوماتية وتعتبر الغرامة في جرائم التزوير المعلوماتي عقوبة مالية توقع على المجرم المعلوماتي قد تكون أصلية وقد تكون اختيارية لوجود عقوبة أخرى معها، فالقضاء هو الذي يحدد أما أن يحكم بها مع العقوبة الأصلية أو لا يحكم.

ثانيا: العقوبات التكميلية

إلى جانب العقوبات الأصلية المطبقة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، اقر المشرع عقوبات تكميلية التي تطبق على كافة صور المساس بأنظمة المعالجة الآلية للمعطيات وهي العقوبات المنصوص عليها بالمادة 394 مكررة على النحو التالي مع الاحتفاظ بحقوق الغير حسن النية بحكم مصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت يعلم مالكها ومن نص هذه المادة يمكن حصر العقوبات التكميلية في:[2]

1- المصادرة

كما عرفتها المادة 15 فقرتها الأولى من قانون العقوبات هي: الأيلولة النهائية إلى الدولة المال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء وتشمل المصادرة فيما يتعلق بهذه الجرائم أجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة مع مراعاة حقوق الغير حسن النية، ولا تكون المصادرة بالنسبة لهذه الجرائم عقوبة وجوبية.

---

1 – المادة 394 مكرر 2 ،ف 2 ، من الأمر 66-156 ، السابق الذكر.

[2]– غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر،2015، ص 221

2- إغلاق الموقع

يتعلق الأمر بالواقع التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

3- إغلاق المحل أو مكان الاستغلال

شرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي سمح من خلاله بالدخول عبر المصرح به لمختلف الأنظمة وسمح بالتلاعب بالمعطيات مثل مقاهي الانترنت وهنا وجب التأكد واثبات ركن العلم لدى الأخير اذ يمكن أن يكون غير مرتكب الجريمة وعليه لا تطبق عليه العقوبة التكميلية بعد إدانة الجاني وبالنسبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من ق ع ج، وعليه يمكن أن تكون مؤيدة أو مؤقتة .[2]

وفيما يخص العقوبات التكميلية الخاصة بالجريمة التزوير للمثل في حرمان مرتكب التزوير من تولي بعض الوظائف وغيرها من العقوبات المذكورة في المادة 394 مكرر ومكرر1 من الأمر66-156 المتضمن قانون العقوبات المعدل والمتمم، أما فيما يخص تطبيق عقوبة المصادرة على هذا النوع من الجرائم فتتم بالمصادرة الأجهزة التي استعملت في ارتكاب جريمة التزوير كجهاز الحاسب الآلي وغيره من المعدات المستعملة في الجريمة أو كانت معدة للاستعمال وذا ما ذكرته المادة 394 مكرر3.[3]

الفرع الثاني: العقوبات المطبقة على الشخص المعنوي

نص المشرع الجزائري على مسألة الشخص المعنوي وتطبيق عقوبات خاصة به تطبيقا التوصية الواردة بالمادة 12 والتي نصت على وجوب أن يسال الشخص المعنوي عن هذه الجرائم سواء بصفه فاعلا أصليا أو شريكا أو متدخلا، كما يسال عن الجريمة العامة أو الشروع فيها شرط أن تكون الجريمة في ارتكبت الحساب الشخص المعنوي وبواسطة أحد أعضائه أو ممثليها.[4]

---

[1]- غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر،2015، ص 222

[2]- المادة 394، مكرر 06، من الأمر رقم 66 -156 ، السابق الذكر.

3- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى ألمغاربي حول القانون والمعلوماتية المزعم عقده بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009،

4- المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي.

أولا: العقوبات الأصلية

أخذ المشرع الجزائري بمبدأ مسؤولية الشخص المعنوي عامة مستقلة عن مسؤولية الشخص الطبيعي بعد تعديل قانون العقوبات بموجب القانون 06-23 المؤرخ في 2006/12/20 في المادة 18 مكرر، والتي تنص فيها على العقوبات المطبقة على الشخص المعنوي فيما يخص الجنايات والجنح وهي كالآتي:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر المدة 5 سنوات.
- مصادره الشيء المستعمل في ارتكاب الجريمة.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

وبالنسبة للعقوبات المطبقة على الشخص المعنوي في حال ارتكابه أحد الجرائم الماسة أنظمة المعالجة الآلية للمعطيات فقد نصت عليها المادة 394 مكرر4 من ق ع ج على النحو الآتي :

- يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة لشخص الطبيعي.
- ويشترط تبعا لذلك التقرير مسؤولية الشخص المعنوي ثلاث شروط:
- يشترط في الشخص المعنوي أن يكون عاما أو خاصا باستثناء الدولة.
- يجب أن ترتكب الجريمة الصالح الشخص المعنوي.
- يجب أن ترتكب الجريمة من طرف حشو أو ممثل الشخص المعنوي دون أن تؤثر على مسؤولية الشخص الطبيعي بالإضافة إلى هاته العقوبات هناك عقوبات أخرى مقررة في حالة الاعتداء على الجهات العامة والتي نصت عليها المادة 394 مكرر3 من ق ع ج والتي

تنص تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق العقوبات أشد.[1]

ثانيا: العقوبات التكميلية

وهي نفس العقوبات التكميلية المطبقة على الشخص الطبيعي والمنصوص عليها بالمادة 394 مكرر التي جاءت شاملة والتي سبق أن تناولتها بالشرح بالمطلب الأول الخاص بالجزاءات المطبقة على الشخص الطبيعي، مع الاحتفاظ بحقوق الغير حسن النية بحكم بمصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة فقد ارتكبت بعلم مالك كما أنه لابد من الإشارة إلى عقوبة الشروع والاشتراك في الجريمة الالكترونية باعتبار أن المشرع يعاقب على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة في عقوبة الجريمة الأشد.[2]

وقد المادة 394 مكرر5 من قانون العقوبات نصت على شروط للعقاب على الاتفاق الجنائي وهي كالأتي:[3]

- مجموعة أو اتفاق.
- يهدف لتحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.
- القصد الجنائي.

فمن خلال استقراء المادة السابقة فان المشرع لم يخرج عن القواعد العامة لمعاقبة الشريك، حيث رصد لها نفس عقوبة الفاعل الأصلي، لك ان جرائم الاعتداء على نظم المعالجة الآلية المعطيات عليها لتم في شكل جماعات، وان كان لم يسبق اتفاق بينها على ارتكاب هذه الجريمة، ولكن نتيجة الجريمة من اتفاق ضمني بين أفراد المجموعة، إلا أن هذه

---

[1]– المادة 394، مكرر3، من الأمر 66–156، السابق الذكر.

[2]– امال قارة ، **الجريمة المعلوماتية**، مذكرة ماجستير، كلية الحقوق جامعة الجزائر،2001–2012، ص 131

3 – المادة 394 مكرر 5 ، من الامر 66–156 السابق الذكر.

الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص لآخر وان لم يكن هناك بينهما معرفة سابقة، كما يستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية.[1]

أما عن عقوبة الشروع فقد نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع في المادة 394 مكرر 7 من قانون العقوبات يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة لجنحة ذاتها[2].

مما سبق يمكن القول أن الجرائم الواقعة على التوقيع الالكتروني تتميز بخصوصية أنها صعبة الكشف عن التحايل والغش الذي وقع فيها ، حيث تستعمل فيها أساليب تقنية دقيقة مقارنة بتزوير التوقيع التقليدي وتتميز هذه الجرائم كذالك بتعدد صورها، وبذلك فالمشرع الجزائري أصدر قوانين صارمة في حق الشخص الطبيعي أو المعنوي لردعهم على ارتكاب الجرائم الماسة بالتوقيع الالكتروني ومختلف الجرائم الالكترونية .

1- خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010، ص 129

2- المادة 394، مكرر7، من الأمر 66-156، السابق الذكر.

خلاصة الفصل الأول

إن الثقة والأمان أساس كل التعاملات الالكترونية ، ومن أهم الركائز في المجال الالكتروني ،لهذا كان لابد بإحاطتها بنوع من الحماية لضمان هوية المتعاقدين ولتحديد حقيقة التعامل ومضمونه من جهة ، والمحافظة على حرمة الحياة الخاصة لهم من جهة ثانية ، وكذا تكريس سرية انتقال المعلومات من جهة أخرى ، فظهر التوقيع الالكتروني لمواكبة التطور الحاصل في المجال التكنولوجي خاصة في المعاملات التجارية والمصرفية وفي مجال الاتصالات.

فأصدرت كل التشريعات والتوجيهات الاسترشادية الأطر القانونية للتوقيع الالكتروني حيث حددت له شروطا يجب توافرها فيه لتحقيق الكفاءة وكسبه الحجية في الإثبات كما حددت له صوره، وكذا استحداث هيئات تعمل على حماية البيانات الشخصية للمتعاقدين وحقوقهم باعتبار أن العقود الالكترونية تكون في عالم افتراضي رقمي ، وهذه الهيئات هي جهات التصديق.

وباعتبار أن الجرائم الواقعة على التوقيع الالكتروني تتميز بخصائص أو خصوصية لأنها صعبة الكشف على مرتكبيها نظرا لاحترافيتهم في المجال الالكتروني باستعمالهم لأساليب تقنية دقيقة، ولردع مرتكبي هذه الجرائم تم وضع قوانين تطبق على الشخص الطبيعي أو المعنوي.

الفصل الثاني:

الحماية الجزائية الإجرائية

للتوقيع الالكتروني

تمهيد:

إن التطور الهائل الواقع في عالم تكنولوجيا المعلوماتية إلى تعاظم دورها في شتى المجالات خاصة في ميدان التجارة الالكترونية، وأصبح المواطن يعتمد عليها بشكل شبه كلي في تسيير شؤونه اليومية وتسيير مختلف المرافق الإدارية و الاقتصادية، ورغم الإيجابيات والفوائد الكثيرة لهذا التطور التكنولوجي فإن له سلبيات أبرزها الجرائم الالكترونية التي تعد من الجرائم الخطيرة التي يصعب اكتشافها ومكافحتها .

وتعد الجرائم الواقعة على التوقيع الالكتروني من الجرائم الإلكترونية، وفي ظل عدم مسايرة القوانين الوضعية للتطور الحاصل في عالم تكنولوجيا المعلومات وتقيد القاضي الجزائي بمبدأ الشرعية، فهو لا يستطيع أن يجرم أفعالا لم ينص عليها المشرع فعمدت أغلب التشريعات إلى إصدار قوانين جديدة تماشى مع التطور الحاصل

فالمشرع الجزائري حاول استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم والوقاية منها ومكافحتها بشكل فعال، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانون العقوبات والإجراءات الجزائية وتم تدعيمها بالقانون 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، تلاه المرسوم الرئاسي رقم: 15-261 المؤرخ في: 08أكتوبر 2015، يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وباعتبار أن الجرائم الواقعة على التوقيع الالكتروني من الجرائم الإلكترونية سنتطرق في هذا الفصل إلى الحماية الجزائية الإجرائية للتوقيع الالكتروني في مبحثين:

المبحث الأول: التحري و التحقيق في الجرائم الماسة بالتوقيع الالكتروني

المبحث الثاني: سلطة القاضي في قبول وتقدير الدليل الجنائي في الجرائم الماسة بالتوقيع الالكتروني

المبحث الأول: التحري و التحقيق في الجرائم الماسة بالتوقيع الالكتروني

تعد مرحلة التحقيق الأولي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم الماسة بالتوقيع الالكتروني و المتمثلة في جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني ، جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، و جريمة تزوير التوقيع الإلكتروني و جريمة إتلاف و تعييب التوقيع الإلكتروني التي تطرقنا إليهم في الفصل الأول ونظرا للطبيعة التقنية لهذه الجرائم والخصوصية التي تتمتع بها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى أن الجاني في الجرائم المعلوماتية لا يترك دليل مادي.
التقليدي وعليه سوف نحاول توضيح ما سبق من خلال هذا المبحث حيث سنتطرق فيه إلى من خلال مطلبين التحري والتحقيق في الجرائم الماسة بالتوقيع الالكتروني

المطلب الأول: أجهزة التحقيق المتخصصة في البحث والتحري.

المطلب الثاني: إجراءات المتابعة والتحقيق في الجرائم الماسة بالتوقيع الالكتروني.

المطلب الأول : أجهزة التحقيق المتخصصة في البحث والتحري

تدعيما لأحكام المادة 13 من القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، أصدر المشرع الجزائري المرسوم الرئاسي رقم: 15-261 المؤرخ في:08 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وكذا القانون رقم 14/04 المؤرخ في: 21 نوفمبر 2004 المتعلق بالأقطاب الجزائية المتخصصة التي تختص بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم، ولتوضيح ذلك سيتم دراسة هذا المطلب من خلال الفرعين التاليين:

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري.

الفرع الثاني : الهيئات القضائية الجزائية المتخصصة.

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري

الهيئات الفنية المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهام الوقاية ومكافحة الجرائم الإلكترونية والتي منها الجرائم الواقعة على التوقيع الالكتروني والتي تتميز بتشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية .

أولا :الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

وقد استحدثها المشرع الجزائري بموجب قانون رقم 04/09 المؤرخ في: 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015.[1]

ومن مهامها تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[2]

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، و مسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، تضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية، وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

---

[1]- المرسوم الرئاسي رقم 15-261 المؤرخ في 05 أوت 2009 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 53، في 2015/10/08.

[2]- فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017.

ثانيا :جهازي الأمن الوطني والدرك الوطني.

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام.[1]

أ -الوحدات التابعة لسلك الأمن الوطني: تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية و هي كالآتي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن.[2]

---

[1]- محمد السعيد زناتي، **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017 ، المركز الجامعي إليزي الجزائر، ص34 -35.

[2]- سعيدة بوزنون، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر، 2019، ص51.

ب -الوحدات التابعة للقيادة العامة للدرك الوطني: يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها:

- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.

يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء.[1]

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية حيث يوجد بهذا المركز قسم الإعلام الآلي ولإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.[2]

الفرع الثاني :الهيئات القضائية الجزائية المتخصصة

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 14-04 المؤرخ في 10 نوفمبر 2004،[3] وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،

---

[1]- يوسف جفال، **التحقيق في الجريمة الإلكترونية**، مذكرة شهادة الماستر الأكاديمي، جامعة محمد بوضياف، المسيلة، الجزائر، 2017/2016، ص 21.

[2]- سعيدة بوزنون، المرجع السابق، ص 54.

[3]- بموجب القانون رقم 14-04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155/66 المؤرخ في:18 صفر 1386 الموافق: 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية، عدد 71 بتاريخ 10 نوفمبر 2004.

بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم.[1]

ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية :دعم حقوق الإنسان وتسهيل حق اللجوء غلى القضاء وإعادة الاعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة، ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايد في العلميات الإرهابية وتزايدا في أعمال المنظمات الإجرامية واستعمالها القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف.[2]

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 10/05/ 2006 المعدل والمتمم بالمرسوم التنفيذي

---

[1]- بعرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة**، مذكرة ماستر في الحقوق، تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015-2016 ص 51.

[2]- كريمة علة، **الجهات القضائية الجزائية ذات الاختصاص الموسع**، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 11، 2015، ص 117.

رقم 267/16 المؤرخ في17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3-4-5 المعدلة للمواد3-4-5 من المرسوم السابق وجاء التقسيم كالتالي:

- محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية :الجزائر، الشلف، الأغواط، البليدة، تيزي وزوو، الجلفة، المدية، المسيلة، وبومرداس، البويرة، وعين الدفلى.[1]

- محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.

- محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، وغرداية.

- محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية :وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تيموشنت، وغليزان.

بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنوبا، شرقا، وغربا، وذلك لدى أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترونية.[2]

المطلب الثاني: إجراءات التحقيق والمتابعة في الجرائم الواقعة على التوقيع الالكتروني

تعتبر الجرائم الواقعة على التوقيع الالكتروني من الجرائم الإلكترونية، ونظرا للطبيعة التقنية لهذه الجرائم، التي تمتاز بصعوبة إثباتها وصعوبة إيجاد الدليل الذي يدين مرتكب الجريمة، حيث يسهل محو الأدلة والتلاعب فيها، لأنها لا تترك آثار خارجية مادية ملموسة (الركن المادي).

[1]- سعيدة بوزنون، المرجع السابق، ص 65.

[2]- المرجع نفسه، ص65.

في هذه المرحلة يجب على المحقق أن يتمتع بخبرة كافية ومهارات عالية في مجال الجرائم الواقعة على التوقيع الإلكتروني من خلال جمع الأدلة والتحقيق والتحري فيها ولتوضيح ذلك سيتم دراسة هذا المطلب من خلال الفروع التالية:

الفرع الأول: مرحلة جمع الأدلة.

الفرع الثاني: مرحلة التحقيق في الجرائم الواقعة على التوقيع الالكتروني.

الفرع الثالث: الاختصاص المحلي والنوعي في الجرائم الواقعة على التوقيع الالكتروني

الفرع الأول: مرحلة جمع الأدلة

يجب على المحقق في حالة وقوع أي جريمة الكترونية أن يستظهر أركانها الثلاثة الشرعي، المادي والمعنوي للجريمة محل التحقيق.

أولا: إظهار الركن المادي يتطلب النشاط أو السلوك الإجرامي في جرائم الانترنت وجود بنية رقمية واتصال بالانترنت أيضا معرفة بداية هذا النشاط والشروع في نتيجته.

ثانيا: إظهار الركن المعنوي للجريمة الالكترونية: يتمثل في الحالة النفسية التي يكون عليها الجاني التي دفعت به إلى ارتكاب الجريمة والعلاقة التي تربط بين الشخص الجاني والفعل المرتكب أو المكون للجريمة ويتمثل أساسا في العلم والإرادة المعروف بإسم القصد الجنائي العام.[1]

من أهم السيمات التي يجب أن تتوفر في المحقق يمكننا أن نذكر دقة الملاحظة في تتبع المتهمين والشهود أثناء التعامل معهم، سرعة الأداء، كتمان السر حتى لا يضر بمصالح الغير، الترتيب والدقة والتأني وبذل العناية، الصبر، قوة الذاكرة.[2]

حسب المادة 04 من المرسوم الرئاسي رقم: (15-261)[3] المؤرخ في 08-10-2015 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه من مهام الهيئة مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها.

---

[1]- خالد ممدوح إبراهيم، **التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي، مصر، 2008، ص59.

[2]- مروك نصر الدين، **محاضرات في الإثبات الجنائي**، دار هومة، الجزائر، 2011، ص 81.

[3]- المادة 04 من المرسوم الرئاسي رقم 261/15، مرجع سابق.

أولا : تلقي البلاغات في الجريمة الإلكترونية.

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوي التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند ورودها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل :إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص المكاني أو النوعي بها، في حين أن الواجب اتخاذ الإجراءات المقرة بشأنها، تم إخطار جهة الاختصاص وإحالة المحضر إليها.

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى إجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.[1]

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجوه صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية.

ثانيا: الاستجواب وسماع الشهود في الجريمة الإلكترونية.

1- الاستجواب: وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وان لم يقدر يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق بذلك.[2]

2- سماع الشهود في الجريمة الإلكترونية.

سماع الشهود هو إجراء من إجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن

[1]- خالد عباد الحلي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة، الأردن،2011 ،ص 79.

[2]- المرجع نفسه، ص 80.

الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية.[1]

الفرع الثاني: مرحلة التحقيق في الجرائم الواقعة على التوقيع الإلكتروني

عند تلقي مصالح الضبطية القضائية بلاغ أو شكوى تفيد بوقوع جريمة إلكترونية يبلغ المحقق بذلك والذي بدوره يخطر وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها إلا انه تجدر الإشارة الى أن مسرح الجريمة الالكتروني بالإضافة الى المسرح المادي يوجد مسرح الكتروني متمثل في البيئة الالكترونية التي يجد فيها المحقق صعوبة استخلاص الدليل منها مما يدفعه بالاستعانة بالخبراء الفنيين في هذا المجال.

أولا: التفتيش وضبط الأدلة

1- التفتيش: تتميز الجريمة الإلكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها وتتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم العادة الأخرى، نظرا لسرعة ارتكابها ومحو آثارها وخطيها الحدود الوطنية.

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ماله علاقة بها أو بفعالها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه يتكون من شقين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص.[2]

وحسب المادة 04 من القانون رقم 09-04[3] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أجاز المشرع للسلطات القضائية المختصة كذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد في الحالتين التاليتين:

- تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

---

[1]- خالد عباد الحلي، المرجع السابق، ص81 .

[2]- بكري يوسف بكري، **التفتيش عن المعلومات في وسائل التقنية الحديثة**، دار الفكر الجامعي، مصر،2012 ، ص74.

[3]- المادة 04 من القانون رقم 09- 04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تفتيش منظومة تخزين المعلوماتية.

بالنسبة للحالة الأولى فإذا كانت هناك أسباب تدعو الى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الدخول إليها انطلاقا من المنظومة الأولى، فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام الجهة القضائية المختصة بذلك.

أما إذا تبين مسبقا بأن المعطيات المبحوث عنها يمكن الدخول إليها انطلاقا من المنظومة الأولى، هي مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فيمكن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات دولية ذات صلة.

ونص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية بإمكانية التفتيش والضبط على المكونات ا لمعنوية للحاسوب بنصه على انه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق ان يقوم باي عملية تفتيش أو الحجز ليلا او نهارا وفي أي مكان على امتداد التراب الوطني أو بأمر ضباط الشرطة القضائية للقيام بذلك "[1]

2– ضبط الأدلة: هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط في اغلب الأحيان هو غرض التفتيش وان لم يكن له السبب الوحيد، فقد يتم الضبط استنادا لأسباب أخرى غير التفتيش من ذلك المعاينة وما يقدم المتهم والشهود لمأموري الضبط القضائي، لذا يرى جانب من الفقه أن الضبط ليس من اجراءات التحري بل من إجراءات الاستدلال خاصة إذا تم في مكان يجوز لسلطات الضبط دخوله مثل الأشياء التي يتم العثور عليها خارج المساكن أو في الطريق العام أو في الحقول أو غيرها.

والضبط لا يخرج من كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقارا أو منقولا الضبط حسب الأصل لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات، المادية للكومبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير مشروع أو إتلافه بوسائل تقليدية كالكسر، الحرق، لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف

[1]-- المادة 47 ف3 من الأمر رقم 66-155 ، السابق الذكر.

البرامج مثل الفيروس وفي ضبط البيانات الكمبيوتر لعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثواني معدودات ولعدم معرفة كلمة السر أو ثغرات المرور أو ترميز البيانات. [1]

بالرجوع إلى أحكام المادة 06 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بنصها:" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ومرتكبيها أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع وفقا للقواعد المقررة في قانون الإجراءات الجزائية"[2]

ثانيا: المعاينة وندب الخبراء في الجريمة الالكترونية

1- المعاينة: المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يري المحقق أن لها صلة بالجريمة، والأصل أن إجراء المعاينة متروك لتقدير المحقق، لا يقوم بها إلا إذا كمان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية ملتبس بها، يجب على القائمين بالمعاينة تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة وأخطاره مسبقا حتى يستعد من ناحية الفنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية.[3]

ويمكن الاستعانة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من طرف السلطات القضائية المختصة في المعاينة أثناء وقوع الجرائم المتصلة

---

[1]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير المعلوماتي**، دار الكتب القانونية المجلة الكبرى، ط1، ص 238.

[2]- المادة 06 من القانون رقم 09-04، السابق الذكر.

[3]- عبد الفتاح بومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، مصر، ط1، د س، ص 237

بتكنولوجيا الإعلام والاتصال ومنها الجرائم الواقعة على التوقيع الالكتروني وذلك حسب المادة 04 من المرسوم الرئاسي 15-261.[1]

2- ندب الخبراء:

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.[2]

حسب المادة 04 والمادة 12 من المرسوم الرئاسي 15-261[3] تقوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بمساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك الجرائم الواقعة على التوقيع الالكتروني بتزويدهم بالخبراء والخبرات القضائية.

الفرع الثالث: الاختصاص المحلي والنوعي في الجرائم الواقعة على التوقيع الالكتروني

يتصل القاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب الافتتاحي لإجراء تحقيق، وإما عن طريق شكوى جزائية مقدم من المضرور وهذا ما أكدته المادة: 38 فقرة 03 من قانون الإجراءات الجزائية الجزائري على "... يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73.

ويتقيد قاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 03/67 و04 من قانون الإجراءات الجزائية ... "ولقاضي التحقيق سلطة الاتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه، فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع.[4]

---

[1]- المادة 04 من المرسوم الرئاسي رقم 15-261، مرجع سابق.

[2]- ضريفي نادية، **سلطات القاضي الجاني في تقدير الدليل الإلكتروني**، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04 ، العدد02 ،219، ص 124

[3]- المادة 04 و12 من المرسوم الرئاسي رقم 15-261، المرجع نفسه.

[4]- بعرة سعيدة، المرجع السابق،ص 92

يختص القضاء الوطني في الفصل في الدعاوى الجزائية في الجرائم الإلكترونية ومنها الجرائم الواقعة على التوقيع الالكتروني وذلك حسب الإجراءات المعمول بها في الجرائم الأحرى

1- الاختصاص المحلي في الجريمة الإلكترونية

طبقا نص المادة 37 من قانون الإجراءات يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط في أو المكان إقامة المتهم أو مكان الضبط، كما نصت أحكام المرسوم التنفيذي رقم 348 06 المؤرخ في 5 أكتوبر 2006على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة اختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي أمحمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران وفي نطاق الجرائم الإلكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان أخر، فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، وتعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الأنترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها ومتى كانت الجريمة الإلكترونية، أيا كان نوعها، فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام و الاتصال إذا ارتكبت خارج الإقليم الوطني، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.[1]

و الجرائم الواقعة على التوقيع الالكتروني هي من الجرائم الالكترونية وذلك حسب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

2- الاختصاص النوعي في الجريمة الإلكترونية.

يتحدد الاختصاص النوعي للمحكمة الفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم

[1]- بعرة سعيدة، المرجع السابق، ص 93.

[2] - القانون 09-04 ، السابق الذكر.

الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 قانون الإجراءات الجزائية.

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبيض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذا جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى وهذا ما نصت عليه المواد37 ،40 والمادة 329 من قانون الإجراءات الجزائية أثر التعديل الذي جاء به القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة، قسنطينة، وهران، ورقلة.[1]

ومما سبق نستنتج أن المشرع الجزائري اصدر عدة قوانين ومراسيم تتعلق بالجرائم الالكترونية والتي تنطوي تحتها الجرائم الماسة بالتوقيع الالكتروني هذه القوانين تتعلق بمرحلة التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الالكترونية وكذا الاختصاص المحلي والنوعي لها.

[1]- بعرة سعيدة ، المرجع السابق، ص 93.

المبحث الثاني: سلطة القاضي في قبول وتقدير الدليل الجنائي

لما كان عبء الإثبات في المادة الجزائية واقعا على سلطة الاتهام، فقد كان دور هذه الأخيرة في الإثبات الجزائي ذو أهمية بالغة في تقصي المسؤولية الجزائية، وإثباتها غير أن ذلك لا ينفي دور القاضي الجزائي – جهات التحقيق والحكم – في البحث عن الأدلة الملائمة، وتقدير قيمتها في إثبات المسؤولية الجزائية، فالتزام القاضي الجزائي بإدراك الحقيقة الواقعية والمادية، استجابة لمقتضيات التجريم القائم على الحق والشرعية قد فرض عليه دورا إيجابيا، في البحث عن الأدلة التي يدرك بمقتضاها تلك الحقيقة من جهة، ومنحه بذلك سلطة واسعة محاطة بضمانات العدالة الجزائية، في مجال تقييم هذه الأدلة وتقدير قيمتها في إثبات عدم مشروعية الأنشطة المعلوماتية المرتكبة، ويتجلى كل ذلك من خلال السلطة التي يتمتع بها القاضي الجزائي في قبول الأدلة المقدمة لإثبات المسؤولية الجزائية محل البحث، واستناده لأسس قانونية، وقضائية متعارف عليها في الحدود القانونية المرسومة لذلك، وكذا ما يتمتع به من سلطة في تقدير قيمة الأدلة المقدمة إليه في شأن إثبات المسؤولية الجزائية، بأن منحه القانون حق إخضاعه لقناعته الوجدانية، تبعا للأطر والضوابط القانونية المقررة لهذا الاقتناع، لذلك سنتناول في هذا المبحث (المطلب الأول) سلطة القاضي الجزائي في قبول الأدلة الإلكترونية و (المطلب الثاني) سلطة القاضي الجزائي في تقدير الأدلة الإلكترونية.

المطلب الأول: سلطة القاضي الجزائي في قبول الأدلة الإلكترونية

تعد مرحلة قبول الأدلة الإلكترونية والاعتداد بها في إثبات عدم مشروعية الأنشطة المعلوماتية الخطوة الإجرائية الأولى، التي يمارسها القاضي الجزائي تجاه هذه الأدلة، وصولا لتقدير قيمتها في الإثبات، ويقصد بهذه المرحلة ذلك النشاط الإجرائية التي يمارسه القاضي الجزائي على الأدلة المقدمة من سلطة الاتهام، لبحث مدى صحتها وصولا لمناقشة مدى مشروعيتها، على أن يتم قبول هذه الأدلة على أسس علمية، تحقيقا لغايات العدالة المرجوة من المتابعة الجزائية وأن يمارس القاضي سلطته هذه في حدود المشروعية التي يرسمها القانون.

الفرع الأول: أساس سلطة القاضي الجزائي في قبول الأدلة الإلكترونية

يتحدد الأساس الذي تقوم عليه سلطة القاضي الجزائي في قبول الأدلة الإلكترونية على نظام الإثبات السائد في الدولة. ولا كان التشريع الجزائري ينتمي إلى العائلة ذات الأصل اللاتيني، التي لم تضع- أصل عام- نصوصا قانونية تمنع أو تقيد الأخذ بهذه الأدلة، فهو يستند إلى نظام الإثبات الحر، الذي يعد الأساس التي تقوم عليه سلطة القاضي الجزائي في قبول أدلة الإثبات.[1]

أولا: مفهوم مبدأ الإثبات الحر

يعد مبدأ حرية الإثبات من المبادئ الثابتة، و المستقر عليها في نظرية الإثبات الجزائي، وهو ما يميزها عن نظيرتها في القانون المدني؛ فهذا الأخير يحدد سلفا الطرق والوسائل واجبة الإتباع في شأن إثبات الوقائع محل النظر أمام القضاء المدني.

1- تعرف مبدأ حرية الإثبات ومبرراته: يعني مبدأ حرية الإثبات تمتع كل أطراف الخصومة الجنائية بحق تقديم كل الأدلة المتاحة لتأكيد الادعاء أو في مزاعم باقي الأطراف، كلما توفرت في هذه الأدلة شروطها القانونية،[2] ويرتكز هذا المبدأ على الحرية الممنوحة للقاضي الجزائي في تكوين اعتقاده من أي دليل يطرح أمامه، والاعتراف له بسلطة تقدير قيمة كل دليل و قوته الثبوتية،[3] فهذا النظام يمنح القاضي الجزائي دورا فعالا حيال الدليل المقدم إليه، كما منحه كامل الحرية في الاستعانة بكافة طرق الإثبات تقصيا للحقيقة.[4]

وجد هذا النظام مبرراته في ورود الإثبات على وقائع قانونية ماضية، يصعب الحصول على دليل سابق عليها، كما يعد مبدأ حرية الإثبات نتيجة منطقية لتقرير المبدأ ، والذي يسمح في الوقت نفسه السماح للقاضي بالاستعانة جميع وسائل الإثبات التي يتمتع بها، ويطمئن إليها، هذا ويعد نظام الإثبات الحر بمثابة إقرار ضمني بعدم قدرة الأدلة

---

[1]- رشيدة بوكر، **الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد السابع والعشرون، العدد 02، 2011، ص 314

[2]- اغليس بوزيد، **تلازم مادة الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي**، دار الهدى، د.ط، عين مليلة، الجزائر، 2010، ص 92.

[3]- سامي جلال، حسين فقي، **الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، دراسة مقارنة، دار الكتب القانونية، د.ط، مصر، 2001، ص 69.

[4]- ماروك نصر الدين، المرجع السابق، ص62.

التقليدية فيما لو تم حصرها عن مواجهة الجرائم المستحدثة، ومنها الجرائم المرتبطة بالتوقيع الالكتروني.[1]

2- موقف المشرع الجزائري من نظام الإثبات الحر: لما كان نظام الحر يضمن للقاضي الجزائي سلطة تقديرية مع استقلالية في تكوين قناعته، بأن خول له تقدير قيمة كل دليل يصل إليه أو يطرح عليه أثناء نظر الدعوى، والتنسيق بين الأدلة لاستخلاص منطقية الحكم بالإدانة أو بالبراءة،[2] فقد كان هذا النظام منسجم مع السياسة الإجرائية الجزائية الحديثة مما دفع المشرع الجزائري إلى اعتناقه وتبقيه – كأساس عام للإثبات – حيث أقر القانون الجزائي الإجرائي الجزائري هذا المبدأ كأصل عام، من خلال خصوص عدة؛، ومنها نص في المادة 212 من قانون الإجراءات الجزائية التي قضت: " بجواز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".[3]

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات، والتي حصلت المناقشة فيها حضوريا أمامه " وما قضت به المادة 213 من ذات القانون يقولها:" الاعتراف شأنه شأن جميع عناصر الإثبات، يترك لحرية تقدير القاضي،" فرية الإثبات أضحت مبدأ مسلما به قانونيا، بعدما أظهره الفقه والقضاء من جماد في شأن تكريس هذا المبدأ، وإرساء معالمه النظرية.[4]

ثانيا: النتائج المترتبة عن تبني مبدأ الإثبات الحر

يترتب عن إقرار نظام الإثبات الحر في شان نظر المسؤولية الجزائية لمتعهدي الإيواء المعلوماتي نتائج عدة؛ تتجلى في منح القاضي الجزائي سلطة ايجابية، في شأن توفير الأدلة اللازمة لإثبات هذه المسؤولية، وكذا تمكينه من دور إيجابي حيال تقدير القيمة القانونية لهذه الأدلة.

---

[1]- اشرف عبد القادر قنديل، **الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة**، د.ط، الإسكندرية، مصر، 2015، ص 197.

[2]- الهام صالح بن خليفة، **دور البصمات والآثار المادية الأخرى في الإثبات الجنائي**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، المملكة الأردنية الهاشمية، 2014، ص 28

[3]- المادة 212 الأمر رقم 66-155 ، السابق الذكر.

[4]- المادة 212 الأمر رقم 66-155 ، السابق الذكر.

1- الدور الإيجابي للقاضي الجزائي في توفير الأدلة الإلكترونية: يراد بالدور الإيجابي للقاضي الجزائي في توفير ما يثبت مسؤولية متعهدي الإيواء المعلوماتي عدم التزامه بما يقدمه أطراف الدعوى الجزائية من أدلة، وإنما يتوجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات التي من شأنها تحقيق الدعوى، وإثباتها، والكشف عن الحقيقة الفعلية للمسؤولية محل النظر عموما، والتنقيب عن الأدلة التي من شأنها أن تكون عقيدته بشأن مسؤولية متعهدي الإيواء المعلوماتي على الوجه الصحيح، خصوصا وأنه يسعى إلى اكتشاف الحقيقة، ودور القاضي الجزائي – تبعا لهذا الوصف - مختلف عن دور القاضي المدني، إذ يقوم عمل هذا الأخير على مجرد قبول الأدلة المقدمة من الخصوم في الدعوى، من غير أن يبادر من تلقاء نفسه إلى البحث عن أي دليل أو تقديمه، أو إلى توجيه أحد الأطراف إلى تقديم دليل بعينه، خلاف القاضي الجزائي التي لا يتخذ هذا الدور السلبي، فمن حقه بل من واجبه أن يتحرى ويبحث عن الحقيقة بجميع الوسائل مالم ينص القانون على خلاف ذلك.[1]

2- الدور الايجابي للقاضي الجزائي في قبول الأدلة الإلكترونية: لما كان نظام الإثبات الحر يقوم في مضمونه على أن القوة الدامغة لكل دليل – مقدم لإثبات الوقائع محل النظر – ليست مفروضة مقدما، ولكن حجيتها تتكشف، وترتبط باقتناع القاضي الجزائي فليسلم القاضي الجزائي بمشروعية وقائع الإيواء المعلوماتي من عدمها، لابد من أن يقتنع بانطباق أحد الأوصاف المجرمة على هذه الوقائع أو انتفائها، فليست هناك أدلة بناتها يكون وجودها كافيا، أو لازما لاقتناع القاضي، وتخلفها يرتب حتما عدم اقتناع القاضي الجزائي في شأن مساءلة متعهدي الإيواء المعلوماتي، فكل الأدلة في ذلك سواء. وتعد مرحلة قبول الأدلة الإلكترونية في مجال مساءلة متعهدي إيواء المواقع الإلكترونية جزائيا الخطوة أو المرحلة الثانية – بعد البحث عن هذا الدليل وتقديمه – لأجل الوصول إلى حالتي اليقين والاقتناع المطلوبين لدى القاضي الجزائي، كأساس الإصدار حكمه إدانة متعهدي الإيواء المعلوماتي،

[1]- عائشة بن قارة مصطفى، **حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامعة الجديدة، ط1، الإسكندرية، مصر، 2010، ص190.

أو لتأكد براعتهم محترما بذلك القواعد الموضوعية والإجرائية المقررة الصحة الأدلة الإلكتروني، وسائل الإثبات في المواد الجزائية.[1]

الفرع الثاني: القيود الواردة على سلطة القاضي الجزائي في قبول الأدلة الإلكترونية

برغم ما تمتع به مبدأ حرية القاضي الجزائي في قبول الأدلة الإلكترونية، كوسيلة لإثبات مسؤولية متعهدي الإيواء عن جرائم التخزين والاستضافة من عمومية، إلا أنه ليس مطلقا بل ترد عليه مجموعة من القيود، منها ما يتعلق بطبيعة هذه الوسيلة في ذاتها، فيما يتصل بمشروعيتها، ومنها الحالات أو المسائل التي تخرج في الأصل عن اختصاص القاضي الجزائي لاقترانها مسائل مدنية.

أولا: قيد المشروعية في الإثبات الجزائي

إذا كان صحيحا أن الإثبات الجزائي قد عرف تطورا متسارعا، فلم تعد فكرة الدليل القانوني على النحو الذي صارت معه كل وسائل الإثبات جائزة أمام القضاء الجزائي، إلا أن ذلك لا يعني بمقبولية كل الأدلة أمام هذا القضاء، بل يلزم لذلك أن يكون مشروعا مطابقا للقانون. [2]

1- مفهوم مشروعية الأدلة الإلكترونية: يقصد بقاعدة المشروعية في مجال إثبات المسؤولية الجزائية المتعدي الإيواء المعلوماتي وجوب أن يستمد القاضي الجزائي اقتناعه بإدانة هؤلاء المتعهدين عن عدم مشروعية الخدمات التي يقدمونها، من أدلة صحيحة ومشروعة؛ بمعنى عدم قبول أية أدلة إلكترونية لإدانة متعهدي الإيواء المعلوماتي يكون البحث عنها أو الوصول إليها قد تم بطرق غير مشروعة.[3] المبدأ حرية القاضي الجزائي في إثبات مسؤولية متعهدي الإيواء لا يعني أن يجري البحث عن الأدلة أو الحصول عليها في طريق كانت، بل أن هذا البحث مفيد واحترام حقوق الدفاع من جهة، وقيم العدالة وأخلاقياتها من جهة ثانية، ومقتضيات الحفاظ على الكرامة الإنسانية من جهة أخيرة. هنا ويستلزم مبدأ مشروعية الأدلة الإلكترونية عدم قبول أي دليل لإدانة متعهدي الإيواء وتقرير مسؤوليتهم

---

[1]- عائشة بن قارة مصطفى، المرجع السابق، ص 195.

[2]- محمد زكى ابو عامر، **الإثبات في المواد الجنائية، محاولة فقهية وعملية لإرساء نظرية عامة**، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2011، ص 119.

[3]- ماروك نصر الدين، المرجع السابق، ص 519.

الجزائية عن الإخلال بمشروعية خدمات التخزين والاستضافة، يكون حمله إلى القضاء وإقامته أمامه قد جاء بالمخالفة للقانون، أو حقوق الدفاع.[1]

2- نتائج تقرير قيد مشروعية الأدلة الإلكترونية: يترتب عن تبني القيد المذكور قاعدة كية تتضمن القول باستبعاد كل دليل مقدم لإثبات مسؤولية متعهدي الإيواء المعلوماتي، كون تحصيله، أو تقديمه قد ثم بالمخالفة للقانون. وإذا كانت هذه القاعدة لا تثير إشكالية من ناحية تبنيها فإنها تثير خلافا في حدود إعمالها الأخذ بها، وفي هذه الأخيرة درج الفقه والأنظمة القانونية على اتجاهات عدة من حيث معالجة قيمة الأدلة الإلكترونية غير المشروعة، ولكنهم استقروا في نهاية المطاف ضمن رأيين؛ يقول الأول منها باستبعاد هذه الأدلة بصورة نهائية، بغض النظر عن مضمون هذه الأخيرة ومؤداها فالأدلة غير المشروعة مستبعدة من ملف الدعوى سواء كان أدلة إدانة أو أدلة براءة، وميزهم في ذلك عدم صحة فكرة الغاية تبرر الوسيلة من جهة ومن جهة أخرى قد يتضمن الدليل الواحد إدانة وبراعة في الوقت ذاته بعد أن ذهبت الطائفة الأخرى إلى القول بالاستناد إلى الأدلة الإلكترونية غير المشروعة، متى تضمنت إثبات للبراءة مبررة توجعها هناء بالقول بأن البراءة أصل في الإنسان، ولا حاجة للمحكمة في أن تثبتها، فكل ما تحتاج إليه المحكمة هو التشكيك في الإدانة، مع ظهور اتجاه يحاول التوسط بين سابقيه بمحاولة التمييز بين الإخلال بقاعدة المشروعية، التي يشكل جريمة، وبين ذلك الذي يقع مجرد مخالفة للإجراءات، فيهدر قيمة الأدلة الإلكترونية في الحالة الأولى دون الثانية. [2]

ثانيا: قيد إثبات المسائل غير الجزائية

تعير المسائل غير الجزائية عن الوجه الثاني لتضييق سلطة القاضي الجزائي في الاستناد إلى أدلة الإثبات الإلكترونية – إلى جانب قيد مشروعية هذه الأدلة – وذلك تبعا للطبيعة الخاصة، والطابع المميز لهذه المسائل، والتي تتحلى بها حال توفر الشروط اللازمة لإكسابها هذا الوصف.

1- مفهوم المسائل غير الجزائية: ضد هذه المسائل تلك الحالات التي تعترض سير الدعوى العمومية، ويتوقف عليها الحكم فيها، ولكن ليس للمحكمة أن تفصل فيها، لأنها لا

[1]- محمد زكي ابو عامر، المرجع السابق، ص 120.

[2]- ماروك نصر الدين، المرجع السابق، ص 524

تدخل في اختصاصها؛ فهي تعبير عن تلك القضايا التي تثار أمام المحكمة الجزائية أثناء نظر الدعوى العمومية، والتي تخرج – بحسب الأصل – عن اختصاصها، ويكون الفصل في الدعوى متوقفا على الفصل فيها، لأنها تدخل على نحو ما في البنيان القانوني للجرعة موضوع الدعوى الجزائية. ويقوم هذا القيد على خصائص ثلاثة، الأولى: أن إثارة هذه المسائل غير الجزائية يكون أثناء نظر الدعوى الجزائية، لمفهوم المسائل غير الجزائية لا يتحقق منى لم تثر هذه المسائل بعد تحريك الدعوى الجزائية؛ وذلك إما في مرحلة التحقيق أو مرحلة المحاكمة، من قبل أحد أطراف الدعوى الجزائية، وعلى شكل دفوع، أو أن المحكمة الجزائية تثيرها من تلقاء نفسها، والثانية: أن هذه المسائل غير الجزائية لا تدخل في الأصل ضمن اختصاص المحكمة الجزائية.[1]

إذ لا يتحقق مفهوما بمجرد إثارتها أثناء نظر الدعوى الجزائية فحسب، بل لابد أن تكون هذه المسائل خارجة عن اختصاص القاضي الجزائي وفق القواعد العامة في الاختصاص، أما الثالثة: فيجب أن يكون الفصل في المسائل العارضة، مما يتوقف عليها حقيقة الفصل في الدعوى الجزائية.[2]

2- شروط المسائل غير الجزائية: لما كان التزام القاضي الجزائي بوسائل الإثبات المدنية في بعض المسائل التي تعرض عليه مجرد فبد يرد على حريته في الإثبات. كان لابد من توافر شروط لصحة هنا القيد؛ منها ألا تكون الواقعة المراد إثباتها مدنيا في بناتها واقعة التجريم بمعنى أن تكون الواقعة المقترنة بالقوانين غير الجزائية ، وليست هي المكون السلوك الإجرائي ذاته؛ ومنها أن تكون الوقائع المتعلقة بالقوانين غير الجزائية لازمة للبت في الدعوى العمومية، ففصل القاضي الجزائي في هذه المسائل لا يصح، متى لم يكن هذا الفصل لازما للبت في الدعوى العمومية. والفصل في الوقائع محل النظر بأن تكون الوقائع غير الجزائية عنصرا من عناصر المسؤولية المراد إثباتها، والفصل فيها، أو مقوما من مقومات الجرعة المنشئة لهذه المسؤولية.[3]

---

[1]- عادل بوزيدة، **المسؤولية الجزائية لمتعهدي إيواء المواقع الالكترونية**، أطروحة دكتوراه، جامعة تبسة،2017/2016، ص191.

[2]- عادل بوزيدة، المرجع السابق، ص191.

[3]- المرجع نفسه، ص 192.

المطلب الثاني :سلطة القاضي في تقدير الأدلة الرقمية

تعتبر مسألة تقدير القاضي الجنائي للدليل الإلكتروني خاصة في الجرائم الواقعة على التوقيع الالكتروني من المسائل المهمة في مجال الإثبات على اعتبار أن أهم المشاكل التي تطرح في إثبات الجرائم الواقعة عبر التعامل الإلكتروني هو ما يقع على القاضي في تقدير الأدلة الإلكترونية ومدى الاقتناع بها، نظرا لأن السلطة التقديرية للقاضي لهذا النوع من الأدلة يثير إشكالا كبيرا نظرا لتصنيفها كنوع من أنواع الأدلة العلمية التي تعتمد على وسائل تقنية من أجل الوصول إلى الحقيقة، أضف إلى ذلك ضرورة توافر شروط معينة في الأدلة الإلكترونية مع بلوغ القاضي إلى درجة الاقتناع اليقيني بهذه الأخيرة، وهو ما استوجب بيانه في النقاط التالية:

الفرع الأول :حرية القاضي الجنائي في تقدير الدليل الإلكتروني

يعتبر تنامي دور الإثبات العلمي مع بروز الدليل الإلكتروني المستحدث في إطار الجرائم الواقعة عبر التعامل الإلكتروني هو عامل هام في مجال الإثبات الجنائي، يستدعي ضرورة تعامل القاضي معه بشكل مخالف عن الأدلة التقليدية، وخاصة مع نقص الثقافة المعلوماتية وتعقد طبيعة الأدلة الإلكترونية وسبل استخدامها في مجال الإجرام الإلكتروني.

وإن كانت العملية القضائية التي يجريها القاضي الجنائي هدفها النهائي هو التوصل إلى الحقيقة الواقعية أي الوقوف على الحقائق كما حدثت، ففي حالة توصل القاضي إلى حالة ذهنية استجمع فيها كافة عناصر الحقيقة وارتاح إليها ضميره، فهنا يمكن القول أن القاضي قد وصل إلى حالة الاقتناع القضائي. ففيما تتمثل ماهية الاقتناع القضائي بالدليل الجنائي الإلكتروني، وما تأثير طبيعة الدليل الإلكتروني على اقتناع القاضي الجنائي؟

أولا: مفهوم مبدأ الاقتناع القضائي

عرف بعض الفقه الاقتناع القضائي بأنه حالة ذهنية وجدانية يصل إليها القاضي الجنائي وهي عبارة عن محصلة منطقية يستنتجها من وقائع القضية، فأهم مبادئ الإثبات الجنائي مبدأ الاقتناع القضائي والذي يجعل القاضي يقبل جميع الأدلة التي يقدمها إليه أطراف الدعوى مادامت تعدت مرحلة القبول، أي امتثالها للشروط المحددة مسبقاً في التشريع، ولها بعد ذلك أن تخضع لمرحلة السلطة التقديرية الكاملة وذلك بوزن قيمة كل دليل على حدى، وفي

النهاية سلطة التنسيق بين الأدلة التي قدمت إليه واستخلاص نتيجة منطقية من الأدلة مجتمعة ومتساندة تتمثل في تقدير البراءة أو الإدانة.[1]

وذهب البعض الآخر من الفقه إلى تعريف الاقتناع القضائي بأنه حالة ذهنية يتوصل لها القاضي في حالة توافر مجموعة من الأدلة الوضعية ما يكفي لتسبيب تسليمه بالوقائع، ولقد أقرت معظم التشريعات بهذا المبدأ، حيث أخذ به المشرع الفرنسي في قانون الإجراءات الجزائية في المادة 303 التي نصت بأنه":لا يطلب القانون من القضاةحساباً بالأدلة التي اقتنعوا بها، ولا يفرض قاعدة خاصة تتعلق بتمام وكفاية دليل ما، وإنما يفرض عليه أن يتساءلوا في صمت وتدبر، وأن يبحثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجحة ضد المتهم ووسائل دفاعه[2]. "

أما المشرع الجزائري فلقد كرس المبدأ في قانون الإجراءات الجزائية بحيث نص أنه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص". [3]

وورد ذات المبدأ في نص المادة: 302 فقرة01 من قانون الإجراءات الجزائية المصري التي نصت على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته." كما أنه يتحدد مجال تطبيق مبدأ الاقتناع القضائي إما وفق طبيعة القضاء أو من حيث مراحل الدعوى الجنائية، بحيث أنه يمتد تطبيق مبدأ الاقتناع القضائي إلى كل أنواع المحاكم الجنائية سواء كانت محاكم الجنايات أو الجنح أو المخالفات، وهو ما صرح به المشرع الفرنسي من خلال نص المادة 353 من قانون الإجراءات الجزائية التي تنص على تطبيق المبدأ أمام محاكم الجنايات، وأما نص المادة 427 من ذات القانون فتنص على تطبيق هذا المبدأ أمام محكمة الجنح، أما المادة 536 فهي مخصصة لمحاكم المخالفات.

---

[1]– محمود إبراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الإلكترونية**، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2014، ص 644.

[2]– المادة 303 من قانون الاجراءات الجزائية الفرنسي .

[3]– المادة 212 ، من الأمر155/66 ، السابق الذكر.

ثانيا: تأثير طبيعة الدليل الإلكتروني على مسألة الاقتناع القضائي

إذا كان العلم قد استحدث الكثير من أساليب الإثبات وأمدت سلطات التحقيق بوسائل متطورة، إلا أن اقتناع القاضي الجنائي يأتي على قمة هذه الوسائل، لا كوسيلة من وسائل الإثبات، ولكن كمبدأ يحمي العدالة من سوء استخدام الوسائل العلمية الحديثة، بحيث أن طبيعة الأدلة الإلكترونية التي تجعلها أدلة مستمرة في التطور ومتعددة في التركيب، وتقوم في الأغلب على خاصية علمية تجعلها تكتسب من الدقة والنتائج المحددة إلى نسبة كبيرة، كل هذا له تأثير مباشر قوي على اقتناع القاضي يتجاوز في تأثيره كل أنواع وسائل الإثبات الأخرى، بحيث تجعله أكثر جزماً ويقيناً ، كما تقلل من نسبة الأخطاء القضائية والاقتراب من العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة[1].

وإن كانت الأدلة الإلكترونية تخضع إلى تقدير القاضي الجنائي وبالتالي اقتناعه، إلا أن هذا الأمر يكون في إطار خطين متوازيين، الأول يتعلق بالقيمة العلمية القاطعة للدليل، والثاني للظروف والملابسات التي وجد فيها الدليل، فتقدير القاضي لا يتناول الأمر الأول؛ وذلك لأن قيمة الدليل تقوم على أسس علمية كما ذكر سابقاً ، وبالتالي لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم مباشرة سواء بالإدانة أم البراءة دون بحث الظروف والملابسات، فالدليل الإلكتروني ليس آلية معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة، وبهذا يبقى للقاضي دور إيجابي في حرية تقدير الدليل الإلكتروني والاقتناع به من عدمه دون أي تأثير صادر من طبيعته، أو من قبل تقارير الخبرة التي تساعد على ثبوتيته وتأكيده.[2]

الفرع الثاني: بلوغ القاضي درجة الاقتناع اليقيني بالدليل الإلكتروني

إن الحكم الصادر من القاضي الجنائي يبنى على اقتناع القاضي اليقيني بالأدلة الإلكترونية المستخرجة من النظام المعلوماتي أو شبكة الانترنت، وبهذا يتجنب حكم الإدانة أو البراءة بناء على الشك، فلا مجال لدحض قرينة البراءة أو افتراض عكسها إلا في حالة الجزم واليقين، وعليه إذا كانت الأدلة الإلكترونية التي ساقها القاضي في حكمه قد انتهت به إلى

---

[1]– اشرف عبد القادر قنديل، المرجع السابق، ص 231.

[2]– شيماء عبد الغني عطاالله، **الحماية الجنائية للتعاملات الإلكترونية**، دار الجامعة الجديدة، الإسكندرية، 2007، ص 523.

ترجيح وقوع الجريمة من المتهم، فإن هذا الحكم يوصم بمخالفته للقانون على حسب أن أي شك يتطرق إلى اقتناع القاضي في ثبوت التهمة يجب على المحكمة أن تقضي بالبراءة مهما كان احتمال الثبوت ودرجته، وهو ما يمكن التوصل إليه من خلال ما يعرض من الأدلة الإلكترونية على اختلاف صورها، وتنوع وسائل الحصول عليها، فيأخذ القاضي دور الممحص في الأدلة تمحيصاً حسياً وعقلياً يجعله يشيد قناعته اليقينية بالدليل، مستبعدا ما قد ينطبع في تصوره الذهني من احتمالات أو استضعاف للقوة الثبوتية لأي دليل، مما يؤثر على حقيقة نسبة الجريمة إلى المتهم من عدمه.

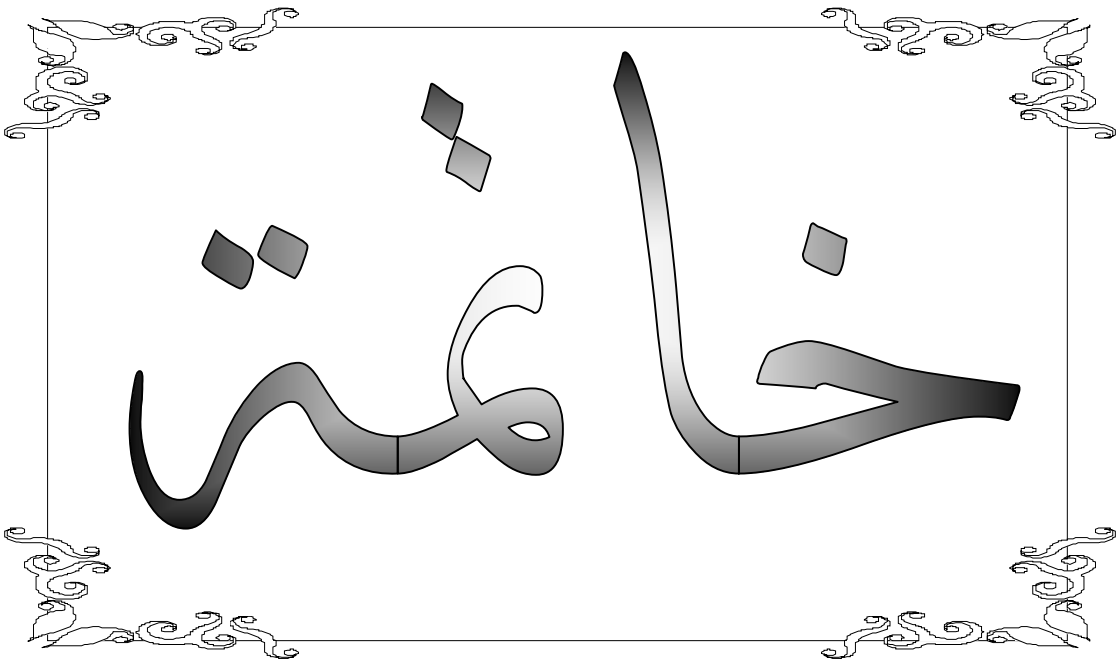
ومما يساعد بلا شك من تحقق الاقتناع اليقيني للقاضي الجنائي هو خضوع تلك الأدلة للتقسيم الفني بوسائل علمية تمكن من فحصها للتأكد من سلامتها، وكذا صحة الإجراءات المتبعة في تحصيل الدليل الإلكتروني لتجنب الأخطاء التي قد تنال من أصالتها أو قوتها الثبوتية .[1]

[1]– هلالي عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، مصر، 1999، ص 91

خلاصة الفصل الثاني:

في ظل التطور الرهيب الذي يشهده العالم في مجال تكنولوجيات الإعلام والاتصال والتجارة الالكترونية وبالمقابل انتشار واسع ورهيب للجرائم الالكترونية وخاصة الجرائم الواقعة على التوقيع الالكتروني والذي تسبب في أضرار مادية ومالية للعديد من الضحايا وحتى من الجانب النفسي.

ورغم المحاولات الجديرة بالاحترام التي قام بها المشرع الجزائري من خلال إصدار وسن قوانين تتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنطوي تحتها الجرائم الواقعة على التوقيع الالكتروني تبقى الحماية الجزائية لها عاجزة عن مواكبة التطور الرهيب الذي يشهده الإجرام في هذا المجال.


خاتمة

خاتمة

تعد دراستنا هذه حصيلة جهد متواضع قمنا به بهدف التطرق إلى لهذا الموضوع الذي ظهر نتيجة التطور المذهل الذي يعرفه العالم في مجال التطور العلمي و التكنولوجي، وخاصة في جانب التعاملات الالكترونية بفعل انتشار أجهزة الحواسيب والشبكات الالكترونية واستخدام التوقيع الالكتروني خاصة في مجال المعاملات التجارية والمصرفية والذي يعد كذلك أحد أكثر المواضيع القانونية حركية في الوقت الحاضر، حيث سعت الدول ومنها الجزائر إلى وضع قوانين تضفي المشروعية على التوقيع الالكتروني وتكسبه الصبغة القانونية والثبوتية، حيث أن المشرع الجزائري اعترف بالتوقيع الالكتروني في ظل القانون المدني(05-10) ومن أجل حماية التوقيع الالكتروني و تأمينه عمد المشرعين إيجاد بعض الوسائل المتمثلة في التوثيق (التصديق) بالإضافة إلى التشفير حيث ساير المشرع الجزائري هذه الحماية من خلال القانون رقم: (15-04) المتعلق بالتوقيع والتصديق الإلكترونيين ، واتبعه بالقانون رقم: (09-04) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وانشأ بموجبه المرسوم الرئاسي رقم: (15-261) الذي يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ولقد وجدت هذه الوسائل لحماية التوقيع الالكتروني خاصة من الجرائم الماسة به والمتمثلة في جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، و جريمة تزوير التوقيع الإلكتروني و جريمة إتلاف وتعييب التوقيع الإلكتروني وبالتالي حاول المشرع وضع مجموعة من العقوبات التي وجب تطبيقها على الشخص الطبيعي أو المعنوي مرتكب هذه الجريمة من خلال تعديلات هامة في قانون العقوبات و قانون الاجراءات الجزائية، إلا أن وسائل الحماية هذه تبقى عاجزة عن مواكبة التطور الرهيب الذي يشهده الإجرام في هذا المجال.

حيث أن القانون 09-04 جاء بأحكام تخص الجرائم الالكترونية بصفة عامة ولم يتم التفصيل في الجرائم الماسة بالتوقيع الالكتروني خاصة في الجانب الإجرائي للحماية الجزائية

للتوقيع الالكتروني فإتباع التحري والتحقيق وإجراءات المتابعة في الجرائم الماسة بالتوقيع الالكتروني جاء استنتاجينا من خلال إدراج هذه الجرائم ضمن الجريمة الالكترونية

وحتى سلطة القاضي في تقدير الأدلة الالكترونية لا يوجد نص واضح يوقع الإثبات على مرتكبي جرائم الماسة بالتوقيع الالكتروني، بل تم إدراجها في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات إستنتاجيا من قانون الإجراءات الجزائية .

ومما سبق نقول أن النصوص التشريعية المقررة للحماية الجزائية للتوقيع الالكتروني جاءت في شكل عام ولم تمس الجرائم الواقعة على التوقيع الالكتروني بشكل خاص حيث بقيت جرائم الاحتيال، التزوير، الدخول والبقاء الغير المصرح به منظمة تحت القواعد العامة لقانون العقوبات.

نتائج الدراسة :

خلصنا إلى جملة من النتائج :

– من خلال التعريف بمفهوم التوقيع الالكتروني في الفقه والقانون وكذا التشريعات الأجنبية خلصنا إلى أنه يشير إلى:" ما يوضع على محرر الكتروني ويتخذ شكل حروف او أرقام أو رموز أو إشارات أو غيرها ، ويكون له طابع متميز ومنفرد يسمح بتحديد هوية صاحب التوقيع" ، ويمكن القول أن أغلب التشريعات أعطت للتوقيع الالكتروني الحجية القانونية في الإثبات بالدرجة نفسها مع التوقيع التقليدي بشرط توفر الشروط القانونية لصحة التوقيع.

– سلطات التصديق هي جهة توفر الأمان لدى المتعاملين والمتعاقدين الالكترونيين من خلال حمايتهم من شتى طرق الاحتيال وعدم تعرضهم لأي شكل من المساس سواء ماديا أو من ناحية حماية البيانات الشخصية لهم.

– نطاق الحماية الموضوعية هو أن الجرائم الواقعة على التوقيع الالكتروني تتميز بخصائص أو خصوصية صعبة الكشف على مرتكبيها نظرا لاحترافيتهم في المجال الالكتروني باستعمالهم لأساليب تقنية دقيقة، ولردع مرتكبي هذه الجرائم تم وضع قوانين تطبق على مرتكبها سواء كان شخصا طبيعيا أو معنويا.

– آليات الحماية الجزائية الإجرائية أقرها المشرع على الجرائم الالكترونية و جرائم الماسة بأنظمة المعالجة الآلية للمعطيات ولم يقر نصوصا صريحة على الجرائم الماسة بالتوقيع الالكتروني.

التوصيات:

بناءا على النتائج المتوصل إليها خلال الدراسة يمكن تقديم بعض التوصيات:

– على المشرع الجزائري إصدار مراسيم تنظيمية خاصة بالتوقيع الالكتروني للإلمام بمختلف جوانبه وتعديل القانون (15–04) لتدارك الثغرات الموجودة به بإدخال جميع بالجرائم الماسة بالتوقيع الالكتروني و إصدار العقوبات المقررة لها.

– النص صراحة على إعطاء الأدلة الرقمية الحجية القانونية في الإثبات لتطبيقها قضائيا.

– توفير الإمكانيات البشرية والمادية للهيئات والأجهزة والمراكز المختصة في الوقاية مكافحة شتى الجرائم الماسة بالتوقيع الالكتروني.

– تكوين رجال الضبطية القضائية ورجال الأمن المكلفين بالبحث والتحري حول كيفية التعامل مع الأدلة وضبطها، وإرسالهم لإجراء تربصات بالدول المتقدمة حول الجرائم الالكترونية وكيفية تطورها.

قائمة المصادر والمراجع

أولا: المصادر

1- المراسيم

1. المرسوم التنفيذي رقم (07-162) المؤّرخ في 30 ماي2007 ، المتعلق بنظام الاستغلال المطّق على كل أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية يعدل ويتمم المرسوم التنفيذي رقم : (01-123) مؤرخ في 09 جويلية 2001 ج، ر،ع 27 الصادرة في 13 جويلية 2001.

2. المرسوم الرئاسي رقم 15-261 المؤرخ في 05 أوت 2009 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 53، في 2015/10/08.

3. المرسوم التنفيذي رقم(16-134) مؤرخ في 05-04-2016، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، الجريدة الرسمية للجمهورية الجزائرية، العدد 62.

2- القوانين

1. قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية مع دليل الإشتراع 2001 ، منشورات الأمم المتحدة نيويورك ،2002 .

2. القانون رقم 14-04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155/66 المؤرخ في:18 صفر 1386 الموافق: 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية، عدد 71 بتاريخ 10 نوفمبر 2004.

3. القانون رقم 09- 04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

4. القانون رقم (15-04) مؤرخ في 01 -02-2015، يحدّد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 60.

3- الأوامر

1. الأمر66-156 المؤرخ في: 18صفر1386 الموافق 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات، المعدل والمتمم بالأمر 20-01 المؤرخ في: 30 يوليو سنة 2020.

2. الأمر 75-58 المؤرخ في : 26 سبتمبر 1975 ، المتضمن القانون المدني الجزائري ج،ر،ع 78 مؤرخة في 30سبتمبر 1975 ، معدل ومتمم .

ثانيا: المراجع

1- الكتب

1. اشرف عبد القادر قنديل، **الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة**، د.ط، الإسكندرية، مصر، 2015.

2. اغليس بوزيد، **تلازم مادة الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي**، دار الهدى، د.ط، عين مليلة، الجزائر، 2010.

3. العبودي عباس، **تحديات إثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها**، ط1 ، منشورات الحلبي الحقوقية، .لبنان، 2010 .

4. الهام صالح بن خليفة، **دور البصمات والآثار المادية الأخرى في الإثبات الجنائي**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، المملكة الأردنية الهاشمية، 2014.

5. بشار محمود دودين، **الإطار القانوني للعقد المبرم عبر شبكة الإنترنت**، ط2 ، دار الثقافة للنشر والتوزيع، الأردن،2010 .

6. بكري يوسف بكري، **التفتيش عن المعلومات في وسائل التقنية الحديثة**، دار الفكر الجامعي، مصر،2012 .

7. حسام محمد نبيل الشنراقي، **الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني**، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013 .

8. حسن عبدالباسط جميعي ، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت ، دار النهضة العربية ، مصر 2000 .

9. خالد عباد الحلي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة، الأردن،2011 .

10. خالد مصطفى فهمي ، **النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات** الدولية ، دار الجامعة الجديدة ، مصر ، 2007 .

11. خالد ممدوح إبراهيم، **إبرام العقد الإلكتروني**، ط1، دار الفكر الجامعي، مصر، 2006.

12. خالد ممدوح إبراهيم، **التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي، مصر، 2008.

13. خيثر مسعود، **الحماية الجنائية لبرامج الكمبيوتر في التشريع الجزائري**، دار الهدى، الجزائر، 2010.

14. سامي جلال، حسين فقي، **الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، دراسة مقارنة، دار الكتب القانونية، د.ط، مصر، 2001.

15. شيماء عبد الغني عطاالله، **الحماية الجنائية للتعاملات الإلكترونية**، دار الجامعة الجديدة، الإسكندرية، 2007.

16. عائشة بن قارة مصطفى، **حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامعة الجديدة، ط1، الإسكندرية، مصر، 2010.

17. عاطف عبد الحميد حسن، **التوقيع الإلكتروني، (مفهومه، صوره، حجيته في الإثبات في نطاق المعاملات المدنية)** د ط، دار النهضة العربية، القاهرة،2009 .

18. عبد الفتاح بومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، مصر، ط1، د س.

19. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، ط1، دار الفكر الجامعي، الإسكندرية،2005 .

20. عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير المعلوماتي**، دار الكتب القانونية المجلة الكبرى، ط1.

21. علاء محمد نصيرات، **حجية التوقيع الالكتروني في الإثبات (دراسة مقارنة)**،ط1، دار الثقافة للنشر والتوزيع، الأردن، 2005.

22. غنية باطلي، **الجريمة الالكترونية، دراسة مقارنة**، الدار الجزائرية للنشر والتوزيع، الجزائر،2015.

23. فيصل سعيد الغريب ، **التوقيع الالكتروني وحجيته في الإثبات** ، المنظمة العربية للتنمية الإدارية ، مصر ، 2005 .

24. لزهر بن سعيد ، **النظام القانوني لعقود التجارة الالكترونية** ، دار هومة للطباعة والنشر و التوزيع ، الجزائر ،2012.

25. لورنس محمد عبيدات ، **إثبات المحرر الالكتروني** ، دار الثقافة للنشر والتوزيع ، الأردن 2005 .

26. محمد المرسي زهرة، **الحاسوب والقانون**، ط1 ، مؤسسة الكويت للتقّدم العلمي، الكويت ،1995.

27. محمد زكى ابو عامر، **الإثبات في المواد الجنائية، محاولة فقهية وعملية لإرساء نظرية عامة**، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2011.

28. محمد سعيد أحمد إسماعيل، **أساليب الحماية القانونية لمعاملات التجارة الإلكترونية دراسة مقارنة**، ط1، منشورات الحلبي الحقوقية، لبنان،2009 .

29. محمود إبراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الإلكترونية**، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2014.

30. مروك نصر الدين، **محاضرات في الإثبات الجنائي**، دار هومة، الجزائر، 2011.

31. نادية ياس البياتي، **التوقيع الإلكتروني عبر الانترنيت ومدى حجيته في الإثبات**، ط1 ، دار البداية ناشرون وموزعون، الأردن، 2014 .

32. هلالي عبد الله احمد، **حجية المخرجات الكمبيوترية في المواد الجنائية**، دار النهضة العربية، القاهرة، مصر، .1999

2- المذكرات والرسائل

3. امال قارة ، **الجريمة المعلوماتية**، مذكرة ماجستير، كلية الحقوق جامعة الجزائر،2001-2012.

4. بعرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة**، مذكرة ماستر في الحقوق، تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015-2016.

5. حابت آمال، **التجارة الإلكترونية في الجزائر**، رسالة لنيل شهادة دكتورة في العلوم، تخصص قانون، كلية الحقوق، جامعة .مولود معمري، تيزي وزو، 2015 .

6. حنان براهمي، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه، كلية الحقوق ،جامعة بسكرة ،2015.

7. صالح شنين، **الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، رسالة دكتوراه، جامعة تلمسان، 2013.

8. عادل بوزيدة، **المسؤولية الجزائية لمتعهدي إيواء المواقع الالكترونية**، أطروحة دكتوراه، جامعة تبسة،2017/2016.

9. عباس حفصي، **جرائم التزوير الإلكتروني– دراسة مقارنة–**، رسالة دكتوراه، جامعة أحمد بن بلة، وهران1،2015 .

10. محمد هشام صالح عبد الفتاح ،جريمة الاحتيال دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، لجامعة النجاح الوطنية، نابلس، فلسطين ،2008.

11. يمينة حوحو، **عقد البيع الإلكتروني دراسة مقارنة**، أطروحة دكتوراه، جامعة ابن عكنون، الجزائر 2012.

3– المجلات والملتقيات

2. أسامة بن غانم لعبيدي،"**حجية التوقيع الإلكتروني في الإثبات**"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28 العدد 56، جامعة نايف للعلوم الأمنية، السعودية ،2012.

3. حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، كلية الحقوق، جامعة أكلي محند أولحاج، العدد الثاني، 2016.

4. رشيدة بوكر، **الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد السابع والعشرون، العدد 02، 2011.

5. سعيدة بوزنون، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر، 2019.

6. ضريفي نادية، **سلطات القاضي الجاني في تقدير الدليل الإلكتروني**، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04 ، العدد02 ،2019.

7. عابد فايد عبد الفتاح فايد، **الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني** :دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني، دار الجامعة الجديدة، الإسكندرية، 2004 .

8. عبد العزيز سمية ، **التوقيع الالكتروني وسيلة حديثة للإثبات –دراسة مقارنة**– مجلة معارف (مجلة علمية محكمة) قسم العلوم القانونية ، السنة الثامنه – العدد 17/ ديسمبر 2014 .

9. عبد العزيز سمية، **التوقيع الالكتروني وسيلة حديثة للإثبات – دراسة مقارنة**– مجلة علمية محكمة، قسم العلوم القانونية، السنة الثامنة، العدد 17/ديسمبر 2014.

10. عيسى الصمادي ، **الإثبات في عقد نقل التكنولوجيا الالكتروني – عبر شبكة الانترنت** –، مجلة دراسات قانونية ، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية ، الجزائر ، ع 06، 2010.

11. فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى ألمغاربي حول القانون والمعلوماتية المزعم عقده بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009.

12. فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017.

13. كريمة علة، **الجهات القضائية الجزائية ذات الاختصاص الموسع**، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 11، 2015.

14. محمد السعيد زناتي، **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017 ، المركز الجامعي إليزي الجزائر.

15. يوسف جفال، **التحقيق في الجريمة الإلكترونية**، مذكرة شهادة الماستر الأكاديمي، جامعة محمد بوضياف، المسيلة، الجزائر، 2016/.2017

4- المواقع الإلكترونية

1. أحمد السيد كردي ،**التوقيع الإلكتروني مفهومه التكنولوجي وحمايته"** ، 32 سبتمبر 2011 **http://kenanaonline.com/users/ahmedkordy/posts/323677**

2. أمجد حمدان الجهني،**"جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنيت"**،موقع الكتروني، تم الاطلاع **http://www.cojss.com/article.php?a=219**

3. محمد محروك، **خصوصيات التوقيع الإلكتروني وحجيته في الإثبات"**، 4 فيفري 2013، **https://www.marocdroit.com**

4. ياسر العدل، **التوقيع الإلكتروني**، 2009/09/29، **https://www.m.ahewar.org/index.asp?ry=5&r=50&cid=0&i=1005&u=&q=**

الملخص

ملخص

تبقى الحماية الموضوعية والإجرائية مهما بلغت درجتها عاجزة عن مسايرة التطور الرهيب الذي تشهده الجرائم الواقعة على التوقيع الالكتروني، وهو ما أدى إلى استفحال الجريمة الالكترونية وتسبب في أضرار مادية ومالية وحتى نفسية للعديد من الضحايا.

حيث تبين من هذه الدراسة مدى خطورة الجرائم الماسة بالتوقيع الالكتروني، وهذا راجع إلى خصوصيتها خاصة من الجانب التقني، وصعبة الإكتشاف و الإثبات، حيث وقفت مختلف النظم القانونية عاجزة عن مواكبة تطور هذه الجرائم ومكافحتها، وأمام هذه الوضعية حاول المشرع الجزائري الحد من خطورة هذه الجرائم، من خلال إدراجه لتعديلات هامة على قانون العقوبات وقانون الإجراءات الجزائية، وسن قوانين ومراسيم تتعلق بالتوقيع الالكتروني من خلال قانون التوقيع والتصديق الالكتروني.

Summary

Objective and procedural protection, regardless of its degree, remains unable to keep pace with the terrible development witnessed by the crimes committed against the electronic signature, which led to the exacerbation of electronic crime and caused material, financial and even psychological damage to many victims.

This study showed the extent of the seriousness of the crimes related to the electronic signature, and this is due to its specificity, especially from the technical side, and difficult to discover and prove, as the various legal systems were unable to keep pace with the development of these crimes and combat them, and in the face of this situation, the Algerian legislator tried to reduce the seriousness of these crimes , by including important amendments to the Penal Code and the Code of Criminal Procedure, and the enactment of laws and decrees related to electronic signature through the Electronic Signature and Certification Law.

الفهرس

الفهرس

المحتوى	الصفحة
شكر وعرفان	–
مقدمة	01
الفصل الأول: الحماية الجزائية الموضوعية للتوقيع الإلكتروني	
تمهيد	06
المبحث الأول: التوقيع الالكتروني كمحل للحماية	07
المطلب الأول: التكوين التقني للتوقيع الالكتروني	07
الفرع الأول: التوقيع التقليدي	07
الفرع الثاني: تعريف التوقيع الالكتروني	08
الفرع الثالث: صور التوقيع الالكتروني وخصائصه	12
المطلب الثاني: التصديق الإلكتروني	16
الفرع الأول: مفهوم التصديق الإلكتروني وطبيعته	17
الفرع الثاني: جهات التصديق الالكتروني	18
الفرع الثالث: شهادات التصديق الالكتروني	21
الفرع الرابع: سلطات التصديق الالكتروني	23
المبحث الثاني: نطاق الحماية الموضوعية للتوقع الالكتروني في القانون الجزائي	26
المطلب الأول: تجريم المساس بالتوقيع الالكتروني	26
الفرع الأول: خصائص الجرائم الواقعة على التوقيع الالكتروني	26
الفرع الثاني: صور الجرائم الواقعة على التوقيع الالكتروني	28
المطلب الثاني: العقاب على الاعتداء على التوقيع الإلكتروني	39
الفرع الأول: العقوبات المطبقة على الشخص الطبيعي	39
الفرع الثاني: العقوبات المطبقة على الشخص المعنوي	42

خلاصة الفصل الأول	46
الفصل الثاني: الحماية الجزائية الإجرائية للتوقيع الالكتروني	
تمهيد:	48
المبحث الأول: التحري و التحقيق في الجرائم الماسة بالتوقيع الالكتروني	49
المطلب الأول : أجهزة التحقيق المتخصصة في البحث والتحري	49
الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري	50
الفرع الثاني :الهيئات القضائية الجزائية المتخصصة	52
المطلب الثاني: إجراءات التحقيق والمتابعة في الجرائم الواقعة على التوقيع الالكتروني	54
الفرع الأول: مرحلة جمع الأدلة	55
الفرع الثاني: مرحلة التحقيق في الجرائم الواقعة على التوقيع الإلكتروني	57
الفرع الثالث: الاختصاص المحلي والنوعي في الجرائم الواقعة على التوقيع الالكتروني	60
المبحث الثاني: سلطة القاضي في قبول وتقدير الدليل الجنائي	63
المطلب الأول: سلطة القاضي الجزائي في قبول الأدلة الإلكترونية	63
الفرع الأول: أساس سلطة القاضي الجزائي في قبول الأدلة الإلكترونية	64
الفرع الثاني: القيود الواردة على سلطة القاضي الجزائي في قبول الأدلة الإلكترونية	67
المطلب الثاني :سلطة القاضي في تقدير الأدلة الرقمية	70
الفرع الأول :حرية القاضي الجنائي في تقدير الدليل الإلكتروني	70
الفرع الثاني: بلوغ القاضي درجة الاقتناع اليقيني بالدليل الإلكتروني	72
خلاصة الفصل الثاني	74
خاتمة	76

قائمة المصادر والمراجع	80
خلاصة الموضوع	–
الفهرس	–