جـــامـــعـــة أمـــحـــمـــد بـــوقـــرة بـــومـــرداس

كـلـيـة الـحـقـوق والـعـلـوم الـسـيـاسـيـة

قـسـم الـقـانـون الـعـام

الـحـمـايـــة الـجـنـائـيـة لـلـتـوقـيـع الالـكـتـرونـي وفـق الـقـانـون الـجـزائـري

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في القانون

تخصص: قانون عام

إعداد الطالبة:

- مـكـور فـريـدة

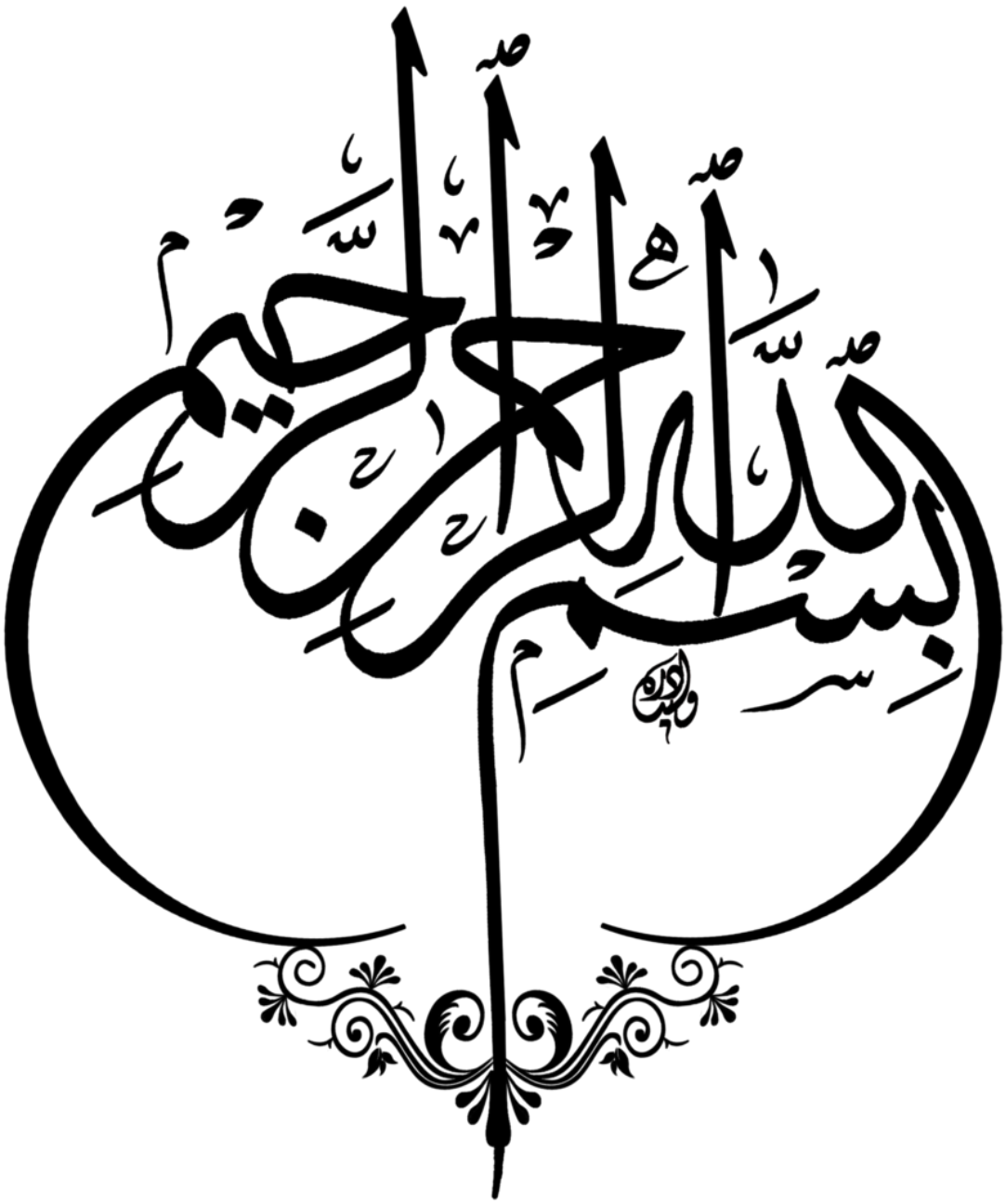
إشراف الأستاذ:

- أوصيف سعيد

لجنة المناقشة:

الاسم واللقب	الرتبة	الجامعة	الصفة
زوبة سميرة	أستاذة محاضرة –أ–	أمحمد بوقرة بومرداس	رئيسةً
أوصيف سعيد	أستاذ محاضر –أ–	أمحمد بوقرة بومرداس	مشرفا ومقررا
سليماني لامية	أستاذة مساعدة –أ–	أمحمد بوقرة بومرداس	ممتحنةً

السنة الجامعية: 2023-2024


بسم الله الرحمن الرحيم

إهـداء

الحمد لله حبا وشكرا وامتنانا الذي بفضله ها أنا أنظر اليوم لحلم طال انتظاره وقد أصبح واقعا افتخر به.

أهدي هذا العمل المتواضع إلى منبع الحب والحنان "أمي" الغالية، التي كانت نور حياتي ودعمي الدائم في كل خطوة خطوتها.

وإلى من قيل فيه:

{سَنَشُدُّ عَضُدَكَ بِأَخِيكَ}

أخي أدامك الله ضلعا ثابتا لي.

إلى كل من علمنا حرفا.

شكر وتقدير

مصداقا لقوله تعالى " وإن شكرتم لأزيدنكم '' نحمد الله تبارك وتعالى حمدا كما يحب ويرضى، ونشكره كما ينبغي لجلال وجهه وعظيم سلطانه فهو سبحانه ولي كل نعمة، وبتوفيقه تتم الصالحات، والصلاة والسلام على خير الخلق محمد صلى الله عليه وسلم

اعترافا بالفضل لأهل الفضل، أتوجه بالشكر والعرفان إلى الأستاذ **"أوصيف سعيد"** لقبوله الإشراف على هذه المذكرة والى كل مساعداته وتوجيهاته القيمة لإثراء الموضوع جزاه الله عنا خير الجزاء.

كما لا يفوتني أن أتوجه بالشكر إلى أعضاء لجنة المناقشة التي تحملت عناء قراءة وفحص هذه المذكرة المتواضعة وتصويب أخطائها راجين من الله ان يجعل ذلك في ميزان حسناتهم.

قائمة المختصرات:

أولا: باللغة العربية.

ج.ر.ج.ج: الجريدة الرسمية الجمهورية الجزائرية.

د.ط: دون طبعة.

ص: صفحة.

/: فقرة.

دج: دينار جزائري.

ق.ع: قانون العقوبات

ثانيا: باللغة الأجنبية.

Uncitral : United Nations Commission on International Trade Law.

Article : art.

مـــقـدمـــــة

مقدمة:

أسفرت الثورة التكنولوجية والتطور التقني الكبير في استخدام الحواسيب تغيير عميق في نمط التفكير والاتجاه من العالم المادي والمحسوس إلى العالم الافتراضي، فقد حولت هذه التغييرات العالم إلى قرية صغيرة تتناقل فيها المعلومات بسرعة وبطريقة إلكترونية، فبعدما كانت وسائل الاتصال محصورة في الهاتف والفاكس والتلكس، ظهر البعد الآخر مع بروز شبكة الإنترنت الضخمة، ولا شك أن ظهور هذه الشبكة وامتداد استخدامها في مختلف المجالات جعل التعاملات الإدارية، والمصرفية والمالية، والخدماتية و غيرها تتم بطريقة إلكترونية، وخاصة في المجال التجاري الذي يُعتبر من أكثر القطاعات استجابة للتقدم والابتكار التكنولوجي، وقد ساهمت هذه التطورات في ظهور مفاهيم جديدة ونوع جديد من المبادلات، يقوم على التدفق السريع للمعارف والاستجابة الفورية للتغيرات المفاجئة، وإلغاء القيود والحدود المادية والجغرافية، وهو ما يعرف اليوم بالتجارة الإلكترونية التي أخذت بفكرة إبرام العقود الإلكترونية، والدفع الإلكتروني، والفوترة الإلكترونية... مما جعل معظم التعاملات تتم بواسطة الكتابة الالكترونية والمحررات الإلكترونية.

وقد أدى التعقيد الفني للمعاملات الإلكترونية إلى ظهور تحديات قانونية تتعلق بأمنها وموثوقيتها في العالم الافتراضي، حيث لا يمكن ضمان الأمن الكامل، واستجابة لهذه المخاوف سعى الخبراء القانونيون والتقنيون إلى اتباع نهج بديل، وذلك بابتكار وسيلة إلكترونية بأشكال متنوعة تحاكي خصائص التوقيعات التقليدية مع تعزيز الأمن والخصوصية في المعاملات وهي ما يُعرف "بالتوقيع الإلكتروني"، الذي تتزايد أهميته في أنه يرد ضمن أشكالا متنوعة تلبي الاحتياجات المختلفة، مما يوفر المرونة والقدرة على التكيف في سياقات مختلفة، ومن خلال استخدام هذه التقنية يمكن للمؤسسات تبسيط عملياتها وتعزيز الكفاءة وتخفيف المخاطر المرتبطة بالتوقِيعات الورقية التقليدية كما أنه لا يوفر الراحة فحسب، بل يتيح اكتشاف الاحتيال أو التلاعب ومنعه، وبالتالي خلق بيئة إلكترونية آمنة وموثوقة. وبناءً على اهمية التوقيع الإلكتروني فإن تنظيم وتوجيه جوانبه أصبح أمرًا لا غنى عنه، لذلك سارعت الجزائر بخطى ثابتة نحو تطبيق هذه التقنية وتفعيلها التي أصبحت ضرورة ملحة، خاصة وأن الذي يتعامل مع التوقيع الإلكتروني يجد نفسه أمام ظاهرة تقنية جديرة بالتنظيم.

وبينما تسعى الدول لاستغلال تقنية التوقيع الإلكتروني لتعزيز النمو الاقتصادي، وتسهيل المعاملات، وتلبية مختلف المتطلبات الخاصة والعامة، هناك عوائق عديدة تعيق هذا التقدم، ويتمثل أحد التحديات الكبيرة في ظهور الأنشطة الإجرامية المستحدثة، والتي أصبحت ممكنة بفضل الأدوات والأساليب المتطورة المتاحة، ومن الأمثلة الواضحة الانتشار المتصاعد للجرائم الالكترونية، وفي هذا السياق يؤكد المختصون أن جرائم الاعتداء على التوقيع الإلكتروني تعتبر من بين أخطر الجرائم في هذا المجال.

لذلك كان من الضروري على المشرع الجزائري اتباع سياسة جنائية تهدف إلى حماية التوقيع الإلكتروني من مختلف الاعتداءات التي تطاله، خصوصا ان الجناة في هذه الجرائم يتمتعون بمهارات تسمح لهم بالتلاعب بتقنيات الحاسوب، التي أتاحت إمكانيات جديدة لارتكاب أعمال إجرامية لم تكن ممكنة في السابق، لذلك لا يمكن التعامل مع جريمة اليوم بنفس الطريقة التي كنا نتعامل بها مع الجريمة في الماضي، حيث ان المجرم يقوم الآن بالتخطيط بعناية قبل ارتكابه لنشاطه الإجرامي، دون ترك أي أدلة مادية تثبت تورطه.

يكتسي موضوع الحماية الجنائية للتوقيع الإلكتروني **أهمية** متزايدة تنبع أساسا في القيمة القانونية التي يتمتع بها للتوقيع الالكتروني حيث يعتبر أحد المظاهر الجديدة في مجال المعاملات الالكترونية، ولا يكفي الاعتراف بحجية التوقيع الإلكتروني في الإثبات، دون العمل على إيجاد الآليات الكفيلة ببعث الثقة والاطمئنان لدى المتعاملين به، وتحقيق الحماية الضرورية للتوقيع الإلكتروني من مخاطر التي يتعرض لها والحفاظ على الدور الوظيفي المنوط به من أي اختراق أو تحايل إلكتروني، ويكون بذلك هذا البحث إضافة للمكتبة القانونية.

إن اختيارنا لهذا الموضوع يعود لعدة **أسباب** منها ما هو شخصي ومنها ما هو موضوعي، أما **الأسباب الموضوعية** فتمحورت في:

– ظهور تشريعات جديدة برهنت نجاعة استخدام التوقيع الإلكتروني وتحدد العقوبات الجنائية المرتبطة بانتهاكه يفرض الحاجة لدراسة معمقة لفهم هذه القوانين وتأثيرها.

– تزايد الاعتداءات التي تطال التوقيعات الإلكترونية، يبرز الحاجة لفهم كيفية تطبيق الحماية الجنائية وما يترتب عليها من مسؤوليات قانونية.

– المساهمة في إثراء البحث الأكاديمي واقتراح توصيات تساعد في تحسين السياسات والإجراءات المتعلقة بالتوقيع الإلكتروني.

أما **الأسباب الذاتية** فترجع إلى رغبتنا في تسليط الضوء على موضوع نرى بأنه من المواضيع الشائكة والمعقدة الذي يتعلق بعالم افتراضي يستهوينا لمعرفة خباياه وأطره القانونية، وبالتالي إثراء الرصيد المعرفي في مثل هذه المواضيع المستحدثة.

–الشعور بشغف كبير نحو التكنولوجيا والقانون، ونجد في موضوع الحماية الجنائية للتوقيع الإلكتروني فرصة فريدة تجمع بين هذين المجالين بطريقة مثيرة ومفيدة.

–فهم التحديات القانونية المتعلقة بالتكنولوجيا الحديثة يمثل بالنسبة لنا مجالًا غنيًا للاستكشاف، حيث يمكننا دراسة كيفية تطبيق القوانين التقليدية على السياقات الرقمية، هذا الاهتمام ينبع من رغبتنا في فهم أعمق لتقنية التوقيع الإلكتروني وآليات حمايتها من الجرائم الإلكترونية.

تهدف هذه الدراسة إلى تسليط الضوء على الحماية الجنائية المقررة للتوقيع الإلكتروني من خلال الوقوف على توجهات المشرع الجزائري في تنظيمه للتوقيع الالكتروني، محددا المعايير القانونية والفنية لضمان موثوقيته، والتركيز على الصور التي يقر المشرع الجزائي الجزائري بأنها تشكل جرائم اعتداء على التوقيع الالكتروني، مع بيان أحكامها الموضوعية، ووسائل الحماية الجنائية التي اعتمدها لمواجهة الجرائم الماسة بالتوقيع الالكتروني من خلال استعراض أساليب التحري ودور الهيئات المختصة في مكافحتها، مع مناقشة العقوبات القانونية المطبقة على هذه الجرائم وتقييم فعاليتها في الردع والحماية.

بعد البحث العميق في موضوع الدراسة تبين أنه لا تعد هذه الدراسة الاولى في هذا السياق، وانما توجد **دراسات سابقة** نذكر منها:

–فارس خطابي، الحماية الجزائية للتوقيع الإلكتروني، أطروحة لنيل شهادة الدكتوراه في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج الأخضر،2021.

–مصطفى صحراوي، الحماية الجزائية للتوقيع والتصديق الالكترونيين في التشريع الجزائري، أطروحة للحصول على شهادة الدكتوراه ل.م.د في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، 2021.

–زهرة بالخير، الحماية الجنائية للتوقيع الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون –تيارت– 2021،.

ومن بين **الصعوبات** التي واجهتنا خلال إعداد هذه الدراسة النقص البارز في الدراسات المتخصصة في هذا المجال، نظراً لحداثة الموضوع في النظام القانوني الجزائري الذي صدر في عام 2015 ، وكون هذا الموضوع يحتاج للدقة ووقت طويل للدراسة نظرا لتشبعه واحتوائه على الكثير من التفاصيل، وبالتالي صعوبة الإلمام بكل جوانبه باعتباره يجمع بين بعدين على قدر كبير من الأهمية وهما القانون والمعلوماتية، الأمر الذي يقتضي عدم التركيز على الناحية القانونية وحسب، بل أيضا الجانب التقني، وهذا ما خلق صعوبة في الإلمام بالمصطلحات والمفاهيم التقنية لعدم التخصص فيها.

وبهذا ارتأينا **طرح الإشكالية** الاتية:

ماهي التدبير الجنائية التي أقرها المشرع الجزائري لحماية التوقيع الالكتروني؟

من اجل الاجابة على الإشكالية المطروحة اقتضت هذه الدراسة الاعتماد على **المنهج** الوصفي والتحليلي، حيث استخدم المنهج الوصفي لتوضيح مختلف المفاهيم المتعلقة بالتوقيع الإلكتروني، كما استخدم المنهج التحليلي في تحليل النصوص القانونية المختلفة ذات الصلة بالموضوع وتبيان مضمونها.

وقمنا بوضع خطة بحث مكونة من فصلين ولكل فصل مبحثين، تناولنا في الفصل الأول الحماية الجنائية الموضوعية للتوقيع الالكتروني فكان المبحث الأول عن ماهية التوقيع الالكتروني، أما المبحث الثاني فخصصناه لتجريم المساس بالتوقيع الإلكتروني، أما

بالنسبة للفصل الثاني فتناولنا فيه إجراءات الحماية الجنائية للتوقيع الالكتروني وقسمناه الى مبحثين، المبحث الأول جاء تحت عنوان التحري في الجرائم الواقعة على التوقيع الالكتروني، والمبحث الثاني عن العقوبات المقررة للاعتداء على التوقيع الالكتروني.

الفصل الأول: الحماية الجنائية الموضوعية للتوقيع الالكتروني.

قديما، اعتمد إبرام العقود في الغالب على الأساليب التقليدية، وذلك باستخدام المستندات المادية واشتراط التوقيعات المكتوبة بخط اليد كشكل قانوني للتصديق من قبل الأطراف المعنية. ومع ذلك فإن تطور التكنولوجيا في العصر الحديث قد أدخل آليات إلكترونية تجعل التوقيع الورقي التقليدي مرهقًا وعفا عليه الزمن بسبب طبيعته الملموسة، وقد سهّل هذا التحول ظهور "التوقيع الإلكتروني" وهو بديل رقمي مصمم ليتماشى مع هذه التطورات التكنولوجية، وبالتالي تعزيز كفاءة وفعالية المعاملات عبر مختلف القطاعات، بما في ذلك التجارة والمصارف والاتصالات، ولسوء الحظ ساهم الانتقال إلى العمليات الافتراضية وتناقص الاعتماد على المستندات المادية في زيادة الأنشطة الاحتيالية والتلاعبات التي تؤثر على المعاملات، واستجابة لذلك قامت أغلب التشريعات بتقديم إطار قانوني لتحديد معنى التوقيع الإلكتروني وشروط صحته، علاوة على ذلك فقد تم بذل جهود متضافرة لصياغة قوانين تجرم المساس بمثل هذه التقنية الحديثة.

وبناء على ذلك تم تقسيم هذا الفصل إلى مبحثين رئيسيين، يتعمق المبحث الأول في ماهية التوقيع الإلكتروني، وبعد ذلك سنناقش في المبحث الثاني تجريم المساس بالتوقيع الإلكتروني.

المبحث الأول: ماهية التوقيع الالكتروني.

يعتبر التوقيع جزءاً حيوياً من عملية تأكيد إرادة الأطراف في المعاملات القانونية، حيث تعتبر الكتابة بدون توقيع مصدراً للشك وعدم الثبوت، يُضفي التوقيع الشرعية والموثوقية على المستند، ويكتسي هذا الأمر أهمية بالغة في حالة العقود التي تُبرم عبر وسائل الاتصال الحديثة، حيث تحول مفهوم الموثوقية من التوقيع التقليدي إلى التوقيع الإلكتروني، الذي يُعد بديلاً فعالاً يمكنه تعويض اللقاء المباشر بين الأطراف، ومن هنا تسعى التشريعات إلى تعزيز الثقة والأمان في التوقيع الإلكتروني من خلال وضع إطار قانوني مناسب يمكّنه من الاعتمادية والتطبيق الفعّال.[1]

لذلك سوف نتطرق من خلال هذا المبحث إلى مفهوم التوقيع الالكتروني في المطلب الأول، ومن ثم نوضح شروط صحته وعملية التصديق عليه في المطلب الثاني.

المطلب الأول: مفهوم التوقيع الالكتروني.

نلاحظ في الآونة الاخيرة تداول مصطلح التوقيع الإلكتروني بين الأفراد والمؤسسات وهذا بسبب ظهور الحواسيب وتطور التكنولوجيا، ومع ذلك فإن فهم مفهومه الحديث يظل غير واضح بالنسبة للكثيرين، فالتوقيع سواء التقليدي أو الإلكتروني يعد الضامن الأساسي للتأكد من هوية الموقع عليه في المستندات الرسمية وغير الرسمية، ولكن مفهوم التوقيع الإلكتروني يختلف تماماً عن التوقيع التقليدي، لذا سنقوم بتعريفه في الفرع الأول، ومن ثم نستعرض خصائصه وأشكاله في الفرع الثاني.

---

[1]- عائشة قصار الليل ،**حجية المحرر والتوقيع الإلكتروني في الإثبات**، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة –،2017 ص 78.

الفرع الأول: تعريف التوقيع الالكتروني.

تنوعت التعاريف المقدمة للتوقيع الإلكتروني بناءً على اختلاف وجهات النظر والتفسيرات الفقهية، فضلاً عن تباين التشريعات في الدول التي اعتمدت هذا النوع من التوقيع، لذا سنقوم بتوضيح التعريف الفقهي أولاً، ومن ثم نستعرض التعريف القانوني (ثانيا).

أولا: التعريف الفقهي للتوقيع الإلكتروني.

تعددت التعريفات التي أوردها الفقه القانوني للتوقيع الإلكتروني فقد عرفه البعض على أنه «كل اشارات او رموز او حروف مرخص بها من الجهة المختصة باعتماد التوقيع مرتبطة ارتباطا وثيقا بالتصرف القانوني تسمح بتمييز شخص صاحبهم وتحديد هويته وتعبر دون غموض عن رضاه بهذا التصرف القانوني».[1]

وعرف البعض الآخر التوقيع الالكتروني بأنه «بيان مكتوب بشكل الكتروني يتمثل بحرف او رقم او رمز او اشارة أو صوت او شفره خاصة ومميزه ينتج عن اتباع وسيلة امنه وهذا البيان يلحق أو يرتبط منطقيا ببيانات المحرر الإلكتروني (رسالة بيانات) للدلالة على هوية الموقع ورضاهم بهذا التصرف القانوني».[2]

كما عرفه جانب اخر على أنه «مجموعة من الرموز او الارقام او الحروف او الاشارات او الاصوات مؤلفة على شكل بيانات الكترونية تتصل برسالة معلومات (محرر الكتروني) هدفها تحديد هوية الموقع وإعطاء اليقين بموافقته على مضمون الرسالة».[3]

كما عرفه آخرون بأنه «توقيع يقوم على مجموعة من الإجراءات والوسائل التي يتاح استخدامها عن طريق الرموز او الارقام ليتم إخراجه على شكل رسالة الكترونية تتضمن

---

[1]-ثروت عبد الحميد، **التوقيع الإلكتروني ماهيته- مخاطره- وكيفية مواجهتها- مدى حجيته في الإثبات**، دار الجامعة الجديدة دون طبعة، الإسكندرية 2007 ص 50.

[2]-عيسى غسان ربضي، **القواعد الخاصة بالتوقيع الإلكتروني** ،دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2012 ، ص 56.

[3]-منصور محمد حسنين، **الاثبات التقليدي والالكتروني** ،دار الفكر الجامعي، دون طبعة، الإسكندرية، 2006، ص 106.

علامات مميزة للموقع عن غيره، ومشفره بإحدى طرق التشفير ويتم تداول الرسالة الكترونيا من خلال الوسائل الإلكترونية»[1].

ثانيا: التعريف التشريعي.

اهتمت القوانين على مختلف الأصعدة بمسألة التوقيع الإلكتروني، حيث أصبح هذا الأمر محور اهتمام المنظمات الدولية والإقليمية على حد سواء، وفي مرحلة لاحقة بادرت الدول بما فيها الجزائر في وضع تشريعات شاملة لتنظيم هذه التقنية بشكل أكثر دقة وفعالية.

أ. التوقيع الالكتروني في قانون الأونسيترال:

1. مفهوم التوقيع الإلكتروني في قانون الأونسيترال النموذجي بشأن التجارة الالكترونية:

كانت الخطوة الاولى الفعلية لميلاد التوقيع الإلكتروني تشريعيا هي صدور القانون النموذجي الأونسيترال للتجارة الالكترونية الدولية لسنة 1996 [2] وقد عرف التوقيع في المادة السابعة منه على أنه: "عندما يشترط القانون وجود توقيع من شخص يستوفى ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

(أ) استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات، و

(ب) كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق متصل بالأمر."

تشير هذه المادة إلى أهمية أن يحمل التوقيع الإلكتروني نفس الوظائف التقليدية للتوقيع الورقي، والتي تشمل تحديد هوية الشخص وتعبيره عن موافقته في العمل القانوني، وفقاً لما هو موضح في الفقرة (أ). بالإضافة إلى ذلك، يجب أن تكون طريقة التوقيع الإلكتروني المستخدمة في الفقرة (ب) موثوقة.

---

[1]–علاء محمد نصيرات، **حجية التوقيع الالكتروني في الاثبات –دراسة مقارنة–** ،دار الثقافة للنشر والتوزيع، الطبعة الأولى ،عمان ،2005 ، ص 30.

[2] -UNCITRAL model Law on electronic commerce with guide to enactment adopted décembre 16 ,1996, with additional article 5 bis as adopted in 1998, Posted on the site https://uncitral.un.org .

2-تعريف التوقيع الالكتروني حسب ما جاء به قانون الأونسيترال بشأن التوقيعات الإلكترونية.

وعملت لجنة الأمم المتحدة للتجارة الالكترونية في دورتها الرابعة والثلاثين على استحداث قانون الأونسيترال النموذجي المتعلق بالتوقيعات الالكترونية في يونيو 2001 تضمن هذا القانون 12 مادة، ورد في المادة الثانية الفقرة (أ) تعريف التوقيع الالكتروني[1] بأنه "يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقته على المعلومات الواردة في رسالة البيانات".

من خلال هذا التعريف يتبادر إلى الذهن أن قانون الأونسيترال النموذجي يستند على الجانب غير المادي لرسالة البيانات وعلى دور التوقيع، كما أنه لم يُحدد بدقة كيفية استخدام التوقيع الإلكتروني، مما يسمح بفتح المجال أمام اعتماد أي تقنية معلوماتية تقوم بتوليد التوقيع الإلكتروني.

ب- تعريف التوقيع الإلكتروني في توجيهات الاتحاد الأوروبي:

بدراسة عميقة للواقع القانوني والتحديات الناشئة من تطور التكنولوجيا، أدركت المجموعة الأوروبية وهيئاتها أن الاهتمام الجاد بتطوير القوانين ضروري لمواكبة التحولات الرقمية الحديثة، لذلك ركزت على تعزيز التنسيق بين التشريعات الدولية للدول الأعضاء، مدركة تباين الأسس والمعايير القانونية بينها، وعلى وعي بأن تحقيق التوافق بين هذه التشريعات يسهم بشكل كبير في بناء بيئة أكثر أمانًا وثقة داخل السوق الأوروبية، التي تعتبر الثقة في أمان العمليات الإلكترونية أمرًا حاسمًا لاستقرارها وازدهارها المستقبلي.[2]

لذلك أصدر الاتحاد الأوروبي التوجيه رقم 1999-93 الصادر عن البرلمان الأوروبي في 13 ديسمبر 1999 المتعلق بالتوقيعات الإلكترونية[3] حيث جاء في المادة الثانية منه

[1] -UNCITRAL Model Law on Electronic Signatures of the United Nations Commission on International Trade Law with guide to enactment 2001, posted on the site https://uncitral.un.org .

[2]- ثروت عبد الحميد، مرجع سابق، ص157

[3]-DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community Framework for electronic signatures, posted on the site Https://eur-lex.europa.eu.

تعريف التوقيع الإلكتروني على أنه:" يعني بيانات في شكل إلكتروني هي ملحقة مرتبطة منطقيا بغيرها من البيانات الإلكترونية والتي تكون بمثابة طريقة للمصادقة ".

كما أضافت المادة نفسها في الفقرة الثانية ان التوقيع الإلكتروني المتقدم يعني التوقيع الإلكتروني الذي يستوفي المتطلبات التالية:

أ- أن يكون مرتبطا بالموقع حصرا،

ب- أن يتمكن من التعرف على الموقع،

ج- أن يتم إنشاؤه باستخدام وسائل يمكن للموقع أن يحتفظ بها تحت سيطرته وحده،

د- أن يكون مرتبطا بالبيانات التي تتعلق به بحيث يمكن اكتشاف أي تعديل لاحق للبيانات.[1]

جـ-تعريف التوقيع الإلكتروني في القانون الجزائري.

أدرك المشرع الجزائري أهمية التوقيع الإلكتروني في سياق التحولات الرقمية والتطورات الاقتصادية على الصعيدين الوطني والدولي، فتم تعديل القانون المدني بموجب القانون رقم 05-10 المؤرخ في 20 جويلية 2005 [2]حيث يعد هذا التحديث أحد أبرز الخطوات التشريعية التي أدخلت تعديلات وتحديثات هامة على القانون المدني الجزائري، ومن بين هذه التعديلات جاءت المواد التي تتعلق بالكتابة الإلكترونية والتوقيع الإلكتروني، حيث تم تنظيمها بشكل جديد ومحدث ليتناسب مع الواقع الحديث واعتماد التكنولوجيا في العمل القانوني.

حيث نصت المادة 323 مكرر المستحدثة على ما يلي: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت

[1]Art 2"-Advanced electronic signature' means an electronic signature which meets the Following requirements :

(a) It is uniquely linked to the signatory ;

(b) It is capable of identifying the signatory ;

(c) It is created using means that the signatory can maintain under his sole control ; and

(d) It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. "

[2]-قانون رقم 05-10 مؤرخ في 20 جويلية 2005 المعدل والمتمم للأمر رقم 75/58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني المعدل والمتمم المنشور في الجريدة الرسمية للجمهورية الجزائرية، عدد 44 ، لسنة2005.

الوسيلة التي تتضمنها وطرق إرسالها" وأضافت المادة 323 مكرر 1 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".

أما بخصوص التوقيع الإلكتروني فإنه يمكن القول أن التشريع الجزائري استعمل هذا المصطلح لأول مرة في أحكام المادة02/327 من القانون 05-10 التي تنص " يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر 1".

ومن ثم يظهر أن المشرع الجزائري في هذا السياق لم يقدم تعريفا صريحا للتوقيع الالكتروني ويقر به بدلا من ذلك شريطة استيفائه شروط محددة، هذه الشروط تشمل إمكانية التحقق من هوية الشخص الموقع بشكل قاطع وذلك لمنع الغش والاحتيال بالإضافة لحفظ التوقيع الالكتروني بطريقة تكفل سلامته من أي تلاعب او تغيير لضمان صحة البيانات الموقعة.

وتم التصدي لهذا الأمر عندما أصدر المشرع الجزائري المرسوم التنفيذي رقم 162/07 لسنة 2007 [1] فعرف التوقيع الالكتروني في نص المادة الثالثة منه انه «**التوقيع الالكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 1 من الامر 75 -58 المؤرخ في 20 رمضان 1395 الموافق ل 26 سبتمبر 1975 والمذكور أعلاه**».

إضافة إلى الفقرة (2) من المادة (03) من المرسوم السابق الذكر، تضمنت التوقيع المؤمن وعرفته على أنه: «توقيع إلكتروني يفي بالمتطلبات الآتية:

-يكون خاصا بالموقع.

- أن يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت رقابته الحصرية.

- يضمن مع الفعل المرتبط به صلة، بحيث يكون كل تعديل لاحق للفعل قابل للكشف عنه».

[1]-المرسوم التنفيذي رقم 07-162 مؤرخ في 13 جمادى الاولى 1428 الموافق ل 30 ماي 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 مؤرخ في 15 صفر 1422 الموافق ل 9 ماي 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادر في 7 جوان 2007.

وصولا الى تعريف المشرع الجزائري للتوقيع الإلكتروني في قانون خاص رقم 15- 04 المتعلق بالتوقيع والتصديق الالكترونيين[1] بصورة صريحة حيث يعرف التوقيع الإلكتروني العادي في المادة 2 الفقرة 1 من القانون 15- 04 بأنه " بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".

في حين عرفت المادة 7 التوقيع الالكتروني الموصوف بأنه: " التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.
- أن يرتبط بالموقع دون سواه.
- أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.
- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات."

من خلال النظر إلى مجموعة التعاريف المتعلقة بالتوقيع الإلكتروني في مختلف القوانين، يمكن أن نلمح الى وجود وحدة في المضمون والغاية من هذه التشريعات، على الرغم من اختلافات الصياغة الشكلية، فقد تختلف العبارات المستخدمة في التعريفات المختلفة، لكن الفكرة الأساسية والمضمون العام يبقى واضحًا ومتجانسًا.

بالتالي يتبين أن توحيد المضمون رغم اختلاف الصياغة يعكس استناد القوانين المختلفة إلى معايير ومبادئ مشتركة، مما يسهم في تعزيز الثقة في التوقيع الإلكتروني وتسهيل استخدامه بين الأطراف المختلفة في العلاقات التجارية والقانونية.

الفرع الثاني: خصائص التوقيع الإلكتروني وصوره.

من خلال التعاريف السابقة للتوقيع الالكتروني سواء كانت فقهية او قانونية يلاحظ ان للتوقيع الالكتروني خصائص وصور تميزه عن غيره من التوقيعات العادية أو التقليدية لذلك سنتناول بالدراسة خصائص التوقيع الالكتروني ومن ثم صوره.

[1]–قانون رقم 15-04 مؤرخ في 1 فيفري 2015 يحدد القواعد العامة للتوقيع والتصديق الالكترونيين، الجريدة الرسمية للجمهورية الجزائرية ،العدد 06 ،صادر في 10/02/2015.

أولا: خصائص التوقيع الالكتروني.

يتمتع التوقيع الالكتروني بجملة من الخصائص نذكر منها:

1. يوفر الخصوصية: تحقيق الحماية للبيانات ينطوي على منع الاستخدام غير المشروع، من خلال تحديد صلاحيات الوصول للبيانات ومنع الأفراد الذين لا يمتلكون الصلاحيات الكافية من تنفيذ أي إجراء عليها، ويتم ذلك بتنشيط صلاحيات الوصول أثناء حفظ بيانات التوقيع الإلكتروني على البطاقة الذكية، والتي تظل محمية برقم سري، ويُعتبر هذا التوقيع الإلكتروني ميزة تهدف إلى التأكد من أن الشخص المعني هو الوحيد الذي يمكنه الوصول إلى الوثيقة المرسلة.[1]

2. عدم القدرة على الانكار: يتناول هذا المفهوم عدم قدرة الأفراد على نفي تفاعلاتهم عبر الإنترنت، سواء كانوا مرسلين أو متلقين نظرًا لوجود جهة ثالثة قادرة على إثبات تنفيذ فعل إلكتروني محدد من جانب أحد الأطراف، بالإضافة إلى ذلك يعزى هذا العجز أيضًا إلى تعذر إنكار متلقي الرسالة لاستلامها، حيث يُثبت المفتاح العام عملية الاستلام من قِبل المتلقي من خلال إرسال رد يُفيد بوصولها مما يُظهر الالتزام بالتفاعل، هكذا يُحقق مفهوم عدم الانكار حماية فعّالة للوثائق والعقود الإلكترونية، حيث يتيح التأكد من نزاهة العمليات الرقمية ويعزز الثقة بين الأطراف المعنية، مما يُسهم في ترسيخ الأساس لبيئة رقمية موثوقة ومأمونة.[2]

3. يوفر وحدة البيانات والسرعة والدقة في إنجاز المعاملات: توفير وحدة البيانات بواسطة التوقيع الإلكتروني يعني تأمين البيانات ضد التلاعب أو الاستبدال بواسطة بيانات أخرى، حيث يتم ذلك من خلال تقنيات تشفير البيانات ومقارنة بصمة الرسالة المرسلة ببصمة الرسالة المستقبلة الامر الذي يُمكن مستقبل الرسالة من اكتشاف أي تغيير أو تعديل على المستند أثناء الإرسال، مما يحول دون التزوير.

---

[1]-راضيه لالوش، **أمن التوقيع الالكتروني**، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعات مولود معمري –تيزي وزو– ،2012، ص 36.

[2]-فراح مناني، **العقد الالكتروني وسيلة إثبات حديثة في القانون المدني الجزائري**، دار الهدى للطباعة والنشر والتوزيع، دوم طبعة، عين مليلة –الجزائر–، 2009 ص 196.

فيما يتعلق بسرعة ودقة إنجاز المعاملات يساهم التوقيع الإلكتروني بشكل فعّال في زيادة سرعة المعاملات الإلكترونية وتحسين دقتها، كما يقلل من التأخير المحتمل في إرسال واستلام العقود والوثائق التجارية وغيرها، مما يعزز التفاعل الفوري عبر الإنترنت.[1]

ثانيا: صور التوقيع الالكتروني.

يأتي التوقيع الالكتروني في العديد من الصور والاشكال بما في ذلك التوقيع القائم على الرقم السري، التوقيع بالرقم الالكتروني، التوقيع البيو متري، التوقيع الرقمي، وهذه الصور تعتبر الأكثر شيوعا واستخداما وقد جاءت على سبيل المثال وليس على سبيل الحصر، أي كأمثلة لتمهيد الطريق لظهور أنواع اخرى من التوقيعات الإلكتروني في المستقبل وليس حصريا.

أ-التوقيع باستخدام البطاقة الممغنطة مع الرقم السري:

كانت التوقيعات التي تستخدم البطاقات الممغنطة مع الرقم السري هي الشكل الأول والأكثر شيوعا لتقنية التوقيع الإلكتروني، وقد استحدث هذا الشكل من أشكال التوقيع الإلكتروني بواسطة التكنولوجيا المستخدمة لتسريع إنجاز المعاملات المصرفية، تصدرت البنوك بطاقات إلكترونية مزودة بأرقام سرية وتمنحها للعملاء لسحب وإيداع الأموال ودفع تكاليف السلع والخدمات وغيرها.[2]

والتطبيق العملي لهذا التوقيع، المعاملات التي تتم من خلال أحد البنوك حيث يتم وضع البطاقة في المنطقة المخصصة في ماكينة الصراف الالي ويتم ادخال الرقم السري لحامل البطاقة والضغط على زر التفويض على مفتاح الصراف الالي لإتمام المعاملة مما يسمح للعميل بسحب اي مبلغ من الرصيد في الوقت المطلوب، وبمجرد اكتمال اجراء السحب تصدر ماكينة الصراف الالي شريطا ورقيا للعميل يحمل تفاصيل دقيقة حول المبلغ

[1]-فتيحة حواس، **(توقيع الالكتروني -الخصوصيات والتطبيقات-)**، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص المقارن بكلية الحقوق والعلوم السياسية، جامعة حاسي باب بن بوعلي -الشلف-، المجلد 07، العدد 1، جوان 2021، ص 2993.

[2] -عيسى غسان ربضي، مرجع سابق، ص 58.

المسحوب والوقت والرصيد المتبقي. وتحل هذه الاجراءات محل التوقيع التقليدي نظرا لموثقتيها وامانها ولتمييزها لحامل البطاقة.[1]

وتعتمد أجهزة الصراف الآلي على نظامين أساسيين، الأول هو بنظام الدفع غير المباشر **(off-line)** عند استخدام هذا النظام تسجل العملية التي أجراها العميل على شريط مغناطيسي ويظل موقف العميل دون تحديث حتى يتم توثيقها من قبل موظف البنك عند نهاية ساعات العمل الرسمية ليتم تسجيل العملية على سجلات البنك، أما النظام الثاني فيعرف بنظام الدفع المباشر **(on-line)** حيث يتم تحديث الحالة المالية للعميل فور اتمام المعاملة ؛ ويشترط الجانب القانوني في الرقم السري الخاص بالعميل، ان يُعد ويُسلم بطريقة محكمة وسرية للعميل حصراً، وفي حالة فقدان البطاقة أو سرقتها، أو نسيان الرقم السري ، يتم تجميد جميع العمليات المرتبطة بالبطاقة بمجرد إخطار البنك بهذا الشأن، الامر الذي يضفي على هذا الشكل من اشكال التوقيع الالكتروني مستوى عالي من الامن والثقة.[2]

ب- التوقيع بالقلم الإلكتروني:

يتم تنفيذ هذه العملية من خلال توقيع الشخص نفسه الذي يقوم بنقل المستند يدويًا إلى جهاز الماسح الضوئي، يقوم هذا الاخير بقراءة التوقيع والتقاط صورة له، مما يحوله إلى مجموعة رسوم بيانية يتم حفظها داخل الكمبيوتر، يتحول التوقيع بعد ذلك إلى توقيع إلكتروني يمكن إضافته إلى المستند المراد التوقيع عليه، وقد تم تحسين هذا النوع من التوقيع باستخدام قلم إلكتروني حسابي، حيث يمكن للشخص كتابة التوقيع على شاشة الحاسوب باستخدام برنامج مخصص، يقوم البرنامج بالتقاط التوقيع والتحقق من صحته مما يتيح قبوله إذا كان صحيحًا ورفضه إذا لم يكن كذلك.[3]

ج- التوقيع البيو متري:

يمثل التوقيع البيو متري أسلوب من أساليب التعرف على الشخصيات البشرية، حيث يعتمد على الخصائص الفريدة والمميزة لكل شخص، ويقوم العلم بيوميترولوجي (علم

---

[1]-عائشة قصر الليل، مرجع سابق، ص 104.

[2]- عيسى غسان ربضي، مرجع سابق، ص 59.

[3]- نجوى سديرة، **(الحماية القانونية للتوقيع الالكتروني كآلية لتدعيم الثقة في المعاملات الالكترونية عبر الانترنت)**، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس -المدية-، المجلد 08، العدد 2، جوان 2022 ص 338.

القياسات الحيوية) بدراسة السمات المميزة لكل شخص مثل بصمات الأصابع ومسح شبكية العين، نغمة الصوت، بصمة الشفاه، الحمض النووي الجيني، ملامح اليد البشرية، وتشمل كذلك تحليل الخصائص الشخصية في مظهر اليد الخارجي مثل درجة ضغط القلم ومقدار الاهتزاز الذي تحدثه اليد أثناء الكتابة بالإضافة الى تحليل بداية الحروف ونهايتها ومختلف جوانب الكتابة، هذه الخصائص البيومترية تساعد في تمييز هوية الأفراد بشكل دقيق وموثوق به، مما يجعل التوقيع البيومتري أداة فعالة في مجالات متعددة مثل الأمن والمراقبة والتحقيقات الجنائية.[1]

والجدير بالذكر أن المشرع الجزائري أصدر قرارا في 19 يوليو 2010 يقضي بشمول إصدار جوازات السفر البيومترية، واعتماد هذا النوع من التوقيع، استجابة لدعوة المنظمة الدولية للطيران لإصدار جوازات السفر البيو مترية، وبالإضافة إلى ذلك اعتمد المشرع الجزائري هذا النوع من التوقيع للتوقيع على بطاقات التعريف الوطنية البيومترية ورخص القيادة البيومترية للاستفادة من قدرة التكنولوجيا على تحديد الهوية المكانية من خلال الخصائص الطبيعية والفزيائية.[2]

د- التوقيع الرقمي:

التوقيع الرقمي يعتبر وسيلة فعالة في إبرام التصرفات القانونية عبر وسائل الاتصال الإلكترونية لاسيما عبر شبكة الإنترنت، يقوم هذا النوع من التوقيع على استخدام أنظمة تشفير متطورة ومن هنا جاء لقب "التوقيع الرقمي" وهو معروف على نطاق واسع بمستوى الأمان والثقة الفائقين اللذين يوفرهما، وحظي باعتراف دولي على نطاق واسع، ويتكامل نظام تشفيره مع تحويل بيانات المحرر الإلكتروني إلى صيغة غير قابلة للقراءة حتى لا يتمكن الغير من استخدامه، ويعود إلى صيغته الأصلية في حالة استخدامه من قبل الموقع، ويعزز بعملية حسابية دقيقة يمكن أن تكون هذه العملية تماثلية باستخدام مفتاح واحد أو غير متماثلة بالاعتماد على التشفير بالمفتاح المزدوج.[3]

---

[1]- عبد القادر بوهنتالة، **حجية التوقيع الالكتروني في التشريع الجزائري**، أطروحة مقدمة لنيل درجة الدكتوراه العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر -باتنة-، 2016، ص61.

[2]- عبد القادر بوهنتالة، مرجع سابق، ص 63.

[3]- عيسى غسان ربضي، مرجع سابق، ص66.

التشفير المتماثل يتجلى في فكرة تبادل رقم سري بين الطرفين، حيث يظل هذا الرمز محفوظًا لكل منهما، ويعمل في بيئة منفصلة مثل نظام التلكس واستخدام البطاقات البلاستيكية، حيث يكون الرقم السري معروفًا فقط لصاحبه والجهاز؛ في المقابل يرتقي عالم التشفير غير المتماثل إلى آفاق جديدة من الأمان، باعتماد زوج المفاتيح المفتاح العام يكون معروفًا للجميع، ومفتاح خاص يكون فقط لصاحبه، يجب على صاحب المفتاح الخاص الاحتفاظ به بسرية، ومن خلاله يمكنه تشفير رسالته بشكل فريد، هذا النظام يمتاز بعدم إمكانية استنتاج المفتاح الخاص من المفتاح العام وبأن كل مفتاح يقوم بعكس عمل الآخر، مما يعني أن ما يشفره المفتاح الأول يمكن فقط فك تشفيره بواسطة المفتاح الثاني مما يجسد تقنية متطورة تعزز من أمان البيانات بشكل استثنائي.[1]

المطلب الثاني: شروط التوقيع الالكتروني والتصديق عليه.

تشترط معظم تشريعات الدول التي اعتمدت التوقيع الالكتروني ومنحته القوة الثبوتية ومن بينها الجزائر على الزامية تلبية مجموعة من الشروط بهدف موثوقية هذا النوع من التواقيع وضمان صحة الوثائق التي تحمله؛ ومع التطور التكنولوجي الحديث أصبحت اغلب المعاملات تجرى على شبكة الانترنت، حيث تكون العقود التي تبرم عبرها غالبا بين أطراف بعيدة المسافة، الامر الذي يستدعي وجود جهة ثالثة موثوقة لتوثيق المعاملات و التأكد من هوية الأطراف و صحة توقيعاتهم الإلكترونية ،حيث يعتبر وجود جهة تصديق الكترونية ذات مصداقية امرا حاسما لتعزيز الثقة في عمليات التوقيع الالكتروني.

الفرع الأول: شروط التوقيع الالكتروني.

استنادا الى القانون 15-04 نلاحظ ان المشرع الجزائري أهتم بنوعين من التوقيعات الالكترونية، التوقيع الإلكتروني البسيط او العادي والتوقيع الإلكتروني الموصوف وقد اعتمد في بيان شروط التوقيع الإلكتروني على تحديد المعايير الضرورية لصحة التوقيع الإلكتروني الموصوف، عددتها المادة 7 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، وفيما يلي سنتناول مسالة تعدادها مع بعض التفصيل.

أولا: ان يرتبط بالموقّع دون سواه.

[1]- علاء محمد نصيرات، مرجع سابق، ص 37.

وفقا لنص المادة 2 من القانون رقم 15-04، يُفهم من مصطلح "الموقع" «شخص طبيعي يحوز بيانات إنشاء التوقيع الالكتروني ويتصرف لحسابه الخاص او لحساب الشخص الطبيعي او المعنوي الذي يمثله».

يُشدد هذا الشرط على أهمية أن يكون التوقيع مرتبطًا بالموقع بشكل حصري، مما يعني وجود رابط دائم وفعّال يربط التوقيع الإلكتروني بالهوية الفردية للشخص، وهو الأمر الذي يضفي النزاهة للمحرر الإلكتروني وحمايته من المخاطر التي تحيط به أثناء الإرسال عبر شبكة الإنترنت، وتأكيدًا على أهمية السيطرة الحصرية للموقع على التوقيع، يبرز دورها في حماية المحتوى من الوصول غير المخول أو التعديلات غير المرغوب فيها من طرف شخص آخر غير الطرف المتعاقد.[1]

ثانيا: أن يمكن من تحديد هوية الموقع.

أصبح تحديد هوية الموقع ممكنًا من خلال استخدام التوقيع الإلكتروني، وتأكيد هذا الأمر يأتي من نص المادة 06 في القانون 15-04 التي تنص بأن "يستعمل التوقيع الالكتروني لتوثيق هوية الموقع، وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني". هذا يعني أن التوقيع الإلكتروني هو علامة خاصة للشخص الموقع، تميزه عن الآخرين وتحدد هويته بشكل فعّال.

وبناءً على ذلك يتطلب هذا الشرط أن يمكن للتوقيع الإلكتروني التعرف على شخصية الموقع، على غرار التوقيع التقليدي الذي يمكن أن يتضمن أشكالًا مثل الختم والبصمة والتوقيع، والتي تشير إلى شخصية مالكها، وبالتالي يجب أن يحدد التوقيع الإلكتروني هوية الموقع على الرسالة الإلكترونية، حتى لو لم يكن يحتوي على اسم الموقع ويمكن القيام بذلك عبر الرجوع إلى جهات إصدار التوقيعات الإلكترونية التي تشهد على هوية المستخدم، فعلى سبيل المثال يحدد التوقيع الرقمي شخصية الموقع لأنه يعود إليه، ويعبر عن اختياره الشخصي لهذا الشكل ليعبر عن هويته.[2]

---

[1]- فاطمة الزهراء تبوب، **(التوقيع والتصديق الالكترونيين في ظل القانون رقم 15- 04 المؤرخ في أول فبراير 2015)**، مجلة حوليات، جامعة الجزائر 1، العدد 29، الجزء الثاني جوان 2016 ص 315.

[2]- لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، دار الثقافة والنشر والتوزيع، الطبعة 1، عمان، 2009، ص 103.

ثالثا: أن يكون مصمّما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

تناول المشرع الجزائري في المادة 2 ف 4 من القانون 15-04 آلية إنشاء التوقيع الإلكتروني، حيث يُمكن أن يتجلى هذا على شكل جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني، ولضمان تصميم هذا التوقيع الإلكتروني بشكل احترافي، يجب اللجوء إلى آلية إنشاء مؤمنة وفقًا لما جاء في أحكام المادة 10 من القانون رقم 04-15 حيث تنص على ضرورة أن تكون الآلية المستخدمة في إنشاء التوقيع الإلكتروني مؤمنة، حسبما نصت المادة 11 التي توضح المعايير اللازمة لتحقيق هذه الموثوقية، وتفرض ان تتوفر فيها متطلبات الآتية:

1- يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ – ألاّ يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرّة واحدة وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد،

ب – ألاّ يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد،

ج – أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين،

2 – يجب ألا تُعدّل البيانات محل التوقيع وألا تمنع أن تعرض هذه البيانات على الموقّع قبل عملية التوقيع.

رابعا: أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقّع.

هذا الشرط يتطلب سيطرة صاحب التوقيع على منظومة التوقيع، سواء كان ذلك أثناء استخدامه أو أثناء إنشائه. وفي هذا السياق، ينص القانون الجزائري بوضوح في المادة 7 فقرة 5 من القانون 04/15 على أن يتم إنشاء التوقيع بواسطة وسائل تكون تحت التحكم الحصري للموقع.

ولضمان فعالية السيطرة على هذا الأمر ينبغي أن تظل عملية توقيع الوثائق سرية تمامًا، حيث يجب ألا يكون هناك إفصاح لأي شخص آخر بخصوص تلك العملية، يأتي ذلك من أجل تجنب إساءة استخدامها من جانب اي جهة اخرى، خاصةً أن توقيع الوثائق

يحمل تبعات قانونية لها تأثير على حقوق الموقع وحقوق الأطراف الأخرى؛ ومن الجانب التقني يتحقق التحكم الكامل والسيطرة عبر الموقع الإلكتروني من خلال حيازته على أداة حفظ المفتاح الشخصي للتوقيع الإلكتروني، تتضمن هذه الأداة بطاقة ذكية مؤمنة والرقم السري المرتبط بها، وذلك لتعزيز الأمان ومنع الوصول غير المصرح به للوثائق الحساسة.[1]

خامسا: أن يكون مرتبط بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

ان تأكيد سلامة المضمون الإلكتروني يشكل ركيزة أساسية للبنية الأمنية والثقة، خاصة في غياب تاريخ تفاعل أو ترابط بين الأطراف والمتعاملين في ساحة التكنولوجيا الحديثة وشبكة الإنترنت، وفي سعينا لتحقيق هذه الثقة، يظهر أن توفير بيئة إلكترونية آمنة يكون له أهمية خاصة، وهي ذات أهمية استثنائية خصوصا في ميدان التجارة الإلكترونية؛ وتعتبر هذه الحاجة أمرًا لا غنى عنه، حيث يفوق نطاق الاعتماد على صحة وسلامة إجراءات التوقيع الإلكتروني بحد ذاته، بل يتطلب الأمر التحقق من عدم تلاعب أو تعديل أو استبدال التوقيع الإلكتروني، ولتحقيق هذا الهدف يلزم استخدام برمجيات متقدمة تتيح اكتشاف أية تعديلات، حيث يمكن لأي تعديل يمس التوقيع أو محتوى الرسالة الموقعة أن يؤدي إلى تقليل قيمته القانونية، ويجعله غير صالح للاعتماد القانوني.[2]

وفضلا عن الشروط التي سبق ذكرها لضمان صحة وموثوقية التوقيع الإلكتروني تنص المادة 7 فقرة 1 على أن صحة التوقيع الإلكتروني تستند إلى تأسيسه على أساس شهادة التصديق الإلكتروني الموصوفة، سيتم استعراض وشرح هذا الجانب بدقة في العناوين القادمة.

الفرع الثاني: التصديق الالكتروني.

تظهر الحاجة الملحة لتأمين البيانات الشخصية والمعاملات الإلكترونية المتعلقة بمختلف المعاملات التي تجرى عبر الإنترنت، ويتم تحقيق هذا من خلال إشراك جهة ثالثة

---

[1]– عزالدين منصور، **حجية التوقيع الإلكتروني في الإثبات**، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر –بسكرة–، 2016 ، ص 40.

[2]– خلود حملاوي، نورة بركاوي، **التوقيع الإلكتروني وحجيته في الإثبات**، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر في القانون، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 –قالمة–،2020 ، ص 94.

خارجة عن أطراف العقد، حيث يُكلَّف بتوثيق البيانات والتحقق من التوقيع الإلكتروني، دون تورطه في مصالح شخصية تتعلق بهذه البيانات يُعرف هذا الدور بمقدم خدمات التصديق الإلكتروني، الذي يضمن النزاهة والتأكد من صحة وسلامة التوقيع الإلكتروني.

أولا: تعريف التصديق الالكتروني.

عند الحديث عن التصديق الإلكتروني، نقصد عملية ذات أهمية كبيرة تقوم على أساس التحقق من صحة الكتابة والتوقيع الالكترونيين؛ يتم هذا الإجراء عن طريق جهة تصديق يطلق عليها اسم "مقدم خدمات التصديق" أو "مؤدي خدمات التصديق" أو ببساطة "جهة التصديق"، ينبغي أن تكون هذه الهيئة مستقلة اي غير مرتبطة بأطراف العقد الإلكتروني لضمان الحياد والموضوعية،[1] ويتيح هذا النهج للأطراف المتعاقدة الثقة في الصحة الكاملة للوثائق والتوقيعات الإلكترونية، مما يساهم في تحقيق الأمن والثقة في بيئة الأعمال الإلكترونية.

وبالرجوع للمشرع الجزائري نجده لم يتطرق إلى تعريف التصديق الإلكتروني واكتفى باستعمال مصطلح "سياسة التصديق" وذلك في الفقرة 15 من المادة 2 من القانون15-04 المتعلق بالتصديق والتوقيع الالكترونيين والتي عرفها بأنها: "مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الالكترونيين".

ثانيا: جهات التصديق الالكتروني.

وقد تناول المشرع الجزائري موضوع خدمات التصديق الإلكتروني في مختلف القوانين والمراسيم منها المرسوم رقم 162/07 لسنة 2007 تحدد المادة 03 منه مؤدي خدمات التصديق بأنهم الأفراد الذين يقومون بتسليم الشهادات الإلكترونية أو غيرها من الخدمات المتعلقة بالتوقيعات الإلكترونية، وهذا يسلط الضوء على نطاق الأفراد المشاركين في تقديم مثل هذه الخدمات في المجال الإلكتروني، علاوة على ذلك تحدد الفقرة 8 من المادة 8 من القانون رقم2000-03 [2] مقدم الخدمة بأنه أي شخص اعتباري أو طبيعي يقدم الخدمات

---

[1]– آمنة كبير، (**التصديق الالكتروني – دراسة مقارنة–**)، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية –أدرار–، المجلد 06، العدد 01، ص 135.

[2]–قانون رقم 2000 –03، مؤرخ في خمسة جمادى الاولى 1421 الموافق لـ 5 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية، العدد 48 لسنة 2000.

من خلال قنوات الاتصال السلكية واللاسلكية يشكل هذا التعريف الأوسع نطاقًا واسعًا من مقدمي الخدمات الذين يستخدمون طرق اتصال مختلفة.

علاوة على ذلك، فإن القانون رقم 15-04 لسنة 2015، وتحديدا في الفقرة 12 من المادة 02 يحدد مقدمي خدمات التصديق على انه "مؤدي خدمات التصديق الالكتروني كل شخص طبيعي او معنوي يقوم بمنح شهادات تصديق الكترونية موصوفة، وقد يقدم شهادات أخرى في مجال التصديق الالكتروني".

وفي هذا الإطار نص المشرع الجزائري على ضرورة الحصول على ترخيص تمنحه السلطة الاقتصادية للتصديق الالكتروني لممارسة نشاط التصديق الإلكتروني في المادة 33 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، التي تنص " يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني."

كما ألزم المشرع طالب الترخيص بموجب نفس القانون بمجموعة من الشروط الفنية والتقنية كأن يكون خاضع للقانون الجزائري في حالة ما إذا كان شخص معنوي او يتمتع بالجنسية الجزائرية إذا كان شخص طبيعي أو التمتع بقدرة مالية كافية ومؤهلات وخبرة ثابتة في ميدان تكنولوجيا الاعلام والاتصال للشخص الطبيعي أو المسير لمشخص المعنوي وألا يكون قد سبق الحكم عليه في جناية او جنحة تتنافى مع نشاط خدمات التصديق الالكتروني.[1]

ثالثا: شهادة التصديق الالكتروني.

قام المشرع الجزائري بالتمييز بين الشهادة الالكترونية البسيطة والشهادة الالكترونية الموصوفة، حيث ورد وصف الاولى في المادة 2 فقرة 7 من القانون 15-04 بانها وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التوقيع الإلكتروني والموقع اما الشهادة الثانية فقد عرفها في المادة 15 على انها "شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

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

[1]-المادة 34 من القانون 15-04.

2 – أن تمنح للموقّع دون سواه،

3 – يجب أن تتضمن على الخصوص:

أ – إشارة تدلّ على أنه منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصفة.

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

ج – اسم الموقّع أو الاسم المستعار الذي يسمح بتحديد هويته،

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

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

و– الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني،

ز– رمز تعريف شهادة التصديق الإلكتروني،

ح – التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني،

ط – حدود استعمال شهادة التصديق الإلكتروني عند الاقتضاء،

ي – حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني عند الاقتضاء،

ك – الإشارة إلى الوثيقة التي تثبت تثيل شخص طبيعي أو معنوي آخر عند الاقتضاء."

المبحث الثاني: تجريم المساس بالتوقيع الالكتروني.

أصبح التوقيع الإلكتروني تدبيرا أساسيا من تدابير الحماية المدنية لمختلف المعاملات التي تتم إلكترونيا ويتطلب الانتقال التدريجي إلى التوقيعات الإلكترونية وقبولها وجود أطر تنظيمية تكفل القواعد والشروط اللازمة لصحتها وحمايتها من التلاعب بها، ومن الوصول إليها دون إذن لأغراض إجرامية، خاصة وأن المجرمين يطورون باستمرار تقنياتهم وجرائمهم جنبا إلى جنب مع تقدم تكنولوجي، وهذا يتيح لهم استغلال مواطن الضعف وارتكاب الجرائم. ونتيجة لذلك، ظهرت أشكال جديدة من الجرائم في البيئة الرقمية، ارتُكبت بالوسائل الإلكترونية، المعروفة بجرائم الفضاء الحاسوبي أو جرائم المعلومات؛ ولذلك من الضروري وضع لوائح قانونية تضمن سلامة التوقيعات الإلكترونية وأمنها ومصداقيتها، لضمان حماية جميع الأطراف المشاركة في المعاملات الإلكترونية.[1]

المطلب الأول: مفهوم جرائم الاعتداء على التوقيع الالكتروني.

في معظم القوانين، يُعتبر التوقيع الإلكتروني جزءًا من المعاملات القانونية عندما يتم استخدامه بطريقة صحيحة وموثوقة، ولكن استخدامه بشكل غير قانوني والجرائم التي تقع عليه تندرج ضمن الإطار الواسع للجرائم المعلوماتية أو جرائم التكنولوجيا الحديثة، لأنها تنطوي على استعمال التكنولوجيا الرقمية للقيام بأعمال غير قانونية تنتهك سلامة وأمن البيانات الالكترونية.

الفرع الأول: تعريف جرائم الاعتداء على التوقيع الالكتروني.

تعرف الجريمة بشكل عام في إطار القانون الجنائي على أنها كل فعل غير قانوني ينبع من إرادة جنائية، وله عقوبة محددة بموجب القانون.[2]

وتندرج جرائم التوقيع الإلكتروني ضمن فئة الجرائم المعلوماتية التي يشير إليها المشرع الجزائري بالجرائم المتعلقة بتكنولوجيا المعلومات والاتصال، ويتم تعريفها طبقا لأحكام

[1]–راضيه لالوش، مرجع سابق، ص 132.

[2]–المرجع نفسه، ص 133.

المادة2 الفقرة أ من القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.[1]

وتعرف الفقرة الثانية من المادة الثانية من القانون 09-04 السالف الذكر المنظومة المعلوماتية انها «اي نظام منفصل او مجموعة من الأنظمة المتصلة ببعضها البعض او المرتبطة، يقوم واحد منها أو أكثر بمعالجة آليه للمعطيات تنفيذا لبرنامج معين».

وتجدر الإشارة إلى أنه نظرا لطبيعته المتقدمة وتطوره المستمر في مجال علوم الكمبيوتر، فإن مصطلح "نظام معالجة البيانات الآلي" يعتبر تعبيرا تقنيا يصعب على الممارسين القانونيين فهم معناه بسهولة.

ولم تحدث ما يسمى بالهجمات على أنظمة معالجة البيانات الآلية في النظام القانوني الوطني الا بعد تعديل القانون الجنائي على أساس القانون رقم 04-15 بتاريخ 10 نوفمبر 2004[2]، حيث استكمل المشرع الفصل الثالث من الباب الثاني من الكتاب الثالث بقسم جديد القسم السابع مكرر يتضمن المواد من 394 مكرر إلى 394 إلى 7، وانطلاقا من فحوى هذه المواد يمكن تعريف جرائم الاعتداء على التوقيع الالكتروني بانها " كل فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويكون محلها الاعتداء على التوقيع الالكتروني، اما بإتلافه أو استنساخه او تزويره أو تقليده او استعماله مزورا مع علم الجاني بذلك، أو إفساد بياناته أو استخدامها في غير الغرض المقدم من اجله ".[3]

[1]-قانون رقم 09 -04، مؤرخ في 14 شعبان عام 1930 الموافق ل 5 غشت سنة يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، لسنة 2009.

[2] -قانون رقم 04-15 مؤرخ في 10/11/2004 يعدل ويتمم الأمر رقم 66-156 مؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، لسنة 2004.

[3]-مصطفى صحراوي، **الحماية الجزائية للتوقيع والتصديق الالكترونيين في التشريع الجزائري**، أطروحة للحصول على شهادة الدكتوراه ل.م.د في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، 2021، ص48.

الفرع الثاني: خصائص جرائم الاعتداء على التوقيع الالكتروني.

يعد التطرق الى الخصائص الجوهرية التي تتصف بها جرائم الاعتداء على التوقيع الإلكتروني أمر بالغ الأهمية هو ما سيتم التطرق اليه على النحو الآتي:

أولا: الجاني في جرائم التوقيع الالكتروني.

الشخص الذي يرتكب جرائم التوقيع الإلكتروني هو أي فرد بغض النظر عن جنسه أو عمره، يقوم بأفعال متعمدة تجعل التكنولوجيا تلعب دورًا في ارتكاب جريمة تضر بحق أو مصلحة الآخرين، وما يميز الجاني هو قدرته على التكيف اجتماعيا، على عكس الجناة بالمفهوم التقليدي كمرتكبي الجرائم العنيفة الذين يعتبرون أعداء للمجتمع، هذا الامر يجعل الجاني أكثر خطورة حيث يبقى مخفيا كعضو صالح في المجتمع ويطور أساليب جديدة القيام بالجرائم.[1]

ونظرا لخصوصية هذه الجرائم وما تتميز به، فإنها تتطلب من الجاني أن يكون ملمًا بمستوى معين من المعرفة والخبرة في مجال تكنولوجيا المعلومات وعلوم الحاسوب، وتحديدا يتطلب الأمر وجود قدرة عقلية وذهنية متقدمة ومستوى عالٍ من الذكاء، حيث يعتمد الجاني بشكل رئيسي على مهاراته التقنية في استخدام أجهزة الحاسوب والتحكم بشكل متقن في البرمجيات وتلاعبها، دون اللجوء إلى العنف، وتأتي هذه الجرائم بغض النظر عن دوافعها وأهدافها المرجوة[2].

ثانيا: جرائم المساس بالتوقيع الالكتروني عابرة للحدود.

في العصر الحديث، لا توجد حواجز تقف أمام تدفق المعلومات بين الحسابات الآلية المنتشرة في مختلف أنحاء العالم عبر شبكات الاتصالات، يُمكن نقل كميات هائلة من البيانات بسرعة فائقة بين حساب وآخر حتى لو كانت المسافة بينهما تمتد عبر آلاف الكيلومترات في غضون ثوانٍ قليلة، فبفضل تطور شبكة الإنترنت، أصبح من الممكن ارتكاب الجرائم في دول معينة والتأثير على الضحية في دولة أخرى في فترة زمنية قصير

[1]–نسيمة جدي، **جرائم المساس بأنظمة المعالج الآلية للمعطيات**، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014، ص 28.

[2]–المرجع نفسه، ص 28

للغاية، ن دور شبكة الإنترنت أصبح أكثر أهمية مع مرور الوقت، مما يزيد من التحديات التي تواجه إدارة الأمن والحماية.[1]

ذلك أن قدرة تكنولوجيا على تقليص المسافات وتعزيز التواصل بين مختلف مناطق العالم، تأثرت طبيعة الأعمال الإجرامية حيث يقوم المجرمون بشكل متزايد باستخدام هذه التقنيات في انتهاك القوانين، هذا يعني أن ساحة الجريمة لم تعد محلية بل عالمية، ففي ظل عدم تواجد الجاني على مسرح الجريمة، وارتكابه للجريمة عن بُعد، هذا النوع من الجرائم يحتل مكانة متقدمة في المجتمع الإجرامي الحديث. [2]

ثالثا: صعوبة اكتشاف جرائم المساس بالتوقيع الالكتروني.

هذه الجرائم لأنها ذات طابع خفي اي تعتمد على التمويه والاختباء، مما يجعلها تحديًا كبيرًا للكشف عنها، يعود ذلك جزئياً إلى عدم ترك أثر خارجي واضح في الموقع، بالإضافة إلى قدرة الجاني على تدمير الأدلة بسرعة وفعالية، يشكل هذا التحدي تحدياً كبيراً أمام المحققين، حيث يحتاجون إلى استخدام أدوات فنية متقدمة للكشف عن هذه الجرائم وإثباتها، والتي تعتمد على التمويه والتضليل، في كل الأحوال يتطلب مواجهة هذا النوع من الجرائم خبرة فنية متخصصة وعالية المستوى في مجال التحقيقات الجنائية؛ ويتأثر اكتشاف جرائم الاعتداء على التوقيع الالكتروني وتحديدها بشكل كبير بمدى تعاون المجني عليه، حيث يميل معظم الأفراد أو المؤسسات التي تتعرض للاختراق إلى عدم الكشف عن الحادثة حتى داخليا، حريصين على تجنب الإضرار بسمعتهم ومكانتهم.[3]

رابعا: جرائم المساس بالتوقيع الالكتروني هادئة مغرية للمجرمين.

تنطوي الجرائم التقليدية على استعمال القوة البدنية لممارستها مثل العنف والأذية في جرائم مثل السرقة والقتل والاختطاف وغيرها، بينما جرائم الاعتداء على التوقيع الالكتروني

---

[1]–راضيه لالوش، مرجع سابق، ص137.

[2]–محمد رحموني، **(خصائص الجريمة الإلكترونية ومجالات استخدامها)**، مجلة الحقيقة، جامعة أحمد دراية –أدرار–، العدد 41، جانفي 2018، ص 441.

[3]–دليله مزرقن، **جريمة المساس بأنظمة المعالجة الآلية للمعطيات**، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2016، ص 16.

لا تتضمن عنفا أو قتلا أو دما وإنما تحتاج إلى مهارة في التعامل مع أجهزة الكمبيوتر لارتكاب أفعال غير قانونية.[1]

المطلب الثاني: صور الجرائم الواقعة على التوقيع الالكتروني.

مع تزايد التبادلات الإلكترونية وأساليب الاتصال الحديثة، حدث تحول كبير في طبيعة الجرائم التي تؤثر على هذه المعاملات، ويؤثر هذا التحول بصفة خاصة على الثقة في الصفقات التي تتم بالاتصال الحاسوبي المباشر، مما يبرز الدور الحاسم للتوقيعات الإلكترونية كآلية رئيسية في المعاملات الإلكترونية عبر العقود التجارية والمصرفية ومختلف أنواع العقود الإلكترونية؛ والتوقيعات الإلكترونية باعتبارها مجموعة من البيانات الإلكترونية، معرضة لمختلف أشكال الهجمات، هذا الضعف يؤكد أهمية حماية التوقيعات الإلكترونية لضمان أمن وسلامة المعاملات الإلكترونية، ويعد تنفيذ أساليب تشفير قوية والشهادات الرقمية، وبروتوكولات توثيق مأمونة، ووضع أطر قانونية واضحة خطوات أساسية لتعزيز أمن التوقيعات الإلكترونية وموثوقيتها.[2]

وعلى ضوء ما تقدم سوف نقسم هذا المبحث الى مطلبين نتناول في المطلب الأول الجرائم الماسة بالتوقيع الالكتروني والواردة في قانون العقوبات ثم نتناول في المطلب الثاني جرائم التوقيع الالكتروني المستحدثة من خلال القانون15-04.

الفرع الأول: جرائم الاعتداء على التوقيع الالكتروني في إطار قانون العقوبات.

بالنظر إلى آلية إنشاء التوقيع الالكتروني المنصوص عليها في المادة الثانية من الفقرة الرابعة من القانون 15-04 التي اعتبرها جهاز أو برنامج معلوماتي مُعد لتطبيق بيانات إنشاء التوقيع الإلكتروني، فإن التوقيع الإلكتروني مشمول ضمن أنظمة معالجة البيانات الآلية بموجب أحكام القانون 04-15 المذكورة أعلاه.

---

[1]-دليلة مزرقن، مرجع سابق، ص 18.

[2]-زهرة بالخير، **الحماية الجنائية للتوقيع الإلكتروني**، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون -تيارت-،2021، صفحة 42.

لذلك سوف نتناول الجرائم التي تنتمي إلى فئة الجرائم المعلوماتية والتي تتخذ من النظام المعلوماتي للتوقيع الالكتروني موضوعا لها وهي:

أولا: جريمة الدخول والبقاء غير المصرح به على قاعدة بيانات خاصة بالتوقيع الالكتروني.

جاء النص على هذه الجريمة في نص المادة 394 مكرر من قانون العقوبات على أنه:" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج الى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج".

عند التصدي لجريمة الدخول والبقاء غير المصرح به، من المهم التمييز بين الدخول غير المصرح به والبقاء غير المصرح به، إذ يتحقق الدخول غير المصرح به من خلال خرق نظام التوقيع الإلكتروني، في حين تنتج الإقامة غير المصرح بها عن الدخول غير المصرح به أو الدخول القانوني الذي يعقبه إقامة مطولة تتجاوز الحدود المسموح بها، وفي هذه الحالة الأخيرة يصبح الفرد مجرما حتى لو كان الدخول الأولي قانونيًا.[1]

أ- **الركن المادي:** يأخذ الركن المادي في هذه الجريمة صورتين:

1- **فعل الدخول غير المصرح به:** يتجلى الفعل المادي للدخول كعنصر أساسي، إلا أنه لا يقتصر على الدخول المادي إلى مكان ما أو الدخول الفعلي إلى أنظمة الحاسوب ومواقع تواجدها، بل يُنظر إليه كظاهرة معنوية تشبه تلك التي نجدها في استخدامنا لمفهوم الوصول إلى أفكار أو عمليات الفكر لدينا، وهذا يعني الاندماج في عمليات العقل التي يتولاها نظام المعالجة الآلية للبيانات. لذا، يمكن تشبيه الدخول إلى النظام المعلوماتي بالدخول إلى ذاكرة

[1]-حسام محمد نبيل الشنراقي، **جرائم المعلوماتية -دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني-** ، د.ط، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الامارات، 2013، ص 137.

الإنسان، حيث يتم التفاعل مع المعلومات ومعالجتها بطريقة تشبه تلك التي يتعامل بها العقل البشري.[1]

ويعتبر الدخول غير المصرح به إلى النظام عن طريق الوصول على معلومات مخزنة دون علم المالك أو موافقته، ولا يمكن الوصول إلى هذا النظام إلا للأشخاص المخولين فقط ولم تحدد التشريعات طريقة أو وسيلة الدخول، ولذلك فإن أي محاولة للوصول إلى النظام دون إذن تعتبر عملا إجراميا، بصرف النظر عن الطريقة أو الوسائل المستخدمة، سواء كانت مباشرة أو غير مباشرة، مادام الدخول مقصودا.[2]

والوصول غير المصرح به إلى نظام معلومات، وفقاً للحكم المذكور أعلاه، لا يتطلب من النظام أن تكون له حماية تقنية محددة من الاقتحام، وهذا الحكم عام وينطبق على جميع نظم المعلومات دون استثناء، ولا تؤثر التدابير الأمنية للنظام على تصنيف الجريمة، فالوصول غير المأذون به هو الفعل الإجرامي، سواء كان النظام محميا من الناحية التقنية أم لا؛ ولا يميز القانون بين مختلف أنواع النظم أو مستوى ضمانها الحظر مطلق وينطبق على جميع نظم المعلومات.[3]

2- فعل البقاء غير المصرح به: يشير فعل البقاء إلى استمرارية الوجود داخل نظام المعالجة الآلية للبيانات دون إذن صريح من الشخص المسؤول عن هذا النظام، يمكن أن يتم فعل البقاء بشكل مستقل عن عملية الدخول إلى النظام، أو يمكن أن يحدث الاثنان معًا، يُعاقب على فعل البقاء بشكل مستقل عن الدخول إلى النظام عندما يكون الدخول قانونيًا، مثل حدوث الدخول عن طريق الصدفة أو الخطأ، في هذه الحالة يجب على الدخيل أن يحد من تواجده داخل النظام والخروج، وإذا استمر في البقاء رغم ذلك، فإنه يُعاقب على جريمة البقاء غير المشروع. ويُعتبر البقاء جريمة أيضًا عندما يقوم الشخص بنسخ المعلومات في الوقت الذي يُسمح له فيه بالاطلاع فقط عليها، وينطبق ذلك أيضًا على الخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، حيث يمكن للشخص الحصول على الخدمة دون

---

[1]-زهرة بالخير، مرجع سابق، ص 61.

[2]-عطاء الله فشار، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، 2009، ص 488.

[3]-عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح -ورقلة-، 2019، ص 26.

دفع الرسوم المطلوبة أو الحصول على مدة أطول مما دفع مقابلها. يشمل فعل البقاء أيضًا البقاء داخل النظام بعد انتهاء الوقت المحدد للدخول القانوني، بهدف تجنب الدفع، وذلك عن طريق استخدام وسائل احتيالية.[1]

إذا في حال استمر الشخص في البقاء داخل النظام بعد انتهاء المدة المحددة له، فإننا نكون أمام جريمة الاستمرار في البقاء داخل النظام بشكل غير قانوني. وفي حال دخول شخص ما إلى النظام دون إذن من الجهة المسؤولة عنه وبقائه في داخله، فإن نكون أمام جريمتي الدخول غير مصرح به وبقاءً غير قانوني.

وبالنظر إلى الطبيعة المتشابكة لجريمتي الدخول غير المصرح به والبقاء غير المشروع في إطار النظام الآلي لتجهيز البيانات دون ترخيص، فإن هذا يثير تساؤلات قانونية بشأن تحديد الخط الفاصل بين الجريمتين أو النطاق الزمني لكل منهما وهي تتعلق تحديدا بتعرف على الوقت الذي تنتهي فيه جريمة الدخول غير المأذون به وبدأ جريمة الإقامة غير المصرح بها، وقد اتفق الفقه الجنائي على أن بدء جريمة البقاء تبدأ منذ اللحظة التي يبدأ فيها الجاني في التجول والإبحار داخل النظام، غير أنه إذا دخل الجاني النظام وظل فيه لفترة طويلة، فإنه لا يزال يعتبر دخولا غير مصرح به حتى اللحظة التي يبدأ فيها الجاني في التجول والتنقل داخل النظام، وهذا التمييز حاسم في تحديد الأحكام والعقوبات القانونية الواجبة التطبيق.[2]

ب- الركن المعنوي :الدخول والبقاء على قاعدة بيانات تتعلق بالتوقيع الإلكتروني هو جريمة عمدية تتطلب وجود قصد جنائي عام من قبل الجاني، حيث يجب عليه أن يكون على علم بأن دخوله أو بقاؤه غير قانوني، وأن تكون إرادته موجهة نحو ارتكاب هذا الفعل دون الحاجة إلى وجود نتائج محددة لتحقيق الجريمة، حتى إذا كانت دوافعه تتعلق بالفضول أو إظهار المهارات في هذا المجال.[3]

---

[1]-عائشة نايري، **الجريمة الإلكترونية في التشريع الجزائري**، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية -أدرار-، 2017 ص28.

[2]-راضيه عيمور، **الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، مخبر الحقوق والعلوم السياسية جامعة الاغواط، المجلد السادس، العدد الأول، مارس 2022، ص 101

[3]-نسيمة جدي، مرجع سابق، ص 55.

ثانيا: جرائم الاعتداء القصدي على معطيات التوقيع الالكتروني.

نص المشرع الجزائري على هذا النوع من الجرائم في المادة 394 مكرر 1 من قانون العقوبات على النحو التالي "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال وعدل بطريق الغش المعطيات التي يتضمنها".

أ- الركن المادي:

يأخذ النشاط الإجرامي في هذه الجريمة ثلاثة أشكال رئيسية وهي الإدخال، المحو، والتعديل، ولا يلزم ان تتواجد جميع هذه الأشكال معًا، فإحدى هذه الأشكال كافية لتحقيق الجانب المادي للجريمة؛ وتتضمن هذه الأشكال التلاعب بالبيانات الموجودة في نظام معالجة المعلومات المادية سواء عن طريق إضافة بيانات جديدة أو حذف، أو تعديل البيانات الموجودة بالفعل.[1]

1- فعل الإدخال: هو عملية إضافة معلومات جديدة إلى دعامة محددة، سواء كانت الدعامة خالية تمامًا أو تحتوي بالفعل على بيانات. يمكن لعملية الإدخال ان تنطوي على إدخال بيانات زائفة في نظام معلومات بقصد تضليل البيانات الموجودة أو التشويش عليها.[2]

2- فعل الإزالة: يقصد بهذه العملية إزالة جزء من البيانات المحفوظة على الذاكرة الرئيسية، سواء عبر حذف هذه البيانات بشكل نهائي، أو تحطيم الدعامة التي تحتفظ بها، أو نقل هذه البيانات إلى منطقة خاصة بالذاكرة للاحتفاظ بها.[3]

3- فعل التعديل : تتضمن عملية التعديل تغيير المعلومات داخل النظام وتبديلها ببيانات جديدة، ويتم تنفيذ ذلك عادةً من خلال استخدام برامج متخصصة تمتلك القدرة على

[1]-فارس خطابي، **الحماية الجزائية للتوقيع الإلكتروني**، أطروحة لنيل شهادة الدكتوراه في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج الأخضر،2021، ص130.

[2]- المرجع نفسه، ص 131.

[3]محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن**، دار الجامعة الجديدة، دون طبعة، الإسكندرية -مصر- ،2008، ص 188.

إزالة المعلومات بالكامل أو جزئياً، أو تعديلها، باستخدام أدوات مثل القنابل الإلكترونية وبرمجيات الممحاة، أو برامج الفيروسات بشكل عام لتحقيق فعل التعديل بشكل عام.[1]

وقد ورد ذكر الأفعال السابقة (الإدخال، المحو، والتعديل) على سبيل الحصر، وبالتالي، لا تجب المعاقبة على أي فعل آخر حتى لو كان يتضمن انتهاكاً لبيانات التوقيع الإلكتروني بطرق مختلفة.

ب- الركن المعنوي: جريمة التلاعب بمعطيات التوقيع الإلكتروني على النحو المبين في المادة 394 مكرر 1 من قانون العقوبات جريمة عمدية تتطلب وجود قصد جنائي عام، ويشهد على ذلك مصطلح "الغش" الذي يشير إلى ضرورة وجود قصد جنائي عام في العملية، وبالتالي يجب أن تكون إرادة الجاني موجهة نحو ارتكاب سلوك إجرامي بإحدى الطرق المذكورة سابقًا، سواء عن طريق إدخال معطيات جديدة في نظام المعالجة الآلية للمعطيات، أو حذف المعطيات الموجودة بالفعل في النظام، أو بتغييرها، مع العلم بأن الجاني على علم بأنه غير مسموح له بذلك أو أن ذلك يتجاوز حدود سلطته، أو أن فعله سيؤدي بالضرورة إلى نتيجة معينة مثل إزالة المعلومة أو تغييرها أو تعديلها بصرف النظر عما إذا كان حائز التوقيع على علم بها.[2]

الفرع الثاني: جرائم الاعتداء على التوقيع الالكتروني في إطار بعض القوانين الخاصة.

تُعالج صور الجرائم الواقعة التوقيع الإلكتروني ضمن إطار بعض القوانين الخاصة التي تهدف إلى حماية المعلومات الرقمية وتوفير بيئة آمنة للتعاملات الإلكترونية، من بين هذه القوانين يبرز قانون التوقيع والتصديق الإلكترونيين، الذي ينظم كيفية استخدام التوقيعات الإلكترونية وضمان صحتها وسلامتها. كما يتناول هذا القانون الإجراءات الواجب اتباعها للتصديق على التوقيعات الإلكترونية، بما يضمن موثوقيتها ويمنع التلاعب بها.

إضافة إلى ذلك يأتي قانون مكافحة التزوير واستخدام الوثائق المزورة ليفرض هذا القانون عقوبات صارمة على الأفراد الذين يحاولون تزوير التوقيعات الإلكترونية أو استخدام

[1]- فارس خطابي، مرجع سابق، ص 131.

[2]-نسيمة جدي، مرجع سابق، ص68.

توقيعات مزورة في تعاملاتهم، وذلك للحفاظ على نزاهة المعاملات الإلكترونية ومنع الجرائم الرقمية.

أولا: جرائم الاعتداء على التوقيع الالكتروني في إطار القانون 04/15.

في البداية يوفر قانون العقوبات الجزائري الحماية الجنائية للتوقيعات الإلكترونية على النحو المبين في قانون العقوبات، وبيد أنه استجابة للمطالب التكنولوجية المتطورة، أصدرت الحكومة الجزائرية القانون رقم 15-04 بشأن التوقيع والتصديق الإلكترونيين في 1 شباط/فبراير 2015، ووسّع هذا القانون نطاق الحماية التي تتمتع بها، ويعترف بأن التوقيعات الإلكترونية تخضع لعملية من خطوتين بما في ذلك مرحلة التوقيع الإلكتروني ومرحلة التوثيق الإلكتروني، لضمان قدر أكبر من المصداقية والموثوقية.

أ-جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة التصديق الالكتروني الموصوفة:

نص عليها المشرع الجزائري في المادة 66 من القانون 15/ 04 المتعلق بالتوقيع والتصديق الالكترونيين بانه: «يعاقب بالحبس من ثلاثة (3) أشهر الى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20,000 دج) الى مائتي ألف دينار (200,000 دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوف».

وتقوم هذه الجريمة على ركنين أساسين رئيسيين.

1-الركن المادي: ويقتضي الركن المادي توفير معلومات كاذبة لدى جهات التصديق الإلكتروني، مع العلم على أن البيانات المقدمة يجب أن تكون غير صحيحة. وتُرتكب جريمة الإدلاء ببيانات كاذبة بتقديم أي معلومات غير صحيحة، حتى وإن كانت البيانات الأخرى دقيقة، وليس من الضروري أن تكون جميع البيانات المقدمة كاذبة؛ فتوفير حتى قطعة واحدة من المعلومات الكاذبة يكفي لارتكاب الجريمة، حتى وإن كانت البيانات المتبقية دقيقة، وسواء قُدمت المعلومات الكاذبة شفويا أو قُدمت في وثائق مكتوبة أو في شكل إلكتروني يحتوي على معلومات غير صحيحة، فإن القانون لا يحدد كيفية الإدلاء بها،[1]ومن

[1]-فارس خطابي، مرجع سابق، ص171.

الإلزامي كذلك تقديم هذه المعلومات إلى جهة تصديق الكتروني حاصلة على رخصة لممارسة وظيفة تصديق التوقيع الالكتروني.

2-الركن المعنوي: تعتبر هذه الجريمة من الأعمال الإجرامية العمدية التي تتطلب وجود قصد جنائي عام مدعوم بعنصري العلم والإرادة، بحيث يجب على الجاني أن يكون على علم بأن سلوكه غير قانوني وأنه يقدم معلومات كاذبة لمقدمي خدمات التصديق الإلكتروني من أجل الحصول على شهادة تصديق إلكترونية مزورة، وعلى علم بأن هذه الأفعال ممنوعة قانوناً. ومع ذلك، تتجه إرادته نحو ارتكاب هذه الأعمال الإجرامية من خلال تقديم معلومات كاذبة.[1]

ب- جريمة الإخلال بإخبار السلطة الاقتصادية عن التوقف:

بداية ممارسة نشاط التصديق يتطلب الحصول على رخصة من الجهات المختصة، وعند وقف النشاط، يكون من الإلزامي إبلاغ السلطة الاقتصادية بالوقف، الذي يشكل، إذا لم يبلغ عنه، انتهاكا لعدم إبلاغ السلطة الاقتصادية بالوقف[2] على النحو المنصوص عليه في المادة 67 من قانون التوقيع والتصديق الالكترونيين ، حيث جاء في هذه المادة بأنه : « يعاقب بالحبس من شهرين (2) إلى سنة (1) واحدة، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) ، أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و 59 من هذا القانون».

1-الركن المادي: يتحقق الركن المادي في هذه الجريمة عندما يتخذ الجاني مؤدي الخدمات موقف سلبي يتمثل في عدم إبلاغ السلطة الاقتصادية بالتوقف عن نشاطه، وبالتالي فإن السلوك الاجرامي المكون للركن المادي يتحقق بامتناع والكيان المرخص له إصدار شهادة التصديق الالكتروني عن الاستمرار في اصدار الشهادات دون إخطار السلطة المختصة

---

[1]-ماني صلاح الدين، رمضان انور، **الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري**، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة اكلي محند اولحاج -البويرة-، 2021، ص 93.

[2]-فارس خطابي، مرجع سابق، ص 182.

سواء في الظروف العادية أو الاستثنائية المنصوص عليها في المواد 58 و59 من ذات القانون.[1]

وتستمر مدة الترخيص الممنوح لمؤدي خدمات التصديق الالكتروني خمس سنوات قابلة للتجديد [2]، وأي توقف للنشاط قبل نهاية هذه الفترة القانونية، سواء كان راجعا إلى أسباب ارادية أو غير ارادية من جانب مقدم خدمات التصديق الإلكتروني، دون إخطار السلطة الاقتصادية لإصدار الشهادات الإلكترونية، قد يعرضهم للمسؤولية القانونية.

يجب أن يكون السلوك الإجرامي المتمثل في عدم الإبلاغ مرتبط بإيقاف خدمة التصديق الإلكتروني بشكل كامل، ولا يجب أن يحدث إذا تم التوقف جزئياً ثم استئناف النشاط مرة أخرى، على سبيل المثال إذا حدث خلل تقني يؤدي إلى توقف الخدمة لبضعة أيام، إذ يجب أن يتم إيقاف الخدمة بشكل نهائي لمقدم الخدمات لتقع الجريمة.[3]

2-الركن المعنوي: تعتبر هذه الجريمة من الأعمال الاجرامية المتعمدة التي يظهر فيها عنصر القصد الجنائي بشكل واضح، حيث يتمثل العنصران العلمي والإرادي في هذا النوع من الجرائم. فالعلم يتطلب من الجاني معرفة تماماً بالنشاط الإجرامي الذي يقوم به، والذي يتمثل في عدم إبلاغ السلطات المختصة بوقف النشاط المخالف، بينما تتجه إرادة الجاني نحو ارتكاب الفعل الإجرامي وتحقيق النتيجة المرغوبة. ولا يلتفت إلى الأسباب التي دفعت الجاني إلى خرق هذا الالتزام.[4]

ج-جريمة حيازة او إفشاء او استعمال بيانات إنشاء التوقيع الالكتروني موصوف خاصة بالغير.

نصت على هذه الجريمة المادة 68 من قانون 15/ 04 المتعلق بالتوقيع والتصديق الالكترونيين «يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة

---

[1]-نسيمة ترجمان، الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة، أطروحة لنيل شهادة دكتوراه طور الثالث ، جامعة ابن خلدون -تيارت-، كلية الحقوق والعلوم السياسية، 2021 ، ص136.

[2]-المادة 40 من القانون 15 -04.

[3]-مصطفى صحراوي، مرجع سابق، ص113.

[4]-زهرة بلخير، مرجع سابق، ص78.

من مـلـيـون دينـار (1.000.000 دج) إلى خمسة ملايين دينار (5.000.000 دج) أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير».

ولقيام هذه الجريمة لابد من توافر ركنين هما:

1-الركن المادي: يتمثل السلوك الإجرامي في هذه الجريمة بقيام الجاني بأحد الأفعال الآتية: "الحيازة، الإفشاء، الاستعمال " وبالتالي يعد القيام بأحد هذه الافعال كافيا لقيامها. فأما الحيازة فتتمثل في حيازة الجاني بيانات التوقيع الالكتروني خاصة بالغير، والافشاء هو البوح او إحاطة علم الغير ببيانات التوقيع الإلكتروني او الوسائط الالكترونية أو معلومات من الجهة المرخص لها بإصدار شهادة التصديق الإلكتروني وهي جهة التصديق الإلكتروني.[1]

الإفشاء: ينطوي على كشف أو بث تلك التوقيعات الالكترونية أو المعلومات ذات الصلة بوسائل الكترونية أو بواسطة السلطة المأذون لها بإصدار الشهادات، وهي هيئة التصديق الالكترونية.

الاستعمال: استخدام البيانات هنا يشير إلى استغلال المعلومات التي تم تقديمها في إطار التوقيع الإلكتروني للأفراد الآخرين. يُفهم تحت مصطلح "الآخرين" هنا كل شخص طبيعي أو اعتباري حائز على توقيع إلكتروني. يعتبر استخدام هذه البيانات غير قانوني، وذلك خاصة في السياقات التي تؤديها التوقيعات الالكترونية في الشؤون القانونية والتجارة الالكترونية أو أي نشاط آخر ينطوي على معاملات رسمية.[2]

2-الركن المعنوي: تعد هذه الجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الاجرامي وهو حيازة

[1]-فارس خطابي، مرجع سابق، ص 149 و ص 150.

[2]-عبد الجبار الحفيص، **(الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجنائي)**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011، ص 191.

بيانات التوقيع الالكتروني او استخدامها وإفشاؤها، واتجاه إرادة الجاني إلى ارتكاب الفعل المعاقب عليه قانونا.[1]

د- جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني.

نص المشرع الجزائري على هذه الجريمة في نص المادة 69 من القانون 15-04 بأنه «يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة.»

وجاء نص التجريم انطلاقا من ان المشرع الجزائري أخضع مؤدي خدمات التصديق الإلكتروني عند عملية منح شهادة التصديق الإلكتروني إلى إلزامية التحقق من هوية طالبها وعند الاقتضاء التحقق من صفاته الخاصة طبقا لأحكام المادة 44 من القانون15-04.

وعليه لقيام هذه الجريمة لابد من توفر ركنين هما:

1- **الركن المادي:** يتمثل الركن المادي في هذه الجريمة في اخلال مؤدي خدمات التصديق الإلكتروني بالتزام تحديد هوية الشخص طالب شهادة التصديق الإلكتروني كما سبق ذكره، وبما أن الحائز يمكن أن يكون شخصا طبيعيا أو كيانا اعتباريا، فإن عملية تحديد الهوية تتخذ شكلين: فبالنسبة للأشخاص الطبيعيين يتم التحقق من الهوية بصورة مباشرة، ويكون التحقق من هوية بالنسبة للشخص المعنوي من جانب مقدّم خدمات التصديق الإلكتروني الذي يقوم بالتحقق من هوية الممثل القانوني الذي يستخدم التوقيع الإلكتروني وتسجيلها، وتكفل هذه العملية التحديد الصحيح لهوية الحائز، سواء أكان فردا أم منظمة.[2]

2-الركن المعنوي: تعتبر جريمة الاخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني من الجرائم العمدية التي تستلزم توافر القصد العام بصورتيه، الأولى: ان يعلم مؤدي خدمات التصديق الالكتروني بانه بصدد منح شهادة تصديق الكترونية موصوفة دون

[1]-نسيمة ترجمان، مرجع سابق، ص132

[2]-مصطفى صحراوي، مرجع سابق، ص114.

التحقق من هوية طالبها وأن هذا الفعل يجرمه القانون، والثانية أن تتجه ارادته الى اقتراف هذا الفعل المجرم.[1]

هـ-جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني :

جرم المشرع الجزائري انتهاء سرية بيانات شهادة التصديق الالكتروني من خلال نص المادة 70 والمادة 73 من القانون 15 04 السالف الذكر، حيث تنص المادة 70 على أنه: «يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون».

وتضيف المادة 73 أنه «يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) وإلى مائتي ألف دينار (200.000 دج) أو بـ إحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق».

يلاحظ في المواد 70 و73 من النص السابق أن القانون يحمي سرية بيانات شهادات التصديق الإلكتروني، ومع ذلك يوجد اختلاف بينهما فيما يتعلق بالشخص الذي قد يكون مسؤولاً عن انتهاك هذه السرية، فالمادة الأولى تتعلق بمزودي خدمات التصديق الإلكتروني، بينما المادة الثانية تنص على أي شخص يكلف بالتدقيق في هذه البيانات.

1-الركن المادي:

يتحقق الركن المادي في هذه الجريمة عن طريق الكشف عن هذه المعلومات أو الأسرار، أي نشرها أو نقلها أو إفشائها للآخرين بعد أن كانت محفوظة بسرية وكتمان، وكانت معرفتها مقتصرة على مقدمي خدمات التصديق الذين تمت ائتمانهم بها بسبب وظيفتهم، ويتساوى في الأهمية بين المعلومات التي يتم نشرها أن تكون مكتوبة على ورق أو مسجلة على وسائط إلكترونية.[2]

[1]- نسيمة ترجمان، مرجع سابق، ص 140.

[2]-فارس خطابي، مرجع سابق، ص169.

2-الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية التي يظهر فيها الركن المعنوي بشكل واضح كقصد جنائي، حيث يجمع بين العلم والإرادة. فالعلم يتطلب من الجاني معرفة حقيقة النشاط الإجرامي ويجب أن يكون على علم بأن الجريمة محظورة، ومع ذلك يختار القيام بالفعل الجنائي ويوافق على النتائج المترتبة عنه، وهي إفشاء بيانات شهادة التصديق الإلكتروني.[1]

و- جريمة جمع البيانات الشخصية للمُوقع واستخدامها في غير غرضها:

باعتبار التوقيع الإلكتروني عبارة عن ملف رقمي يحمل العديد من البيانات، بما في ذلك البيانات الشخصية للمستخدم، فإنه يجب أن يتم جمع هذه البيانات بطريقة آمنة واستخدامها فقط للأغراض المشروعة. وفي حالة استخدام هذه البيانات بطريقة غير قانونية، يُعتبر هذا سلوكًا مخالفًا ومجرمًا وفقًا للقانون الجزائري[2]، وتنص المادة 71 من القانون رقم 15-04 على أنه «يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون.»

وبالرجوع إلى المادة 43 من نفس القانون نجدها تنص على أنه لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة، وليس له أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني ولا يمكن استعمال هذه البيانات لأغراض أخرى.

1-الركن المادي:

يقوم مقدم خدمات التصديق بجمع بيانات صاحب التوقيع للتحقق من صحتها ومطابقتها لصاحبها، وذلك لمنحه الملف الرقمي الشخصي المصادق عليه. تشمل البيانات الشخصية للموقع اسمه، تاريخ ميلاده، عنوانه، وغيرها من البيانات ذات الصلة، وبموجب المادة 71 من قانون التوقيع والتصديق الإلكتروني يقوم الركن المادي على جمع البيانات الشخصية للموقع دون موافقة صريحة منه، وحتى إذا وافق صاحب التوقيع الإلكتروني على

[1]-نسيمة ترجمان، مرجع سابق، ص31.

[2]-فارس خطابي، مرجع سابق، ص174.

جمع البيانات الشخصية، يجب على جهة التصديق الإلكتروني جمع البيانات الشخصية الضرورية فقط وفقًا للمادة 43 فقرة 2.[1]

2-الركن المعنوي: تتصف هذه الجريمة بأنها من الأفعال الاجرامية المتعمدة، حيث يتم فيها استغلال الركن المعنوي لغرض جنائي، مع احتواء العمل على عنصري العلم والإرادة، فالشخص الذي يقوم بهذه الجريمة يكون على علم تام بأن أفعاله مخالفة للقانون، ومع ذلك يقوم بجمع البيانات الشخصية واستخدامها بطريقة غير قانونية، وهذا يعتبر انتهاكاً خطيراً لخصوصية الأفراد.[2]

ز-جريمة مزاولة نشاط التصديق الالكتروني بدون رخصة:

جاء النص على هذه الجريمة في المادة 72 من القانون 15-04 على نحو الآتي: «يعاقب بالحبس من سنة (1) واحدة إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليوني دينار (2.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه...».

وتقوم هذه الجريمة على ركنين مادي ومعنوي.

1-الركن المادي: يتحقق الركن المادي في هذه الجريمة عندما يتم انتحال صفة مزود خدمات التصديق المرخص بشكل غير قانوني، وبمعنى آخر يتم إصدار شهادات تصديق إلكتروني دون الحصول على الترخيص اللازم من الجهات المختصة، أما الجانب الثاني من هذه الممارسات فهو عملية إصدار شهادات تصديق إلكتروني بعد سحب الترخيص من الجهات المختصة في منحه.[3]

وتعرض المادة 33 والأحكام اللاحقة من القانون رقم 15-04 سلسلة من الالتزامات التي تنطبق على أي شخص طبيعي أو اعتباري يسعى إلى الانخراط في أنشطة خدمات

---

[1]-فارس خطابي، مرجع سابق، ص 175.

[2]- زهرة بلخير، مرجع سابق، ص 75.

[3]- عبد الفتاح بيومي حجازي، **التوقيع الالكتروني في النظم القانونية المقارنة**، دار الفكر الجامعي، دون طبعة، الإسكندرية، 2005، ص 540.

تصديق الالكتروني، ومن بين هذه الالتزامات نظام الترخيص الذي يتسم بأهمية خاصة، حيث تمنحه السلطة الاقتصادية للتصديق الالكتروني وفقا لشروط ومؤهلات محددة يجب أن يستوفيها مقدم طلب الترخيص، وبالإضافة إلى ذلك هناك أطر زمنية مقررة قانوناً لممارسة هذا النشاط، ومن الواضح أن عدم الامتثال للمادة 72 من شأنه أن يؤدي مباشرة إلى تطبيق المواد 33 إلى 40 من نفس القانون، التي تشترط الحصول على ترخيص لممارسة النشاط، إلى جانب مجموعة من المؤهلات المطلوبة، وعدم الامتثال لهذه الالتزامات يمكن أن يؤدي إلى عواقب وخيمة، بما في ذلك تطبيق العقوبات بموجب القانون.

2-الركن المعنوي: يجب على الشخص المتورط في هذه الجريمة العمدية أن يكون على علم بأنه يقوم بنشاط غير مصرح به قانونيًا، وهو إصدار شهادات تصديق إلكترونية في غير الحالات المسموح بها قانونًا، أو أنه قد أصدر شهادة تصديق إلكترونية بعد سحب الترخيص منه، وذلك بنية واضحة للقيام بالفعل المادي المتمثل في إصدار شهادة تصديق إلكترونية بدون ترخيص أو بعد سحب الترخيص.[1]

ح-جريمة الاستعمال غير المشروع لشهادة التصديق الإلكتروني:

إذا كان المشرع الجزائري قد نص في المادة 71 على استعمال بيانات شهادة التصديق الإلكتروني لأغراض أخرى غير تلك المخصص لها، فإن المادة 74 من نفس القانون نصت على أنه "«يعاقب بغرامة من ألفي دينار (2.000 دج) إلى مائتي ألف دينار (200.000 دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها».

فالفرق بين المادتين يكمن انه في الحالة الثانية يكون الاعتداء من قبل صاحب الشهادة نفسه.

1-الركن المادي: شهادة التصديق الإلكترونية تستخدم في المجالات المرخص لها قانونيًا. إذا تم استخدامها في غير هذه الحالات، يُعتبر ذلك جريمة استخدام غير شرعي، على سبيل المثال استخدام شهادة تصديق إلكترونية في معاملات إلكترونية محظورة قانونًا كشراء مخدرات أو بطاقات ائتمان مزورة أو القمار عبر الإنترنت، وتُعتبر هذه الجريمة من الجرائم

[1] -فارس خطابي، مرجع سابق، ص 178.

الخطرة حيث يتم ارتكاب الجريمة بمجرد استخدام شهادة التصديق الإلكترونية بطريقة غير قانونية بغض النظر عن تأثيرها الضار.[1]

2-الركن المعنوي: تعد هذه الجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي وهو الاستعمال غير المشروع لشهادة التصديق الالكتروني واتجاه إرادته إلى ارتكاب فعل او أفعال معاقب عليها قانونا.[2]

ثانيا: جرائم الاعتداء على التوقيع الالكتروني في ظل القانون02/24.

تندرج جريمة تزوير التوقيع الإلكتروني تحت مظلة الاحتيال في مجال تكنولوجيا المعلومات، على النحو الذي تعرّفه اتفاقية بودابست على النحو التالي: "التزوير المرتبط بالحواسيب، الذي ينطوي على استحداث أو تغيير البيانات غير المأذون به في سياق المعاملات القانونية، وبالتالي تغيير صحة البيانات المستخرجة بقصد خداع المصالح القانونية المحمية".[3] ويسلط هذا التعريف الضوء على أهمية الجرائم الالكترونية، ولا سيما التزوير الإلكتروني في التلاعب بالبيانات في إطار المعاملات القانونية، مما يؤدي إلى أنشطة احتيالية تقوض سبل الحماية القانونية.

وبالرجوع للقانون الجزائري ورد تعريف التزوير من خلال نص المادة ثلاثة من القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور[4] بأنه: "كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون، بأي وسيلة، من شأنه إحداث ضرر، ويهدف أو من شأنه أن يترتب عليه إقرار حق أو صفة أو واقعة ترتب آثارا قانونية.

ويشمل التزوير، التقليد والتزييف النصوص عليها في هذا القانون".

---

[1]- فارس خطابي، مرجع سابق، ص 187.

[2]-نسيمة ترجمان، مرجع سابق، ص 182.

[3]- مصطفى صحراوي، مرجع سابق، ص 86.

[4]- قانون رقم 24-02، مؤرخ في 16 شعبان عام 1445 الموافق ل 26 فبراير سنة 2024 يتعلق بمكافحة التزوير واستعمال المزور، ج.ر.ج.ج، العدد 15، لسنة 2014.

والمشرع الجزائري لم يجرّم صراحة تزوير التوقيع الإلكتروني في القانون رقم 15-04، وبدلا من ذلك فإنه يشدد فقط على ضرورة حماية التوقيعات الإلكترونية من التزوير باستخدام الوسائل التكنولوجية المتاحة في الفقرة (ب) من المادة 11، التي تنص على ما يلي: " ...وأن يكون هذا التوقيع الإلكتروني محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد"، ويشير ذلك إلى أنه في حين يعترف القانون بخطر التزوير في التوقيع الإلكتروني، فإنه لا يعاقب عليه صراحة.

و بالرجوع الى النصوص القانونية التي تعاقب على التزوير المستحدثة بموجب القانون 24-02 الذي يتعلق بمكافحة التزوير واستعمال المزور، يمكننا القول بإمكانية تطبيق هذه النصوص على جريمة تزوير التوقيع الإلكتروني و نستند في ذلك ان مصطلح " المحرر" الذي استخدمه المشرع في نص المادة أعلاه هو مفهوم واسع تندرج ضمنه المحررات التقليدية و الالكترونية وفقا لما جاء في نص المادة الثالثة فقرة 2 من القانون 24-02 التي تنص : "المحرر هو كل مكتوب ورقي أو إلكتروني يسمح بمعرفة الشخص الذي صدر عنه ويتضمن ذكر واقعة أو تعبير عن الإرادة من شأنه إنشاء مركز قانوني أو تعديله أو إنهائه أو إثباته، سواء أعد المحرر لذلك أساسا أو ترتب عليه هذا الأثر بقوة القانون. "

وللتوقيع الإلكتروني، عندما يفي بجميع متطلباته، نفس القيمة الإثباتية التي يتمتع بها التوقيع التقليدي، كما يؤكد ذلك التعديل الذي تم بموجب القانون 05-01 المؤرخ 2005/06/20 في المادة 323 ومكرر 1 والمواد 9 و8 و6 المتعلقة بالتوقيع والتصديق الإلكترونيين، وعلى النحو المنصوص عليه في القانون 15-04 المتعلقة بالتوقيع والتصديق الإلكترونيين فإن التوقيع الالكتروني يكون محلا للحماية الجنائية تبعا للقاعدة العامة التي تنص على ان التوقيع الالكتروني الذي لا يتمتع بالحجية في الإثبات ليس محلا للتزوير.[1]

أ- الركن المادي لجريمة تزوير التوقيع الإلكتروني:

يتمثل الركن المادي لجريمة تزوير التوقيعات الإلكترونية في الأفعال الآتية:

[1]- مصطفى صحراوي، مرجع سابق، ص 87.

1- تغيير الحقيقة: "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".[1]

وتتجلى جريمة التزوير في تغيير الحقائق الموجودة على الوثائق الإلكترونية، حيث يعتمد وجود هذه الجريمة على تعديل المعلومات بشكل متعمد، وإذا لم يحدث هذا التغيير، فلن يحدث التزوير. ونظرًا لأن التوقيع الإلكتروني يعتبر جزءًا لا يتجزأ من المستند الإلكتروني، فإن حدوث التزوير فيه يُعَد انتهاكًا مقصودًا، وذلك بتغيير الحقائق المنصوص عليها في الوثائق أو الملفات التي تُنتجها الأنظمة الحاسوبية. ويتوقف وجود الضرر على انتشار هذا التغيير في البيانات المخزنة في أنظمة الحاسوب، مما يؤدي إلى انخفاض مستوى الثقة في الوثائق الإلكترونية.[2]

2- وسائل وطرق التزوير :ومن أشيع الأساليب المستخدمة في التزوير التوقيع الإلكتروني استخدام برمجيات حاسوبية متخصصة أو نظم معلومات مصممة لهذا الغرض، وقد صُممت هذه البرامج والنظم على نحو يحاكي مظهر ووظائف تطبيقات التوقيع الإلكتروني المشروع، ويحاول بعض الأفراد كسر الشفرة والوصول إلى البيانات الرقمية الفريدة المرتبطة بالتوقيع الإلكتروني، ثم نسخها وإعادة استخدامها لأغراض احتيالية، ويمكن أن يكون من الصعب كشف هذا النوع من التزوير، لأن التوقيع المنسوخ قد يبدو مطابقا للأصل.[3]

وطرق تغيير الحقيقة في التزوير حددها المشرع الجزائري على سبيل الحصر في نص المادة 31 من القانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور وتتمثل في:

- إما بتقليد أو تزييف الكتابة أو التوقيع،
- وإّما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات لاحقا،

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 253.

[2]- نسيمة ترجمان، مرجع سابق، ص 99.

[3]- زهره بالخير، مرجع سابق، ص 59.

- وإما بإضافة أو بإسقاط أو بتزييف شروط أو إقرارات أو وقائع أعدت هذه المحررات لتلقيها أو لإثباتها،
- وإما بانتحال شخصية الغير أو الحلول محلها.

ويبين النص أن هناك طرقاً مختلفة للتزوير، سواء أكان تزويراً مادياً أم معنوياً، ويتم التشديد على أهمية التمييز بين الاثنين من حيث دلالتهما وعقوبتهما؛ ينتج عن التزوير المادي تغيير واضح في المحتوى الأصلي أو يترك آثارًا مادية تشير إلى أن الوثيقة قد تم تغييرها، ويشمل ذلك إضافة شروط أو تعديلات بعد إنشاء المستند أو إنشاء مستند مزور بالكامل، بما في ذلك التوقيعات الإلكترونية، في مثل هذه الحالات لا توجد حاجة لإثبات التلاعب في الأحداث أو الأرقام أو الرموز، ويعاقب على التزوير حتى لو كان المحتوى صحيحاً.[1]

وفيما يتعلق بتزوير المعنوي، يشير هذا النوع من التزوير إلى التلاعب بالمحتوى دون وجود أي تغييرات مادية تظهر بوضوح، مما يجعل من الصعب اكتشافه عبر العلامات الظاهرية كالتواقيع أو العلامات الإلكترونية، يتم تحقيق هذا التزوير من خلال تشويه المعنى الأصلي للنص وبالتالي يصعب اكتشافه بمجرد النظر إلى المحتوى، و للكشف عن هذا النوع من التزوير يتطلب التحقيق البحث عن الحقيقة من خلال مصادر خارجية، مثل تحديد نية الشخص الذي يُنسب إليه النص المزور، أو مقارنة الوقائع الحقيقية بتلك المدونة في النص المشكوك فيه و إذا تبين وجود اختلاف بين الوقائع، فإن ذلك يُعتبر دليلاً قاطعاً على وجود التزوير، وهذا ينطبق أيضًا على التوقيع الإلكتروني.[2]

ب- الركن المعنوي:

لا تكتمل جريمة تزوير التوقيع الإلكتروني أو الوثائق المعلوماتية إلا بوجود الركن المعنوي الذي يجب أن يكون موجودًا جنبًا إلى جنب مع الركن المادي كما هو الحال في بقية الجرائم، وبالتالي يعتبر هذا النوع من الجرائم جرائم عمدية.[3]

---

[1]- عبد الحق غلاب، **(خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري)**، مجلة الدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 8، العدد 1، 2022، ص 502.

[2]-عبد الحق غلاب، مرجع سابق، ص 502.

[3] - زهرة بلخير، مرجع سابق، ص 60.

والركن المعنوي هنا يتمثل في علم المرتكب بأنه يقوم بتغيير الحقيقة، وأن هذا التغيير يستهدف انتحال صفة شخص آخر بطرق محظورة قانونيًا، على الرغم من علمه بأن فعله محظور ويعاقب عليه لكنه يخطط للقيام به ويوافق على النتائج المحتملة، كما ينبغي أن تنحصر نية المرتكب في جريمة تزوير التوقيع الإلكتروني في التلاعب به من أجل تحقيق هدف محدد وهو استخدام التوقيع الإلكتروني بطرق غير مشروعة؛ ولكي يتوفر الركن المعنوي لجريمة التزوير لا يكفي توافر القصد الجنائي العام إذ يجب أن يكون لدى الجاني نية خاصة لاستخدام الوثيقة المزورة للغرض الذي زورت من أجله، وإذا لم تكن هناك نية خاصة لاستخدام الوثيقة المزورة للغرض الذي زورت من أجله، ينتفي الركن المعنوي تلقائيا، وفي هذه الحالة لا تكون جريمة التزوير قد ارتكبت.[1]

[1]– حنان براهمي، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة الدكتوراه، كلية الحقوق، جامعة بسكرة، 2015، ص 84.

خلاصة الفصل الأول:

نخلص من خلال ما تم توضيحه في الفصل الأول ان التطورات التكنولوجية و شيوع استعمال الوسائط الالكترونية أدى إلى ظهور التوقيع الإلكتروني الذي يعرف على أنه مجموعة من البيانات الإلكترونية المرتبطة أو المضافة إلى مستند إلكتروني، و جاء يقر للتعاملات المبرمة عبر الوسائط الالكترونية القوة الثبوتية, ويرسي جو من الثقة فيها مع قدرته على تحقيق نفس الوظائف التي يؤديها التوقيع التقليدي، ولكن بدقة بالغة والتي تسمح له بتمييز شخص صاحبها وتحديد هويته والتعبير عن إرادته ورضاه بالتصرف القانوني وفقا لما ورد في المحرر الموقع عليه، كما رأينا أن هذا التوقيع يأخذ صورا متعددة من بينها التوقيع الرقمي، التوقيع البيومتري، التوقيع بالقلم الإلكتروني...، وحتى يكون لهذا التوقيع حجية قانونية في الإثبات تعادل حجية التوقيعات التقليدية، لابد من توافر جملة من الشروط لضمان صحة الوثائق التي تحمله على غرار ارتباطه بالموقع دون غيره، وسيطرة صاحب التوقيع عليه سيطرة كاملة وعدم قابلية هذا التوقيع للتعديل أو التغيير، فضلا على وجود جهة ثالثة وظيفتها الرئيسية خلق بيئة تعاملات إلكترونية آمنة، وتضمن سلامة محتوى البيانات المتداولة من خلال إجراءات موسومة بالتصديق الإلكتروني .

ورغم الإيجابيات التي يقدمها التوقيع الالكتروني الا انه كان هدفا لعدة اعتداءات، والمشرع الجزائري بدوره استدرك الفراغ المتعلق بوجوب إضفاء حماية لهذه التقنية وعمل على تجريم مختلف أشكال الاعتداء التي تقع على هذا التوقيع من خلال ما جاء في القانون رقم 04-15 والقانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، بالإضافة للقانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور.

الفصل الثاني: إجراءات الحماية الجنائية للتوقيع الالكتروني.

بعد تحليل جوانب الحماية الجنائية الموضوعية للتوقيع الإلكتروني، يظهر أن هذه الدراسة ترتكز أيضا على جانب آخر وهو الجانب الإجرائي الذي يكمل فهم تلك الحماية ويعززها. فالجوانب الإجرائية تعد جزءاً حيوياً في تحويل مفهوم الحماية من مجرد نظرية إلى تطبيق عملي، حيث تنقل الحماية المقررة للتوقيع الإلكتروني من مجرد نصوص قانونية إلى مرحلة التنفيذ؛ وعند التطبيق الفعلي لهذه الحماية تظهر تحديات أمام الجهات القانونية في مواجهة هذا النوع من الجرائم، نظراً لدهاء المجرمين الإلكترونيين وتعقيدات البيئة الافتراضية التي تشكل مسرحاً لهذه الجرائم، تلك التحديات تجعل من الصعب على المحققين كشف تلك الجرائم وضبط مرتكبيها، مما يستدعي تخصيص جهود مكثفة في سبيل ذلك.

لذلك خصصنا هذا الفصل للتعرف على الهيئات المختصة في مكافحة هذا النوع من الجرائم، والتعرف على الإجراءات القانونية التي تتبعها هذه الهيئات لمواجهة هذا التحدي؛ وفي هذا السياق يتم التطرق إلى الجزاءات المفروضة على مرتكبي جرائم الاعتداء على التوقيع الإلكتروني.

المبحث الأول: التحري في الجرائم الواقعة على التوقيع الالكتروني.

وضعت مختلف القوانين إجراءات محددة للتحقيق في الجرائم من مختلف الأنواع بهدف الكشف عنها، وتحديد هوية مرتكبيها، وتقديم الأدلة المتصلة بها. وتشكل الجرائم المعلوماتية بما فيها الجرائم التي تنطوي على توقيعات إلكترونية فئة هامة من هذه الجرائم، وبالنظر إلى الطابع الحساس لهذه الجرائم التي تنطوي على شواغل تتعلق بالخصوصية، أقرت الهيئة التشريعية مجموعة من الإجراءات المتخصصة التي تتماشى مع خصائص هذه الجرائم، وقد أنيطت هذه الإجراءات بفئات محددة قادرة على التعامل مع هذه الجرائم بفعالية.

المطلب الأول: الجهات المختصة بالتحري عن جرائم الاعتداء على التوقيع الإلكتروني.

يعتبر جهاز الضبطية القضائية الجهة المخولة بشكل عام بالتحقيق في الجرائم المختلفة، وعلى الرغم من ذلك تُخصص بعض القوانين صلاحيات استثنائية لبعض الجهات والهيئات المتخصصة نظرًا لخبرتها الفريدة في مجال معين، مما يجعلها أكثر كفاءة في كشف الجرائم ضمن اختصاصها التقني، ومع ذلك يظل من الضروري تنسيق الجهود بين هذه الجهات وجهاز الضبطية القضائية التقليدي لضمان تحقيق أقصى درجات الفاعلية في مجال الضبط القضائي.[1]

لذلك سنحاول من خلال هذا المبحث استعراض أهم الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم الإلكترونية، والتي تتولى عادة مهام الوقاية والمكافحة ضد الجرائم التي تستهدف التوقيع الإلكتروني.

[1]–عبد الرؤوف بوديسة، **آليات التحرير عن الجريمة الإلكترونية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة ماستر مهني في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي –برج بوعريريج–، 2022، ص 38.

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري.

تلعب الهيئات الفنية المتخصصة في مجال مكافحة الجريمة المعلوماتية دوراً حيوياً في حفظ أمان وسلامة البيانات والشبكات، تعتمد هذه الوحدات على فرق متخصصة تهتم بمكافحة الجرائم الإلكترونية، بما في ذلك الجرائم ذات الصلة بالتوقيع الإلكتروني، وتتميز هذه الفرق بتنوع تشكيلتها البشرية إذ تضم محققين ذوي خبرة عميقة في مجالات التحقيق الرقمي والتقنيات الأمنية، وبفضل إضافة صفة الشرطة القضائية إلى خبراتهم، يصبحون قادرين على التعامل بكفاءة وفعالية مع تحقيقات الجرائم الإلكترونية، مع معرفتهم الواسعة بالنظم المعلوماتية والتقنيات الحديثة في هذا المجال.[1]

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

تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في عام 2009 تحديدًا في 5 أغسطس 2009 تاريخ صدور القانون 09-04 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بحيث جاء في نص المادة 13 من القانون على أنه «تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم».

وترك أمر تحديد تشكيلة الهيئة وكيفيات سيرها للتنظيم الصادر بموجب المرسوم الرئاسي 21 -439 المؤرخ في 2 ربيع الثاني 1443 الموافق ل 7 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] ويهدف هذا المرسوم الى تحديد تشكيلة وتنظيم وكيفية سير الهيئة.

---

[1]- يوسف بوزيدة، **الحماية الجزائية للتوقيع الإلكتروني**، مذكرة مقدمة لنيل شهادة ماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي -تبسة-، 2021 ،ص 50.

[2]-المرسوم الرئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني 1443 موافق ل 7 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 86، لسنة 2021.

أ- التعريف بالهيئة: بموجب المرسوم الرئاسي المذكورة أعلاه، تُعتبر "الهيئة" سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تتبع الهيئة رئيس الجمهورية[1] وتتخذ مقرها في مدينة الجزائر، إلا أنه يمكن نقلها إلى أي مكان آخر بالتراب الوطني بموجب مرسوم رئاسي.[2]

ب- مهام الهيئة: طبقا للمادة 14 من القانون 09-04 تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام الآتية:

أ - تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

ب - مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج - تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم."

وتضيف المادة 4 من المرسوم 21-439 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ان هذه الهيئة تمارس المهام المنصوص عليها في المادة 14 من القانون 09-04 المذكور سابقا تحت رقابة السلطة القضائية وتكلف الهيئة على الخصوص ما يأتي:

- تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ،

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

---

[1]-المادة 2 من المرسوم الرئاسي رقم 21 -439.

[2]-المادة 3 من نفس المرسوم.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة،

كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول.

– تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية،

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تحيين المعايير القانونية في مجال اختصاصها،

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية،

– تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

ج–تشكيل الهيئة: وفقا لنص المادة 5 من مرسوم رئاسي رقم 21–439 تتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت سلطة رئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهم.

1. مجلس التوجيه: جاء فيه بأن يتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه الذي يتشكل من الأعضاء الآتي ذكرهم الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، قائد الدرك الوطني، المدير العام للأمن الداخلي ، المدير المركزي لأمن الجيش لأركان الجيش

الوطني الشعبي ، المدير العام للأمن الوطني، رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية، و يتولى المدير العام للهيئة أمانة مجلس التوجيه.[1]

ويقوم مجلس التوجيه بتوجيه عمل الهيئة والإشراف عليه ومراقبته، دراسة كل المسائل المتعلقة باللجوء للمراقبة الوقائية للاتصالات الإلكترونية وضبط برنامج عمل الهيئة، وتحديد شروط وكيفيات تنفيذه، بالإضافة إلى قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، كما تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه دون إغفال دراستها للتقرير السنوي لنشاطات الهيئة والمصادقة عليه.[2]

2. المديرية العامة: بناء على نص المادة 9 منه فانه يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي، وتنهى مهامه حسب الأشكال نفسها كما تعد وظيفة المدير العام وظيفة عليا في الدولة يتولى القيام فيها بالمهام المنصوص عليها في نص المادة 10 من المرسوم، وتضم المديرية العامة مديريات ومصالح وملاحق حسب نص المادة 11 وفقا لما يلي: مديرية المراقبة الوقائية واليقظة الالكترونية، مديرية الإدارة والوسائل، مصلحة الدراسات والتلخيص، مصلحة للتعاون واليقظة التكنولوجية، ملحقات جهوية.

ويحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار من الأمين العام لرئاسة الجمهورية، بناء على اقتراح من المدير العام للهيئة.[3]

ثانيا: الهيئات التابعة للجهاز الأمني.

بالإضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، هناك هيئات تابعة للجهاز الأمني تتدخل لمواجهة الجرائم المتعلقة

[1]–المادة 6 من المرسوم الرئاسي رقم 21–439.

[2]–المادة 7 من نفس المرسوم.

[3]–المادة 13 من نفس المرسوم.

بالاعتداء على التوقيع الإلكتروني على المستوى التطبيقي في الجزائر، يمكن تصنيف هذه الهيئات إلى نوعين:

أ- أجهزة الأمن الوطني المختصة: تفخر المديرية العامة للأمن الوطني بالهياكل الأساسية والأجهزة المتطورة في مجال مكافحة الجرائم نظم المعلومات وجرائم الإنترنت التي تندرج ضمنها الجرائم الواقعة على التوقيع الالكتروني، وتماشيا مع الجهود التعاونية التي تبذلها الأجهزة الأمنية الدولية واستجابة لمشروع المنظمة الدولية للشرطة الجنائية (الإنتربول) التكنولوجي وما يتصل به من متطلبات قواعد البيانات، أنشئ المعهد الوطني للشرطة الجنائية في عام 1999، ويتمثل هدفه الرئيسي في التحري و التحقيق في الأدلة وجمعها، إلى جانب أربعة مختبرات إقليمية تقع في قسنطينة و وهران وبشار وتمنراست، وتضم هذه المختبرات فروعا تقنية متقدمة، بما في ذلك خلية الاعلام الالي التي تعمل بالتنسيق مع فرق متخصصة للبحث عن الجرائم المعلوماتية والتحقيق فيها على مستوى كل مديريات الأمن الولائي.[1]

ب- الوحدات التابعة للقيادة العامة للدرك الوطني: بالإضافة إلى الهيئات التابعة للأمن الوطني توجد هيئات تابعة للدرك الوطني تلعب دوراً بارزاً في مكافحة الجريمة المعلوماتية، تتميز هذه الهيئات بخبرة وكفاءة عالية، حيث تشارك المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بفعالية في هذا المجال، وعلى المستوى المركزي تعمل هيئات متخصصة في مكافحة هذا النوع من الإجرام بكفاءة عالية يمكن إجمالها في:[2]

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام: يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني مكسبا يدعم قدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجزائية.

[1]- مصطفى صحراوي، مرجع سابق ، ص 133

[2]- سعاد رابح، **(ضوابط مكافحة الجريمة المعلوماتية)** ، **مجلة القانون العام الجزائري والمقارن**، جامعة جيلالي اليابس -سيدي بلعباس-، المجلد السابع، العدد 1، جوان 2021، ص 280.

أنشئ المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم-04 183 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي[1] وذلك من خلال المادة رقم 01 منه، والمعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يوضع تحت وصاية وزير الدفاع الوطني، ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، وبهذه الصفة فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية.[2]

حدد مقر المعهد بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني، كما يمكن إحداث ملحقات عند الحاجة بقرار من وزير الدفاع الوطني.[3]

يساهم المعهد الوطني للأدلة الجنائية وعلم الإجرام في معاينة الجريمة الإلكترونية من خلال تقديم الخبرات التطبيقية والمعاينات اللازمة التي تساعد في التحقيقات القضائية والكشف عن الجرائم بالأدلة العلمية، وذلك من خلال الدوائر المتخصصة في مجالات مختلفة أهمها دائرة الإعلام الآلي والالكترونيك المتخصصة التي تنقسم بدورها إلى ثلاثة مخابر هي مخبر الإعلام الآلي، مخبر الفيديو ومخبر الصوت.

ب- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: تأسس مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية في عام 2008، بهدف تأمين نظام المعلومات لخدمة الأمن العام، و يُعتبر المركز مركزًا توثيقيًا يتمركز في بئر مراد رايس، يُكرس المركز جهوده لتحليل بيانات الجرائم المعلوماتية التي تندرج ضمنها جرائم الاعتداء على التوقيع الالكتروني وتحديد مرتكبيها، سواء كانوا أفرادًا أو عصابات بهدف

[1]- المرسوم الرئاسي رقم 04-183 المؤرخ في 8 جمادى الأولى عام 1425 الموافق ل 26 يونيو 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج، العدد 41، لسنة 2004.

[2]- المادة 2 من نفس المرسوم.

[3]- المادة 3 من نفس المرسوم.

تأمين وحماية الأنظمة المعلوماتية خاصة تلك المستخدمة في المؤسسات الرسمية والبنوك وحماية حقوق الأفراد.[1]

كما يهدف المركز الوقاية من الجرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني الى مساعدة باقي الاجهزة الأمنية الاخرى في أداء مهامها، وقد تمكنت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وكذلك من خلال الملتقيات ذات الطابع الوطني والدولي وتبادل الخبرات مع الدول الاخرى، ان توفر القوى المؤهلة وذات الكفاءة من مهندسي الاعلام الالي ورجال القانون وذلك من اجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها.[2]

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.

المشرع الجزائري أنشأ الأقطاب الجزائية بهدف سد الفجوة المتعلقة بالعجز القائم في مكافحة الإجرام المستحدث، هذا النوع من الإجرام أثبت صعوبة التعامل معه من قبل القضاء العادي، مما دفع المشرع إلى إنشاء هيئات قضائية متخصصة ومؤهلة لمواجهة هذه الظاهرة، الهدف الرئيسي هو التقليل من الآثار الوخيمة لهذا الإجرام على الصعيدين المحلي والدولي.

اولا: الأقطاب الجزائية المتخصصة.

تم إنشاء جهاز قضائي متخصص لمعالجة القضايا الخطيرة، ويتمثل هذا الجهاز في الأقطاب الجزائية المتخصصة وفقًا للمرسوم التنفيذي رقم 06-348 الصادر في 5 أكتوبر 2006[3] يحدد هذا المرسوم الأقطاب الجزائية المتخصصة ويوسع الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق، وقد تم تحديد أربع محاكم على مستوى البلاد لتنفيذ هذا النظام، وهي محكمة سيدي أمحمد في الجزائر العاصمة، ومحكمة قسنطينة، ومحكمة

---

[1]– سميحة بلقاسم، حميد بوشوشة، **(الجريمة الإلكترونية بعد جديد للإجرام في الجزائر واقعها وآليات مجابهتها(، مجلة العلوم الانسانية**، جامعة أم البواقي، مجلد 10، العدد 1، جوان 2023، ص 551.

[2]–سميحة بلقاسم، حميد بوشوشة، مرجع سابق، ص552.

[3]–مرسوم تنفيذي رقم 06-348، مؤرخ في 12 رمضان 1427 الموافق لـ 5 أكتوبر 2006 يتضمن التمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج، العدد 63، لسنة 2006.

وهران، ومحكمة ورقلة، بالإضافة إلى ذلك تم إنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر رقم 21-11.[1]

وهذه الأقطاب المتخصصة هي هيئات قضائية أو محاكم محلية ذات اختصاص موسع، تركز على القضايا التي تعتبر خطيرة ومعقدة، بما في ذلك القضايا التي تنطوي على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وغيرها من السلطات الممنوحة لها وهذا ما تنص عليه صراحة المادة 37فقرة 2، والمادة 40، فقرة 2، والفقرة الأخيرة من المادة 329 من قانون الإجراءات الجزائية المعدل والمتمم بالقانون04-14[2]، وتيسر هذه المواد عمل المحاكم المتخصصة عن طريق توسيع نطاق الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق.

فقد نصت المادة 37 فقرة 2 من قانون الإجراءات الجزائية المعدل والمتمم بأنه يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

وأضافت المادة 40 فقرة 2 أنه يجوز تمديد الاختصاص المحلي لقاضي التحقيق الى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجرائم المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

كما جاء في الفقرة الاخيرة من المادة 329 أنه يجوز تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم اخرى عن طريق التنظيم، في جرائم المخدرات والجريمة

[1]-أمر رقم 21-11 مؤرخ في 16 محرم 1443 الموافق ل 25 غشت 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج،العدد 65، لسنة 2021.

[2]-قانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، عدد71، 2004.

المنظمة عبر الحدود الوطنية والجرائم الماسة بالمعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

وقد تم بالفعل صدور المرسوم التنظيمي الذي مدد الاختصاص لأربع جهات قضائية وهو المرسوم رقم 06-348 المؤرخ في 05/10/2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016[1] والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف وذلك على النحو الآتي:

1- القطب الجزائي المتخصص لمحكمة سيدي امحمد بالجزائر العاصمة ويمتد اختصاصه الإقليمي إلى المجالس القضائية الآتية: الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلى.

2- القطب الجزائي المتخصص لمحكمة قسنطينة يمتد اختصاصه الإقليمي إلى المجالس القضائية الآتية: قسنطينة وأم البواقي وباتنة وبجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالمة وبرج بوعريريج والطارف وخنشلة وسوق أهراس وميلة.

3- القطب الجزائي المتخصص لمحكمة ورقلة ويمتد اختصاصه الإقليمي إلى المجالس القضائية الآتية: ورقلة وأدرار وتامنغست وإيليزي وبسكرة والوادي وغرداية.

4- القطب الجزائي المتخصص لمحكمة وهران ويمتد اختصاصه الإقليمي إلى المجالس القضائية الآتية: وهران وبشار وتلمسان وتيارت وتندوف وسعيدة وسيدي بلعباس ومستغانم ومعسكر والبيض وتيسمسيلت والنعامة وعين تموشنت وغليزان.

ثانيا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

تم إنشاء هذا القطب بموجب الأمر رقم 21-11 المؤرخ في 25 غشت 2021 المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ويتواجد على مستوى مقر مجلس القضاء بالجزائر، ومنح له المشرع الجزائري صلاحية الفصل بشكل حصري في الجرائم المتصلة

[1]- مرسوم تنفيذي رقم 16-267 مؤرخ في 15 محرم عام 1448 الموافق ل 17 أكتوبر 2016 يعدل ويتمم المرسوم التنفيذي 06- 348 المؤرخ في 12 رمضان عام 1427 الموافق لـ 5 أكتوبر 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم وكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج، العدد 62، لسنة 2016.

بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها وذلك من خلال نص المادة 211 مكرر 24 من قانون الإجراءات الجزائية والتي جاء فيها: «مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي تحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

– الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني،

– جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع،

– جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،

– جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،

– جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين،

– جرائم التمييز وخطاب الكراهية.»

المطلب الثاني: وسائل وأساليب التحري عن جرائم الاعتداء على التوقيع الالكتروني.

في ظل التطورات المتسارعة في مجال الجريمة المعلوماتية، أقر المشرع الجزائري مجموعة من القواعد الإجرائية الجديدة ذات طبيعة خاصة، جاءت هذه الإجراءات في نص المادة 65 مكرر 5 و65 مكرر 11 من قانون الإجراءات الجزائية تتمثل في اعتراض المراسلات، تسجيل الأصوات، التقاط الصور، والتسرب، علاوة على ذلك سن المشرع القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جاء هذا القانون لتلبية مستلزمات التحريات والتحقيقات القضائية من خلال وضع ترتيبات تقنية تشمل مراقبة الاتصالات الإلكترونية، تجميع وتسجيل هذه الاتصالات في الحين، إجراء تفتيش للمنظومة المعلوماتية، و تنفيذ إجراءات

الحجز داخل هذه المنظومة، وبهذا لم ينحرف المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، بل قام بتطويرها بإضافة قواعد جديدة تتماشى مع المستجدات في مجال الجريمة المعلوماتية.

الفرع الأول: أساليب التحري في ظل قانون الإجراءات الجزائية.

نظرًا لتعقيدات الجريمة الإلكترونية وصعوبة تحديد الجناة بالطرق التقليدية أدخل المشرع الجزائري آليات تحقيق متقدمة بموجب التعديل الجديد لقانون الإجراءات الجزائية رقم 06-22[1]، تشمل هذه الآليات التسرب الإلكتروني أو الاختراق، اعتراض المراسلات وتسجيل الأصوات، وهو ما سيتم استعراضه في هذا الفرع.

أولا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

نتناول كل منها على مدى باعتبار كل منها يشكل إجراء مستقبل.

أ- **اعتراض المراسلات:** تعرف عملية اعتراض المراسلات بأنها تتبع سري ومتواصل للشخص المشتبه به قبل وبعد ارتكاب الجريمة، بهدف القبض عليه متلبسًا بارتكابها، ويُعرَف أيضاً كإجراء تحقيقي يتم سراً وينتهك سرية المحادثات الخاصة، تأمر به السلطة القضائية وفقاً للإجراءات المحددة قانوناً بهدف الحصول على دليل غير مادي يثبت تورط الشخص في الجريمة.[2]

وفقًا للمادة 65 مكرر 5 ق.إ.ج الجزائري، يُسمح لضابط الشرطة القضائية بالتدخل في مراسلات تتم عبر وسائل الاتصال السلكية واللاسلكية بعد الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق، وتثير هذه المادة تساؤلات حول تأويل هذه الوسائل لتشمل

[1]- قانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق ل 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 84، لسنة 2006.

[2]- سفيان عبد الحميد، **(أساليب التحري الخاصة في قانون الإجراءات الجزائية)** ، **مجلة صوت القانون**، كلية الحقوق والعلوم السياسية جامعة لونيسي علي، المجلد 9، العدد 2 ماي 2023، ص 209.

المراسلات المتبادلة بواسطة أجهزة الحاسوب الخاصة بالمتهمين وأطراف أخرى يتبادلون المراسلات معه، وهناك آراء ترى أن الهدف الأساسي من هذه الإجراءات هو التنصت على المكالمات الهاتفية، مما يتطلب بشكل كبير مراقبة المحادثات الهاتفية خلال عمليات التحري والتحقيق، فقد لعبت وسائل الاتصال الحديثة دورًا كبيرًا في تسهيل ارتكاب الجرائم المنظمة، سواء عبر المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عبر الشبكات المعلوماتية.[1]

وقد أجازت اتفاقية بودابست للجرائم الإلكترونية التدخل الشرعي في جميع أشكال نقل البيانات الإلكترونية سواء عبر التليفون، الفاكس أو البريد الإلكتروني، وتشمل هذه الاتصالات المتاحة للتدخل أو اعتراض المحتوى غير المشروع أو الدليل على أفعال إجرامية خطيرة، مما يستوجب ضرورة التدخل في المراسلات الإلكترونية المتبادلة عبر الحواسيب لمنع ومحاربة الجرائم ومعاقبة الجناة، وبالنسبة للمشرع الجزائري فقد فهم هذه الحاجة بوضوح عندما أذن بالتدخل في المراسلات السلكية واللاسلكية، وفيما يوحي به توجه المشرع من خلال أحكام قانون 09-04 المتعلق بالوقاية ومكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، حيث سمح المشرع بوضع التدابير التقنية لمراقبة الاتصالات الإلكترونية وتنفيذ عمليات التفتيش والحجز داخل أنظمة المعلوماتية تحت إشراف السلطة القضائية.[2]

ب-تسجيل الأصوات: عملية تسجيل الأصوات تمثل النقل الآلي والمباشر للموجات الصوتية من مصادرها الأصلية بكل تبايُناتها وخصائصها الفريدة ومميزاتها الشخصية على جهاز مخصص لهذا الغرض، يتيح هذا الجهاز إعادة تشغيل الصوت المسجل وتحليل محتواه والتعرف على سماته المميزة التي تُستخدم في عمليات المقارنة عند مقارنته بصوت الشخص الذي يعود إليه، مما يسهل تحديد هويته أو نفيها، ويُعتبر التسجيل تجسيدًا لشخصية صاحب الصوت يفوق ما يمكن تمثيله من خلال صورته البصرية.[3]

---

[1]- جميلة محلق، **(إعراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري)**، **مجلة التواصل في الاقتصاد والإدارة والقانون**، صادرة عن كلية الحقوق والعلوم السياسية جامعة باجي مختار عنابة، مجلد 21، العدد 42، جوان 2015، صفحه 178.

[2]- المرجع نفسه.

[3]- بدرة صرياك، **أساليب التحري في جرائم الفساد**، مذكرة مقدمة لنيل متطلبات شهادة الماستر في القانون الجنائي والعلوم الجنائية، معهد الحقوق والعلوم الاقتصادية، المركز الجامعي سي الحواس -بريكة-، 2019 ص 55.

فبعد منح المشرع للمشتبه به الحق في الصمت، يتم إدراج استثناء لهذا الحق بشكل غير مباشر وفق المادة 65 مكرر 5، هذا الاستثناء يتيح السماح باستخدام اعتراف الشخص ضد نفسه دون موافقته أو رضاه من خلال تسجيل أي تصريحات خاصة أو سرية يقوم بإطلاقها.

وفي هذا السياق تنص المادة 65 مكرر 5 فقرة 3 من قانون الإجراءات الجزائية على ضرورة وضع الترتيبات الفنية اللازمة لتنظيم عمليات التسجيل والاعتراض على المراسلات بشكل صحيح، وذلك لضمان احترام حقوق الأفراد وتنفيذ الإجراءات القانونية بشكل صحيح وعادل.

ج- التقاط الصور: عملية التصوير هي عملية مراقبة بصرية تُنفذ باستخدام كاميرات وأجهزة خاصة قادرة على التقاط الصور وتسجيل الصوت لتوثيق حالة معينة لشخص أو مجموعة من الأشخاص، تمثل هذه العملية مراجعة مادية بصرية لحالة شخص أو جماعة معينة في الزمان والمكان الذي كانوا يَشهدونه خلال التقاط الصور، وتقوم بربط الزمان والمكان والأشخاص في آن واحد، بالإضافة إلى ذلك يمكن أن تمتد النتائج المأخوذة من هذه العملية إلى توثيق دليل مادي للجريمة والبيئة المحيطة بها.[1]

وتقنية التصوير تقدم فوائد متعددة وحيوية في مجالات التحقيق والتحقيق الجنائي، حيث يساهم توثيق مسرح الجريمة من خلال التصوير الاحتفاظ بحالته الأولية والتي كانت عليها أثناء ارتكاب الجريمة لفترة زمنية ممتدة، مما يتيح للمحققين فرصة مراجعتها وتحليلها بدقة كلما اقتضت الضرورة مما يزيد من فرص إلمامهم بالتفاصيل المهمة وتوثيق الأدلة بدقة.

ومن أجل صون الحرية الفردية، أحاط المشرع استخدام هذه الأساليب بقيود قانونية لمنع أي تعسف، وتتمثل هذه الشروط فيما يلي:

1 – مراعاة الجرائم التي تجوز فيها هذه الإجراءات: أي لا يتم اللجوء إلى اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إلا في الجرائم المحددة حصرا في قانون الإجراءات الجزائية الجزائري، وتتمثل في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات

[1]– بدرة صرياك، مرجع سابق، ص59.

والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.[1]

2 – ترخيص السلطة القضائية ومراقبتها: يعني أن ضابط الشرطة القضائية لا يُجيز له التدخل في المراسلات إلا بعد الحصول على إذن كتابي وصريح من وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، يشترط في هذا الإذن تحديد نوع الجريمة التي أدت إلى الحاجة للاستقصاء أو التحقيق القضائي، وكذلك الموضوع المراد الاعتراض عليه أو التنصت عليه في المراسلة والاتصال. يجب أن يتم هذا الإجراء تحت إشراف مباشر من السلطة التي أذنت به.[2]

3– كتمان السر المهني: يسمح الإذن لضابط الشرطة القضائية المأذون له أو المناب باعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور دون المساس بالسر المهني، يُؤكد المشرع على ضرورة حماية هذه السرية من خلال تعيين أفراد مؤهلين للوصول إلى الأسرار وفرض عقوبات على من يكشف أسرار الأشخاص بشكل ينتهك قواعد الإجراءات الجزائية. كما يتضمن وضع قواعد وتنظيم الإجراءات التي يجب على أفراد الشرطة القضائية اتباعها.[3]

4–مراعاة مدة الإجراء: حددتها الفقرة 2 من المادة 65 مكرر 7 ب أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، حسب تقدير نفس السلطة مصدرة الإذن لمقتضيات التحقيق.

---

[1]– المادة 65 مكرر 5 من القانون 06–22.

[2]– جمال براهيمي، **(مكافحة الجرائم الالكترونية في التشريع الجزائري)**، **المجلة النقدية للقانون والعلوم السياسية**، كلية الحقوق والعلوم السياسية، جامعة مولود معمري–تيزي وزو–، المجلد 11، عدد 2، ص 140.

[3]– المادة 65 مكرر 6 من القانون 06–22.

5- أن تنفذ من عون مؤهل: حيث يجوز لوكيل الجمهورية أو لضابط الشرطة القضائية أو لقاضي التحقيق أن يسخر كل عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة للتكفل بالجوانب التقنية للعملية المطلوب إنجازها.[1]

6-تحرير محضر حول عملية الاعتراض: أي يجب على سلطات التحقيق المختصة تحرير محضرا عن تفصيل كل عملية اعتراض وتسجيل المكالمات والمراسلات وعن عملية التقاط والتسجيل الصوتي أو السمعي البصري، كما يُذكر بالمحضر تاريخ بداية هذه العمليات ونهايتها.[2]

ثانيا: التسرب.

في سبيل حماية التوقيع الالكتروني من مختلف الجرائم التي تطاله ، يمكن اللجوء إلى إجراء التسرب حيث يعتبر هذا الأخير تقنية جديدة أدرجها المشرع الجزائري بموجب القانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5) ، والذي أفرد الفصل الخامس منه تحت عنوان" في التسرب"، والذي تضمن 8 مواد، من المادة 65 مكرر 11 حتى المادة 65 مكرر 18 ، وتناول من خلالها تحديد مفهوم هذه العملية في المادة 65 مكرر 12 بانها «يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية ، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف »

أي أن التسرب يتمثل في تلك العملية الأمنية المنسقة بدقة من قبل جهات الضبط القضائي، حيث تهدف إلى تسلل أحد أفراد الشرطة داخل جماعة إجرامية بهدف كسب ثقتها، ومن ثم الكشف عن حقيقة الأنشطة الإجرامية التي تقوم بها وتحركاتها، وذلك لتسهيل عملية اعتقالها من قبل الجهات الأمنية.[3]

---

[1]- المادة 65 مكرر 8 من القانون 06-22.

[2]- المادة 65 مكرر 9 من نفس القانون.

[3]- خدوجة الذهبي، **الحماية الجزائية للمعاملات الالكترونية -دراسة مقارنة-**، رسالة مقدمة لنيل شهادة دكتوراه علوم في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية -أدرار-، 2019، ص 227.

ولضمان نجاح عملية التسرب في الكشف عن جرائم التوقيع الالكتروني، يلتزم المتسرب القيام بهذه العملية بكل الإجراءات المحددة قانونا وتتمثل في:

-صدور إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.[1]

-أن يكون الإذن مكتوبا ومسببا وذلك تحت طائلة البطلان، وتذكر فيه مبررات اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، كما تحدد مدة التسرب التي لا يمكن أن تتجاوز 4 أشهر مع امكانية تجديد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.[2]

وتنطوي عملية التسرب في هذا النوع من الجرائم على دخول ضابط الشرطة القضائية إلى العالم الافتراضي عن طريق خرق مواقع شبكية محددة واستغلال نقاط ضعف إلكترونية، ويجوز لهم إجراء محادثات في غرف الدردشة أو إجراء اتصالات مباشرة مع المشتبه فيهم، كما لو كانوا واحداً منهم باستخدام الأسماء المستعارة والخواص الوهمية لاستخلاص معلومات المهمة، وقد سمح المشرع باستخدام طرق وتقنيات خاصة للتسرب، رغم أنها قد تعتبر غير قانونية بموجب مبدأ حرمة الحياة الخاصة، ومع ذلك يمكن للمشرع أحيانًا تجاوز حرمة الحياة الخاصة باستناد إلى القواعد الإجرائية في بعض الظروف لضمان تحقيق العدالة وضبط الجريمة بفعالية.[3]

ولهذا يمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا، القيام بما يأتي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها،

---

[1]-المادة 65 مكرر 11 من القانون 06-22.

[2]- المادة 65 مكرر 15، من نفس القانون.

[3]- فاطمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية** ، ملخص لمذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021، ص55.

-استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ويمنع بشكل قاطع على المتسرب الكشف عن هويته تحت أي ظرف كان أثناء تنفيذ عملية التسرب، باستثناء عند التواصل مع رؤسائهم فقط، لان إفشاء الهوية يمكن أن يؤدي إلى إفشال الخطة المعدة لاعتقال المشتبه بهم، بالإضافة إلى تعريض العميل الذي تم الكشف عن هويته للخطر.

كما عاقب المشرع الجزائري في المادة 65 مكرر 14 من القانون 06-22 كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 200.000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 200.000 دج إلى 500.000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من 500.000دج إلى 1.000.000 دج،

وفي الحالة التي يتقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة أربعة (4) أشهر، يخبر القاضي الذي أصدر الرخصة المنصوص عليها في المادة 65 مكرر 11 أعلاه، في أقرب الآجال. وإذا انقضت مهلة الأربعة (4) أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، يمكن هذا القاضي أن يرخص بتمديدها لمدة أربعة (4) أشهر على الأكثر.[1]

[1]- المادة 65 مكرر 17 من القانون 06-22.

الفرع الثاني: أساليب التحري في ظل قانون 09-04.

تتمثل هذه الإجراءات في مراقبة الاتصالات الالكترونية وتفتيش منظومة التوقيع الالكتروني وحجز المعطيات بالإضافة الى بعض الالتزامات التي تقع على عاتق مؤدي الخدمات.

أولا: المراقبة الالكترونية :

تعد مراقبة الاتصالات الإلكترونية من بين أهم الإجراءات التي تساهم في الكشف عن الجرائم الواقعة على التوقيع الإلكتروني، باعتبار أنه يتم تضمين بيانات التوقيع الإلكتروني وشهادة التصديق الإلكترونية كذلك في المراسلات محل هذا الإجراء الوارد في القانون 09-04، وذلك وفقًا لتعريف الاتصالات الإلكترونية المبين في المادة العاشرة من القانون 18-04 الذي يحدد القواعد العامة للبريد والاتصالات الإلكترونية " كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

وهو نفس ما جاءت به أحكام المادة 2 من القانون 09-04 التي عرفت الاتصالات الإلكترونية على أنها «الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.»

ومحل المراقبة هو ذلك الهدف الذي تتم مراقبته وتتبع حركاته وتصرفاته في نطاق المراقبة الإلكترونية محل المراقبة هو الحاسوب الرقمي أو الموقع عبر شبكة الانترنت أو البريد الالكتروني بما يحتويه من مراسلات الكرتونية وحلقات نقاش وغرفة دردشة، وقد يكون محلها الهاتف النقال المتصل بشبكة الإنترنت وحتى ساعة اليد الذكية أو اللوح الرقمي، إذن محل المراقبة يشمل الاتصالات الالكترونية الخاصة والتي عرفتها المادة الثانية من القانون 09-04[1] وقد استعمل المشرع الجزائري مصطلح مراقبة الاتصالات الالكترونية في نص المادة 4 من القانون 09-04 وبيّن الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وتتمثل:

[1]-عبد الرؤوف بوديسة، مرجع سابق، ص 58.

ا- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

ب - في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج - مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د - في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما بين أنه لا يجوز إجراء عمليات المراقبة في الحالات المذكورة في نص المادة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

نلاحظ من خلال هذه المادة أن إجراء المراقبة الالكترونية في جرائم التوقيع الالكتروني يتم اللجوء إليه في حالة احتمال الاعتداء على منظومة معلوماتية متعلقة بالتوقيع الالكتروني بشرط أن يكون هذا الاعتداء يهدد ويمس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، والتي تخضع للسلطة التقديرية للأمر بالإجراء.

كان المشرع قد أسند مهمة تنفيذ عملية مراقبة الاتصالات الالكترونية لجهة حصرية وحدد أشخاصا معينين للقيام والإشراف على هذه العملية بموجب المادة 26 من القانون 21-439 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التي نصت على أنه «يمكن الهيئة، لتنفيذ عملية مراقبة الاتصالات الإلكترونية أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية، يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية تحت إدارة ومراقبة قاض لدى الهيئة، وبمساعدة ضابط من الشرطة القضائية أو أكثر ينتمي للهيئة، تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلمة من السلطة القضائية.

وتدون أشغالها في محاضر تعد طبقا لأحكام قانون الإجراءات الجزائية.»

ثم خول مراقبة الاتصالات الإلكترونية إلى مديرية المراقبة الوقائية واليقظة الالكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث جاء في المرسوم 21-439 أن مديرية المراقبة الوقائية واليقظة الإلكترونية تكلف بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول.[1]

ثانيا: تفتيش منظومة التوقيع الإلكتروني.

لم يقدم المشرع تعريفا دقيقاً ومحدداً للتفتيش رغم اعتبار هذا الإجراء من أهم إجراءات التحري والتحقيق، ويراعى تحديد قواعد صارمة لتنظيمه، وبالرجوع للدستور الجزائري نجده نص على عدم جواز المساس بحرية الأشخاص وكرامتهم حيث جاء فيه ان التفتيش لا يكون إلا بمقتضى القانون وبأمر مكتوب صادر عن السلطة القضائية المختصة.[2]

وقد استحدث إجراء تفتيش المنظومة المعلوماتية من خلال نص المادة 5 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 09-04 انه «يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى: أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.»

من خلال نص المادة أعلاه نلاحظ أن المشرع الجزائري في تفتيش في المنظومة المعلوماتية يميز بين ما إذا كانت المنظومة متصلة بنظام آخر داخل الإقليم الجزائري أو كانت المنظومة متصلة بمنظومة معلوماتية تقع خارج الإقليم الوطني.

---

[1]– المادة 14 من المرسوم الرئاسي رقم 21-439.

[2]– المادة 48 من المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 سبتمبر 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج.ر.ج.ج، العدد 82، لسنة 2020.

في الحالة المنصوص عليها في الفقرة– أ– من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.[1]

إذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.[2]

والمشرع الجزائري يجيز الدخول الى المنظومة المعلوماتية دون إذن صاحبها بغرض التفتيش، ونظرا لصعوبة تنفيذ هذا الإجراء من الجانب التقني أجاز للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.[3]

يقع على عاتق الخبير مسؤولية توضيح كيفية تشغيل الأنظمة بشكل كافٍ، بالإضافة إلى شرح طرق الوصول إليها وإلى البيانات المخزنة أو المعالجة أو المنقولة بطريقة قابلة للفهم والتفاعل، ويكفل هذا الامر استنارة العملية القضائية بأحدث المعارف العلمية والتقنية، مما يعزز دقة الحكم ونزاهته[4].

غير أن تقديم الخبرة العلمية المتعلقة بجرائم التوقيع الإلكتروني أمام قاضي الحكم، تخضع لسلطته التقديرية، فالقاضي ليس ملزمًا بنتائج الخبير حيث تخضع هذه النتائج

---

[1]– المادة 5 من قانون 09-04.

[2]– المرجع نفسه.

[3]– المرجع نفسه.

[4]–رضا هميسي، **(تفتيش المنظومة المعلوماتية في القانون الجزائري)** ، **مجلة العلوم القانونية والسياسية**، صادرة عن كلية الحقوق والعلوم السياسية جامعة الشهيد حقه لخضر بالوادي، دون مجلد، العدد 5، جوان 2012 ،ص 172.

اقتناعه الشخصي، وبالتالي فإن الخبرة العلمية بغض النظر عن مدى دقتها وموضعيتها، لا تُلزم القاضي بالضرورة باتخاذ قرار معين.[1]

ثالثا: حجز المعطيات المعلوماتية.

بالإضافة لإجراء المراقبة الالكترونية والتفتيش أجاز المشرع من خلال المادة 6 من القانون 09-04 المشار إليه سابقا حجز المعطيات المخزنة داخل النظم المعلوماتية إذا كانت تفيد في الكشف عن الجرائم التي تمس بالتوقيع الالكتروني ومرتكبيها.

أما عن طريقة حجز المعطيات المعلوماتية الخاصة بالتوقيع الالكتروني فإنها تتم بنسخ المعطيات محل البحث والمعطيات الضرورية لفهمها على دعامة تخزين إلكترونية، وتكون قابلة للحجز ثم توضع في احراز طبقا لأحكام قانون الاجراءات الجزائية ويتم اللجوء إلى عملية النسخ عندما يكون من غير الضروري حجز كل المنظومة المعلوماتية المتعلقة بالتوقيع الالكتروني، وفي ذات السياق اوجب المشرع في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط ألا يؤدي ذلك إلى المساس بمحتوى المعطيات.[2]

أما بالنسبة الحالة الثانية فهي الحجز عن طريق منع الوصول إلى المعطيات، وتتم إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.[3]

---

[1]-فارس خطابي، مرجع سابق، ص 295.

[2]-المادة 6 من القانون 09-04.

[3]-المادة 7 من نفس القانون.

كما يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.[1]

رابعا: التزامات مؤدي الخدمات.

لقد أورد المشرع الجزائري مجموعة من الالتزامات التي تقع على عاتق مقدمي الخدمات نظرا لأهميته في البحث والتحري للكشف عن جرائم الاعتداء على التوقيع الالكتروني نذكر منها ما جاء في القانون 09-04.

أ- التزام مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من نفس القانون تحت تصرف السلطات المذكورة، كما يتعين على مقدمي الخدمات كتان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[2]

ب-الالتزام بحفظ المعطيات المتعلقة بحركة السير: حيث ألزم القانون 09-04 بموجب المواد 11و12 مقدمو الخدمات بحفظ: - المعطيات التي تسمح بالتعرف على مستعملي الخدمة، - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع اطلع عليها.

[1]-المادة 8 من القانون 09-04.

[2]- المادة 10 من نفس القانون.

-التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

المبحث الثاني: العقوبات المقررة للاعتداء على التوقيع الالكتروني.

نظرًا لأهمية بروز التوقيع الإلكتروني في مجالات الأعمال التجارية والقضايا القانونية، يجب توفير حماية قانونية قوية لضمان صحة وثبات هذا النوع من التوقيعات، يأتي ذلك نتيجة للمسؤوليات القانونية التي قد تنشأ في حالة مخالفة الالتزامات المتعلقة بالتوقيع الإلكتروني، وعليه قامت التشريعات المختلفة بما فيما التشريع الجزائري بتوفير حماية للتوقيع الإلكتروني من خلال فرض عقوبات صارمة على الأفعال غير المشروعة التي تستهدف هذا النوع من التوقيعات.

المطلب الأول: العقوبات المقررة في إطار قانون العقوبات.

يمتاز التوقيع الإلكتروني بمستوى عالٍ من الأمان التقني والقانوني يضمن عدم تلاعب به أو انتهاكه، وقد أبدى المشرع الجزائري اهتمامًا فائقًا بتعزيز هذا الجانب من خلال تضمين مجموعة من العقوبات الجزائية في القانون رقم 04/15 التي تنطوي على مسؤولية قانونية لكلٍ من الأفراد والكيانات القانونية على حد سواء.

الفرع الأول: العقوبات المقررة للشخص الطبيعي.

نتناول من خلال هذا الفرع العقوبات التي تفرض على الاشخاص الطبيعيين نتيجة اعتدائهم على التوقيع الالكتروني، بهدف ردع هذه الأفعال وحماية المجتمع الرقمي، وتنقسم هذه العقوبات إلى أصلية وأخرى تكميلية.

أولا: العقوبات الأصلية :

تعرف العقوبات الأصلية طبقا لنص المادة 4 من قانون العقوبات انها تلك التي يجوز الحكم بها دون أن تقترن بها أية عقوبة أخرى، والمشرع صنف جرائم المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الإلكتروني الواردة في قانون العقوبات على انها جنح بسيطة وقرر لها عقوبات سالبة للحرية بالإضافة للغرامة، كما أنه اعتمد سلما تصاعديا للعقوبات حسب خطورة الجريمة والتي يمكن تقسيمها إلى ثلاث فئات:

- عقوبة الدخول أو البقاء غير الشرعي البسيطة.
- عقوبة الدخول أو البقاء غير الشرعي المشددة.
- عقوبة المساس العمدي بالمعطيات.

أ- عقوبة الدخول أو البقاء غير الشرعي في النظام المعلوماتي للتوقيع الالكتروني:

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

1- في صورتها البسيطة: يعاقب المشرع الجزائري طبقا لنص المادة 394 مكرر الفقرة 1 من قانون العقوبات بالحبس من ثلاثة (3) أشهر الى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج على كل دخول أو بقاء غير مصرح به على قاعدة بيانات تتعلق بالتوقيع الالكتروني مالم يترتب عن هذه الأفعال اي اعاقة او افساد لهذا النظام.

2- في صورتها المشددة: طبقا لنص المادة 394 مكرر الفقرة 2 و3 ضاعف المشرع الجزائري العقوبة الواردة في الفقرة الأولى إذا ترتب عن الدخول أو البقاء غير الشرعي حذف أو تغيير للمعطيات، كما نصت الفقرة الاخيرة من نفس المادة أنه إذا أدى الدخول أو البقاء إلى تخريب نظام اشتغال المنظومة فالعقوبة المقررة تكون من ستة أشهر إلى سنتين حبس وغرامة من 50.000 دج الى 150.000دج.

ب- العقوبة المقررة للاعتداء القصدي على معطيات التوقيع الالكتروني:

كما ذكرنا سابقا ان هذه الجريمة تتمثل في فعل الإدخال، الإزالة أو التعديل وتعاقب المادة 394 مكرر 01 بالحبس 06 ستة أشير إلى 03 ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

وتضاعف وتشدد العقوبات المشار إليها في المادة 394 مكرر و394 مكرر 1 و2 إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر3.

ثانيا: العقوبات التكميلية.

بالإضافة للعقوبات الأصلية التي فرضت من قبل المشرع الجزائري، تم اتخاذ عقوبات تكميلية تعتبر عادة عقوبات اضافية لتعزيز فعالية الردع وتتمثل في:

أ-المصادرة: تعرف المادة 15 فقرة 1 من قانون العقوبات المصادرة بأنها الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء، وتشمل المصادرة فيما يتعلق بهذه الجرائم الأجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة مع مراعاة حقوق الغير الحسن النية طبقا لما جاء في المادة 394 مكرر 6 من قانون العقوبات.

ب- غلق المواقع: حيث نصت المادة 394 مكرر 06 بإغلاق المواقع التي تكون محلا لجرائم المساس بالمعالجة الآلية للمعطيات، مع إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

الفرع الثاني: العقوبات المطبقة على الشخص المعنوي.

إذا كان المشرع قد عبر وبصفة صريحة عن موقفه من مسؤولية الشخص المعنوي جزائيا وهو ما يتضح من خلال نص المادة 51 مكرر من قانون العقوبات التي تنص «باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام يكون

الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك...».

أولا: العقوبات الأصلية.

تنص المادة 18 مكرر من قانون العقوبات المعدل بموجب القانون 06/23 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 لمدة لا تتجاوز 5 سنوات ات.
- مصادرة الشيء المستعمل في ارتكاب الجريمة أو نتج عنها
- نشر وتعليق 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 إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فقد نصت عليها المادة 394 مكرر 4 من ق العقوبات على النحو الآتي: «يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.»

ثانيا: العقوبات التكميلية.

"العقوبات التكميلية" تشير إلى نفس العقوبات المفروضة على الأفراد الطبيعيين كما هو مبين في المادة 394 من قانون العقوبات، والتي تم شرحها سابقًا في الفرع الأول المخصص للجزاءات المفروضة على الأشخاص الطبيعيين، ويُحتفظ بحقوق أصحاب النية

الحسنة بقرار يتضمن مصادرة الأجهزة والبرامج والوسائل المستخدمة، بالإضافة إلى إغلاق المواقع التي تُستخدم كمكان للجرائم المعاقب عليها وفقًا لهذا النص، ويمكن أيضًا إغلاق المحل أو الموقع المستغل في حالة ارتكاب الجريمة بمعرفة صاحبها.[1]

والمشرع الجزائري لم يكتف بتجريم هذه الأفعال فقط وانما جرم قبل ذلك أي اتفاق على المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني، والحكمة من تجريم الاتفاق على التخطيط لارتكاب أي من الجرائم المنصوص عليها في إطار قانون المعالجة الآلية للمعطيات يعكس استهداف المشرع لاحتواء جرائم التخطيط في مراحلها الأولى، تسبق حتى مرحلة الشروع، لأن الاتفاق على ارتكاب الجريمة يضفي عليها بُعداً تنظيمياً يستدعي التدخل المبكر لمنع حدوثها ، وقد جاء في المادة 394 مكرر5 من قانون العقوبات « كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها»، يتضح أن المشرع لم يخرج عن القواعد العامة في معاقبة الشريك وإنما جعله معرضًا لنفس العقوبة المفروضة على الشخص الأصلي في الجريمة، ويستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية.[2]

أما عن عقوبة الشروع فقد نصت عليها المادة 394 مكرر 7 من القانون 06-22 بأن يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

المطلب الثاني: العقوبات المقررة في إطار بعض القوانين الخاصة.

عمل المشرع الجزائري على تعداد مختلف الجرائم التي تطال التوقيع الالكتروني وكذا شهادة التصديق الإلكتروني لارتباطها المباشر به، من خلال القانون 15-04 الذي يحدد

[1]– يوسف بوزبيدة، مرجع سابق، ص 44.

[2]– فارس خطابي، مرجع سابق، ص132 و ص133.

القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني وكذا القانون 24-02، وعليه سوف يتم التفصيل في هذا المطلب في العقوبات الواردة في كلا القانونين.

الفرع الأول: العقوبات المقررة في إطار القانون 15-04.

إن تحليل العقوبات المقررة لجرائم الاعتداء على التوقيع الالكتروني في ظل القانون 15-04 نهدف من خلاله للتعرف على السياسة العقابية التي انتهجها المشرع الجزائري لمواجهة والحد من هذه الجرائم.

أولا: العقوبات المالية.

فرض المشرع الجزائري على مقدمي خدمات التصديق على التوقيع الالكتروني عقوبات في حالة إخلالهم بمسؤولياتهم ونصت على هذه العقوبات المواد 64 و65 من القانون 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني.

فقد نصت المادة 64 من القانون 15-04 أنه في حالة عدم احترام مؤدي خدمات التصديق الإلكتروني أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به والموافق عليها من طرف السلطة الاقتصادية تطبق عليه هذه السلطة عقوبة مالية يتراوح مبلغها بـ مائتي ألف دينار (200.000 دج) وخمسة ملايين دينار (5.000.000 دج) حسب تصنيف الأخطاء المنصوص عليها في دفتر الأعباء الخاص بمؤدي الخدمات، وتعذره بالامتثال بالتزاماته في مدة تتراوح بين ثمانية (8) أيام وثلاثين (30) يوما حسب الحالة. وتبلّغ المآخذ المتخذة ضد مؤدي الخدمات حتى يتسنى له تقديم مبرراته الكتابية ضمن الآجال المذكورة سابقا.

ثانيا: العقوبات الإدارية.

في حالة عدم امتثال مؤدي الخدمات للأعذار تتخذ ضده السلطة الاقتصادية للتصديق الإلكتروني قرار سحب الترخيص الممنوح له وإلغاء شهادته حسب الحالة بعد

موافقة السلطة، وتحدد كيفيات تحصيل المبالغ المتعلقة بالعقوبة المالية المنصوص عليها في الفقرة الأولى من هذه المادة عن طريق التنظيم.[1]

وتضيف المادة 65 من نفس القانون أنه في حالة انتهاك مؤدي خدمات التصديق الإلكتروني للمقتضيات التي يتطلبها الدفاع الوطني والأمن العمومي تقوم السلطة الاقتصادية للتصديق الإلكتروني بالسحب الفوري للترخيص وذلك بعد موافقة السلطة.

وتكون تجهيزات مؤدي خدمات التصديق الإلكتروني محل تدابير تحفظية طبقا للتشريع المعمول به وذلك دون الإخلال بالمتابعات الجزائية.

ثالثا: العقوبات الجزائية.

إلى جانب العقوبات المالية والإدارية فرض المشرع أيضا مجموعة من العقوبات الجزائية والتي نص عليها في القانون 15- 04 السالف الذكر من المادة 66 إلى 75.

أ-العقوبة المقررة لجريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق الالكتروني:

يعاقب المشرع الجزائري على جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة التصديق الالكتروني حسب نص المادة 66 من القانون 15- 04 بالحبس من ثلاثة (3) أشهر الى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20,000دج) الى مائتي ألف دينار (200,000 دج) أو بإحدى هاتين العقوبتين فقط.

وتضاعف الغرامة المذكورة أعلاه خمس (05) مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي اي أنها تقدر بمليون دينار جزائري (1.000.000 دج) وفقا لنص المادة 75 من قانون التوقيع والتصديق الالكترونيين.

وباستقراء المادة 45 من القانون15-04 نلاحظ ان المشرع أعطى لمؤدي خدمات التصديق الإلكتروني الحق في إلغاء شهادة التصديق الالكتروني الموصوفة إذا تبين له أنه قد تم منحها بناء على معلومات خاطئة أو مزورة، أو إذا أصبحت المعلومات الواردة

[1]-المادة 64 من القانون 15-04.

في شهادة التصديق الإلكتروني غير مطابقة للواقع أو إذا تم انتهاك سرية بيانات إنشاء التوقيع.

ب- عقوبة الإخلال بأخبار السلطة الاقتصادية بوقف نشاط التصديق الإلكتروني:

يعاقب الشخص الطبيعي بالحبس من شهرين (2) إلى سنة (1) واحدة، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن النشاط وفقا لنص المادة 67 من قانون التوقيع الالكتروني.

وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف هو شخص معنوي اي بغرامة قدرها خمسة ملايين دينار جزائري (5.000.000 دج) وفقا لنص المادة 75 من قانون التوقيع والتصديق الالكترونيين.

ج- عقوبة حيازة أو إفشاء أو استعمال بيانات إنشاء التوقيع الالكتروني موصوف خاصة بالغير:

يعاقب المشرع الجزائري على جريمة حيازة او افشاء أو استعمال بيانات إنشاء التوقيع الالكتروني موصوف خاصة بالغير نص المادة 68 من القانون 15-04 بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000 دج) إلى خمسة ملايين دينار (5.000.000 دج) أو بإحدى هاتين العقوبتين فقط، وتضاعف الغرامة المذكورة أعلاه خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب هذه الجريمة شخص معنوي أي بغرامة مالية قدرها خمسة وعشرون مليون دينار جزائري (25.000.000دج) طبقا لنص المادة 75 من نفس القانون.

د-عقوبة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني:

يعاقب المشرع في نص المادة 69 من القانون 15-04 على جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط. أما في حال كان الجاني شخص معنوي

فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي اي أنها تقدر بمليون دينار (1.000.000 دج) حسب نص المادة 75 من نفس القانون.

هـ-عقوبة انتهاك سرية بيانات شهادة التصديق الإلكتروني:

تعاقب المادة 70 من قانون التوقيع والتصديق الالكترونيين كل مؤدي خدمات تصديق الكتروني اخلى بأحكام السرية المنصوص عليها في المادة 42 من نفس القانون بالحبس من ثلاثة (3) أشهر إلى سنتين وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط.

اما إذا كان مرتكب الجريمة من بين الأشخاص المكلفون بالتدقيق، فان عقوبته حددتها المادة 73 من قانون التوقيع والتصديق الالكترونيين وتتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) وإلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط.

و-عقوبة جمع البيانات الشخصية للمُوقع واستخدامها في غير غرضها:

يعاقب المشرع الجزائري على جريمة جمع البيانات الشخصية للمُوقع واستخدامها في غير غرضها حسب نص المادة 71 من القانون 15-04 بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط.

وتضاعف الغرامة خمس مرات 05 مرات الحد الأقصى إذا كان مرتكبها هو شخص معنوي أي تقدر الغرامة ب خمسة ملايين دينار جزائري (5.000.000 دج) وفقا لنص المادة 75 من نفس القانون.

ز-عقوبة مزاولة نشاط التصديق الالكتروني بدون رخصة:

بالرجوع الى المادة 72 من القانون 15-04 نجد أن المشرع الجزائري قرر لهذه الجريمة عقوبة تتمثل في الحبس من سنة (1) واحدة إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليوني دينار (2.000.000 دج) أو بإحدى

هاتين العقوبتين مع مصادرة التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعمول به.

وهذا في حال كان الجاني شخصا طبيعيا، اما إذا كان شخصا معنويا تضاعف الغرامة حيث يعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي اي تقدر ب عشرة ملايين دينار جزائري (10.000.000 دج).

ح- عقوبة الاستعمال غير المشروع لشهادة التصديق الإلكتروني:

تأتي عقوبة هذه الجريمة على خلاف باقي الجرائم التي سبق ذكرها باعتبارها عقوبة مالية وليست سالبة للحرية حيث جاء في نص المادة 74 من القانون 15-04 على أن يعاقب كل شخص طبيعي يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها بغرامة من ألفي دينار (2.000 دج) إلى مائتي ألف دينار (200.000 دج).

وتضاعف هذه الغرامة خمس مرات 05 مرات الحد الأقصى إذا كان مرتكب جنحة الاستعمال غير المشروع لشهادة التصديق الالكتروني الموصوفة هو شخص معنوي اي بغرامة مالية قدرها مليون دينار جزائري (1.000.000 دج) وفقا لنص المادة 75 من قانون التوقيع والتصديق الالكترونيين.

الفرع الثاني: العقوبات المقررة في ظل القانون 24-02.

كما سبق وقلنا أنه يمكن تصور حصول التزوير في المحررات في نطاق المعلوماتية، وفي هذه الحالة تسمى جريمة التزوير بأنها جريمة تزوير معلوماتية وانطلاقا من أن التوقيع الإلكتروني جزء لا يتجزأ من المحرر الالكتروني فان وقوع التزوير عليه هو أمر وارد وبالرجوع للمشرع الجزائري نجده لم ينص على العقوبة المقررة لجريمة تزوير التوقيع الإلكتروني لذلك نلجأ لتطبيق العقوبات الواردة في القواعد العامة.

أولا: العقوبات الأصلية.

في المجال القانوني لا توجد عقوبة واحدة على التزوير، بل تختلف العقوبة تبعا لوضع مرتكب الجريمة، فعلى سبيل المثال إذا ارتكب قاض أو موظف أو ضابط عمومي تزويراً أثناء عمله، يُحكم عليه بعقوبة أشد بسبب إخلاله بواجباته وخيانة الأمانة التي وُضِعَت عليه وكذلك الأمر بالنسبة للشخص المعنوي، وهذا يبرز أهمية الحفاظ على النزاهة والأمانة في الأدوار المهنية، لأن أي انتهاك لهذه المبادئ يمكن أن يؤدي إلى عواقب وخيمة.[1]

1-عقوبة التزوير الذي يقع من الموظف المختص :

تنص المادة 32 فقرة 1 من القانون السالف الذكر على أنه: «يعاقب بالسجن المؤقت من عشرين (20) سنة إلى ثلاثين (30) سنة، كل قاض أو موظف أو ضابط عمومي، ارتكب عن قصد تزويرا في محررات عمومية أو رسمية أثناء تأدية وظيفته ...»

وتضيف الفقرة الثانية من نفس المادة: «ويعاقب بنفس العقوبة، كل قاض أو موظف أو ضابط عمومي، قام عن قصد أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش، وذلك إما بكتابة اتفاقات خلاف التي دُونت أو أمليت أمامه من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بأن وقائع قد اعترف بها أو وقعت في حصوره أو بإسقاطه أو بتغييره عمدا الإقرارات التي تلقاها».

ويقتضي عند تطبيق المادة 32 فقرة 1 و2 من القانون 24-02 المتعلق بالتزوير واستعمال المزور توافر شرطين أن يكون للجاني صفة معينة وأن ترتكب الجريمة أثناء ممارسة الجاني وظيفته.

[1]- طاهر برهوم، **جرائم التزوير الالكتروني**، مذكرة مقدمة لنيل شهادة الماستر في قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي -باتنة- 2019 ص 48.

2-عقوبة التزوير الذي يقع من طرف أي شخص كان :

إذا كان التزوير مرتكب من طرف شخص آخر عدا أولئك الذين حددتهم المادة 32 فيُعاقب بموجب المادة 31 من القانون 24-02 السالف الذكر بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، إذا ارتكب تزويرا في محررات عمومية أو رسمية بالطرق المحددة في القانون.

وتعاقب المادة 33 الشخص الذي لا يعتبر طرفا في المحرر ويقوم بالإدلاء أمام ضابط عمومي أو موظف بتصريح يعلم أنه غير مطابق للحقيقة بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج

أما بالنسبة للشخص الذي يستخدم المحرر مع علمه بأنه مزور فيُعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج الى 1.000.000 دج استنادا لما جاء في نص المادة 34.

وبالنسبة للشخص المعنوي فتطبق عليه العقوبات المنصوص عليها في قانون العقوبات طبقا لنص المادة 80 من القانون 24-02.

ثانيا: العقوبات التكميلية.

وفيما يخص العقوبات التكميلية الخاصة بجريمة تزوير التوقيع الإلكتروني فقد نصت المادة 74 من القانون رقم 24-02 الذي يتعلق بمكافحة التزوير واستعمال المزور أنه في حالة الإدانة بإحدى الجرائم المنصوص عليها في هذا القانون تأمر الجهة القضائية وجوبا بمصادرة الوسائل المستعملة في ارتكابها والأموال المتحصل عليها، مع مراعاة حقوق الغير حسن النية، كما تأمر الجهة القضائية بإتلاف الوثائق والمحررات محل التزوير.

وتضيف المادة 78 من القانون 24-02 على أنه يمكن للجهة القضائية المختصة أن تطبق على الشخص الطبيعي المحكوم عليه بارتكاب إحدى الجرائم المنصوص عليها في هذا القانون، عقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

خلاصة الفصل الثاني:

مما سبق نستنتج أن المشرع، يعمل على تقرير حماية جنائية للتوقيع الالكتروني، فمن جانب المؤسسات تظهر جهوده من خلال استحداث هيئات ومراكز جديدة تضطلع بأدوار جد هامة والتي من بينها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، أجهزة الأمن الوطني المختصة ، المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني ، بالإضافة للأقطاب الجزائية المتخصصة ، و القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

ومن جملة الترتيبات المتخذة كذلك من قبل المشرع الجزائري لإضفاء الحماية اللازمة للتوقيع الالكتروني، استحداث أساليب تحري خاصة بموجب تعديل قانون الإجراءات الجزائية رقم 06-22 التي يقصد بها العمليات أو الإجراءات والتقنيات التي تستخدمها الضبطية القضائية تحت المراقبة والإشراف المباشر للسلطة القضائية بغية البحث والتحري عن الجرائم الخطيرة، وجمع الأدلة عنها والكشف عن مرتكبها، وذلك دون علم ورضا الأشخاص المعنيين، حيث أن هذا النوع من الأساليب لا يرخص بها إلا في الجرائم المحددة على سبيل الحصر، من بينها الجريمة المعلوماتية التي تنطوي عليها جرائم الاعتداء على التوقيع الالكتروني، والتي تتناسب مع متطلبات الإجرام الحديث، وتتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب، ثم سنّ القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها واستحدث بموجبه إجراء المراقبة الالكترونية والتفتيش والحجز.

كما أبدى المشرع الجزائري اهتماما بتقرير عقوبات صارمة اتجاه كل من تسول له نفسه المساس بالتوقيع الالكتروني سواء كان شخص طبيعي او معنوي.

خـاتـمـة

خـاتـمـة:

نخلص من خلال هذه الدراسة ان التوقيع الالكتروني يُعد إحدى المصالح الجديرة بالحماية خاصة وأن العالم قد شهد تبني سريع لتقنيات التكنولوجيا الحديثة، ونظرًا لكثرة الاعتداءات والمحاولات التي تستهدف هذه التقنية، فإن التفكير في حماية شاملة للتوقيع الإلكتروني من جميع أشكال الجرائم ضروري للغاية، وقد أدى هذا الواقع إلى صدور تشريعات دولية ووطنية لتنظيم التوقيع الإلكتروني ولإزالة الغموض المحيط بهذا المصطلح الحديث وإضفاء حماية عليه، ويُذكر أن القانون الجزائري تأخر نسبيًا في التحاقه بسن قانون خاص بالتوقيع الإلكتروني، إذ تم ذلك في عام 2015 حيث نص المشرع الجزائري على التوقيع والتصديق الإلكترونيين من خلال نصوص مستقلة، وذلك تلبيةً لمتطلبات التقدم التكنولوجي الذي يشهده جميع ميادين الحياة.

ومن خلال ما تم تقديمه نخلص الى **النتائج** الاتية:

– اهتمام مختلف التشريعات الدولية بالتوقيع الإلكتروني بإعطائه قوانين خاصة به تنظمه وتعالج جميع الأحكام الخاصة به، بما فيها التشريع الجزائري الذي أبدى اهتمامه به من خلال سن القانون 15–04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

– في نطاق تحديد مدلول التوقيع الإلكتروني اتضح لنا أن هذا التوقيع هو ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متميز ومنفرد يسمح بتحديد هوية صاحب التوقيع، يقوم على استعمال تقنيات حديثة ومتطورة من شبكة الإنترنت والحاسب الآلي وغيرها، وله القدرة على تحقيق وظائف التوقيت التقليدي.

– هناك عدة صور للتوقيع الالكتروني تختلف حسب التقنية المستخدمة في تشغيل منظومة التوقيع الإلكتروني منها التوقيع باستخدام البطاقة الممغنطة، التوقيع بالقلم الإلكتروني، التوقيع البيومتري، التوقيع الرقمي.

– يجب أن يتوافر التوقيع الإلكتروني على مجموعة من الشروط القانونية والضوابط التقنية التي تجعل منه توقيعا موثوقا به، لان غيابها تؤدي إلى عدم الأخذ به وعدم الاعتراف له بحجيته القانونية في الإثبات.

– تتميز الجرائم التي تتعلق بالتوقيع الإلكتروني بخصائص تجعلها صعبة الكشف عن أصحابها، نظراً لمهارتهم العالية في مجال التكنولوجيا واستخدامهم لأساليب تقنية دقيقة، ولكبح جماح مرتكبي هذه الجرائم، تم وضع قوانين تطبق عليهم سواء كانوا أفراداً طبيعيين أو شركات.

– المشرع الجزائري قد أعطى حماية جنائية موضوعية للتوقيع الإلكتروني في قانون العقوبات من خلال التجريم الخاص بأنظمة المعالجة الآلية للمعطيات من ضمنها معطيات التوقيع الالكتروني في القسم السابع مكرر من قانون العقوبات وأيضا تجريم تزوير التوقيع الإلكتروني المطبق عليه القانون رقم 24–02 المتعلق بمكافحة التزوير واستعمال المزور، بالإضافة لقانون التوقيع والتصديق الإلكترونيين لسنة 2015 من خلال الجرائم الواقعة على التوقيع الإلكتروني في المواد من 66 إلى 74.

– على الرغم من صدور قانون رقم 15–04 الذي ينظم كل ما يتعلق بالتوقيع والتصديق الإلكترونيين في الجزائر، إلا أنه لم يعمل على وضع آليات الحماية الجنائية اللازمة لمواجهة جميع أنواع الاعتداءات على هذه النظام، مثل جرائم الاحتيال والتزوير والدخول غير المصرح به، وهذا يستدعي ضرورة إعادة النظر مرة أخرى في القوانين العامة ضمن إطار قانون العقوبات.

– أقر المشرع آليات الحماية الجنائية الإجرائية لمواجهة الجرائم الإلكترونية والجرائم التي ترتبط بأنظمة معالجة البيانات، ولم يتضمن نصوص صريحة حول الجرائم التي تتعلق بالتوقيع الإلكتروني.

– يمكن القول ان المشرع الجزائري لا يزال في مرحلة مبكرة من تشريع هذا القانون، ولم يصل بعد إلى مستوى يواكب فيه التشريعات المتقدمة، يعود ذلك لعدم جاهزية البيئة الإلكترونية في الجزائر لاستيعاب مستوى التطور التكنولوجي الحالي، فضلاً عن نقص التأطير القانوني المناسب للفاعلين والهيئات القانونية في هذا المجال الناشئ، على الرغم من ذلك فإن صدور قانون ينظم القواعد العامة للتوقيع الإلكتروني يمثل نقطة انطلاق هامة نحو مواءمة التشريعات الجزائرية مع المعايير الدولية المتقدمة في هذا المجال.

مما سبق ويمكن ان نقترح **التوصيات** الاتية:

– نشر الوعي بين الجمهور حول كيفية استخدام التوقيع الإلكتروني بأمان وكيفية حماية معلوماتهم الشخصية.

– على المشرع الجزائري إقرار تعديلات في القانون رقم 15–04 للإلمام بمختلف جوانبه، وتدارك الثغرات الموجودة به، بالإحاطة بجميع الجرائم الماسة بالتوقيع الإلكتروني على غرار الاحتيال والتزوير والدخول والبقاء غير المصرح به، وإصدار العقوبات المقررة لها.

– ضمان القدر الكافي من المرونة في صياغة النصوص الجنائية لمواجهة الإجرام المستحدث بما فيها تلك النصوص التي تحمي التوقيع الالكتروني وذلك حتى تسمح بدخول الصور الإجرامية المستحدثة مستقبلا في النص بما لا يمثل اعتداء على مبدأ الشرعية الجنائية، خاصة وأن توقعات اهل الاختصاص تصب كلها في زيادة حجم الإجرام الإلكتروني مستقبلا.

– ضرورة وضع آلية قانونية يتم من خلالها تفعيل التنسيق بين القانونيين والأخصائيين التقنيين في مجال المعلوماتية وتكنولوجيات الاتصال بغرض ترقية عناصر الأمان والسرية وبث الثقة أكثر في التعاملات الإلكترونية.

– تنظيم ندوات علمية تكنولوجية بهدف متابعة التطورات القانونية والتقنية في مجال التوقيع الإلكتروني، تتضمن هذه الندوات تبادل الخبرات والتجارب مع الخبراء والجهات المهتمة بهذا المجال، خاصة من الدول المتقدمة، للاستفادة من خبراتهم القانونية والقضائية.

قائمة المراجع

قائمة المراجع:

1-النصوص التشريعية:

أ-القوانين:

-قانون رقم 2000 -03، مؤرخ في خمسة جمادى الاولى 1421 الموافق لـ 5 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية، العدد 48 لسنة 2000.

-قانون رقم 04-15 مؤرخ في 10/11/2004 يعدل ويتمم الأمر رقم 66-156 مؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، لسنة 2004.

-قانون رقم 05-10 مؤرخ في 20 جويلية 2005 المعدل والمتمم للأمر رقم 75/58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني المعدل والمتمم المنشور في الجريدة الرسمية للجمهورية الجزائرية، عدد 44، لسنة2005.

-قانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق ل 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 84، لسنة 2006.

-قانون رقم 09 -04، مؤرخ في 14 شعبان عام 1930 الموافق ل 5 غشت سنة يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، لسنة2009.

-قانون رقم 15-04 مؤرخ في 01/02/2015 يحدد القواعد العامة للتوقيع والتصديق الالكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06، لسنة2015.

-قانون رقم 24 -02، مؤرخ في 16 شعبان عام 1445 الموافق ل 26 فبراير سنة 2024 يتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية للجمهورية الجزائرية، العدد 15، ، لسنة2014.

ب-الأوامر:

-أمر رقم 21-11 مؤرخ في 16 محرم 1443 الموافق ل 25 غشت 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 65، لسنة 2021.

ج-المراسيم الرئاسية:

-مرسوم رئاسي رقم 04-183 المؤرخ في 8 جمادى الأولى عام 1425 الموافق ل 26 يونيو 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج. ج، العدد 41، لسنة 2004.

-مرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 سبتمبر 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020 ،ج.ر.ج.ج، العدد 82، لسنة 2020.

-مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني 1443 موافق ل 7 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 86، لسنة 2021.

د-المراسيم التنفيذية:

-مرسوم تنفيذي رقم 06-348، مؤرخ في 12 رمضان 1427 الموافق لـ 5 أكتوبر 2006 يتضمن التمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج، العدد 63، لسنة 2006.

-المرسوم التنفيذي رقم 07-162 مؤرخ في 13 جمادى الاولى 1428 الموافق ل 30 ماي 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 مؤرخ في 15 صفر 1422

الموافق ل 9 ماي 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادر في 7 جوان 2007.

-مرسوم تنفيذي رقم 16-267 مؤرخ في 15 محرم عام 1448 الموافق ل 17 أكتوبر 2016 يعدل ويتمم المرسوم التنفيذي 06- 348 المؤرخ في 12 رمضان عام 1427 الموافق لـ 5 أكتوبر 2006 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم وكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج، العدد 62، لسنة 2016.

2-الكتب:

أ-الكتب العامة:

-حسام محمد نبيل الشنراقي، **جرائم المعلوماتية -دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني-**، د.ط، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الامارات، 2013.

-فراح مناني، **العقد الالكتروني وسيلة إثبات حديثة في القانون المدني الجزائري**، دار الهدى للطباعة والنشر والتوزيع، دوم طبعة، عين مليلة -الجزائر-، 2009.

-محمد حسنين منصور، **الاثبات التقليدي والالكتروني**، دار الفكر الجامعي، دون طبعة، الإسكندرية، 2006.

-محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن**، دار الجامعة الجديدة، دون طبعة، الإسكندرية -مصر- ،2008.

ب-الكتب المتخصصة:

-ثروت عبد الحميد، **التوقيع الإلكتروني ماهيته- مخاطره- وكيفية مواجهتها- مدى حجيته في الإثبات**، دار الجامعة الجديدة، دون طبعة، الإسكندرية 2007.

-عبد الفتاح بيومي حجازي، **التوقيع الالكتروني في النظم القانونية المقارنة**، دار الفكر الجامعي، دون طبعة، الإسكندرية، 2005.

-علاء محمد نصيرات، **حجية التوقيع الالكتروني في الاثبات -دراسة مقارنة-**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان ،2005.

-عيسى غسان ربضي، **القواعد الخاصة بالتوقيع الإلكتروني**، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2012.

-لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، دار الثقافة والنشر والتوزيع، الطبعة 1، عمان، 2009.

3-الأطروحات:

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

-خدوجة الذهبي، **الحماية الجزائية للمعاملات الالكترونية -دراسة مقارنة-**، رسالة مقدمة لنيل شهادة دكتوراه علوم في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية -أدرار-، 2019.

-عائشة قصار الليل، **حجية المحرر والتوقيع الإلكتروني في الإثبات**، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة -،2017.

-عبد القادر بوهنتالة، **حجية التوقيع الالكتروني في التشريع الجزائري**، أطروحة مقدمة لنيل درجة الدكتوراه العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر -باتنة-، 2016.

-فارس خطابي، **الحماية الجزائية للتوقيع الإلكتروني**، أطروحة لنيل شهادة الدكتوراه في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج الأخضر،2021.

-مصطفى صحراوي، **الحماية الجزائية للتوقيع والتصديق الالكترونيين في التشريع الجزائري**، أطروحة للحصول على شهادة الدكتوراه ل.م.د في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، 2021.

-نسيمة ترجمان، الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة، أطروحة لنيل شهادة دكتوراه طور الثالث، جامعة ابن خلدون -تيارت-، كلية الحقوق والعلوم السياسية، 2021، ص136.

4-المذكرات:

-أمير والي، بالعلمي إسحاق، **مكافحة جريمة التزوير الالكتروني في الجزائر**، مذكرة لنيل شهادة الماستر في الحقوق تخصص إعلام ألي، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي-برج بوعريريج-، 2023.

-بدرة صرياك، **أساليب التحري في جرائم الفساد**، مذكرة مقدمة لنيل متطلبات شهادة الماستر في القانون الجنائي والعلوم الجنائية، معهد الحقوق والعلوم الاقتصادية، المركز الجامعي سي الحواس -بريكة-، 2019.

-خلود حملاوي، نورة بركاوي، **التوقيع الإلكتروني وحجيته في الإثبات**، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر في القانون، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 -قالمة-،2020.

-دليلة مزرقن، **جريمة المساس بأنظمة المعالجة الآلية للمعطيات**، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2016.

-راضية لالوش، **أمن التوقيع الالكتروني**، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعات مولود معمري -تيزي وزو-،2012.

-رزيقة بونار، **الجريمة المعلوماتية في التشريع الجنائي الجزائري**، مذكرة مقدمة لنيل شهادة الماستر في القانون العام، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى -جيجل-، 2021.

-زهرة بالخير، **الحماية الجنائية للتوقيع الإلكتروني**، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون -تيارت- 2021،.

-طاهر برهوم، **جرائم التزوير الالكتروني**، مذكرة مقدمة لنيل شهادة الماستر في القانون الجنائي والعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي -باتنة- 2019.

-عائشة نايري، **الجريمة الإلكترونية في التشريع الجزائري**، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية -أدرار-،2017.

-عبد الرؤوف بوديسة، **آليات التحرير عن الجريمة الإلكترونية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة ماستر مهني في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي -، برج بوعريريج، 2022.

-عزالدين منصور، **حجية التوقيع الإلكتروني في الإثبات**، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر-بسكرة-، 2016

-فاطمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، ملخص لمذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021.

-ماني صلاح الدين، رمضان أنور، **الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري**، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة اكلي محند اولحاج -البويرة-، 2021.

-نسيمة جدي، **جرائم المساس بأنظمة المعالج الآلية للمعطيات**، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014.

-يوسف بوزيدة، **الحماية الجزائية للتوقيع الإلكتروني**، مذكرة مقدمة لنيل شهادة ماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي -تبسة-، 2021

5-المقالات:

-آمنة كبير، **(التصديق الالكتروني - دراسة مقارنة-)**، مجلة القانون والمجتمع، مخبر القانون والمجتمع، جامعة أحمد دراية -أدرار-، المجلد 06، العدد 01، جوان 2018.

-جمال براهيمي، **(مكافحة الجرائم الالكترونية في التشريع الجزائري)**، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو-، المجلد 11، عدد 2، نوفمبر 2016.

-جميلة محلق، **(اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري)**، مجلة التواصل في الاقتصاد والإدارة والقانون، صادرة عن كلية الحقوق والعلوم السياسية جامعة باجي مختار عنابة، مجلد 21، العدد 42، جوان 2015.

-راضية عيمور، **(الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري)**، المجلة الأكاديمية للبحوث القانونية والسياسية، مخبر الحقوق والعلوم السياسية جامعة الاغواط، المجلد السادس، العدد الأول، مارس 2022.

-رضا هميسي، **(تفتيش المنظومة المعلوماتية في القانون الجزائري)**، مجلة العلوم القانونية والسياسية، صادرة عن كلية الحقوق والعلوم السياسية جامعة الشهيد حقه لخضر بالوادي، دون مجلد، العدد 5، جوان 2012.

-سعاد رابح، **(ضوابط مكافحة الجريمة المعلوماتية)**، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي اليابس -سيدي بلعباس-، المجلد السابع، العدد 1، جوان 2021.

-سفيان عبد الحميد، **(أساليب التحري الخاصة في قانون الإجراءات الجزائية)**، مجلة صوت القانون، كلية الحقوق والعلوم السياسية جامعة لونيسي علي، المجلد 9، العدد 2، ماي 2023.

-سميحة بلقاسم، حميد بوشوشة، **(الجريمة الإلكترونية بعد جديد للإجرام في الجزائر واقعها وآليات مجابهتها)**، مجلة العلوم الانسانية، جامعة أم البواقي، مجلد 10، العدد 1، جوان 2023.

-عبد الجبار الحفيص، **(الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجنائي)**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011.

-عبد الحق غلاب، **(خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري)**، مجلة الدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 8، العدد 1، 2022.

-فاطمة الزهراء تبوب، **(التوقيع والتصديق الالكترونيين في ظل القانون رقم 15- 04 المؤرخ في أول فبراير 2015،)** مجلة حوليات، جامعة الجزائر 1، العدد 29، الجزء الثاني جوان 2016.

-فتيحة حواس، **التوقيع الالكتروني (الخصوصيات والتطبيقات)**، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص المقارن بكلية الحقوق والعلوم السياسية، جامعة حاسي باب بن بوعلي -الشلف-، المجلد 07، العدد 1، جوان 2021.

-محمد رحموني، **(خصائص الجريمة الإلكترونية ومجالات استخدامها)**، مجلة الحقيقة، جامعة أحمد دراية -أدرار-، العدد 41، جانفي 2018.

-نجوى سديرة، **(الحماية القانونية للتوقيع الالكتروني كآلية لتدعيم الثقة في المعاملات الالكترونية عبر الانترنت)**، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس -المدية-، المجلد 08، العدد 2، جوان 2022.

6-المواقع الالكترونية:

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENTAND OF THE COUNCIL of 13 December 1999 on a Community Framework for electronic signatures, posted on the site Https://eur-lex.euripa.eu.

UNCITRAL model Law on electronic commerce with guide to enactment adopted décembre 16 ,1996, with additional article 5 bis as adopted in 1998, Posted on the site https://uncitral.un.org .

UNCITRAL Model Law on Electronic Signatures of the United Nations Commission on International Trade Law with guide to enactment 2001, posted on the site https://uncitral.un.org .

الـــفـــهـــرس

الفهرس:

مقدمة: 1
الفصل الأول: الحماية الجنائية الموضوعية للتوقيع الالكتروني. 1
المبحث الأول: ماهية التوقيع الالكتروني. 8
المطلب الأول: مفهوم التوقيع الالكتروني. 8
الفرع الأول: تعريف التوقيع الالكتروني. 9
الفرع الثاني: خصائص التوقيع الإلكتروني وصوره. 14
المطلب الثاني: شروط التوقيع الالكتروني والتصديق عليه. 19
الفرع الأول: شروط التوقيع الالكتروني. 19
الفرع الثاني: التصديق الالكتروني. 22
المبحث الثاني: تجريم المساس بالتوقيع الالكتروني. 26
المطلب الأول: مفهوم جرائم الاعتداء على التوقيع الالكتروني. 26
الفرع الأول: تعريف جرائم الاعتداء على التوقيع الالكتروني. 26
الفرع الثاني: خصائص جرائم الاعتداء على التوقيع الالكتروني. 28
يعد التطرق الى الخصائص الجوهرية التي تتصف بها جرائم الاعتداء على التوقيع الإلكتروني أمر بالغ الأهمية هو ما سيتم التطرق اليه على النحو الآتي: 28
المطلب الثاني: صور الجرائم الواقعة على التوقيع الالكتروني. 30
الفرع الأول: جرائم الاعتداء على التوقيع الالكتروني في إطار قانون العقوبات. 30
الفرع الثاني: جرائم الاعتداء على التوقيع الالكتروني في إطار بعض القوانين الخاصة. 35

خلاصة الفصل الأول:..... 50
الفصل الثاني: إجراءات الحماية الجنائية للتوقيع الالكتروني. 51
المبحث الأول: التحري في الجرائم الواقعة على التوقيع الالكتروني..... 53
المطلب الأول: الجهات المختصة بالتحري عن جرائم الاعتداء على التوقيع الإلكتروني.
..... 53
الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري. 54
الفرع الثاني: الهيئات القضائية الجزائية المتخصصة. 60
المطلب الثاني: وسائل وأساليب التحري عن جرائم الاعتداء على التوقيع الالكتروني.. 63
الفرع الأول: أساليب التحري في ظل قانون الإجراءات الجزائية. 64
الفرع الثاني: أساليب التحري في ظل قانون 09-04. 71
المبحث الثاني: العقوبات المقررة للاعتداء على التوقيع الالكتروني..... 77
المطلب الأول: العقوبات المقررة في إطار قانون العقوبات..... 77
الفرع الأول: العقوبات المقررة للشخص الطبيعي. 77
الفرع الثاني: العقوبات المطبقة على الشخص المعنوي. 79
المطلب الثاني: العقوبات المقررة في إطار بعض القوانين الخاصة..... 81
الفرع الأول: العقوبات المقررة في إطار القانون 15-04..... 82
الفرع الثاني: العقوبات المقررة في ظل القانون 24-02..... 86
خلاصة الفصل الثاني: 89
خاتمة:..... 91
قائمة المراجع:..... 95