الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –الطارف
كليّة الحقوق والعلوم السياسية
قسم الحقوق

مذكرة بعنوان:

الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون أعمال

إعداد الطالبة:

- منصوري مروة
- معطى الله ذكرى

إشراف الأستاذ:

د. بركات عماد الدّين

لجنة المناقشة

مزوزي فارس	أستاذ محاضر_أ_	الشاذلي بن جديد -الطارف	رئيساً
بركات عماد الدّين	أستاذ محاضر_أ_	الشاذلي بن جديد -الطارف	مشرفاً ومقرراً
العايب نصر الدّين	أستاذ محاضر-ب	الشاذلي بن جديد -الطارف	ممتحناً

السنة الجامعية: 2024/2023

شكر وتقدير

بعد شكر الله عزّ وجلّ ومنِّهِ ،
الشكر كلّ الشكر، الى:
حضرة **الدكتــور عماد الدّين بركات** الذي كان لنا الشّرف بقبوله الإشراف على مذكرتنا، وعلى الجهد والوقت الذي قدّمه، ولم يبخل علينا بملاحظاته وتوجيهاته القيّمة، وكلمات الدّعم والتشجيع التي كانت شعلةَ التحفيز لإتمام هذا البحث المتواضع.
كما نتوجه بالتقدير والامتنان لأعضاء اللجنة المشرفة الكِرام والمشهود لهم بالكفاءة، كل من **الدكتــور العايب نصر الدّين، والدكتــور مزوزي فارس** على تفضلهما بقبول المشاركة في لجنة المناقشة وملاحظاتهما القيمة التي من شأنها أن ترفع من قيمة هذه المذكرة أكثر فأكثر.
وأخيرا لَابدّ من شكر الجامعة وخصوصا كلية الحقوق والعلوم السياسية بأساتذتها وموظّفيها، الكلية التي كانت وستظل مصدرا للطاقات العلمية ومنبعا للعطاءات.

فائق الشّكر
والاحترام...

الإهداء

الى :

من تعبت وضحَّت وربَّت وأعطت دون كللٍ او مللٍ، ولا زالت تعطي دون أيّ مقابل ..وأيّ مقابل يفي جهد كفَّيكِ ؟ ..الى أمي عتيقة..

أوَّل من علّمني ألف باء الهجاء لأبحر في ميدان العلم،

الى أبي خليف..

من رسخت في عقلي حب المعرفة و الرقي وصولا الى مراتب النجوم،

الى روح أختي ربح مريم..

من تثقا بي وبقدراتي، الى وجودهم وحبّهم اللاّ مشروط،

الى أختاي دنيا زاد و صفاء..

من أمسك بيدي لأبدأ مسيرتي الجامعية، الى من وقف الى جانبي لأستكمل مسيرتي العلمية،

الى أخي محمد ضياء الدين..

من ينيرا و يضئا حياتنا و يملآها بالسّعادة، الى الحبّ و البراءة،

الى محمد يانيس و نوران..

إلى من آمنوا بي وكانوا جرعات المحبّة.

اليكم جميعاً أهدي ثمرة جهدي هذه عربونًا للوفاء واعترافاً بالجميل.

مروة

الإهداء

اهدي ثمرة جهدي وعملي وتعب سنيني الى:

الى من ضحت ولا تزال مستعدة للتضحية من اجل سعادتي، الى من حملتني بين العظام وارضعتني حتى الفطام وعلمتني فصيح اللسان الى النور الذي استضيء به طريقي في هذه الدنيا، الى ملاكي في الحياة الى من ارضعتني الحب والحنان الى من كان دعاؤها سر نجاحي امي الغالية "حورية"

والى ابي العزيز الذي اشقى نفسه علينا، الى الشعلة التي انارت لي طريق حياتي ولا زال ضوئها النور الذي استهدي به

ابي الغالي قدور "

حفظهما الله واطال الله في عمرهما ورزقهم الصحة والعافية.

الى اختي العزيزة الداعمة حفظها الله " لمياء "

الى اخوتي الاعزاء رعاهم الله" عبد الحكيم ـ شهاب ـمحمد اسلام"

الى جميع اعمامي وعماتي واخص بالذكر عمتي" حكيمة "حفظها الله هي وكتاكيتها الصغار

لا يكتمل المشوار الا بمساندة الاصدقاء شكرا لكم على دعمكم لي جزاكم الله الدارين "ميساء، لمياء، رائدة، حنان، نسرين، اميرة، ايناس، سماح، فيروز، عائشة والى كل الأحبة الذين لم يذكرهم قلمي هذا.

والى الداعم الحنون وليد حفظك الله

ذكرى

مقدمة

مقدمة

لقد أدى التطور المتسارع والهائل الذي شهده مجال تكنولوجيا المعلومات والاتصال إلى ظهور أشكال متعددة للوسائل، يتم من خلالها ابرام وتوثيق المعاملات والمبادلات الخاصة بالتجارة الالكترونية، وبالتالي لم تعد الوسيلة التقليدية في اثبات التصرفات القانونية "التوقيع التقليدي ملائمة للتعاقدات الحديثة التي تتم في الشكل الالكتروني، لذا ظهر التوقيع الالكتروني ليكون بديلاً عن التوقيع التقليدي، ليتوافق وطبيعة التعاقدات القانونية والعقود التي تتم باستخدام الوسائل أو الأجهزة الالكترونية الحديثة.

والذي يعد أهم الأساليب الحديثة لعجز التوقيع التقليدي على مواكبة هذا التطور التكنولوجي، وهو ما جعل المشرع يتدخل في العديد من المرات لأجل وضع نظام قانوني يواكب التطور التكنولوجي الحاصل وما نجم عنه من سلبيات على المستوى الدولي والوطني، ومن بين هذه القوانين نجد مثلا القانون 23/06 المؤرخ في 20 ديسمبر 2006 المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]، وكذا القانون رقم 04/15 المؤرخ في 02/01/ 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

فالتطور التكنولوجي الحديث بصفة عامة وفي مجال التجارة الالكترونية على وجه الخصوص فرض علينا ضرورة البحث عن إمكانية توفير الحماية القانونية لما يتم ابرامه من صفقات بالوسائل الالكترونية الحديثة والتي يطلق عليها "بالصفقات الالكترونية "

وباعتبار أن العمل التجاري يحتاج إلى الثقة في التعامل والسرعة في انجاز المعاملات التجارية التي تعتمد اعتمادا أساساً على شبكة الانترنت، ولتحقيق مبدأ الثقة والأمان في المبادلات التجارية الالكترونية احاطه المشرع بجملة من شروط الأمان ووضع له آلية آمنة لإنشائه ،ثم حدد الجهات

[1]-القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966، المتضمن قانون العقوبات، ج.ر العدد 84، الصادرة بتاريخ 24 ديسمبر 2006.

المكلفة بالمصادقة الالكترونية من أجل اعتباره توقيعاً الكترونياً مؤمناً، وحجته في اثبات التصرفات القانونية بين المتعاقدين في التجارة الالكترونية ،هذا التوقيع الالكتروني الآمن يعطي للأطراف المتعاقدة وخاصة المستهلك الأمان والاطمئنان مما ينعكس إيجاباً على المبادلات التجارية بالظر إلى الحجية القانونية القوية التي يوفرها هذا التوقيع المستند إلى آلية انشائه

- **أهمية الموضوع**

تظهر أهمية دراسة هذا الموضوع من خلال الوقوف بداية على مفهوم التوقيع الالكتروني من حيث هو أحد المظاهر الحديثة في مجال المعاملات الالكترونية، وتسليط الضوء على مختلف صوره ومجموع الشروط القانونية التي يتطلبها لإضفاء الحجية القانونية عليه في الاثبات.

ومن ثم التعرف على مفهوم نظام التشفير والتصديق الالكتروني كوسيلة لحماية التوقيع الالكتروني من المخاطر التي تواجهه، والتي تشكل خطراً هاجساً على المتعاقدين، وبث الثقة والأمان لدى المتعاملين وضمان موثوقية هذه المعاملات

بالإضافة إلى الوقوف على مختلف صور جرائم الاعتداء الواقعة على التوقيع الالكتروني، والوسائل التي كفلها المشرع لضمان الحماية الجنائية لهما، والتصدي للتجاوزات التي قد تحول دون ترقية استعمال هذه الآليات والحد من مساهمتها في تسهيل المبادلات.

كما تتجلى أهمية البحث أيضاً في محاولة الوقوف على توجيهات المشرع الجزائري في تنظيمه للتوقيع والتصديق الالكترونيين ووسائل الحماية الجنائية التي اعتمدها، لمواجهة جرائم الاعتداء على هذه المنظومة الالكترونية

- **أسباب اختيار الموضوع**

من الأسباب التي أدت الى اختيار الموضوع هناك بعدين احدهما بعد موضوعي والآخر بعد شخصي وذاتي، فالبعد الموضوعي يتمثل في الحداثة القانونية والتشريعية للحماية الجنائية للتوقيع

الالكتروني ،فهذا الشيء الذي يدفعنا الى معرفة مدى انسجام النصوص التشريعية لتلك المنظومة مع المستجدات الراهنة في مجال المعاملات الالكترونية خاصة في ظل أهمية التوقيع الالكتروني، وأهمية ما يضفي عليه من حجية في الاثبات، فضلاً عن وسائل الحماية الجنائية المعتمدة من قبل المشرع لمواجهة جرائم الاعتداء على التوقيع الالكتروني..

أما بالنسبة للبعد الذاتي فيتمثل في الإحساس بالأهمية البالغة وضرورة البحث في هذا الموضوع ،إضافة الى ذلك الرغبة في معرفة التطورات والمستجدات الجديدة في ميدان القانون الجنائي مما يولد الرغبة في التعمق فيه والإطلاع على ما هو جديد بخصوصه على المستويين الوطني والدولي، بغرض اثرائه، من خلال البحث مدى انسجام وتوافق النصوص القانونية الحالية مع التطورات الحاصلة في المستجدات العالمية

كما أن لها دوافع أخرى كان لها اثرها في اختيار الموضوع والتي قد تنطلق من نقص الكتابات في هذا الموضوع خاصة الجزائرية منها وذلك لحداثة قانون التوقيع الالكتروني الى جانب قلة الاحكام والاجتهادات القضائية في هذا المجال.

- **صعوبات الدراسة**

تعد الصعوبات التي واجهت اعداد هذا البحث متنوعة ومختلفة باختلاف متطلبات اعداده ففكرة التوقيع الالكتروني تعد من المسائل التي ظهرت حديثا في الفكر القانوني، وتغلب الطابع التقني والفني عليه فهذا الأخير ينقسم الى جانب معرفي وآخر فني وتقني ، إضافة الى غموض النصوص القانونية الحالية التي اعتمدها المشرع الجزائري في تنظيم التوقيع الالكتروني والتي تنص على حمايته من الاعتداءات الخارجية والداخلية بشكل كامل، وندرة الاحكام القضائية التي تدرس الاختراقات والاعتداءات الحاصلة على نظام التوقيع الالكتروني خاصة القسم التقني.

ناهيك عن قلة المراجع والكتابات الوطنية الشاملة التي تتناول موضوع التوقيع الالكتروني بصفة عامة والجرائم الالكترونية بصفة خاصة إذ أن جل الكتابات وإن وجدت تستند إلى مراجع أجنبية عربية.

- **اهداف الدراسة**

نسعى من خلال هذه الدراسة الى تحقيق اهداف مختلفة أهمها تسليط الضوء على الاطار المفاهيمي للتوقيع الالكتروني، وكذا تبيان خصائصه وصوره مع توضيح شروط ووظائفه واهم تطبيقاته ،بالإضافة الى توضيح الخطوط العريضة لجرائم الاعتداء على التوقيع الالكتروني ومدى نجاعة العقوبات الجنائية في الحد من هذه الجرائم، والاسهام في الكشف عن احد صور الاجرام الالكتروني الحديث وما تضيفه الدراسة للباحثين في مجال جرائم التوقيع الالكتروني، والجريمة المرتكبة بالوسائل الالكترونية والجرائم المعلوماتية، من أجل الاستفادة منها كدراسة سابقة.

- **إشكالية الدراسة:**

انطلاقا من الأهمية التي اصبح يكتسبها التوقيع الالكتروني في مختلف مجالات المعاملات والتصرفات الالكترونية بين الدول والمؤسسات والافراد حيث اصبح مجال استعماله واسعا في شتى مختلف التصرفات القانونية التي تتم عبر الوسائل الالكترونية ذلك لعدم ملائمة التوقيع التقليدي بحكم طبيعته المادية للمعاملات الالكترونية.

اذ يعد التوقيع الالكتروني عنصرا هاما واساسيا لصحة وسلامة مختلف المحررات الالكترونية التي نجد فيها التصرفات والمعاملات القانونية المنجزة لوسائل الكترونية.

ومن هنا يمكن طرح الإشكالية على الشكل الاتي:

ما مدى فعالية الحماية الجنائية التي أقرها التشريع الجزائري للتوقيع الالكتروني؟

وتتضمن هذه الإشكالية مجموعة من التساؤلات نوجزها على الشكل التالي:

-ما مفهوم التوقيع الالكتروني ؟وماهي صوره ووظائفه؟

-ماهي اهم صور الاعتداءات الواقعة على التوقيع الالكتروني ؟

-ماهي طرق ووسائل الحماية الجنائية التي وفرها المشرع الجزائري والتشريعات المقارنة للتوقيع الالكتروني؟

- **مناهج البحث**

تم الاعتماد على المنهج التحليلي من خلال تحليل واستقراء ما تضمنته بعض التشريعات الأجنبية والوطنية، وبالأخص ما جاء به التشريع الجزائري في كل ما تعلق بجرائم الاعتداء على التوقيع ووسائل حمايته جنائيا. وكذلك المنهج الوصفي يظهر من خلال الوصف الدقيق للنصوص القانونية المجرمة لأفعال الاعتداء التواقيع الالكترونية في التشريع الجزائري وبعض التشريعات الأخرى.

كما اعتمدنا في بعض المواضع من الدراسة على المنهج المقارن الذي أصبح المنهج المفضل في الدراسات القانونية الحديثة، لما يوفره من مزايا التعرف على أوجه التشابه والاختلاف بين التشريعات الغربية والعربية، وهو ما تم على مستوى دارستنا حيث اعتمدنا على بعضها في المسائل التي تتطلب ذلك.

- **تقسيم الدراسة**

وللإجابة على الإشكالية الرئيسية للموضوع وما ينبثق عنها من تساؤلات فرعية قمنا بتقسيم دراستنا هذه الى فصلين وكل فصل يندرج ضمنه مطلبين موضح كالاتي:

خصصنا الفصل الأول لدراسة الاطار المفاهيمي للتوقيع الالكتروني ومدى حجية هذا التوقيع في الاثبات ،اما الفصل الثاني تطرقنا فيه أساليب ووسائل الحماية الجنائية للتوقيع ودراسة اهم جرائم الاعتداء الواقعة عليه.

الفَصْل الأَوّل

الإطار المفاهيمي للتوقيع الالكتروني

الفصل الأول

الإطار المفاهيمي للتوقيع الالكتروني

لقد شهد العالم تغييرا جذريا في جميع المعاملات مواكبا للعصرنة الإلكترونية التي مهدت لظهور ما يعرف " بالمعاملات الإلكترونية " .

فنظراً للوسائل والطرق الحديثة التي أفرزها الواقع العملي في إبرام هاته المعاملات، أجبرت السلطة التشريعية للدول على إحداث منظومة قانونية معتمدة في ذلك على الفقه والسابقة القضائية في مجال الإلكترونيات من أجل استنباط الأحكام المعالجة للإشكاليات الواردة، تسهيلاً لعمليات الاتصال والتعاقد عبر الأنترنت، وكانت هذه المعاملات بحاجة إلى تواقيع تتلاءم مع طبيعتها كبديل للتوقيع وتكون وسيلة إثبات حفاظا على الثقة والإئتمان بين المتعاملين.

وفي ظل استخدام هاته التكنولوجيا الحديثة من طرف البنوك والمؤسسات ظهر ما يسمى " بالتوقيع الإلكتروني " لمنح المصداقية للوثيقة على الدعامة الإلكترونية، وتماشيا مع هذه التطورات الواقعة في ميدان معالجة المعلومات.

ومن هذا المنطلق ارتأينا في هذا الفصل بيان الإطار المفاهيمي للتوقيع الالكتروني، وبالتالي سنتناول في المبحث الأول: ماهية التوقيع الإلكتروني أما في المبحث الثاني: شروط التوقيع الإلكتروني في التوقيع الإلكتروني.

المبحث الأول :ماهية التوقيع الإلكتروني

إن التطور الحاصل في تقنية الإتصالات والمعلومات وظهور التعاقد من خلال شبكة الأنترنت، أدى إلى إفراز واقع عملي بطرق ووسائل حديثة أتاحت التعامل بنوع جديد من الكتابة والتوقيع بأسلوب الكتروني متوافق وطبيعة التجارة الإلكترونية، فالكثير منا يسمع بمصطلح التوقيع الإلكتروني في وقتنا الحالي غير مدركين لمفهوم هذا المصطلح الحديث، الذي أنتشر بظهور الحاسب الآلي في إجراء المعاملات بين الأفراد سواء كانوا تجاراً أو أفراداً عاديين، وكذلك بينهم وبين مختلف المؤسسات.

كما أن ظهور الشبكة الالكترونية العالمية "الانترنت" غيّر الموازين والقواعد التقليدية المتعارف عليها بعد أن أصبحت صلة الوصل الأساسية في تبادل المعلومات والخدمات والصفقات، مما أدى إلى ضرورة تطوير التوقيع الالكتروني ومن ثم إعطائه شكلا عدديا ورقميا وهو ما يعرف بالتوقيع الالكتروني، خاصة مع ظهور السندات الالكترونية إذ أنّ الاعتراف بفعاليتها يبقى ناقصا إذا اعتمد فقط على التوقيع بخط يد صاحبه، مما استوجب بالمشرع الأخذ بالتوقيع الالكتروني لبسط الحماية على هذه السندات والعقود الالكترونية.

فالتوقيع بصفة عامة تقليدي كان أم إلكتروني هو عبارة عن تعبير صادر من إرادة الشخص في الإلتزام بتصرف قانوني، والكتابة بدونه تظل مصدر شك كدليل إثبات فهو الشرط الأساسي لها سواء كانت رسمية أو عرفية[1]، ولمعرفة المزيد عن ذلك قمنا بتقسيم هذا البحث إلى مطلبين نتطرق في

[1] حسان سعاد، إثبات التعاملات الإلكترونية وفقاً للقانون الجزائري والتشريعات المقارنة، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2019، ص 69.

المطلب الأول لمفهوم التوقيع الإلكتروني من خلال التوسع في التعريف به أما المطلب الثاني فخصصناه لأهمية وأهداف التوقيع الإلكتروني.

المطلب الأول: مفهوم التوقيع الإلكتروني

إن التطور الحاصل في مجال الثورة الرقمية التي يعرفها العالم اليوم أصبح يشكل العصب الرئيسي للمجتمعات الحديثة، بل أصبح واقعا يفرض نفسه في مجال التعاملات عن بعد واختزال المسافات مما جعل العالم عبارة عن قرية صغيرة، وفتح المجال أمام إبرام العقود عبر أدوات ووسائل التواصل الحديثة. إن الوضع السائد أفرز تغيرات جديدة في مجال العقود والمعاملات التجارية فظهرت ما يعرف بالتجارة الالكترونية ، والعقد الالكتروني .

والتوقيع الإلكتروني الذي جاء استعماله إلى جانب ما هو متعارف علية في العقود التقليدية في البيئة الإلكترونية، والتوقيع الإلكتروني كوسيلة من الوسائل التي تثبت صلة الشخص بتصرف معين ونسبته إليه، يأخذ أشكال عدة منها كالحروف والأرقام أو رموز أو إشارات أو غيرها تدرج في شكل الكتروني أو رقمي على سبيل المثال وفقا لشروط يحددها القانون.

لقد أصبح التوقيع الإلكتروني يلعب دور كبير في مجال المعاملات الإلكترونية يشبه بذلك العقود التقليدية، سيما في مجال الإثبات لما للإثبات من دور في استقرار التعاملات وإعطاء الأمن والثقة في التعاملات الإلكترونية.

إن التوقيع الإلكتروني قد أحدث ضجة كبيرة بظهوره كبديل للتوقيع التقليدي، فقد اختلفت التشريعات سواء الفقهية أو التشريعية في استيعاب هذا النمط الجديد وتحديد مفهومه[1]، بحيث عرف

[1] حسان سعاد، المرجع السابق، ص 70.

لأول مرة من طرف المنظمات الدولية وذلك من خلال التجارة الإلكترونية، ومن ثم فقد حاول رجال الفقه القانوني توضيح المقصود بالتوقيع الإلكتروني، كما حظي باجتهاد معظم التشريعات الحديثة وذلك بوضع إطار قانوني وتنظيمي يلم بكافة المسائل والأحكام المتعلقة به في قوانينها الداخلية حتى لا نكون أمام قصور تشريعي، وسيتم تناول هذه التشريعات من خلال الفروع التالية:

الفرع الأول: تعريف التوقيع الإلكتروني

تباينت تعريفات التوقيع الإلكتروني، وذلك بحسب الزاوية التي ينظر منها إليه، فهناك من عرفه بناء على الوسيلة التي يتم بها إجراء التوقيع الإلكتروني، في حين عرفه آخر بحسب ما يقوم به من وظائف، فتنوعت تعريفات التوقيع الإلكتروني سواء من منظور الاتفاقيات الدولية أو التشريعات الوطنية الخاصة بالتوقيع الإلكتروني، إضافة إلى ما قام به الفقه من اجتهادات حول هذا الموضوع، وسنعرض فيما يلي هذه التعريفات، إذ سنتطرق إلى تعريفه من قبل المنظمات الدولية (**أولاً**)، فقهياً (**ثانياً**)، ثم تشريعياً (**ثالثاً**).

أولاً: تعريف التوقيع الالكتروني من قبل المنظمات الدولية

أ: تعريف التوقيع الالكتروني في قواعد الاونسترال بشأن التوقيعات الإلكترونية

أصدرت لجنة الأمم المتحدة للتجارة الإلكترونية " الاونيسترال " قانونا خاصا بالتوقيع الإلكتروني بتاريخ: 05 يوليو 2021 ، تصدت من خلاله لتعريف هذا التوقيع وكيفية استخدامه والقواعد الخاصة به بمساعدة من لجنة للدول في وضع قواعد خاصة بالتوقيع الالكتروني، حيث جاء في المادة (2/ أ) (4) منه هو: " **ان التوقيع الالكتروني بيانات في شكل الكتروني مدرجة في رسالة البيانات أو مضافه إليها، أو مرتبطة بها منطقياً يجوز ان تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات** ".

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

من خلال هذا التعريف يظهر أن منظمة الأمم المتحدة للتجارة الدولية لم تقم بتقييد مفهوم التوقيع الالكتروني بل أوردها بشكل موسع، فهي لم تقم بتحديد الطريقة التي يتم اعتمادها في التوقيع الالكتروني أي أنواعه ، تاركة الأمر بذلك للدول والأفراد في إصدار تشريعاتها الخاصة بتحديد كل نوع من أنواع التواقيع الإلكترونية وإختيار الطريقة التي يتم بها، مادامت تلك الطريقة تسمح بتعيين هوية الموقع وبموافقته على المعلومات الواردة في الرسالة، بل إن هذا الشخص يمكن أن يستوعب أية تقنية تظهر في المستقبل تعني بإنشاء التوقيع الإلكتروني.[2]

ب: تعريف التوقيع الالكتروني في توجيهات الاتحاد الأوروبي

بعد صدور القانون النموذجي حول التجارة الإلكترونية لسنه 1996 الذي أعدته لجنة الأمم المتحدة للقانون الدولي، حيث عرضت اللجنة الأوروبية مشروع التوجيه الأوروبي حول إطار قانون عام للتوقيع الالكتروني لمجلس وزراء المجموعة الأوروبية، الذي وافق عليه البرلمان الأوروبي في 13 ديسمبر 1999.[3]

[1] لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الأولى ، دار هومة للطباعة والنشر والتوزيع، الجزائر ، 2012، ص 153 .154.

[2] باسم محمد فاضل، التعويض عن إساءة استعمال التوقيع الالكتروني، بدون طبعة، دار الجامعة الجديدة، مصر، 2018 ص 20.

[3] التوجيه الأوروبي الصادر في 13 ديسمبر 1999 المنشور على موقع www.europa.eu.int/directives، بتاريخ 22 فيفري 2024، 10:20 سا.

حيث عرف التوجيه الأوروبي التوقيع الإلكتروني بنص المادة الثانية الفقرة الأولى التي مضمونها: " **التوقيع الإلكتروني معلومة معالجة إلكترونيا ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى كرسالة أو محرر، والتي تصلح وسيلة لتمييز الشخص الموقع وتحديد هويته.**" [1]

فمنظمة الاتحاد الأوروبي كغيرها من المنظمات وضعت تعريف للتوقيع الالكتروني، غير أنها قد عرفت نوعين من التوقيع ووضعت لكل منهما تعريفا محددا:

الأول يسمى بالتوقيع الإلكتروني البسيط وهو عبارة عن معلومات وبيانات على شكل الكتروني متعلقة بمعلومات وبيانات إلكترونية أخرى، ومرتبطة بها ارتباطاً وثيقاً ويستخدم أداة للتوثيق أو المصادقة. [2]

أما الثاني فقد ورد في الفقرة الثانية من ذات المادة الثانية والمتمثل في التوقيع الإلكتروني المتقدم أو المؤمن، وهو توقيع يرتبط بشكل غير قابل للفصل بالنص الموقع، ولكي يتصف التوقيع الإلكتروني بأنه توقيع متقدم يجب أن يتوفر على الشروط الآتية :

- الشرط الأول/ أن يرتبط ارتباطا فرديا مع صاحب التوقيع.
- الشرط الثاني/ أن يتيح كشف هوية صاحب التوقيع والتعرف عليه.
- الشرط الثالث/ أن ينشأ من خلال وسائل موضوعة تحت رقابة صاحب التوقيع.
- الشرط الرابع/ أن يكون تابع للبيانات التي وضع عليها التوقيع في الرسالة إلى درجة أن أي تعديل لاحق للبيانات يمكن كشفه.[3]

[1] قانون التوجيه الأوروبي رقم 93/1999 بشأن الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ 13/ 1999/12.

[2] باسم محمد فاضل، المرجع السابق، ص 21.

[3] عيسى غسان ريضي، القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الأولى ، دار الثقافة للنشر والتوزيع، ، الأردن، 2009، ص 49.

ولهذا نلاحظ أن الإتحاد الأوروبي يعترف بما يسمى التوقيع الإلكتروني المتقدم، والذي يتمتع بكافة المزايا التي يتمتع بها التوقيع التقليدي، كما يعترف بالتوقيع العادي الذي يتميز بدرجة أقل من المتقدم من حيث الحجية في الإثبات. [1]

ثانياً: تعريفات فقهية للتوقيع الالكتروني

لم يثر تعريف التوقيع الالكتروني جدلاً كبيراً في الفقه، فجل التعريفات الفقهية التي تحدثت في شأنه تدور كلها حول فكره إظهار شكل التوقيع وإبراز وظائفه، من خلال تحديد هوية الموقع وأهميته في المحررات، ورغم اجماعهم حول فكرة واحدة، إلا أنهم لم يتفقوا على تعريف موحد، وإنما تباينت تعاريفهم تبعا للزاوية التي يرى منها كل فقيه[2].

كما عرفه الدكتور عبد الفتاح البيومي الحجازي بأنه: " التوقيع الإلكتروني إتباع لمجموعة من الإجراءات أو الوسائل التقنية التي يتاح استخدامها عن طريق الرموز أو الأرقام أو الشفرات بقصد إخراج علامة مميزة لصاحب الرسالة التي نقلت إلكترونيا "[3].

وعرفه البعض الآخر بأنه: "علامة أو رمز متمايز يعود على شخص بعينه، من خلاله يعبر الشخص عن إرادته ويؤكد حقيقة البيانات المتضمنة في المستند الذي وقعه "[4].

كما عرفه فادي توكل بأنه: " عبارة عن مجموع من المعلومات مدرجة بشكل إلكتروني في رسالة بيانات أو مضافاً عليهاً أو مرتبطاً بها ارتباطاً منطقياً، تستخدم لتحديد هوية الموقع وإثبات موافقته

[1] نضال اسماعيل برهم ، احكام عقود التجارة الإلكترونية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، الأردن، 2005، ص 171.

[2] محمد محمد سادات، حجية المحررات الموقعة الكترونيا في الاثبات (دراسة مقارنة)، بدون طبعة، دار الجامعة الجديدة، مصر،2011، ص43.

[3] عبد الفتاح البيومي الحجازي، النظام القانوني لحماية التجارة الإلكترونية، بدون طبعة، دار الفكر الجامعي، الإسكندرية، 2002، ص 72.

[4] باسم محمد فاضل، المرجع السابق، ص 24.

على فحوى الرسالة، وتؤكد سلامتها ويشترط فيه ضرورة إتقانه وفقا لإجراءات حسابية وخوارزمية، بحيث يستحيل سرقته وتزوير مضمون السند "[1].

وقد عرف الفقه الفرنسي مفهوم التوقيع الإلكتروني بأنه: " مجموعة من الإجراءات والوسائل التي يتبع استخدامها، عن طريق الرموز أو الأرقام اخراج رسالة إلكترونية تتضمن علامة مميزة من صاحب الرسالة المنقولة إلكترونياً يجري تشفيرها باستخدام زوج من المفاتيح، واحد معلن والآخر خاص بصاحب الرسالة ".

ويعرفه البعض الآخر بأنه: عبارة عن حروف أو أرقام أو رموز أو إشارات ذات طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، وهو الوسيلة الضرورية للمعاملات الإلكترونية في ابرامها وتنفيذها والمحافظة على سرية المعلومات والوسائل[2].

كما عرفه فيصل الغريب بأنه: " مجموعة من الأرقام التي تختلط ببعضها بعمليات حسابية معقدة لتكون كودا سريا خاص بشكل معين "[3].

فأغلب التعريفات تتمحور على أن التوقيع الالكتروني هو الذي ينسب الورقة إلى من يراد الاحتجاج عليه بها، وهو إجراء معين يقوم به الشخص الموقع على محرر، سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو شفرة خاصة، المهم ما في الأمر أن يحتفظ بالرقم أو الشفرة بشكل آمن وسري تمنع استقباله من قبل الغير.

كما تتفق هذه التعريفات السابقة على اعتبار أن التوقيع الإلكتروني، قد تم بوسائل إلكترونية، وأنه يؤدي نفس وظائف التوقيع التقليدي، المتمثلة في بيان موافقة الموقع على مضمون التصرف الموقع عليه وتمييزه عن غيره من الأشخاص.

---

[1] فادي توكل عماد الدين، عقد التجارة الإلكترونية، الطبعة الأولى ، منشورات الحلبي الحقوقية، بيروت، 2010، ص 145.

[2] نادية ياس البياتي، التوقيع الإلكتروني عبر الأنترنت ومدى حجيته في الإثبات دراسة مقارنة بالفقه الإسلامي ،الطبعة الأولى، دار البداية ناشرون وموزعون، عمان ، 2017، ص 178.

[3] الغريب فيصل سعيد، توقيع الالكتروني وحجيته في الإثبات، الطبعة الأولى ، المنظمة العربية للتنمية الإدارية، مصر، 2005، ص 216.

ثالثاً: التعريفات التشريعية للتوقيع الالكتروني

قبل اعتماد الدول تشريعات تنظم التوقيع الإلكتروني، لم يكن هناك أي تعريف قانوني يوضح المقصود باصطلاح التوقيع، ونتيجة ظهور التوقيع الإلكتروني كواقعة مستجدة تحتاج إلى البحث، دفع بالعديد من الدول إلى تحديد مفهوم هذا المصطلح الجديد[1].

وسوف نتطرق الى بعض التشريعات التي لم تتوان على غرار المنظمات الدولية في وضع تعريف للتوقيع الالكتروني، ضمن قانون مستقل خاص به او خاص بالتجارة الإلكترونية، وهذا بهدف مسايرة التطور التكنولوجي الحاصل مستقبلا[2].

أ: تعريف التوقيع الالكتروني وفق التشريعات الأجنبية

سعت الكثير من التشريعات الأجنبية الى تحديد مفهوم التوقيع الالكتروني، حتى وان اختلفت في صياغتها لهذا التعريف غير أن معظمها تتقارب في المحتوى[3].

وهذا ما سنتطرق إليه من خلال التشريعات التالية:

1 . في التشريع الفرنسي

وضع المشرع الفرنسي مفهوماً موسعاً للتوقيع ولم يفرق بين التوقيع التقليدي والالكتروني، ولهما نفس الحجية القانونية في الإثبات[4]

ويرتب آثاره سواء كان مستندا عرفياً أو رسمياً وهو ما تناوله المشرع الفرنسي بموجب القانون رقم 2000 / 230 الصادر في 13 مارس 2000 الخاص بالمبادلات والتجارة الإلكترونية المعدل

[1] عيسى غسان ريضي، المرجع السابق، ص 51.

[2] زينب غريب، اشكالية التوقيع الالكتروني وحجيته في الاثبات، مذكرة لنيل شهادة الماستر في القانون الخاص، جامعة محمد الخامس، الرباط ،2010، ص 20.

[3] إيمان مؤمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، بدون طبعة، دار الجامعة للنشر، الإسكندرية، 2008، ص 298.

[4] الغريب فيصل سعيد، المرجع السابق، ص216.

والمتمم للقانون المدني في نص المادة 1316 / 4 منه، والتي تنص على: " **أن التوقيع الالكتروني إنما يدل على شخصية صاحبه ويضمن علاقته بالواقعة التي أجراها، ويؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه إلى أن يثبت عكس ذلك** "[1] .

2 . في القانون السويسري

عرفت المادة 2 من القانون الفيدرالي السويسري لعام 2004 التوقيع الالكتروني على أنه: " **معطيات الكترونية مجتمعة أو مرتبطة منطقيا بمعطيات الكترونية اخرى تستخدم في التحقق من مصداقيته** ".

وهو حسب هذا القانون فانه يفيد بالمتطلبات التالية:

أ . أن يرتبط فقط بصاحبه.

ب . أن يسمح بالتعرف على الموقع.

ج . أن يكون قد انشا بوسائل يحفظها الموقع تحت رقابته المنفردة.

د . أن يرتبط بالمعطيات التي يتعلق بها بحيث يمكن اكتشاف أي تغيير لاحق عليها[2].

ب: تعريف التوقيع الالكتروني من قبل التشريعات العربية

1 . في القانون المصري

تعرف المشرع المصري التوقيع الإلكتروني في المادة الأولى فقرة ج " من القانون رقم 15 لسنه 2004[1]،بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بأنه " **ما**

[1] ماجد راغب الحلو، العقد الاداري الإلكتروني دراسة تحليلية مقارنة، بدون طبعة، دار الجامعة الجديدة، مصر،2007، ص 81 . 82.

[2] عصام عبد الفتاح مطر، التحكيم الإلكتروني، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 106.

يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو اشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره "[2]

2 . في القانون العراقي

يعرف قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012[3]، التوقيع الالكتروني بأنه" **شخصيه تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أصوات أو غيرها وله طابع منفرد يدل على نسبته إلى الموقع ويكون معتمدا من جهة التصديق**"، .

يتضح من ذلك أن المشرع العراقي في هذا القانون لا يوجد إلتزام بصيغة معينة بالتوقيع، وإنما بين أن هناك أشكال للتوقيع الإلكتروني، ووضع شرطين لهذا التوقيع جاءت ضمن التعريف، الأول أن تكون له صفة مميزة تميزه عن غيره من صور التوقيع، بحيث تؤكد نسبته إلى الموقع، والثاني أن يكون معتمدا من جهة التصديق، ومما يلاحظ على التعريف أنه جمع بين الجانب التقني والوظيفي للتوقيع الإلكتروني، وذلك ببيانه لأشكال التوقيع بأن يكون إما حروف أو غيرها، وضعها المشرع لكي تكون مدخلا لأي وسيلة جديدة تظهر مع التطور التكنولوجي، وأشار المشرع إلى الطابع الذي يميز التوقيع الإلكتروني عن غيره، دون الإشارة إلى الوظيفة الثانية المتعلقة برضاء الموقع على ما تم التوقيع عليه[4].

3 . تعريف التوقيع الإلكتروني في التشريع الجزائري

---

[1] قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، رقم 15 لسنة 2004، الجريدة الرسمية، العدد 17 الصادرة بتاريخ 22 أفريل 2004.

[2] محمد الشهاوي، شرح قانون التوقيع الإلكتروني رقم 15 لسنة 2004 (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر،2010، ص 7.

[3] قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012، الوقائع العراقية، رقم العدد 4256، تاريخ العدد :05-نوفمبر 2011.

[4] ايلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية (دراسة مقارنة)، الطبعة الأولى، المركز العربي للدراسات والبحوث العلمية، مصر، 2019، ص87ـ88.

اعترف المشرع الجزائري بالتوقيع الالكتروني لأول مره بنص المادة 237 /2 من القانون المدني[1]، ومن ثم في القانون المتعلق بنظام الاستغلال المطبق على كل نوع من نواع الشبكات، بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، وصولاً إلى تعريف المشرع الجزائري للتوقيع الالكتروني في قانون خاص بالتوقيع والتصديق الالكترونيين حصراً، متمثلا في القانون رقم (04.15) الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين. [2]

كما اعترف المشرع الجزائري بالتوقيع الالكتروني في القانون المدني في المواد: 323 مكرر1 و 327 ونصت المادة: 323 مكرر1 المستحدثة بالقانون رقم 50. 01 المعدل للقانون المدني على ما يلي:" **ينتج الاثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أي علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق ارسالها** ".

ونصت المادة 323مكرر1 من القانون نفسه على أنه:" **يعتبر الاثبات بالكتابة في الشكل الالكتروني كالإثبات على الورق بشرط امكانية التأكد من هوية الشخص الذي أصدرها وأن تكون مُعَدَةُ ومحفوظة في ظروف تضمن سلامتها**"[3].

أما المرسوم التنفيذي رقم (07 -162) لسنه 2007 فقد عرف المشرع الجزائري التوقيع الالكتروني من خلاله بنص المادة الثالثة (03) منه[4].

---

[1] الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426 الموافق 20 يونيو سنة 2005، ج ر، عدد 44، الصادرة 19 جمادى الأولى عام 1426 الموافق 26 يونيو سنة 2005.

[2] القانون رقم (15 .04) مؤرخ في 01.02 .2015 ،يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية للجمهورية الجزائرية ،العدد 60، الصادرة بتاريخ فبراير 2015.

[3] المواد 323 مكرر1و 327 من الامر 58.75 ، المتضمن القانون المدني الجزائري السالف الذكر

[4] المرسوم التنفيذي رقم (07 -162)، المؤرخ في 30 ماي 2007، المتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات بما فيه االلاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية يعدل ويتمم المرسوم التنفيذي رقم: (01 -123) مؤرخ في 09 جويلية 2001 ج،ر،ع 27 الصادرة في 13 جويلية 2001، ونصها:" **التوقيع الالكتروني هو معطى ينجم عن استخدام اسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر، 323 مكرر1**".

الفرع الثاني: خصائص التوقيع الإلكتروني

للتقنيات الحديثة ومنها التوقيع الإلكتروني مميزات وسمات وخصائص تختلف عن مثيلاتها في المعاملات التقليدية، وإن كانت هذه الخصائص أو السمات لا تختلف كثيرا عن ما يميزه التوقيع التقليدي، إلا أن وجودها له أهمية بالغة في حماية البيانات والمعلومات من الاستغلال الغير مشروع كالتزوير والتقليد وتحديد صلاحيات الوصول إلى تلك البيانات أو المعلومات تحديد مسؤولية كل مستخدميها.

من خلال دراستنا للتوقيع الالكتروني وتعريفاته الفقهية والتشريعية نستنبط أنه يتميز بعده خصائصه أهمها ما يلي:

أولاً: الخصوصية والتعرف على المستخدم

خاصية الخصوصية توفر حماية البيانات ضد الاستخدام غير المشروع ، أي تحديد صلاحيات الوصول للبيانات وعدم السماح للأشخاص بتنفيذ أي إجراء على البيانات التي لا يملكون صلاحيات المساس بها، وتتم عملية تفعيل صلاحية الوصول أثناء حفظ البيانات الخاصة بالتوقيع الإلكتروني الموجود على بطاقه ذكية، ولا يغادرها أبدا ومحمي برقم سري أو تشفير البيانات أثناء إرسالها، وهي إحدى المزايا التي تجعل من الشخص المقصود هو الوحيد الذي يطلع على المستند المرسل [1].

كما تتم عملية التحقق من هوية الأشخاص والتعرف على مصادر البيانات والبطاقات الذكية، أو عن طريق شهادة التصديق الإلكتروني المصدرة من جهة التصديق الإلكتروني، وكلما زادت الحاجة لدقة تحديد الهوية يتم اللجوء إلى عدة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم [2].

---

[1] مولود قارة، " الإطار القانوني للتوقيع والتوثيق الإلكترونيين في قانون المعاملات والتجارة الإلكترونية "، مقال منشور عبر موقع: www.minshawi.com اطلع عليه بتاريخ 08 /02/ 2024.

[2] لا لوش راضية، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012. ص 37.

ثانياً: التوقيع الإلكتروني يوفر وحدة البيانات

هي عملية حماية البيانات ضد التغير أو التعويض عنها ببيانات أخرى، وتتم هذه العملية باستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة المرسلة ببصمة الرسالة المستقبلة. عدم تغيير البيانات أثناء نقلها، وأن مستقبل الرسالة يمكنه معرفة ذلك عند تلقي الرسالة عند تلقي الرسالة، حيث إن حصل أي تغيير أو تعديل على المستند أثناء إرساله اعتبر تزويرا [1] .

ثالثاً: خاصية التوقيت للتوقيع الالكتروني

إن المقصود بالتوقيت هو معرفة تاريخ وساعة اتمام التوقيع ، كما أن التوقيع الرقمي الذي يعد صورة من صور التوقيع الإلكتروني يتمتع بخصوصية التوقيت المسند أيضاً، فالوقت هو إحدى العناصر المهمة في التكنولوجيا بشكل عام وفي العلاقات القانونية بشكل خاص، فلهذه الميزة العديد من الفوائد مثل: تاريخ الرسالة في لحظة ايجادها أو في لحظة إرسالها، إضافة إلى تنظيم تاريخ التبادل للتسجيل في الملف، عداك عن تحكيم العديد من الاوقات المحلية أو الداخلية المتأتية من أنظمة المعلوماتية أو قطاعات الاتصالات عن بعد[2] .

رابعاً: خاصة السرعة

إن توفير الوقت والجهد تحتاجه جميع التعاملات التي تبرم عبر الوسائل الإلكترونية الحديثة، ولكون التوقيع الإلكتروني يتمتع بهذه الخاصية (السرعة)، فإن ذلك ساعد على ازدهار التجارة الإلكترونية بشكل خاص، فبواسطة انتشار الوسائل الإلكترونية تم تبديل الدعائم الورقية واعتماد الإلكترونية بدلاً عنها، لأن الدعامة الورقية تشكل عائق أمام تقدم التجارة الإلكترونية، ومن ثم فإن

[1] صلاح عبد الحكيم المصري، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزه، مذكرة لنيل شهادة الماجستير في ادارة الأعمال، كلية التجارة، الجامعة الإسلامية، غزه، فلسطين, 2007، ص 24 . 25.

[2] فالح جلال عبد الرضا الحسيني، أثر شكلية التوقيع الإلكتروني في القرار الإداري، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2015، ص 26.

وجود هذه الدعامة يمكن الشخص من وضع أحد الأنواع الخاصة بالتوقيع الإلكتروني عليها، حيث إن السرعة تشكل أهمية كبرى بالنسبة للعميل لأنه دائما يسعى أن تتم معاملته بأسرع وقت ممكن[1].

المطلب الثاني: أهمية وأهداف التوقيع الالكتروني

لقد أفرز الواقع العملي هذا النوع المستحدث من التوقيع والذي يختلف بلا شك عن التوقيع التقليدي، ومن ثم فإن نظم معالجة المعلومات تحتاج إلى معنى أوسع وشمولي للتوقيع الالكتروني يختلف من مستخدم إلى آخر وبحسب الاستخدام له، ومن هنا فإن التوقيع الإلكتروني بشكل عام هو التوقيع الناتج عن إتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معروفة مقدماً، ويكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي، ولما كان الاختراع وليد الحاجة فقد أظهرت التقنيات الحديثة صوراً للتوقيع الإلكتروني بهدف تنشيط المعاملات الإلكترونية.

لم يَعُد التوقيع التقليدي في إثبات وتوثيق العقود مناسباً للمعاملات الإلكترونية، وذلك لإحلال الوسيط الإلكتروني محل الوسيط الورقي.

ومن هنا ظهرت الحاجة إلى ضرورة إيجاد بديل إلكتروني يحل محل التوقيع الخطي ويؤدي نفس هدفه والمتمثل في منح القوة الثبوتية للتصرف القانوني، فظهر التوقيع الإلكتروني كتقنية للتبادل الإلكتروني للبيانات. وانطلاقا من هذا قسمنا المطلب إلى فرعين: الفرع الأول يتناول أهمية التوقيع الإلكتروني، أما الفرع الثاني خصصناه لأهداف التوقيع الإلكتروني.

الفرع الأول: أهمية التوقيع الالكتروني

يعتبر التوقيع من المبادئ الأساسية في الاثبات وشرطا مهما لتوثيق اي مستند سواء في المراسلات العادية او الإلكترونية على اختلاف انواعها ووسائطها في داخل المؤسسة او المراسلات التي تتم بين المؤسسات في داخل الدولة أو خارجها، وهذا بدوره يتماشى مع مقتضيات التجارة

[1] ايلاف فاخر كاظم علي، المرجع السابق، ص 91 _92.

الإلكترونية، وفيه استجابة وتيسير لمعاملات التجار الذين يرغبون في إقامة علاقات تعاقديه عبر الانترنت، ومن هنا تكمن مقاصد المشرع من حيث أهميه التوقيع الالكتروني في مدى السرية والضمان الذي يتمتع به، وعليه فانه يمكن الاستفادة من استخداماته في شتى المجالات الأتية: –

أولاً: توفير عامل الوقت والجهد الثمين للمواطن الموظف، وفي هذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته، أو بإستخدام وسائل النقل الأخرى إلى الدوائر الحكومية، والانتظار طويلاً كما هو الحال في معظم الدول النامية بخلاف الدول المتقدمة، حيث أنه بالكاد أن ترى أشخاصاً يتابعون وينهون معاملاتهم الا بأضيق الحالات، وهو ظهور الشخص إن لزم في مسألة شخصية، وبذلك نرى أن التوقيع الالكتروني يسمح بعقد الصفقات عن بعد ودون حضور المتعاقدين.

ثانياً: يمكن الاعتماد عليه كلياً ضمن الاجراءات القانونية والقضائية في المنازعات بين الاشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية، وهنا يكون لقناعة القاضي دور كبير حيث يتم التعويل على الثقة في الجهاز الذي من خلاله تم اجراء التوقيع الالكتروني، ويقيم هذه الاجراءات ومدى قوة اجراءات السرية والتخزين والارسال والحفظ وغيرها، وكفاءة القائمين على هذه الاجراءات، وكفاءة القائمين على هذه الاجراءات، ومدى تقدم التكنولوجيا، كل هذه الاعتبارات ينظرها ويحكم في ضوئها مدى جدارة التوقيع الالكتروني في ان يتم الاعتماد عليه من عدمه.

ثالثاً: يساهم التوقيع في فتح قناة اتصال جديدة بين المواطن والجهات الحكومية يمكن من خلالها النفاذ إلى مستويات الإدارة العليا لزيادة الشفافية في الأعمال الحكومية، وبالتالي يُعَدُ عامل وأداة مهمة لنجاح فكرة الحكومة الإلكترونية.

رابعاً: إن التوسع في استخدام التوقيع الالكتروني يرفع كفاءة العمل الاداري ويساهم في الارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع متطلبات ومستجدات العصر الحديث. وبالتالي يؤدي هذا النمط إلى التخفيف من نمط البيروقراطية التي تؤخر زيادة النشاطات والمعاملات بكافة صورها.

خامساً: بما أن التوقيع الالكتروني يتم استخدامه في جميع المستندات ونماذج الطلبات، فإن ذلك يساعد على توفير الهوية الرقمية لكل مواطن، وهذا يسهم في خلق وعي فكري للمواطن، وتطوير التعامل بالأنترنت، مما يؤثر على التجارة الإلكترونية، فنرى الكثيرين من الأشخاص الأذكياء الذين يملكون شركات ضخمة حققت الكثير من الارباح من دون أن يكون لها مقر بحجم الشركات الكبيرة.

ومن هنا تكمن أهمية التوقيع الرقمي في أنه يوفر الضمان من خلال استخدام عمليات البيع والشراء من المعاملات التجارية الإلكترونية المختلفة، كالبيع وغيرها من العقود والتصرفات القانونية التجارية الأخرى والاستيراد والتصدير وباقي التعاقدات، وحجز تذاكر السفر والفنادق والمعاملات المصرفية بكل أنواعها، والتي تتم في شكل محرر الكتروني موقع توقيعا إلكترونياً، وغير ذلك من المزايا الأخرى التي تؤدي بدورها إلى التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على معلومات منه (التوفير في الورق، الطلبات، الطباعة،.. الخ)[1].

الفرع الثاني: أهداف التوقيع الإلكتروني

ليس الهدف من إنشاء التوقيع الإلكتروني هو الفانتازيا الرقمية، ولكن الهدف يندرج تحت مضمون الأمن والسلامة الرقميين، وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العملية والأهداف المرجوة منها ولعدة أهداف قانونية بحتة تبعد المتطفلين عن التلصص وسرقة البيانات وأهمها:

أ. توثيق التوقيع الالكتروني للموقع

كما شرحنا سابقاً عند إنشاء الشهادة فإنه يتم انشاء مفتاحين (عام وخاص)، وفي حالة إن كان المفتاحان مرتبطين بصاحب التوقيع الإلكتروني، فإن كل وظيفة يقوم بها بإرسال الوثائق من عنده

[1] اياد "محمد عارف" عطا سده، مدى حجيه المحررات الإلكترونية في الاثبات" دراسة مقارنه"، مذكرة لنيل شهادة الماجستير في القانون الخاص، جامعه النجاح الوطنية، كليه الدراسات العليا، نابلس، فلسطين، 2009، ص 68 – 70.

فإنها تكون خاصه به، وهنا لا يمكن القيام بعملية التزوير إلا في حالة واحده وهي أن فقد صاحب التوقيع الالكتروني المفتاح الخاص به أو تم تسريبه.

ب . ضمان توثيق الرسالة

عندما يقوم المستخدم بإنشاء رسالة مصاحبة لتوقيعه الالكتروني فإنها عاده تكون مدمجة مع بعض الشفرات كوظيفه اساسية تسمى' وظيفه الهاش' « hash function » وتستخدم في بداية انشاء التوقيع الالكتروني والتأكد من صحته.

أما الطريقة التي تعمل بها فإنها تقوم على اساس انشاء تمثيل رقمي معين على شكل قيمه رقمية "هاش" او" نتيجة الهاش " عادة تكون هذه القيمة أصغر من الرسالة وتوضع اما في بدايتها او نهايتها وتكون مدمجة بها، وفي هذه الحالة ان تم التلاعب بتلك الرسالة فانه على الفور تختلف قيمة " الهاش" التي تم احتسابها منذ البداية عند انشاء الرسالة، وحتى ان تم التعرف على قيمة " الهاش " الثانية فانه من الصعوبة تقفي اثر قيمة " الهاش " الأولية.

ج . الضمان

عند البدء في انشاء التوقيع الالكتروني بوساطة الهيئات المعتمدة فإنها بالطبع تتطلب ضمانا عاليا حسب المستويات والتراخيص الدولية والتي تتم عادة بموافقه الموقع الالكتروني، وهنا فإنها ومن دون شك تولد اعلى درجات السلامة الأمنية.

د . توسيع التجارة الإلكترونية

ان انتشار التوقيع الالكتروني له من المميزات الكبيرة التي من شانها القيام بالتوسع في التجارة الإلكترونية وتامين جميع معاملاتها على الصعيدين الدولي والمحلي، وحقيقة تذكر ان بعض الدول العربية باتت تعمل في سن قوانين كثيرة تخص التوقيع الالكتروني ومنهجيته ومدى الاستفادة منه في

تامين سريه المعلومات المرسلة مع عدم قدره أحد على الاطلاع عليها او تعديل جزء منها، والتي من شانها ان تقضي على " الواسطة " في بعض البلدان[1].

المبحث الثاني: شروط الواجب توفرها في التوقيع الإلكتروني

إذا كانت الغاية من التوقيع الالكتروني هي اكتساب المحررات والمستندات القوة القانونية المقررة في التوقيع العادي فان الوسيلة لذلك هي توافر مجموعة من الشروط التي بتوافرها يتم اكتساب التوقيع الالكتروني الحجية القانونية.

إلا أنه على الرغم من ذلك لا يمكن التقليل من أهمية الدليل الالكتروني نظرا لإمكانية للتخلص من تلك العيوب مستقبلا وقد نص قانون اليونسترال النموذجي للتجارة الالكترونية على أنه: يعطى للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجية في الاثبات، وفي تقدير حجية رسالة البيانات، فالإثبات يولي الاعتبار لجداره الطريقة التي استخدمت في إنشاء أو تخزين أو إبلاغ رسالة البيانات وبالتصويت عليها، ولجدارة الطريقة التي استخدمت في المحافظة على سلامة المعلومات بالتصديق عليها، وللطريقة التي حددت بها هويه منشئها، ولأي عمل آخر يتصل بالآمر، ولدراسة هذا المبحث قمنا بتقسيمه إلى مطلبين ،حيث سنتناول في المطلب الأول شروط التوقيع الإلكتروني ووظائفه ، أما في المطلب الثاني فقد خصصناه الى حجية التوقيع الإلكتروني في الإثبات.

المطلب الأول: شروط التوقيع الإلكتروني ووظائفه

[1] مصطفى كافي، النقود والبنوك الالكترونية، بدون طبعة، دار رسلان، دمشق، سوريا، 2011، ص199-200.

لا شك أن الثقة والأمان لدى المتعاملين عبر شبكة الإنترنت يأتيان في مقدمة الضمانات التي يتعين توافرها لازدهار التعاملات الإلكترونية، ومع التطور الهائل لوسائل التكنلوجيا الحديثة ظهر التوقيع الإلكتروني والتصديق الإلكتروني كقواعد لإثبات العقد الإلكتروني وقد اقتضت هذه التطورات على مستوى شبكات الإنترنت والمعاملات الإلكترونية، تحديث وتطوير التشريعات كي تواكب مع هذه التطورات وإيجاد نصوص قانونية لتقنين وتنظيم العقود الإلكترونية.

إن تمتع التوقيع الإلكتروني بحجيته في الإثبات يستوجب أن يتوفر من الشروط التي تستوجب القوانين توفرها لصحته، وان الهدف الأساسي من التوقيع الإلكتروني، مهما كان شكله هو إضفاء القوة الثبوتية على المحرر الإلكتروني وهذا الهدف لا يمكن بلوغه إلا إذا حددت وظائف هذا التوقيع.

سنتطرق في الفرع الأول لشروط التوقيع الإلكتروني، أما الفرع الثاني خصصناه لوظائفه.

الفرع الأول: شروط التوقيع الإلكتروني

لقد اعتمد المشرع الجزائري في بيان شروط التوقيع الالكتروني عن طريق تحديد شروط التوقيع الالكتروني الموصوف، فنص عليها في المادة 7 من القانون 15 ـ 04 المتعلق بالتوقيع والتصديق الالكترونيين بحيث يجب أن تتوفر فيه الشروط التالية.

أولاً: ان يرتبط بالموقع دون غيره.

يقصد بهذا الشرط أن يكون لصاحب التوقيع الالكتروني بيانات وشفرة خاصة به عن طريق باقي الموقعين، ذلك انه عندما تصدر بيانات انشاء التوقيع لشخص ما فلا يمكن أن يتم إصدار نفس التوقيع لشخص آخر[1].

فلكي يقوم التوقيع بوظائفه يجب أن يكون له علاقة مباشرة بالموقع والذي نصت عليه المادة 2 من الفقرة 2 من القانون 15 ـ 04 بأنه " **شخص طبيعي يحوز بيانات انشاء التوقيع الالكتروني**

[1] عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات التوثيق، الطبعة الأولى ، دار وائل للنشر والتوزيع، الأردن، 2010، ص 56.

ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله ". بالتالي فانه بتوافر هذا الشرط في التوقيع الالكتروني يؤدي الى اتجاه نية الموقع على المحرر بمضمونه ويكون شاهد على نيته بالالتزام بمضمون العقد الموقع عليه[1].

من الضروري أن يكون التوقيع دالا ومحددا للشخص الموقع ليتحقق بذلك دوره في الاثبات، وبناء على ذلك فانه لا يشترط استخدام صيغة معينه في التوقيع طالما أمكن تحديد الموقع وبذلك يستوي في التوقيع أن يكون باسم الموقع الكامل أو حتى استخدام الأحرف الأولى للموقع أو برسم معين [2].

ثانياً: أن يمكن من تحديد هوية الموقع

يتطلب هذا الشرط في التوقيع الالكتروني أن يكون قادرا على تغيير هوية الشخص الموقع فطريقة التوقيع تشير وتحدد هوية الموقع وهذه من الوظائف الأساسية والمهمة للتوقيع، فكل شكل من أشكال التوقيع سواء كان إمضاء أو بصمة أو توقيعاً الكترونياً أو أي شكل. فانه يحدد هوية الموقع لأنه يعود عليه، بالإضافة الى الشخص الموقع هو الذي اختار هذا الشكل ليعبر عنه ويحدد هويته[3].

وقد تطرأ المشرع الجزائري الى هذا الشرط في الفقرة 3 من المادة 7 من القانون 15 . 04. ومثال هذا الشرط التوقيع بالرقم السري في بطاقات الصراف الآلي، حيث قيام حامل البطاقة بإدخال الرقم السري الخاص به في بطاقات الصراف الآلي، وقيام هذا الأخير بالتعرف على الرقم السري وإدخال الشخص لحسابه لتكون هذه الاجراءات بمجملها كافية للدلالة على هويته.

بحيث يمكن اجراء العمليات التي يريدها، وتحديد هوية مبرم العقد أمر ضروري خاصة في مجال الوفاء بالالتزامات العقدية ليتم تحديد أهلية صاحب التوقيع، فلا يتصور أن يتم منح شخص عديم

[1] لورنس محمد عبيدات، اثبات المحرر الالكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الاردن، 2005، ص129.

[2] محمد ابراهيم ابو الهيجاء، عقود التجارة الإلكترونية، (اثبات العقد الالكتروني، حماية المستهلكين، وسائل الدفع الالكتروني، المنازعات العقدية وغير العقدية، الحكومة الإلكترونية، القانون الواجب التطبيق)، الطبعة الثانية، دار الثقافة، عمان، 2011، ص126.

[3] عبد الفتاح البيومي حجازي، مقدمة في التجارة الإلكترونية والعربية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2003، ص 216 .217.

الأهلية أو ناقصها توقيعاً الكترونياً، لأن هذا الأمر يبنى عليه التزامات كثيرة بحيث يتوجب على صاحب التوقيع الالكتروني أن يكون كامل الأهلية للقيام بها، حتى تتمكن جهة إصدار التوقيع الالكتروني من منح التوقيع لهذا الشخص[1].

فقد نص المشرع الجزائري أيضا على هذا الشرط من خلال نص المادة 323 فقرة 1 من القانون المدني الجزائري والتي تنص على أنه " .... **بشرط امكانية التأكد من هوية الموقع التي أصدرها** "[2] .

فالمشرع من خلال نص المادة، قد أقر بإمكانية الاعتداء بالتوقيع الالكتروني في اثبات من كان كفيلا بالتعريف عن هوية الموقع والتحقق من نسبة التوقيع اليه.

ثالثاً: إنشاء التوقيع الالكتروني بواسطة وسائل خاصة تكون تحت سيطرة الموقع

لكي يتمتع التوقيع الالكتروني بالحجية في الاثبات يجب أن يتم انشاؤه بواسطة أدوات تكون خاضعة لسيطرة الموقع وحده، بحيث لا يستطيع أي شخص معرفة فك رموز التوقيع الخاصة به أو الدخول عليه، وسواء عند استعماله لهذا التوقيع أو عند انشائه[3].

يتضح من هذا الشرط أنه يشترط لتمتع التوقيع الالكتروني الموصوف بالحجية في الاثبات أن يتم انشاؤه بوسائل تحت سيطرة الموقع، أما اذا فقد الموقع هذه السيطرة لأي سبب، فان بيانات التوقيع تفقد طابعها السري بحيث يعلمها كل الاشخاص، مما يفقد التوقيع الالكتروني حجيته في الاثبات، لأن تمييز هويته وتحديد شخصيته يكون مشكوكاً فيه [4].

---

[1] عايض الراشد المرى ، مدى حجية الوسائل التكنولوجية الحديثة في اثبات العقود التجارية ، بدون طبعة ، القاهرة ، 1998، ص 74.

[2] امر رقم 75 ـ 58، المتضمن القانون المدني 2005، السالف الذكر.

[3] لورنس محمد عبيدات، المرجع السابق، ص 31.

[4] مرزوق يوسف، وسائل الاثبات الحديثة، رسالة لنيل شهادة دكتوراه في القانون الخاص، كليه الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012 ، ص62.

رابعاً: أن يكون التوقيع مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التعبيرات اللاحقة بهذه البيانات.

يتناول هذا الشرط مسألة هامة وضرورية يجب على التوقيع الالكتروني أن يستوفيها لاعتباره توقيعاً موصوفاً لضمان سلامة المحرر الالكتروني، وضمان سلامة بيانات انشائه، إن المحرر الالكتروني قد يتعرض للتغيير أثناء عملية نقله من المرسل إلى المرسل اليه، هذا التغيير وقد يكون سببه عطلاً من الوسائل الفنية أو تدخل الغير أو من المرسل اليه[1].

ولابد من اتصال التوقيع اتصالا ماديا بالمحرر حتى يكون دليلاً على إقرار الموقع بما ورد في السند، وعند النظر الى التوقيع الرقمي مثلا والذي يعتمد على مفتاحين عام وخاص، بحيث لا يستطيع أحد أن يطلع على مضمون المحرر الا الشخص الذي يمتلك المفتاح الخاص، فلأن المحرر يرتبط بالتوقيع الالكتروني على نحو لا يمكن فصله أو التعديل فيه الا من صاحب المحرر نفسه.

مفاد هذا الشرط هو عدم امكانية احداث تغيير في المحرر الالكتروني بعد توقيعه الا إذا تم تغيير المحرر الالكتروني نفسه، لأنه لا يمكن الوصول الى المحرر الالكتروني دون معرفة التوقيع الالكتروني، ويقصد من هذا الشرط ليس فقط حماية التوقيع وانما حماية المحرر ايضا[2].

خامساً: وجوب توثيق التوقيع

لقد جاء في كافة التشريعات المتعلقة بالتواقيع الإلكترونية ضرورة توثيق التوقيع الالكتروني لدى جهة معينة تضطلع بالتحقق من مدى مصداقيته، والتأكد من الشخص العائد له ليتم بعد ذلك منح

[1] عيسى غسان ريضي، المرجع السابق، ص 177.

[2] يوسف احمد النوافلة، حجية المحررات الالكترونية في الاثبات وفق القانوني الاثبات والمعاملات الالكترونية، الطبعة الأولى، جامعة أردنية، الأردن، 2005، ص87.

صاحبه شهادة توثيق، والتي تؤكد صحة التوقيع وهناك من التشريعات من يمنح هذه الصلاحية لمجلس الوزراء والبعض الآخر لرئيس الحكومة[1].

الفرع الثاني: وظائف التوقيع الإلكتروني

رغم التكافؤ الوظيفي بين التوقيع التقليدي والتوقيع الالكتروني، إلا أن هذا الأخير يختص بوظائف أخرى غير تلك الممنوحة للأول، وتتمثل وظيفة التوقيع الالكتروني في منح المحرر القوة الثبوتية وهذه القوة لا يمكن تحقيقها إلا إذا تم التوقيع على الوظائف التالية:

أولا: تمييز هوية صاحب التوقيع

حتى يعتد بالتوقيع كدليل قانوني في الاثبات يجب ان تكون يجب ان يكون يجب ان يكون عباره عن علامه مميزه لشخص الموقع تمكن من تحديد هويته وتميزه عن غيره ونجد بان التوقيع الالكتروني يحققه سيما في ظل كل ما يتميز به من قدرة تقنية تعتمد على ارقام سرية خاصة بكل موقع ومدعمة بشهادات مصادقة من قبل جهات التصديق محايدة تشهد عليه وعلى ثبوتة لصاحبه، أيا كانت الصورة التي يتخذها خاصة مع الترقيع الرقمي المعتمد على تقنيات التشفير والشيء نفسه بالنسبة للتوقيع البيومتري المعتمد على تقنيات جد متطورة تفوق حتى الثقة المتنوعة في التوقيع الخطي.

غير أن ذلك لم يمنع البعض من القول بأنه تظل هنالك مشكلة في الحالة المتعلقة بتحديد هوية الشخص في حال تصرفه لحساب شخص آخر، كأن يكون وكيلاً عنه أو ولياً أو وصياً على قاصر أو ممثلاً من شخص معنوي ،إذ يجب عليه في هذه الحالات أن يحدد هويته بأن يوقع باسمه شخصياً، ولا يجوز للوكيل، الولي أو الوصي هنا أن يوقع باسم الوكيل أو القاصر أو أن يقلد توقيعه[2] .

ثانيا: التعبير عن ارادة صاحب التوقيع

[1] بوعمرة اسيا، النظام القانوني للتجارة الكترونية لدراسة مقارنة، رسالة لنيل شهادة الدكتوراه في الحقوق ،تخصص قانون الملكية الفكرية، جامعة الجزائر 01 ،الجزائر، 2012 ،ص 182ـ183.

[2] سعيد السيد قنديل، التوقيع الالكتروني ماهيته، صوره، حجيته في الاثبات بين التداول والاقتباس، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2006، ص 342 ـ 343 .

إن مجرد التوقيع يحمل دلالة الرضا والالتزام على ما تم التوقيع عليه، وذلك تخلص من التوقيع ذاته طالما أمكن نسبة التوقيع الى من صدر عنه.

بالنسبة للتوقيع الالكتروني فيستفاد رضاء الموقع وقبوله الالتزام بمجرد وضع توقيعه بالشكل الالكتروني على البيانات التي تحتويها المحررات الإلكترونية.

لذلك فحين يأخذ التوقيع المعلوماتي شكل الارقام سرية او الرموز محددة وتحفظ في حوزة صاحبها ومن ثم لا يعلمها غيره، فاذا استخدمت هذه الارقام، أي وقع بها صاحبها فان مجرد توقيعه هذا يدل على موافقته على البيانات والمعلومات التي وقع عليها والتي يرغب بالالتزام بها.

في هذه العملية نجد أن العميل صاحب البطاقة قد عبر عن ارادته الصريحة بمجرد توقيعه الالكتروني المترجم في شكل أرقام أو رموز أو شفرة معينة، استعملها حين تعامل مع جهاز الصرف الآلي، ثم انه أعطى أمر للجهاز بسحب المبلغ الذي يريده شخصياً. فان ذلك في جمله يصدر رضا منه وقبوله بمضمون المحرر الالكتروني[1].

يُعَدُ التوقيع الالكتروني من وسائل التعبير عن الإرادة التي يستخدمها الشخص لإنشاء تصرف قانوني معين كالعقد أو الالتزام، ويشكل التوقيع أداه صحة بمعنى أنه يعطي التصرف القانوني قيمة وقوه أكبر، فهو يعبر عن ارادة صاحبها بالموافقة بما ورد في السند[2].

ثالثا: التوقيع دليلا على حضور صاحبه

هذه الوظيفة تتفق تماماً مع طبيعة التوقيع اليدوي، إذ يستلزم لصحته ضرورة وجود شخص الموقع نفسه، أو من ينوبه قانوناً لوضع التوقيع على المحرر الكتابي، فإذا وجد التوقيع على الورقة وتثبت صحته، ونسبته إلى موقعه كان ذلك دليلاً على حضور الموقع شخصياً[3].

[1] عبد الفتاح البيومي حجازي، مقدمة في التجارة الإلكترونية والعربية، المرجع السابق، ص229ـ228.

[2] غازي أبو عرابي، "حجية التوقيع الالكتروني، (دراسة مقارنة في التشريع الأردني)"، مجلة دمشق للعلوم الاقتصادية والقانونية، المجلد 30 ، الطبعة الأولى ،2004، ص 175.

[3] لورنس محمد عبيدات، المرجع السابق، ص 125.

أما بالنسبة للتوقع الالكتروني لا يتصور حضور الأشخاص وانما هو وسيلة حديثة تستخدم في مجال العقود عن بعد، وأن قيام صاحب بطاقة الائتمان بالعملية القانونية ادخال البطاقة مع الرقم السري،

ثم اجابته للجهاز عن قيمة المبلغ المطلوب سحبه فان هذه الاجراءات تعد دليلا على حضور صاحب التوقيع الالكتروني بشخصه أثناء إدخال الرقم السري، وبالتالي إدخال العميل الرقم السري بنفسه يُعَدُ في حد ذاته توقيعاً منه، ودليلاً على أنه صدر منه شخصياً وكان فعلاً موجوداً حين صدر منه التوقيع في صورة أرقام سرية لا يعلمها الا صاحب التوقيع [1].

رابعاً: اثبات سلامة العقد

هذا لا يقصد به أن الهدف من التوقيع اضفاء الحجية على العقد وعلى صحة العقد، بل كقرينه تقبل اثبات العقد على سلامته وصحته وعدم المساس به، إذ من الممكن اثبات صورية العقد أو بطلانه أو عدم حجيته، حتى ولو سبق اثبات سلامته من خلال استخدام التوقيع الالكتروني المشفر الذي يضمن عدم العبث بمحتوى العقد.

فالمحررات الإلكترونية قائمة على بيئة الحسابات وشاشات الكمبيوتر التي تحتفظ بالمعلومات على دعامة الكترونية يسهل التلاعب بها اذ تمكن هنا اهمية التوقيع الالكتروني في اثبات محتوى العقد من خلال استخدامه الرسائل الرقمية المشفرة والمفتاحين العام والخاص لتحويل البيانات الى أرقام

[1] نادية ياس بياتي، المرجع السابق، ص194.

يصعب فكها ثم اعاده تحويلها من أرقام الى بيانات ومقارنة النتائج من قبل المرسل والمرسل اليه لتؤكد من عدم وجود تلاعب بالعقد[1] .

المطلب الثاني: حجية التوقيع الالكتروني في الاثبات

إن للتوقيع أهمية كبيرة في الإثبات حيث إن قواعد الإثبات بوجه عام لا تقبل المستندات العرفية إلا إذا كانت موقعة، ولا تقبل المستندات غير الموقعة إلا كمبدأ ثبوت بالكتابة يستلزم بينة أخرى، فإن قبول القضاء للتعاقد الالكتروني يتطلب إقرار وحجية التوقيع الالكتروني وموثوقيتها، كبنية في المنازعات وكما رأينا سابقا ان للتوقيع الالكتروني أحكام وشروط تحكمه، وقد سعت أيضا كما رأينا اغلب التشريعات لإضفاء عنصر الأمان عليه لضمان ثقة المتعاملين مع وسائل الاتصال الجديدة حتى يتساوى مع التوقيع الكتابي وبالتالي التساوي في الاثبات لذلك سنتناول في مطلبنا هذا كل من الجهود الدولية والوطنية للاعتراف بحجبة التوقيع الالكتروني في الاثبات.

الفرع الأول : حجية التوقيع الالكتروني في التشريع الدولي

أحدثت شبكة الانترنت ثورة هائلة في مجالات الحياة المختلفة وأنتجت بذلك ما يسمى التجارة الالكترونية، التي بطبيعة الحال تحتاج إلى توقيع يتلاءم مع طبيعتها وتحديد بيان حجيته هذا الأخير ،وهذا ما سنتناوله في فرعنا هذا :

أولاً: حجية التوقيع الالكتروني في قانون الاونيسترال النموذجي

لقد حددت المادة 07 من قانون الاونيسترال النموذجين بشأن التجارة الإلكترونية لسنه 1996 للتوقيع الالكتروني نفس الحجية الممنوحة للتوقيع التقليدي لكن بتوافر الشروط الاتية.

[1] يوسف أحمد النوافلة، الاثبات الالكتروني في المواد المدنية والمصرفية، بدون طبعة، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص101ـ102.

- **الشرط الاول**/ إمكانية تحديد هوية الموقع وموافقته على المعلومات الواردة في السجل.
- **الشرط الثاني** / أن تكون الطريقة المستخدمة لتحديد هوية الموقع موثوقة ويمكن الاعتماد عليها."

لكن عند صدور قانون الامم المتحدة النموذجي بشأن التوقعات الإلكترونية الصادرة بتاريخ 05 2001/06. حيث نصت المادة 06 الفقرة الأولى منه على انه: " **حينما يشترط القانون وجود توقيع من شخص ، يعد ذلك الاشتراك مستوفي بالنسبة إلى رسالة البيانات اذا استخدم توقيع الكتروني يعول عليه بالقدر المناسب للغرض الذي أنشأت أو ابلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك اي اتفاق ذي صلة** ... "

" يعتبر التوقيع الالكتروني موثوقا به لغرض الوفاء بالاشتراك المشار اليه في الفقرة الأولى:

أ .كانت بيانات انشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص اخر

ب .كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع لسيطرة الموقع دون أي شخص آخر.

ج .كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف" [1].

حسب نص هذه المادة نجد أنه لا يتم التمييز بين المحررات الإلكترونية والورقية من حيث الحجية في الاثبات ما دامت النتيجة القانونية المترتبة على استخدام التوقيع الالكتروني الموثوق به هو نفس نتيجة استعمال التوقيع العادي على محرر ورقي، وبالتالي إذا ما توفرت الشروط المنصوص عليها قانونا تكون له حجيه في الاثبات[2] .

[1] قانون الاونسيترال النموذجي بشأن التوقيعات الإلكترونية، المؤرخ بـ 05 / 06 / 2001 .

[2] غانم ايمان، المرجع السابق، ص 84.

وان التوقيع الالكتروني صالحاً لإنشاء الالتزامات عندما يتطلب القانون وجود توقيع على محرر معين ، وأن يكون هذا التوقيع الالكتروني موثوقا به ويمكن التعويل عليه بالقدر المناسب للغرض الذي انشئت من اجله رساله البيانات .

كما يتبين لنا من نفس المادة أنها ربطت الحجية القانونية بشرط الموثوقية في التوقيع الالكتروني ودرجه الأمان التي يوفرها، كذلك ترك للأطراف حرية اختيار طرق اثبات موثوقية التوقيع الالكتروني،

أهم ما في هذه المادة هو اعتبارها التوقيع الالكتروني كفيلا ومستوفيا لمتطلبات القانون بوجود توقيع[1]. فقانون الاونيسترال النموذجي فرق بين نوعين من التوقيع الالكتروني فهناك التوقيع الالكتروني العادي، والذي جاء النص عليه في اغلب التشريعات وهو البيانات الإلكترونية التي تتخذ شكل حروف أو رموز أو إشارات وغيرها ، والتي تستخدم للتوقيع على رسالة بيانات عادية بغرض تحديد هوية صاحبها والدالة على شخصيته والتزامه بمضمون ما قام بالتوقيع عليه .

فتقتصر وظيفة هذا النوع من التوقيع على ما يقوم به التوقيع التقليدي من وظائف ودرجة الامان التي يتمتع بها ليس بالدرجة العالية ، مما يجعل حجيته بالإثبات لا ترتقي الى درجة اليقين التام، والذي يؤدي الى اخضاعه للسلطة التقديرية للقاضي لتحديد مدى درجة الأمان المستخدمة في هذا النوع من التوقيعات ومدى تحقيقه لوظائف التوقيع والتي يكون للخبير الفني المكلف من قبل المحكمة دور في ذلك [2].

أما النوع الثاني من التوقيع الإلكتروني فهو التوقيع المحمي، والذي يتخذ هيئة بيان في شكل الكتروني متصل برسالة بيانات ويجب أن يحقق وظائف ومزايا تزيد على التوقيع الإلكتروني العادي، إضافة لتحقيقه هوية الشخص القائم به وتحديد شخصيته، والتزامه بمضمون المحرر الموقع عليه فإنه يستلزم أن يحقق ربطاً بين الموقع والتوقيع، والسماح له بالسيطرة على التوقيع بحيث يصعب تعديل هذا

[1] لملوم كريم، المرجع السابق، ص 151.

[2] عبد الرفيق أورام، العقد الإلكتروني وحجيته في الإثبات المدني، مذكرة لنيل شهادة الماستر، وحدة الماستر القانون المدني والأعمال، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة عبد المالك السعدي، طنجة ، 2007 /2008، ص 79.

التوقيع بعد اجراءه، وعدم إمكانية إصدار نفس التوقيع من شخص آخر ، والذي يمكن من اكتشاف أي تحريف او تغيير أو تعديل في مضمون المحرر أو التوقيع [1].

ثانياً: حجية التوقيع الالكتروني في التوجيه الاوروبي

إن التوجيه الأوروبي نظم بعض الجوانب القانونية للتوقيع الالكتروني مستهدفا التنسيق بين تشريعات الدول الاعضاء في الاتحاد الاوروبي، لأنه عندما يضع نظام مشترك حول شروط التوقيع الالكتروني ومعايير الاعتراف بآثارها القانونية سوف يساهم بشكل كبير في تدليل العقبات التي قد تعترض استخدام هذه الالية داخل السوق الاوروبية[2].

فقد ساعد التوجيه الاوروبي في انشاء إطار قانوني متناسق داخل المجموعة الأوروبية من أجل تدعيم الثقة في وسائل الاتصال الحديثة، ويقر بالاتفاقات المتعلقة بالإثبات والتي بموجبها يتفق أطرافها على شروط قبول التوقيع الإلكتروني في الاثبات[3].

إن التوجيه الاوروبي في القانون رقم 93/ 1999 الخاص بالتجارة الإلكترونية والقانون الخاص بالتوقيع الالكتروني بشأن التوقيع الالكتروني أضفى على هذا النوع من التوقيع نفس الحجية القانونية في الاثبات الممنوحة للتوقيع التقليدي، وذلك في الفقرة الأولى من المادة 05 من هذا التوجيه والتي نصت على أنه:

" على الدول الأعضاء مراعاة أن التوقيع الالكتروني المتقدم المستند إلى شهادة تصديق الكتروني والمنشأ بوسيلة آمنه:

[1] محمد محمد أبو زيد ، تحديث قانون الإثبات ، بدون ناشر ، 2002، ص 185 ـ 186.

[2] زينب غريب، مرجع سابق، ص 113

[3] طارق عبد الرحمان ناجي، التعاقد عبر الأنترنت واثاره(دراسة مقارنة)،بحث لنيل دبلوم الدراسات العليا المعمقة، كلية العلوم القانونية والاقتصادية و الاجتماعية، جامعة محمد الخامس أكدال، 2006، ص 83.

1 . يحقق الشروط القانونية للتوقيع بالنسبة للمعلومات المكتوبة الكترونيا بذات الحجية التي يحققها التوقيع اليدوي بالنسبة للمعلومات المكتوبة يدويا أو المطبوعة على الورق.

2 . يكون مقبولا كدليل أمام القضاء."

كما نص في الفقرة الثانية من ذات المادة على أن:" **على الدول الاعضاء مراعاة أن التوقيع الالكتروني لا يفقد أثره القانوني أو حجيته كدليل اثبات بسبب:**

1 . أن التوقيع جاء في شكل إلكتروني.

2 . لأنه لم يستند إلى شهادة تصديق الكتروني معتمدة من جهة مرخص لها بذلك.

3. لأنه تم انشاؤه أو إصداره من خلال تقنيات تجعله توقيعا إلكترونيا آمنا."

اذن فالتوجيه الاوروبي قد اعترف بالحجية القانونية للتوقيع الالكتروني في التعاملات الإلكترونية، وحتى الدول الأعضاء في الاتحاد الاوروبي على الالتزام بذلك عند استيفائه للشروط اللازمة، وقد ميز بين نوعين من التوقيع الالكتروني والزم الدول الأعضاء بأن يكون التوقيع الإلكتروني المتقدم أو المعزز بالمستند إلى شهاده توثيق، وهو النوع الأول والذي يتم اصداره من خلال تقنيات تضمن له الثقة والأمان، أي يصدر عن طريق آليات أكثر حماية وأمان وأن تعطيه الدول الأعضاء الحجية الكاملة في الإثبات أمام القضاء مثل التوقيع التقليدي، وهو ما نص عليه في الفقرة الأولى من المادة 05 من التوجيه الأوروبي رقم 93/ 1999.

أما النوع الثاني فهو التوقيع الإلكتروني غير المعزز، فالتوجيه الأوروبي لا يفرض على الدول الأعضاء إلا الالتزام بعدم إنكاره كوسيلة اثبات لمجرد كونه في شكل الكتروني، وأنه يرفق بشهادة تؤكد صحته عن طريق استخدام ادوات تأمين التوقيع، فهنا التوجيه الأوروبي وجه للدول الأعضاء عدم إهدار قيمة التوقيع الالكتروني في الاثبات والاعتداد به كدليل، ومنحه الحجية القانونية المناسبة حتى

وإن لم يكن مستوفياً لشروط التوقيع الإلكتروني المتقدم أو المعزز، وهو ما نص عليه في الفقرة الثانية من ذات المادة من التوجيه الاوروبي[1].

فهنا لا يتساوى الاعتراف بحجية التوقيع الإلكتروني مع الاعتراف القانوني المقرر للتوقيع الإلكتروني المتقدم.

يستلزم على من يتمسك بالتوقيع الإلكتروني الذي لا تتوفر فيه المتطلبات القانونية أن يقيم الدليل أمام المحكمة على جدارة التقنية المستخدمة في إنشاء وإصدار التوقيع الالكتروني، وأوجب على الدول الأعضاء تطبيق هذا التوجيه بحلول 19 يوليو 2001 الذي الزم وجوب الاعتراف بحجية التوقيع الإلكتروني في الاثبات[2].

وبالتالي الفقرة الثانية لم تستخدم مصطلح التوقيع الإلكتروني المتقدم، ويمكن تطبيق هذه المادة على التوقيع الإلكتروني البسيط قبل اعتماده من قبل مقدمي خدمات التصديق المعتمدين لدى الدولة، معناه قبول هذا التوقيع الإلكتروني البسيط كدليل اثبات ولكن عند حدوث ازدواجية بين توقيعين إلكترونين أحدهما بسيط والآخر مقدم في هذه الحالة تكون الأولوية للتوقيع المقدم لأنه يتمتع بعناصر أمان يمكن أن تمنحه هذه الأولوية[3].

نجد أنه تم منح التوقيع الإلكتروني المقدم نفس الحجية القانونية الممنوحة للتوقيع الخطي، أي الذي تم اعتماده والمصادقة عليه من قبل الجهة المرخص لها بهذا العمل، كما تم تبني المفهوم الواسع للتوقيع الإلكتروني ليشمل جميع صوره والتي من شأنها تحديد هوية صاحب التوقيع وتمييزه عند استعماله لتقنيات الاتصال الحديثة.

---

[1] عمر هبطي، التوقيع الالكتروني، مذكرة لنيل دبلوم الدراسات العليا المعمقة، في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، كلية الحسن الثاني، الدار البيضاء، 2007/2006،ص49.

[2] سيد عبد القادر جهيدة، شكرون ساسية، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية دراسة تحليلية ومقارنة، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص شامل، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2015/2014، ص 61.

[3] سعيد السيد قنديل، المرجع السابق، ص55.

وقد أصدرت أجهزه الإتحاد الأوروبي تعليمات بشأن التوحيد الأوروبي للتوقعات الإلكترونية بتاريخ 14 يوليو 2003 وبموجب هذه التعليمات أنشات لجنة التوقيع الإلكتروني، التي تقوم بوضع تفاسير وتوصيات بشأن التوحيد القياسي لخدمات التصديق الإلكتروني، كل هذا في اطار إعطاء مصداقيه للتوقيع الإلكتروني[1].

الفرع الثاني حجية التوقيع الالكتروني في التشريعات الوطنية

أفردت بعض التشريعات المقارنة قوانين خاصة للتعاملات الالكترونية بعد دخول هذه الوسائل الحديثة كافة مجالات الحياة وأصبح من الضروريات وهو ما أدى بهذه الدول إلى الاعتراف بالتوقيع الالكتروني نصا في قوانينها.

تأتي حجية التوقيع الإلكتروني من خلال استيفائه للشروط اللازمة للاعتداد به كتوقيع كامل وذلك من خلال تحقيقه لدوره ووظيفته، فللتوقيع الإلكتروني أهمية بالغة في الإثبات، وبالتالي في حماية المتعاملين عبر الوسائط الإلكترونية.

أولاً: حجية التوقيع الالكتروني في الدول الغربية

1.حجية التوقيع الالكتروني في فرنسا

أصدر المشرع الفرنسي قانون التوقيع الالكتروني رقم 230 لعام 2000 في شكل تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متماشية مع تقنية المعلومات وازدياد استخدام التوقيع الالكتروني في التعاملات الالكترونية وقد تم ادراج هذا التعديل ضمن المادة 1316 من قانون التوقيع الالكتروني الفرنسي وقد ورد ضمن احكام هذا القانون ان التوقيع الالكتروني يدل

[1] هدار عبد الكريم، مبدأ الثبوت بالكتابة في ظل ظهور المحررات الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة الجزائر 01، 2014/2013، ص72.

على شخصية الموقع وتضمن علاقته بالواقعة المنسوبة اليه كما يؤكد صحة الواقعة المنسوبة اليها هذا التوقيع إلى أن يثبت العكس وقد اخفى المشرع الفرنسي على الكتابة الالكترونية والمحررات الالكترونية والتوقيع الالكتروني الحجية في الاثبات شأنها في ذلك شأن المحررات الخطية والتوقيع الخطي التقليدي[1].

2. حجية التوقيع الالكتروني في الولايات المتحدة الامريكية

تم اعتماد تشريع فيدرالي جديد بشأن التوقيع الالكتروني في التجارة الداخلية وذلك في أكتوبر 2000م، وقد قنن كذلك حفظ الوثائق الالكترونية التي تملكها الجهات الحكومية، وأورد العديد من الأحكام التي تكمل حماية خاصة للمستهلك في مثل هذه التعاملات.

وقد أصدرت بعض الولايات تشريعات محلية اعترفت من خلالها صراحة بالقيمة القانونية للتوقيع الالكتروني، حيث أصدرت تشريعاً تمنحه الحجية القانونية في التعاملات التي تتم بواسطته [2].

ثانيا: حجية التوقيع الالكتروني في الدول العربية

1. حجية التوقيع الالكتروني في القانون المصري

تنص المادة 14 من قانون التوقيع الالكتروني المصري على ما يلي " **التوقيع الالكتروني في نطاق المعاملات التجارية والمدنية والإدارية ذات الحجية المقررة للتوقيعات في احكام قانون الإثبات في المواد المدنية والتجارية إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا**

[1] منير محمد الحنيهي وممدوح محمد الحنيهي، التوقيع الإلكتروني وحجيته في الإثبات، بدون طبعة، دار الفكر الجامعي، الاسكندرية، 2004، ص 89 ـ90.

[2] فيصل سعيد الغريب، المرجع السابق، ص 256. ـ257.

القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون "، نستنتج من خلال هذه المادة أن المشرع المصري ساوى بين التوقيع الالكتروني والتوقيع التقليدي من حيث الحجية القانونية

إزاء اعترف المشرع المصري بحجية الإثبات للكتابة الالكترونية وللتوقيعات الالكترونية سواء كانت رسمية أم عرفية، فإن هذا يكمل المنظومة الالكترونية في جمهورية مصر العربية، ويصبح للتوقيع الالكتروني والمحررات الالكترونية ذات الحجية الموجودة في قانون الإثبات الشيء الذي يدعم استخدام التقنيات الحديثة والوسائل الالكترونية ويسهل استخدامها من قبل الأفراد والجهات الحكومية والخاصة ويعد خطوة هامة نحو تحقيق فكرة الحكومة الالكترونية E-GOVERNMENT في جمهورية مصر العربية.[1]

إن التوقيع الإلكتروني في ظل ضمانات معينة يمكنه أن يقوم بذات الدور الذي يؤديه التوقيع التقليدي، بل يرى البعض أن التوقيع التقليدي قد لا يجد له مكاناً في ظل المعالجة الإلكترونية للمعلومات، وبذلك يمكن الاعتماد على الرقم السري كوسيلة بديلة أو إضافية للتوقيع التقليدي، يمكنها أن تقوم بذات الدور التقليدي، فضلا عن ملاءمتها لنظم المعلوماتية[2].

2. حجية التوقيع الالكتروني في القانون الأردني

خطت المملكة الأردنية خطوة في اتجاه إطلاق التجارة الالكترونية ومشروع الحكومة الالكترونية بإصدارها القانون المؤقت للمعاملات الالكترونية الأردني الذي بدا العمل به متزامناً مع توقيع الأردن لاتفاقية التجارة الحرة مع الولايات المتحدة التي تضمن بنودا خاصة عند التجارة الالكترونية، وكذلك انضمام الأردن لمنظمة التجارة العالمية وتوقيعه على اتفاقية الشراكة الأردنية الأوروبية[3]، إذ تنص المادة

[1] ثروت عبد الحميد، التوقيع الإلكتروني، بدون طبعة، دار الجامعة الجديدة، الإسكندرية,2007، ص 191.

[2] حجازي عبد الفتاح بيومي، التوقيع الإلكتروني في النظم القانونية المقارنة، بدون طبعة، دار الفكر الجامعي، الاسكندرية ،2004، ص

[3] فيصل سعيد الغريب، المرجع السابق، ص 254

10الفقرة 1 من قانون المعاملات الالكتروني الأردني على ما يلي " **إذا استوجب تشريع نافذ توقيعا على المستند أو نص على اثر ترتيب اثر على خلوه من التوقيع فان التوقيع الالكتروني على السجل الالكتروني يفي بمتطلبات ذلك التشريع** "[1] .

نستنتج من نص هذه المادة أن المشرع الأردني أعطى للتوقيع الالكتروني حجية قانونية في الحالات التي يلزم فيها القانون الأطراف بالتوقيع في حين انه أغفل عن العديد من الحالات سكت عنها.

3. حجية التوقيع الالكتروني في القانون الجزائري

بعدما كان هناك قصور في تنظيم التشريعات المتعلقة بالتوقيع الالكتروني أو في اتخاذ التدابير اللازمة لتطبيقه، وهذا ما نجده في التشريع الجزائري في المرسوم التنفيذي 07. 162، الذي نظم نشاط التصديق الالكتروني من خلال اخضاعه للنظام الترخيص الوارد في المادة 39 من القانون 2000 . 03، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية[2]، علماً أن أول المشاريع تم اطلاقها في 2005 وأن الاطار القانوني المحدد للتوقيع الالكتروني اعتمد في 2007 إلا أنه حصد لسنوات عديدة وصدر القانون الجديد 2015 [3] يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني

حيث تنص المادة 76 منه على ما يلي " **يتعين على الهيئات التي تستعمل التوقيع والتصديق الالكترونيين عند تاريخ اصدار هذا القانون ان تطابق نشاطها مع مقتضيات هذا القانون حسب الكيفيات التي تحدها السلطة ووفق توجيهاتها** ".

---

[1] المادة 10 فقرة1 من قانون المعاملات الإلكترونية الأردني رقم 85 سنة2001، الجريدة الرسمية رقم 4524 الصادرة بتاريخ 03 ديسمبر 2001.

[2]المرسوم التنفيذي 07. 162، المؤرخ في 30 مايو 2007، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، ج.ر العدد 37، الصادرة بتاريخ 07 يونيو 2007.

[3] قانون 15ـ04 المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني.

نستنتج من خلال هذه المادة على الاهمية التي ولاها المشرع في هذا القانون للتوقيع الالكتروني والتصديق واستعمالها فيما يخوله هذا القانون وهو ما يدل على حجية التوقيع الالكتروني في الاثبات.

كما اعتمد المشرع الجزائري التوقيع الإلكتروني لأول مرة في نص المادة 2/327 من القانون المدني الجزائري بحيث اعترف بحجية التوقيع الإلكتروني في الإثبات لكنه لم يبين شروطه بل أحالها لشروط الكتابة وطبقا لنص هذه المادة التي تنص على" :يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 01 ".

ووفقاً لهذا النص يكون المشرع الجزائري قد ساوى في القوة الثبوتية ما بين التوقيع الإلكتروني والتوقيع العادي وهو ما يعرف بمبدأ التعادل الوظيفي بين التوقيع الإلكتروني والتوقيع التقليدي، وللإقرار به يستلزم أن تتوافر فيه الشروط المنصوص عليها في المادة 323 مكرر 1 من القانون المدني والمتمثلة في إمكانية التأكد من هوية مصدر التوقيع، وبأنه هو من انصرفت إرادته إلى إنشاء الالتزام بواسطة وسيلة التوقيع الإلكتروني بإرسال الرسالة إلى طالب المعاملة، وأن يكون معداً ومحفوظاً في ظروف تضمن سلامته،[1] وهي الشروط نفسها المتطلبة في التوقيع الإلكتروني المؤمن وفقاً لمضمون المادة 03 من المرسوم التنفيذي 162/07.

غير أن تحقيق هذين الشرطين يتوقف على تدخل طرف أو جهة ثالثة تتمثل في جهة وسيطة تصادق على هذا التوقيع، وتؤكد صدوره من الشخص المنسوب إليه، مع عدم إحداث أي تحريف أو تعديل فيه [2]،

ولهذا أصدر المشرع الجزائري قانون رقم 15ـ 04 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، والذي نجده قد ميز فيه بين نوعين من التوقيع الإلكتروني مثل نظيره الفرنسي

[1] مسعودي يوسف، أرجيلوس رحاب، مسعودي يوسف، أرجيلوس رحاب، مدى حجية التوقيع الإلكتروني في الإثبات في التشريع الجزائري (دراسة على ضوء أحكام قانون 04/15)، مجلة الاجتهادات للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست، الجزائر،2017، ص 93.

[2] لالوش راضية، المرجع السابق، ص 84.

التوقيع الموصوف والتوقيع البسيط، لكن هذا التمييز من الجانب الوظيفي فقط ومؤدى ذلك أنه لا يجوز إهدار قيمة التوقيع الإلكتروني البسيط في الإثبات لمجرد أنه لا تتوفر فيه شروط التوقيع الموصوف من خلال إنشائه عن طريق آلية غير آمنة ولا يحوز على شهادة تصديق إلكترونية[1].

حيث يختلف التوقيع الإلكتروني المؤمن عن التوقيع الإلكتروني البسيط في أن الأول يستخدم تكنولوجيا مصممة لتحقيق ترابط أكثر بين هوية الموقع وتوقيعه وهو ما يفتقده النوع الثاني، بما يضفي على التوقيع المؤمن نوعا من التصديق أو التوثيق الإلكتروني، وبالتالي منحه قدرة أكثر على الإثبات[2].

وأقر المشرع الجزائري بالتوقيع الإلكتروني الموصوف ومنحه الحجية القانونية ويظهر ذلك ضمن المادة 7 والتي نلاحظ من خلالها أنه قد تم وضع شروط إضافية مقارنة بنص المادة 1/232 من القانون المدني وهذه الشروط لابد من توافرها لإضفاء الحجية في التوقيع الإلكتروني، وعليه ليعتد بالتوقيع الإلكتروني في التشريع الجزائري فلابد من توافر تلك الشروط المنصوص عليها في المادة 7 سالفة الذكر لأن انعدامها يترتب عليه إسقاط صفة الحجية منها في الإثبات.[3]

أما النوع الثاني المتمثل في التوقيع الإلكتروني البسيط أو العادي والذي لا يحوز على الحجية القانونية الكاملة في الإثبات، وبالرغم من كونه بسيط إلا أنه لا يمكن تجاهله بل لابد من الأخذ به وذلك يعود لأحكام نص المادة 9 من القانون رقم 15ـ04، إذ أكدت على أنه لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أما القضاء بسبب شكله الإلكتروني أو أنه لا يعتمد على شهادة التصديق الإلكتروني الموصوفة أو أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني[4]،

---

[1] بودشيشة سمية، إثبات العقد الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2017/2016،ص66.

[2] محمد محمد سادات ، المرجع السابق، ص56 .

[3] مسعودي يوسف، أرجيلوس رحاب، المرجع السابق ص 94.

[4] منصور عز الدين، حجية التوقيع الإلكتروني في الإثبات، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016،2015، ص 58.

فالتوقيع الإلكتروني ثابت حتى وان جاء غير مستوفي لشروط التوقيع الموصوف، ففي حالة إنكار التوقيع الإلكتروني ممن نسب إليه يصبح عبء الإثبات على من يدعي أن هذا التوقيع صادر من خصمه وأنه يتوافر على جميع الشروط التي تجعله صحيحا[1].

نصت المادة 323 مكرر من القانون المدني على انه :" يعتبر **الإثبات في الشكل الإلكتروني كالإثبات بالكتابة على الورق**"...، وعليه فقد كرستا مبدأين واردين في القانون التوجيهي للأونيسترال يعرفان بمبدأ التعادل الوظيفي بين المحررات الإلكترونية والورقية، ومبدأ الحياد التقني بشأن التوقيع الإلكتروني؛ حيث يقصد بمبدأ هذا الأخير أنه لا يمكن للتشريعات أن تعتمد طريقة واحدة فيما يتعلق بالآليات والبرمجيات المتعلقة بالتوقيع الإلكتروني، بل لابد من فتح الباب وترك المجال مفتوح مع اشتراط الأمان فيها واثبات ذلك دون مفاضلة مسبقة[2].

وبذلك يكون المشرع الجزائري قد تبنى موقف معظم التشريعات الحديثة التي اعترفت بالتوقيع الإلكتروني والتي أشارت إلى طبيعة النظام المستخدم وإلى إجراءات التوثيق المعتمدة والتي بتوافرها يعد التوقيع الإلكتروني موثقا، ويعد دليلاً كاملاً قاطعاً في الإثبات.

[1] بودشيشة سمية، المرجع السابق، ص 67 ـ66.

[2] عبد الله أحمد عبد الله غرايبة، حجية التوقيع الإلكتروني في التشريع المعاصر، الطبعة الأولى، دار الراية للنشر، الأردن،2008، ص 123.

خلاصة الفصل الأول

لقد فرضت التجارة الالكترونية تغيير التعامل في التوقيع من الورقي الى الإلكتروني، ظهر التوقيع الالكتروني كألية بديلة للتوقيع الكتابي، ليمارس في نطاق التبادل التجاري والاقتصادي لكن بالرغم من التقدم التكنولوجي في هذا المجال ،التوقيع الالكتروني لم يسلم من الاختراقات الامنية والمخاطر التي سوف تؤثر على سلامة وسرية معاملتهم الالكترونية، هذا ما حفز المشرع الجزائري اعتماد حماية تقنية وقانونية له.

وقد تمخض عن التطور التكنولوجي والرقمنة معاملات وعقود قانونية جديدة، تتم عن طريق الأجهزة الالكترونية ولا تتطلب حضور الأطراف أثناء انعقاد العقد، ونظرا لخطورة هذا النوع من التصرفات، خاصة تلك المتعلقة بالجانب المالي، كان لزاما توفر الضمانات الكفيلة بإزالة هذه العوائق، والتوقيع الالكتروني يعد أحد أهم الضمانات المصاحبة للمعاملات الالكترونية، التي لا يتأتى إسنادها لأصحابها وتحديد هوياتهم إلا عن طريقه.

نخلص مما سبق وبما أن التوقيع الإلكتروني أثبت قدرته على أداء مهام التوقيع الكتابي التقليدي، فلا بد من دعوة المشرع لاعتماد هذا التوقيع الإلكتروني، ومنحه القوة الثبوتية أمام المحاكم، والجهات الحكومية، ولا بد من منح المستندات الإلكترونية القوة الممنوحة للمستندات الورقية التقليدية، إذْ أصبح هذا واقعًا لا مفر منه في ظل التطورات الحالية في المعاملات التجارية الدولية عبر شبكة الإنترنت، وهذا ما جعل الاعتراف بالتوقيع الإلكتروني والمستندات الإلكترونية مسألة ضرورية بما يمكن الأطراف المتعاقدة من تقديم المستندات بعد استخراجها من الحاسب الآلي وتوقيعها إلكترونيا، وعدها أدلة للإثبات تقدم إلى الجهات القضائية[1].

[1] حسن يحي يوسف فلاح، التنظيم القانوني للعقود الالكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص، جامعة النجاح الوطنية ،نابلس، فلسطين، 2007، ص94. 95.

الفَصْلُ الثَّاني

آليات الحماية الجنائية للتوقيع الالكتروني

الفصل الثاني

آليات الحماية الجنائية للتوقيع الالكتروني

ترتب عن اعتماد الأنترنت في ابرام عقود التجارة الإلكترونية زيادة الطلب على أنظمة التشفير من أجل حمايتها من مخاطر القرصنة ويتم ذلك عادة باستخدام برامج خاصة لهذه الانتهاكات الأمر الذي يعرض المتعاقدين عبر شبكة الأنترنت إلى أخطار عديدة كإفشاء أسرار هامة مثل الاطلاع على بيانات شخصية أو اختلاسها وهذا يؤدي إلى إلغاء عنصر الثقة والائتمان في هذه المعاملات وللقضاء على هذه المخاطر ومواجهتها تم استخدام تقنية التشفير كإحدى وسائل حماية سلامة وسرية المعلومات المرسلة عبر شبكة الانترنت وايجاد ضمانات كفيلة بإرساء الأمن القانوني من قبل جهات اخرى محايدة مثل جهة التصديق الالكتروني .

يعتبر التوقيع الالكتروني العنصر الرئيسي الذي تقوم عليها اجراءات التجارة الإلكترونية كونه مرتبط بتوثيق التصرفات القانونية الإلكترونية وتحديد هوية المرسل والمستقبل والتأكد من صحة البيانات وسيلة مدنية لحماية معاملات التجارة الإلكترونية ازاء هذه الأهمية بات من الضروري وجود حماية جنائية له ضد كل تصرف يهدده بالاعتداء أو الضرر فإن أي اعتداء على التوقيع الإلكتروني يمثل اعتداء على مضمون التجارة الإلكترونية عموما وعلى كل جهة تستخدم التوقيع الإلكتروني للتوثيق واثبات الهوية سواء كانت عامة أو خاصة هذا ويعد من أكثر الجرائم تهديدا للتوقيع الإلكتروني جريمة تزوير التوقيع الالكتروني وقد عالجت ذلك التشريعات والقوانين الجزائرية.

لبيان أهمية هذه النقاط سنتطرق سوف نتطرق لدراسة موضوع الحماية التقنية والوقائية للتوقيع الإلكتروني المبحث الاول ثم نتناول موضوع جرائم الاعتداء على التوقيع الإلكتروني في المبحث الثاني

المبحث الأول: الحماية التقنية والوقائية للتوقيع الالكتروني

غياب العلاقة المباشرة بين الأطراف في التصرفات الإلكترونية خاصة التي تتم عبر شبكة الأنترنت، تطلبت توفر عنصر الثقة والأمان في هذه التصرفات، خاصة فيما يتعلق بالتوقيعات الإلكترونية للأطراف المتعاقدة، ولهذا كان من الضروري إيجاد وسائل تقنية لحماية هذا التوقيع من أي مخاطر قد يتعرض إليها من جهة، ولبث الثقة والأمان في التصرفات التي تتم عبر الوسائط الإلكترونية من جهة أخرى[1]، ومن أهم هذه الوسائل تقنية التشفير والتي سنتناولها في المطلب الأول والتصديق الإلكتروني كمطلب ثان.

المطلب الأول: تقنية التشفير كآلية تقنية لحماية التوقيع الالكتروني

التشفير في حقيقته عملية تمويه الرسائل والمعلومات أو البيانات بشكل لا تقرأ من أحد سوى من الموجهة إليه، ويتعين نزع التشفير عن المعلومات قبل قراءتها من المرسل إليه، فالتشفير نظام آمن يوفر الحماية والخصوصية والسرية للمعلومات المتبادلة في التعاقدات والمعاملات الإلكترونية[2]، ويقتضي ذلك التطرق إلى تعريف التشفير في الفرع الأول ثم بيان طرقه في الفرع الثاني.

الفرع الأول: تعريف التشفير

[1] خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، بدون طبعة، دار الجامعة الجديدة، الإسكندرية,2007، ص100ـ103.

[2] عبان عميروش، النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري والتشريعات المقارنة، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد07، العدد 01، جامعة عبد الحميد بن باديس مستغانم، الجزائر,2022، ص 1236.

يعرف نظام التشفير بانه تقنية قوامها خوارزمية رياضية ذكية تسمح لمن يمتلك مفتاحا سريا بان يحول سند الكتروني مقروء إلى سند الكتروني غير مقروء، وبالعكس فانه يسمح لمن يمتلك المفتاح السري ان يستخدم نظام التشفير لفك الشفرة وإعادة السند المشفر إلى وضعه الأصلي[1]

أولاً: التعريف القانوني للتشفير في الدول الغربية

يعتبر نظام التشفير أكثر تقدما في الدول الغربية حيث أصبحت جل المعاملات اليومية في هذه الدول تتم عبر الوسائل الالكترونية وبالتالي اعتماد نظام التشفير لاستيفاء السرية عليها.

1. في القانون الفرنسي

تم صدور اول مرسوم فرنسي بشان التعامل بتقنية التشفير بتاريخ 18افريل 1939 الذي يليه صدور التعديل له بالمرسم الصادر في 18 أفريل 1982،ثم صدر القانون الفرنسي رقم 9/1170 بتاريخ 29 ديسمبر 1990حيث نصت المادة منه على تعريف التشفير بقولها (كل الاعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة باستخدام وسائل مادية أو معالجة الية إلى معلومات أو إشا رات .غامضة للغير ،أو إلى اجراء العملية العسكرية عبر وسائل مادية ا معلوماتية مخصصة لهذا الغرض[2]، بحيث سمح هذا القانون للمشروعات الصغيرة والافراد باستخدام نظام التشفير بعد ما كان مقصورا على المجلات العسكرية و الحكومية فقط.

كما أنه وبموجب القانون الفرنسي رقم 616 بتاريخ 2001/07/11 أدخلت تعديلات على المادة 28 من قانون تنظيم الاتصالات الفرنسي لسنة 1990تجيز تصدير وسائل التشفير التي تؤمن وظيفة السرية لرسالة المعلوماتية، وهذا التعديل التشريعي كان بناءا على توصيات البرلمان الأوروبي

[1] يوسف احمد النوافلة، الاثبات الالكتروني في المواد المدنية والمصرفية دراسة مقارنة، المرجع السابق، ص110.

[2] سمير حامد عبد العزيز الجمال, التعاقد عبر تقنيات الاتصال الحديثة , بدون طبعة, دار النهضة العربية,القاهرة,مصر,2006,ص19.

بتاريخ 2000/06/22 التي ترمي إلى الغاء القيود القائمة على تبادل تقنيات ومنتجات التشفير بين دول أوروبية الاعفاء.[1]

2. في المملكة المتحدة

عام 2002 صدر قانون جديد للحكم في الصادرات لكي يحل محل قانون الاستيراد والتصدير وسلطات الجمارك لعام 1939 الذي نظم إجراءات الحصول على رخص لتصدير المنتجات المشفرة والبرمجيات من المملكة المتحدة.

كما ان هناك تكنولوجيات أخرى استثناها الملحق رقم 1وهي البطاقات الشخصية الذكية ومعدات البث الإذاعي أو التلفزيوني والذي يتضمن تكنولوجيا فك الشفرة للصوتيات والمرئيات[2]

ثانيا: التعريف القانوني للتشفير في البلدان العربية

1. في القانون التونسي

عرف المشرع التونسي التشفير في نصه القانوني في الفصل الثاني من الباب الأول من القانون رقم 83 سنة 2000 في شأن المبادلات والتجارة الالكترونية[3]، حيث نص على أن التشفير هو «**استعمال رمز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو ارسالها**

[1] ترجمان نسيمة, الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة, رسالة لنيل شهادة الدكتوراه طور الثالث في التجريم في قانون الأعمال, جامعة ابن خلدون, تيارت, الجزائر, 2020, ص48.

[2] سمير حامد عبد العزيز الجمال, المرجع السابق, ص 56.

3- القانون رقم 83 سنة 2000، المؤرخ في 09 أوت 2000، يتعلق المبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية، العدد 64، الصادر بتاريخ 11 أوت 2000،

غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها"[1]

كما نص أيضا في الفصل 48 من القانون رقم 2000/83 في حالة الاعتداء على البيانات المشفرة على أنه: "**يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية المتعلقة بإمضاء غيره بالسجن لمدة تتراوح بين ستة أشهر وعامين وغرامة تتراوح بين 1000و10000دينارا أو بإحدى العقوبتين**" .

2. في القانون الجزائري

نص المشرع الجزائري في القانون رقم 04/15 المتعلق بقواعد العامة للتوقيع الالكتروني، في الفقرة الخامسة فقد اعتمد بان التشفير من بيانات التحقيق من التوقيع لم يأتي بتعريف واضح للتشفير بل اعتبره من بيانات انشاء التوقيع الالكتروني وهذا من خلال نص المادة 02 من الفصل الثاني للفقرة 3 من القانون سالف الذكر [2]

فالملاحظ أن المشرع الجزائري لم يتناول تعريف التشفير سواء في قانون التوقيع والتصديق الالكترونيين 04/15 ولا في المرسومين التنفيذيين 134/16 و135/16 واكتفى بتعريف المفتاح الشفري وهو أحد طرق التشفير في الفقرة 08 والفقرة 09 من المادة الثانية من القانون 04/15 السالف الذكر. حيث عرفت الفقرة 08و الفقرة 09 من المادة الثانية مفتاح التشفير على التوالي:

ا. مفتاح التشفير الخاص: هو عبارة عن سلسلة من الاعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

[1] ترجمان نسيمة, المرجع السابق, ص49.

[2] القانون رقم 15 -04, يحدد القواعد العامة المتعلقة بالتوقيع الالكتروني، السالف الذكر.

ب ـ مفتاح التشفير العمومي: هو عبارة عن سلسلة من الاعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الامضاء الالكتروني وتدرج في شهادة التصديق الالكتروني[1].

ثالثا: التعريف الفقهي للتشفير

يقول الأستاذ "بوير "ان أكثر وسائل امن المعلومات فعلية هي التشفير ويعرفه على النحو التالي "تشفير المعلومات هو تغيير مظهرها بحيث يختفي مظهرها الحقيقي بحيث تكون غير مفهومة، حيث يستطيع خبراء امن المعلومات منع الأشخاص غير المرخص لهم من الاطلاع على هذه البيانات وبذلك يحقق التشفير سرية البيانات، كتشفير ارقام بطاقات الدفع أو غيرها من البيانات.

وعرفه أيضا بانه "تقنية قوامها خوارزمية رياضية ذكية تسمح لمن يمتلك مفتاحا سريا بان يحول رسالة مقروءة إلى رسالة غير مقروءة وبالعكس، أي ان يستخدم المفتاح السري لفك الشفرة وإعادة الرسالة المشفرة إلى وضعها الأصلي.

وقد عرفه "ليونال بوشرباغ lionel bchurberg"بانه مجموعة من التقنيات التي تهدف إلى حماية المعلومات بفضل استعمال بروتوكولات سرية، تجعل البيانات مشفرة غير مفهومة لدى الغير بواسطة البرامج المخصصة لذلك.

رغم تعدد التعريفات الفقهية والتشريعية الا انها تصب في تعريف واحد المتمثل في ان التشفير " فرع من فروع الرياضيات يعنى بعملية تحويل البيانات هيئة واضحة مقروءة إلى هيئة رموز أو إشارات غير مقروءة تبدو غير ذي معنى، بحيث لا يمكن فهمها ولا قراءتها الا بواسطة مفاتيح فك التشفير ".

2. أهداف التشفير

استعمل التشفير في حماية وامن وسرية المعلومات والعقود المتبادلة عن بعد في شبكة الانترنت فحسب ،وانما يقوم فضلا عن ذلك بوظائف أخرى منها التحقق من هوية مطلق الرسائل والمصادقة

[1] عبان عميروش، المرجع السابق، ص1237.

على مضمونها و على توقيع أصحابها الكترونيا عليها ،والتأكد من سلامتها فهو يوفر حماية خاصة لغرض بث الثقة والأمان بين المتعاملين.

1. سرية البيانات

يكمن الهدف الأول من عملية التشفير في الحفاظ على سرية المعلومات وخصوصيتها، وذلك با الاحتفاظ بالمعلومات في صيغة مخفية عن أي شخص اخر غير الشخص المقصود، وهذا ما يوفر الثقة والأمان في التعاملات الالكترونية، عن طريق منع الغير من مستخدمي الشبكة من الدخول للبيانات والحفاظ على سريتها باستخدام وسائل الكترونية أو رموز معينة لا يعلمها إلا أطراف التعامل الالكتروني، وذلك باستخدام أدوات ووسائل تحويل المعلومات بهدف إخفاء محتوياتها بما لا يتيح استخدامها بطريقة غير مشروعة.

2. سلامة البيانات

ان سلامة البيانات هي وظيفة موجهة لأغراض احتواء التغيرات غير المسموح بها للبيانات من قبل الأشخاص غير المرخص لهم، وبذلك فالتشفير يحمي البيانات من وصولها مشوهة إلى الطرف الاخر، دون أي خلل أو اعتداء من الغير عليها.[1]

3. عدم الانكار

بعد التشفير بوجه عام وتطبيقاته الكثيرة، الوسيلة الوحيدة تقريبا لضمان عدم انكار التصرفات عبر الشبكات الالكترونية، وبذلك فان التشفير يمثل الاستراتيجية الشمولية لتحقيق اداف الامن من جهة وهو مكون رئيسي لتقنيات ووسائل الامن الأخرى.[1]

[1] عبان عميروش, المرجع السابق, ص06.

فنستنتج من خلال الأهداف المذكورة ان التشفير يهدف إلى تحقيق مبادئ الثقة والمصداقية والأمان وتكامل البيانات واثبات شخصية مصدر البيانات وعدم انكار ما تم اتخاذه من اعمال مسبقة

الفرع الثاني طرق نظام التشفير

يتمثل التشفير من الناحية الفنية في إعادة كتابة رسالة البيانات قبل تصديرها باستخدام رمز أو مفتاح معين، يفرض الربط بين البيانات والأرقام على ان تتوفر لدى المرسل اليه القدرة على استعادة الرسالة في صورتها الاصلية قبل تشفيرها.

أولاً: التشفير المتماثل (المفتاح السري الخاص)

وهو التشفير الذي يعتمد فيه غالبا على (شفرة القيصر) التي تقوم على أساس استبدال النص بأحرف تقابله وهذا من حلال المرور بعدة مراحل للوصول إلى النص المشفر، ويستخدم فيه صاحب الرسالة المفتاح نفسه لإنشاء التوقيع ولفكه بعد الاتفاق المسبق مع المرسل اليه على كلمة السر بينهما ويتضمن المفتاح الذي تم إنشاؤه للمرور حروف كبيرة وحروف صغيرة ورموز أخرى.[2]

فهي أنظمة تستخدم نفس المفتاح في عملية التشفير وفك التشفير، بحيث يستخدمه المرسل و المستقبل بدون كشف المفتاح إلى أي طرف اخر لذلك يتم تسمية هذا النظام بالنظام المتماثل للتشفير

.ثانيا: التشفير اللامتماثل

استخدم التشفير المتماثل مرات عدة ومع عدم نجاحه تم اللجوء إلى البحث عن بديل يحل محله ويحقق الغاية المطلوبة منه على اكمل وجه، ومن خلال البحوث تم التوصل إلى نوع جديد من التشفير

---

[1] درار نسيمة, الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني, دراسة مقارنة , رسالة لنيل شهادة الدكتوراه في القانون الخاص, جامعة أبو بكر بلقايد, تلمسان, الجزائر, 2015, ص139 .

[2] حسينة عبد الحميد شرون, صونيا مقري ,دور التشفير وشهادات المصادقة الالكترونية في حماية الدفع الالكتروني ,مجلة البحوث والدراسات القانونية والسياسية, المجلد 11,العدد 02, جامعة على لونيسي، البليدة 02، الجزائر, ص 131.

الا وهو التشفير اللامتماثل حيث اكتشفت هذه الطريقة في الولايات المتحدة الامريكية عام 1978ثلاثة علماء في الرياضيات وهم shamiand edeman،rivest على عكس التشفير المتماثل الذي يستخدم مفتاح واحد على غرار التشفير اللامتماثل الذي يستعمل مفتاحين اثنين تربط بينهما علاقة رياضية وطيدة ويطلق على هذان المفتاحان بالمفتاح العام public Kay والمفتاح الخاص .peivatkey

ويكون المفتاح الخاص معروفا لدى جهة واحدة فقط أوشخص واحد فقط وهو المرسل ،بحيث يكون المفتاح الأول خصوصي يعرفه مستخدم معين لشبكة الانترنت ويبقيه سريا و خاصا به والمفتاح الثاني عمومي يوزعه ويبلغه إلى المستخدمين الاخرين الذين يود وصول سندات الكترونية مشفرة منهم ،وعلى هذا الأساس فانه بإمكان جميع الأشخاص الحائزين على المفتاح العمومي استخدامه في تشفير السندات وارسالها إلى المستخدم الحائز على المفتاح الخصوص [1]

وفي المقابل فان المستخدم الحائز على المفتاح الخصوص بإمكانه وحده ان يفك تشفير السندات الواردة اليه من المستخدمين الاخرين الحائزين على المفتاح العمومي.[2]

وبالرغم اذ ان كل مزايا عملية وقانونية يمنحها هذا النظام اللامتماثل بالمفتاح العمومي اذ ان كل مستخدم لشبكة الانترنت لا يستخدم سوى مفتاح أورمز سري واحد في تشفير السندات التي يرغب بإرسالها أوفي فك تشفير السند الذي تلقاه، فان هاك صعوبات تواجه هذا النوع من التشفير، والتي تكمن في مدى ضمان المفتاح العمومي لاستخدامه من قبل الحائز على المفتاح الخاص والتي تتدارك بتدخل جهة تقنية حيادية وهي الكاتب العدل الالكتروني.[3]

[1] ترجمان نسيمة، الحماية الجنائية للتوقيع الإلكتروني: دراسة مقارنة، رسالة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون الأعمال، جامعة ابن خلدون، تيارت، 2021 ، ص54.

[2] عبد العزيز سمية, التوقيع الالكتروني وسيلة حديثة للإثبات, دراسة مقارنة, مجلة معارف، العدد17, جامعة اكلي محند اولحاج, البويرة, 2014, ص 204.

[3] حسينة عبد الحميد شرون و صونيا مقري, المرجع السابق, ص 131.

ثالثاً: التشفير المزدوج

يُعَدُ نظاماً خليطاً بين النظام المتماثل والنظام الغير اللامتماثل وفيه يتم تشفير الرسالة بمفتاح خاص ثم تشفير المفتاح الخاص بمفتاح عام وارسال كل من الرسالة المشفرة والمفتاح الخاص المشفر إلى المرسل اليه باستخدام شبكة الاتصالات.

ولقد أقر المشرع الجزائري من خلال نص المادة 8/02 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين، بنظام التشفير المزدوج من خلال نصه على مفتاح التشفير الخاص والتشفير العمومي

وتقوم طريقة التشفير المزدوج على الخطوات الاتية:

- تشفير الرسالة الاصلية المبعوثة من المرسل إلى المرسل اليه بالمفتاح الخاص.
- يشفر المفتاح المتماثل أيضا عن طريق المفتاح العام للمرسل اليه ثم يتم بعث الرسالة المشفرة.
- بعد تلقي المفتاح المتماثل بالمفتاح العام الذي يملكه المرسل عليه يعمل بفك شفرة المفتاح المتماثل المشفر باستعمال المفتاح الخاص ومنه يمتلك المفتاح المتماثل الذي تم استخدامه والذي شفرت به الرسالة الاصلية.
- وأخيرا يعمل المرسل اليه بعد فك شفرة المفتاح المتماثل باستعمال هذا الاخير في فك الرسالة المشفرة.[1]

المطلب الثاني: التصديق الإلكتروني كألية لحماية التوقيع الالكتروني

إن الثقة والأمان لدى أطراف العقد الالكتروني من أهم الأمور التي يجب توافرها في العقود الالكترونية، وذلك نظراً لما تمتاز به هذه العقود من عدم الالتقاء الفعلي بين اطراف التعاقد ،ولكي تتوافر هذه الثقة بين اطراف العقد فان الامر يستلزم وجود طرف ثالث محايد يعمل على التحقق من

[1]مرابط حمزة وداودي منصور، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية، مجلة الحقوق والعلوم السياسية ،المجلد 10، العدد01، جامعة تيارت ابن خلدون ، الجزائر، 2023، ص42.

صحة التوقيع الالكتروني ونسبته إلى الموقع واعطاءه القوة الثبوتية، فمن هنا اطلق المشرع الجزائري على هذه الجهة المختصة بالتصديق على التوقيع الالكتروني طبقا للفقرة 02 من المادة 12 من القانون رقم 04/15 المتعلق بالتوقيع والتصديق الالكتروني.

حيث أنه وتدعيما لمصداقية التجارة الالكترونية وتوفير الثقة و الأمان بين المتعاملين بالوسائط الالكترونية، استحدث المشرع آليات تتولى عملية حماية البيانات والمعلومات المتبادلة إلكترونيا، خاصة في ظل تفشي وباء كورونا، واتخاذ الدول لإجراءات احترازية كالتباعد الجسدي والحجر المنزلي بغية الحد من انتشار المرض. الأمر الذي دفع بالمستهلك والتاجر إلى اللجوء إلى فضاء افتراضي للشراء والبيع، والذي استدعى وجود طرف ثالث موثوق ومحايد، يسمى بمؤدبي خدمات التصديق الالكتروني، يقوم بإصدار شهادة الكترونية تؤكد شخصية المرسل والتحقق من صحة التوقيع الالكتروني، هذا ما يبرر أهمية دراسة آلية التصديق الالكتروني وبيان دورها في ضمان العقود التجارية الالكترونية وحماية المستهلك الالكتروني

الفرع الأول: تعريف نظام التصديق الالكتروني

يعتبر التصديق الالكتروني مصطلح حديث النشأة في مجالات المعاملة الالكترونية حيث ظهر تزامنا مع انتشار وكثرة استخدام مختلف التقنيات التكنولوجية الحديثة التي ساهمت بشكل كبير في تجريد مختلف التصرفات والمعاملات (القانونية –تجارية–مصرفية) من طابعها المادي إلى دعامات الكترونية معترف بها.

ومن أجل مسايرة مستجدات الثرة الرقمية والتطورات التي عرفها الاقتصاد الرقمي تدل المشرع الجزائري ونظم شهادة التصديق الإلكتروني لما لها دور فعال في إبرام التصرفات عبر الوسائط الالكترونية خاصة في مجال الاثبات، حيث قام المشرع الجزائري منذ 2005 بتعديل أحكام الاثبات الواردة في المواد 323 مكرر و323 مكرر1 من القانون المدني، التي تحدثت عن الكتابة الالكترونية من حيث

قيمتها القانونية في الإثبات، وبعد ذلك صدر القانون 04/15 المؤرخ في 1فيفري 2015 الذي حدد القواعد العامة بالتوقيع والتصديق الالكترونيين[1]

أولاً: تعريف القانوني جهة التصديق الالكتروني

يمكن تعريف التصديق الالكتروني على أنه: "وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر الالكتروني، حيث يتم نسبته إلى شخص أو كيان معين عبر جهة موثوق بها أو طرف محايد يطلق عليه اسم مقدم خدمات التصديق أو التوثيق الالكترونيين"

ويقصد به أيضا "التحقق من أن التوقيع الالكتروني قد تم تنفيذه من شخص معين، باستخدام وسائل التحليل للتعرف على الرموز والكلمات والأرقام، وفك التشفير والاستعارة العكسية وآية وسيلة أو إجراءات أخرى تحقق الغرض المطلوب "[2]

يطلق كذلك على جهات التصديق الالكتروني لدى مختلف التشريعات تسمية "مقدم خدمات التصديق الالكتروني "أو" مؤدي خدمات التصديق الإلكتروني"، بحيث عرفها المشرع الجزائري مؤدي خدمات التصديق الالكتروني في المادة 3 من الفقرة 11من المرسوم التنفيذي رقم 2000- 03، يسلم شهادات الكترونية أو يقدم خدمات أخرى في مجال التوقيع الالكتروني [3]

[1] سديري نجوى، الحماية القانونية للتوقيع الالكتروني كآلية لتدعيم الثقة في المعاملات الالكترونية عبر الانترنت، مجلة الدراسات القانونية جامعة الجزائر1، يوسف بن خدة، المجلد 08، العدد 02 ، ، 2022، ص 346-347.

[2] فطيمة الزهراء مصدق، التصديق الالكتروني كوسيلة لحماية التوقيع الالكتروني، مجلة الدراسات والبحوث القانونية، المجلد 05، العدد01، ،جامعة محمد بوضياف، المسيلة، 2020، ص38.

[3] هشام كلو، التنظيم القانوني للتوقيع الالكتروني في القانون الجزائري، مجلة الباحث للدراسات الاكاديمية، جامعة الحاج لخضر، باتنة 01، المجلد 10، العدد01، 2023 ،ص 496 .

فالمشرع الجزائري قد عرف مؤدي خدمات التصديق الالكتروني في نص المادة 02 فقرة 12 من القانون السالف الذكر بقوله "هي شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكترونية موصوفة وقد يقدم خدمات أخرى في مجال التصديق الالكتروني".[1]

وبالرجوع إلى نص المادة 28 من القانون رقم 04/15 الطرف الثالث الموثوق يقدم خدماته تحت رقابة السلطة الحكومية للتصديق الالكتروني التي عرفتها نص المادة 2 من المرسوم التنفيذي 135/16 "**على أنها سلطة إدارية تتمتع بالاستقلال المالي والشخصية المعنوية، واعتبار أن المحرر الرسمي هو كل ما يثبت فيه موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة، ما تم لديه أو ما تلقاه من ذوي الشأن**"[2].

من خلال التعاريف السابقة والخاصة بجهات التصديق الالكتروني يمكن القول أن جهات التصديق الالكتروني قد تكون شخص طبيعياً أو معنوياً، يقوم بإصدار ومنح شهادات تضفي من خلالها للتوقيع الالكتروني الثقة والأمان.

2-التعريفات الفقهية لجهات التصديق الالكتروني

:"البعض عرف جهات التصديق الالكتروني بأنها: شركات أو أفراد أو جهات مستقلة ومحايدة تقوم بدور الوسيط بين المتعاملين لتوثيق معاملاتهم الالكترونية فتعد طرف ثالث محايدا".[3]

وعرفت كذلك جهة التصديق الالكتروني بأنها جهة أو منظمة عامة كانت أو خاصة مستقلة أو محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق معاملاتهم الالكترونية، وذلك بإصدار شهادات التصديق اللازمة لهم.[4]

---

[1] هشام كلو، المرجع نفسه، ص497.

[2] المرسوم التنفيذي رقم 135/16، المؤرخ في 17 رجب1437 الموافق ل 25 ابريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها. ج.ر العدد 26، الصادرة بتاريخ 28 أفريل 2016.

[3] خالد ممدوح إبراهيم ، ابرام العقد الالكتروني (دراسة مقارنة)، ط1، دار الفكر الجامعي الإسكندرية، 2008، ص63.

[4] ايمان مأمون احمد سليمان، المرجع السابق، ص 390.

كما عرفها البعض بأنها: هيئة عامة أو خاصة تعمل على ملء الحاجة إلى وجود طرف ثالث موثوق في التجارة الالكترونية، بإصدار شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الالكتروني ، بتأكيد نسبة التوقيع الالكتروني إلى شخص معين ، وتأكيد نسبة المفتاح العام المستخدم إلى صاحبه.[1]

فجهات التصديق الالكتروني لا يمكنها القيام بخدمة التصديق الإلكتروني وإصدار شهادات التصديق الالكتروني[2]، وأداء مهامها الا بناءا على ترخيص من الجهة المختصة، والذي قد عرفه المشرع الجزائري في نص المادة 02 فقرة 10 من القانون15 /04، يعني نظام استغلال خدمات التصديق الالكتروني الذي يتجسد في الوثيقة الرسمية الممنوحة لمؤدي الخدمات بطريقة شخصية تسمح له بالبدء الفعلي في توفير خدماته.

بالإضافة إلى أن السلطة المختصة التي تمنح الترخيص لممارسة خدمات التصديق الالكتروني في الجزائر هي السلطة الاقتصادية للتصديق وهذا حسب ما جاء به في نص المادة 33 من القانون 04/15 "**يخضع نشاط تأدية خدمات التصديق الالكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الالكتروني**"

فمن خلال ما جاء في نص المادة 33 السابقة الذكر نستنتج أن نشاط تأدية تصديق خدمات التصديق الالكتروني تخضع إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الالكتروني، وهذا ما أقرته المادة 1 من المرسوم التنفيذي رقم 16-134 على ما يلي تطبيق الاحكام المادة 20 من القانون 04/15 يهدف هذا المرسوم إلى تحديد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها.

[1] علاء محمد عبد النصيرات، حجية التوقيع الالكتروني في الاثبات (دراسة مقارنة)، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص 145.

[2] عزولة طيموش، علاوات فريدة، التوقيع الالكتروني في ظل القانون رقم04/15، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص الشامل، جامعة عبد الرحمان ميرة، بجاية، 2015 ، ص 40.

حيث عرفت السلطة الوطنية للتصديق الالكتروني في المادة 2 من نفس القانون بقولها "يحدد مقر السلطة الوطنية للتصديق الالكتروني بمدينة الجزائر، ويمكن نقله إلى أي مكان اخر من التراب الوطني حسب الاشكال نفسها، كما توضح المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني تحت سلطة مديرها العام وهذا ما اشارت اليه المادة 3 من نفس القانون[1]

2- مهام جهة التصديق الالكتروني

من أبرز المهام الملقاة على عاتق التصديق الالكتروني والتي تم التطرق إليها المشرع الجزائري في نص المادة 30 من القانون رقم 04/15 والتي نصت على ما يلي: تكلف السلطة الاقتصادية للتصديق الالكتروني بمتابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذين يقدمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور.

وفي هذا الإطار تتولى المهام الآتية[2]:

- اعداد سياستها للتصديق الالكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها
- منح التراخيص لمؤدي خدمات التصديق الالكتروني بعد موافقة السلطة.
- الموافقة على سياسات التصديق الصادرة عن مؤدي خدمات التصديق الالكتروني والسهر على تطبيقها
- الاحتفاظ بشهادات التصديق الالكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من طرف مؤديي خدمات التصديق الالكتروني بغرض تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء طبقا للأحكام التشريعية والتنظيمية المعمول بها
- نشر شهادة التصديق الالكتروني للمفتاح العمومي للسلطة.

[1] المرسوم التنفيذي رقم 16-134،المؤرخ في 25 ابريل سنة 2016، تحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها، ج،ر،ج،ج، العدد 26، الصادر بتاريخ 28 أفريل 2016.

[2] قانون رقم 04/15، المؤرخ في 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر، العدد 06، الصادرة بتاريخ 10 فبراير 2015.

- اتخاذ التدابير اللازمة لضمان استمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الالكتروني عن تقديم خدماته.
- ارسال كل المعلومات المتعلقة بنشاط التصديق الالكتروني إلى السلطة دوريا أوبناء على طلب منها.
- التحقق من مطابقة طالبي التراخيص مع سياسية التصديق الالكتروني بنفسها أوعن طريق مكاتب تدقيق معتمدة.
- السهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية أو استعادة المنافسة بين مؤديي خدمات التصديق الالكتروني.
- التحكيم في النزاعات القائمة بين مؤديي خدمات التصديق الالكتروني فيما بينهم او مع المستعملين طبقا للتشريع المعمول به.
- مطالبة مؤديي خدمات التصديق الالكتروني أوكل شخص معني باي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها بموجب هذا القانون.
- اعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني وعرضه على السلطة للموافقة عليه.
- اجراء كل مراقبة طبقا لسياسة التصديق الالكتروني ودفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني
- اصدار التقارير والاحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطاتها مع احترام مبدا السرية

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

من خلال تطرقنا لنص المادة 30 من القانون 04/15 يتبين لنا أن السلطة الاقتصادية للتصديق الالكتروني هي سلطة ضبط تعنى على تنظيم عمليات التصديق الالكتروني بالقيام بإعداد سياستها، وكذلك القيام بإجراءات إدارية وتدابير وقائية من أجل ضمان استمرارية نشاطها بشكل محكم.

الفرع الثاني: دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع

تعتبر مرحلة التصديق على التوقيع الإلكتروني أهم المراحل في إبرام المعاملات الإلكترونية بمختلف أنواعها، وذلك لما لهذه المرحلة من دور بارز في انعقاد العقد والتأكد من صحة ما ورد به من بيانات، وكذا التحقق من صحة التوقيع الوارد عليه ونسبه إلى موقعه، وهذا ما نص عليه المشرع الجزائري في المادة 28 من قانون 18-05 المتعلق بتنظيم التجارة الإلكترونية والتي كان مضمونها الإشارة إلى وجوب تأمين مواقع التجارة عبر الأنترنت بنظام التصديق الإلكتروني.

وتتم هذه المرحلة بتدخل طرف ثالث محايد يعرف بجهة التصديق والتي هي عبارة عن هيئة أو جهة معينة تقوم بإصدار شهادات تسمى بشهادات التصديق الإلكتروني. نظرا لأهمية هذه المرحلة فقد سنت العديد من الدول تشريعات قانونية تناولت القواعد العامة المتعلقة به وتحديد الجهات المكلفة بالقيام بهذه المهمة وبيان التزاماتها ومسؤولياتها وهذا ما قام به المشرع الجزائري أيضا من خلال قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

أولاً: تعريف الجهة المختصة بإصدار شهادة التصديق الالكتروني

اختلف الفقه والقانون المقارن في الاصطلاح الذي يطلق على الجهة المختصة بإصدار شهادات التصديق الالكتروني، حيث يستخدم جانب من الفقه اصطلاح "سلطة الاشهار"، وكان التعريف لها بأنها: هيئة عامة أو خاصة تسعى إلى ملئ الحاجة الملحة لوجود طرف ثالث موثوق يقدم خدمات أمنية في التجارة الالكترونية، بأن يصدر شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل

الالكتروني لتوثيق هوية الأشخاص المستخدمين لهذا التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه".[1]

ويرى جانب آخر من الفقه استخدام اصطلاح "مقدم خدمات التصديق الالكتروني" ويعرفه بأنه: شخص طبيعي أو معنوي يستخرج الشهادات الالكترونية، ويقدم الخدمات الأخرى المرتبطة بالتوقيعات الالكترونية، ويضمن تحديد هوية الأطراف المتعاقدة والاحتفاظ بهذه البيانات لمدة معينة، ويلتزم باحترام القاعد المنظمة لعمله.[2]

ويُعَرِفُ جانب آخر من الفقه مقدم خدمات التصديق الالكتروني بأنه: جهة أو منظمة عامة أو خاصة، تستخرج شهادات الكترونية والشهادة هذه تؤمن صلاحية الموقع وحجية توقيعه وكذلك التأكد من هوية الموقع، وتوقع هذه الشهادة من شخص له الحق في مزاولة هذا العمل.[3]

اما المشرع الجزائري فقد تعرض اليها بصفة عرضية في المادة 02من المرسوم رقم 162/08بالنص على أنها: "كل شخص في مفهوم المادة 8-8 من القانون رقم 3/2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية، يسلم شهادات الكترونية أو يقدم خدمات أخرى في مجال التوقيع الالكتروني.[4]

ثانياً: دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع

إن الهدف من إنشاء جهات مختصة في اصدار شهادات التصديق الالكتروني في الدور الذي تقوم به، من خلال دورها في التحقق من هوية الشخص الموقع (المرسل) وصلاحية توقيعه وتحديد أهليته القانونية للتعامل والتعاقد.

---

[1] لالوش راضية ، المرجع السابق ، ص 105.

[2] سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006 ، ص 322.

[3] لالوش راضية، المرجع نفسه، ص106.

[4]عبد العزيز سمية، التوقيع الالكتروني وسيلة حديثة للإثبات، مجلة معارف، المركز الجامعي بريكة، العدد17، 2014، ص197.

فلا يقتصر دور جهات التصديق الالكتروني على تحديد هوية المتعاملين أو تحديد اهليتهم القانونية، بل يتعدى إلى التحقق من مضمون هذا التعامل أو التبادل الالكتروني، وسلامته وبعده عن الغش والاحتيال[1].

كما تقوم هذه الجهة بإصدار التوقيع الرقمي وإصدار المفاتيح الالكترونية سواء المفتاح الخاص أو المفتاح العام الذي يتم بمقتضاه الأول تشفير البيانات والمعاملات عكس الثاني (المفتاح العام) الذي يتم بمقتضاه فك التشفير، فلهذه الجهات أهمية كبيرة وأدوار عدة نذكرها في النقاط التالية:

1- التحقق من هوية الشخص الموقع

يتمثل الدور الرئيسي لجهات المصادقة الالكترونية في القيام بالتحقق من هوية الشخص الموقع ،فإذا قام أحد الأطراف بوضع توقيعه على رسالة البيانات الالكترونية، وقامت جهة التصديق بتأكيد صحتها، فإن هذا يؤكد صدور التوقيع من صاحبه ويستتبع التحقق من هوية الموقع من طرف هيئة التصديق لتحديد الأهلية القانونية للمتعاقد[2].

والمقصود بذلك أنه عندما يضع أحد الأطراف توقيعه الالكتروني على محرر الكتروني، ويقوم بإرساله إلى شخص آخر فان هذه الجهة المكلفة بالتصديق الالكتروني تصدر شهادة الكترونية تكون وظيفتها الربط بين الموقع ومفتاحه العام ، بحيث تحتوي هذه الشهادة على مجموعة من البيانات التي تخص صاحبها (كاسمه-سلطته في التوقيع) بحيث هذه البيانات التي تحتويها الشهادة تحدد للمرسل إليه هوية المرسل الموقع [3]

[1] لالوش راضية، المرجع السابق، ص 112.

[2] حسينة عبد الحميد شرون، صونيا مقري، المرجع السابق، ص 136.

[3] لالوش راضية ، المرجع نفسه، ص113.

وبعد أن يتأكد المرسل إليه من صلاحية الشهادة الالكترونية المرسلة له من خلال الجهة التي أصدرتها يعول على المحرر الالكتروني، وهكذا يتم التبادل بين المرسل والمرسل إليه حتى يتم التوصل إلى الاتفاق النهائي.

2-اصدار مفاتيح الكترونية

من الخدمات التي تقدمها هيئات التصديق أيضاً أنها تتولى اصدار مفاتيح تشفير الكترونية، سواء كانت مفاتيح خاصة، والتي من خلالها يتم تشفير المعاملات الالكترونية ويكون هذا المفتاح محفوظ على أداة ـو وسيلة تستعمل لوضع توقيع الكتروني لشخص موقع على محرر الكتروني، وهو مفتاح خاص بصاحبه لا يعلمه غيره، ولا يكون إلا تحت حيازته وتحت سيطرته، أو مفاتيح تشفير عامة التي من خلالها فك هذا التشفير وهو متاح للكافة.[1]

كما تقوم بإصدار التوقيع الرقمي ويكون ذلك عن طريق تقديم البيانات اللازمة من طالب المصادقة على التوقيع إلى جهة التصديق، والتي تصدر بناءا على ذلك مفتاح خاص بصاحب طلب توثيق التوقيع ولا يمكن هنا استخدام المفتاح الخاص، إلا من جهاز حاسوب واحد وذلك حتى يتم التأكد من أن التوقيع رقمي صادر من صاحبه، لذا يتعين على الموقع أن يحتفظ بالمفتاح الخاص بشكل سري ولا يطلع عليه أحد، في المقابل نجد أن المفتاح العام تحتفظ به جهة التوثيق لتمكن من يريد التعامل مع صاحب المفتاح الخاص منه للتأكد من صحة التوقيع.[2]

هذا بالإضافة إلى الدور الذي تلعبه جهات المصادقة الالكترونية في تعقب المواقع التجارية على الانترنت للتحري عن جديتها ومصداقيتها، فاذا تبين لها عدم امن هذه المواقع فإنها تقوم بتوجيه رسالة تحذيرية للمتعاملين تبين عدم مصداقية هذه المواقع وهذا ما يمثل المجال الاوسع الذي يتجلى فيه دور

[1] رضوان قرواش، هيئات التصديق الالكتروني في ظل القانون 04/15ا لمتعلق بالقواعد العامة للتوقيع والتصديق الالكترونيين (المفهوم والالتزامات)،مجلة العلوم الاجتماعية ، العدد 24، جامعة سطيف 2 ،2017، ص 416..

[2] رضوان قرواش، المرجعً نفسه، ص416

جهات المصادقة الالكترونية في توفير الحماية للمستهلك في مجال المعاملات الالكترونية، ذلك ان اغلب المعاملات تتوزع على عمليات البيع والشراء عبر المواقع التجارية على الأنترنت، خاصة في ظل كثرة الغش والاحتيال في هذا النطاق[1].

3-اثبات مضمون التبادل الالكتروني

تقوم الجهة المختصة بإصدار شهادات التصديق الالكتروني كذلك بالتحقق من مضمون التعامل أو التبادل الالكتروني بين الأطراف المتعاقدة والتيقن من سلامته وجديته وبعده عن الغش والاحتيال، إضافة إلى اثبات وجوده ومضمونه[2].

وحماية المتعاملين من أي غش قد يقعون فيه اثناء تعاملاتهم، حيث نجد أن جهات التصديق الالكتروني تقوم بتعقب المواقع التجارية على الانترنت للتحري عن جديتها أو مصداقيتها فإذا إتضح لها أن هذه المواقع غير حقيقية أو غير جدية فإنها تقوم بتوجيه رسائل تحذيرية للمتعاملين[3].

كما تتولى جهة التصديق الالكتروني تحديد وقت ولحظة ابرام العقد، والقاعدة العامة أنه عند عدم وجود نص خاص، فلا يُعَدُ تاريخ ابرام العقد شرط ضرورياً لصلاحية التصرف، فتحديد لحظة

[1] حسينة عبد الحميد شرون، صونيا مقري، المرجع السابق، ص137-138.

[2] إبراهيم الدسوقي أبو الليل، توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم إلى مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الامارات العربية المتحدة بالتعاون مع غرفة التجارة الالكترونية وصناعة دبي، في الفترة مابين10و 12 ماي 2003، المجلد الخامس، ص187.

[3] إبراهيم الدسوقي أبو الليل، المرجع نفسه، ص 178.

ابرام العقد تُعَدُ مؤشراً لتحديد موعد ترتيب الاثار القانونية لهذا العقد[1]، ولتأكيد سلامة البيانات الالكترونية المتداولة يجب أن تضمن منظومة امن احداث التوقيعات الالكترونية ،مع وجوب الاستعانة بأنظمة مؤمنة لحفظ شهادات التصديق الالكتروني على أي عامل الكتروني تتيح إمكانية الاطلاع عليها عند الحاجة بالشكل الذي أُنشأت وأرسلت أو استعملت به.[2]

المبحث الثاني: جرائم الاعتداء على التوقيع الالكتروني

بالرغم مما حققه التطور التكنولوجي من ايجابيات إلا أن هذا الامر لم يخل من السلبيات، باعتبار أن التطور رافقه تطورا مناظرا له عدة دوافع اجرامية مستغلة لارتكاب العديد من الجرائم التقليدية، والتي اعتدنا مصادفتها منها التزوير والاحتيال. والتي واجهتها العديد من التشريعات التنظيمية من جهة، ومن جهة اخرى استحداث صور تكون معروفة من قبل مثل جريمة الادلاء بالإقرارات الكاذبة للحصول على شهادة التصديق الالكتروني، وجريمة حيازة أو إفشاء بيانات توقيع موصوفة خاصة بالغير.

وهذا الاجرام المستحدث وما صاحبه من مخاطر جسيمة جعل القانون الجنائي عاجزاً عن توفير الحماية الكافية لقصور نصوص القانونية، وعدم قدرته على شمول الوقائع المكونة للركن المادي، لاسيما في ظل مبدا الشرعية الذي يقضي بأن" لا جريمة ولا عقوبة الا بقانون."

في حين يأتي على راس مظاهر التطور العلمي وتكنولوجيا المعلومات، التي شمل استخدامها مجالات التعليم والبحث العلمي والتسيير، والمرافق الضرورية التي تعتبر العصب الأساسي لتقديم

[1] سعيد السيد قنديل، التوقيع الالكتروني، د ط، دار الجامعة الجديدة، الإسكندرية، 2006، ص105.

[2] حسينة عبد الحميد شرون، صونيا مقري، المرجع السابق، ص 136.

المجتمعات ،حتى اصبح استخدام المعلوماتية مؤشرا لثورة صناعية جديدة هي الثورة المعلوماتية، والتي بدورها فتحت افاقا جديدة أمام تبادل المعلوماتية والأموال في أوساط افتراضية كان من الطبيعي ظهور جوانب سلبية من أبرزها ظهور جرائم بصور جديدة ترتكب باستخدام هذه التكنولوجيا .لهذا سنحاول دراسة جرائم الاعتداءات على التوقيع الالكتروني بهذا المبحث كالتالي **المطلب الأول** سندرس جرائم الاعتداء على التوقيع الالكتروني في اطار قانون العقوبات، أما **المطلب الثاني** سندرس فيه جرائم الاعتداء على التوقيع الالكتروني في اطار قانون 15- 04 .

المطلب الأول: جرائم الاعتداء على التوقيع الإلكتروني في إطار قانون العقوبات

إن التوقيع الإلكتروني يعتبر عنصر ذو أهمية كبيرة لأنه العماد الذي تقوم عليه إجراءات التجارة الإلكترونية كونه مرتبطا بتوثيق التصرفات القانونية الإلكترونية، وتحديد هوية المرسل والمستقبل والتأكد من صحة البيانات، ولهذه الأهمية بات من الضروري وجود حماية جنائية له ضد كل التصرفات التي تهدده بالاعتداء أو الضرر.

ولعل من أكثر الجرائم تهديدا للتوقيع الإلكتروني جريمة تزوير التوقيع الإلكتروني وجريمة الاحتيال وجرائم اخرى حديثة متطورة وسريعة، وقد عالجت ذلك تشريعات وقوانين الدول، بل وحفاظا على الثقة والأمان في المعاملات الإلكترونية وحمايتها من مخاطر القرصنة، وعليه سنحاول بيان هذه الاليات والضمانات في الفرعين الموالين: الفرع الأول جرائم التزوير والاحتيال على التوقيع الالكتروني في إطار قانون العقوبات أما الفرع الثاني جرائم المساس بأنظمة المعالجة الإلكترونية.

الفرع الأول: جرائم التزوير والاحتيال

أولاً: جرائم التزوير

إن التزوير بوجه عام هو تغيير الحقيقة أيا كانت وسيلته وأيا كان موضوعه أو شكله، وبهذا المدلول يتسع للعديد من الجرائم، أما التزوير في المحررات فهو حسب تعريفه المستقر في الفقه الفرنسي والمصري "تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون، تغييرا من شانه احداث ضرر مقترن بنية استعمال المحرر المزور فيما اعدا له "[1].

ويقصد بالتزوير المعلوماتي "أي تغيير للحقيقة يرد على المخرجات الحاسب الالي سواء تمثلت في مخرجات ورقية مكتوبة كتلك، التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر المعلوماتي أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها كذلك قد يتم في مخرجات غير ورقية شرط أن يكون المحرر المعلوماتي ذا أثر في اثبات قانوني معين".

ومفهوم ما سبق أن التزوير المعلوماتي يرد على وثائق معلوماتية –حتى ولو كانت محررات باطلة من حيث الشكل. وهي تلك الوثائق التي يتم الحصول عليها بوسائل معلوماتية، أي تكون ناشئة عن جهاز إلكتروني كهرومغناطيسي أو طبع ممغنط.

وإن كان هناك في الفقه من يرى عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية فالوثيقة المعلوماتية هي وثيقة لم تبرمج بعد وتوجد جهات مرخص لها سواء كانت شخصية أو اعتبارية باعتماد التوقيعات الإلكترونية، بشهادات مصدق عليها منهم، وهذه الشهادات يترتب عليها اثار قانونية تتمثل في انشاء التزامات واثبات حقوق بالنسبة لطرفي العقد في التجارة الالكترونية في حالة اعتماد التوقيع الالكتروني بينهما.

1 – أركان جريمة تزوير التوقيع الإلكتروني

[1] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، د ط، دار النهضة العربية القاهرة، 1986، ص193.

التزوير المعلوماتي يتكون من خلق أو تعديل غير مصرح للبيانات المسجلة بطريقة تجعلها تحوز قوة وحجية، بما يؤدي إلى خداع للحقوق القانونية المحمية وهي أمن وسلامة وإمكانية تشغيل البيانات الإلكترونية، كما وان الادخال غير المصرح به للبيانات الصحيحة وغير الصحيحة يخلق موقفا يناظر عمل محرر مزور، وايضا للعمليات اللاحقة للإتلاف كالتعديلات والمحو كواقعة خروج البيانات الممثلة على دعامة والطمس كواقعة حفظ واخفاء بيانات كل ذلك يوازي تزوير محرر صحيح، هذا لارتكاب ذلك الفعل .[1]

أ – الركن المادي لجريمة التزوير في التوقيع الالكتروني

تتطلب جريمة التزوير عنصرين أساسين هما السلوك الاجرامي، والمتمثل في تغيير الحقيقة بالطرق المقررة قانوناً للتزوير سواء كان الأمر يتعلق بمحرر رسمي أو عرفي وكذلك عنصر الضرر.[2]

– السلوك الاجرامي

باستقراء الاحكام المتعلقة بالتزوير فإنه يتضح بأن السلوك الاجرامي لهذه الجريمة، يتمثل في تغيير الحقيقة بالطرق المقررة قانوناً في المحرر تغييرا من شأنه أن يسبب ضرر للغير. وعليه لكي يتضح السلوك الاجرامي في هذه الجريمة لابد من تحديد الأفعال المكونة للنشاط الاجرامي. إن المشرع قد اعترف بإمكانية الاثبات الالكتروني ، غير أنه لم ينص صراحة على حمايته جزائياً في نصوص خاصة.

[1] خالد ممدوح ابراهيم، الحماية الجنائية للتوقيع الالكتروني في القانون الاتحادي رقم 02 / 2006، مجلة الفكر الشرطي، مركز بحوث القيادة العامة لشرطة الشارقة، الشارقة ،2014، ص 156 -157.

[2] راضية مشري، جريمة تزوير التوقيع الالكتروني في التشريع الجزائري، مجلة حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد 20، جامعة 08 ماي، قالمة، 2017، ص 128.

ومهما يكن الأمر فإن مناط العقاب في جريمة التزوير هو الاخلال بالثقة العامة الموجودة في المحرر وهذه الثقة لا تتوفر إلا في محرر يتمتع بقوة قانونية في الاثبات، ما يرتب عليه من أثر قانوني، لكن يمكن ان يشوب المحررات الالكترونية التي تتضمن التوقيع الالكتروني موضوع للتزوير.

هناك من يرى أن المحررات الالكترونية التي تحمل توقيع الكتروني لا يمكن أن تكون محررات رسمية بل محررات عرفية يمكن أن تكون محل تزوير[1]، وعليه ما يقع عليها من تحريف أو تزوير أو تغيير حسب الطرق المحددة قانوناً، وتنطبق عليه احكام المادة 219 من ق.ع. غير أن المشرع المصري[2] بموجب قانون التوقيع الالكتروني رقم 04 / 15 حرص على تجريم تزوير التوقيع الإلكتروني والمحررات الالكترونية بنصوص خاصة في قانون التوقيع الالكتروني وهما (المادتين 23.24) وفرق بين المحررات الالكترونية العرفية وكذا الرسمية إذا توفرت الشروط التي يتطلبها القانون.[3].

على عكس المشرع الفرنسي الذي ذهب إلى صياغة (المادة441 -1) من قانون العقوبات الفرنسي لتعدل ما كان ينص عليه قانون Godfrain سنة 1988[4] الذي كان يتضمن تجريم تزوير المحررات الالكترونية، أياً كان شكلها وذلك متى كان من شأنها الإضرار بالغير، كما امتد التجريم إلى استعمال المحررات الالكترونية المزورة، وبذلك فإن المشرع الفرنسي فضل تعديل النص العام في التزوير لكي ينسحب على تزوير المحررات الالكترونية.

وتجدر الاشارة إلى أن التوقيع الالكتروني إذا توفرت فيه شروط الحماية المشار اليها آنفاً فإنه يحمي جزائياً بغض النظر عن نوع المحرر أو طبيعته أو قيمته، وهذا هو النهج الذي انتهجته معظم الدول التي جرمت تزوير التوقيع الالكتروني.[5]

---

[1] فرقد عبود العرضي، جريمة التزوير الإلكتروني دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، العدد 13، جامعة الكوفة، العراق،2013 ، ص 103.

[2] راضية مشري، المرجع السابق, ص130.

[3] خالد ممدوح ابراهيم، المرجع السابق، ص 159.

[4] القانون الفرنسي رقم19-88 الصادر في 5 يناير سنة 1988.

[5] راضية مشري، المرجع نفسه, ص 130.

2 – طرق جريمة التزوير على التواقيع الالكترونية

حددت المواد 214 إلى 216 ق.ع. ج [1] طرق التزوير وهي نوعين مادي ومعنوي.

- **التزوير المادي:** يعرف التزوير المادي بانه كل تغيير للحقيقة ينصب على مصدر المحرر بان ينسب المحرر إلى غير منشئه أو يتناول بالتعديل صلب المحرر بعد انشائه من المحرر الحقيقي[2]، ويتم في ثلاثة صور هي وضع توقيع مزور، حذف أو اضافة أو تغيير مضمون المحرر، واصطناع المحرر.
- **التزوير المعنوي:** فهو كل تغيير للحقيقة في المحرر يقع اثناء انشاء المحرر لا بعده، وانه لا يترك أثر مادي في المحرر تدركه العين، وعلى هذا الأساس يقع التزوير المعنوي من الشخص المكلف بكتابة المحرر، ويتم بطريقتين اصطناع واقعة، أو اتفاق خيالي استبدال الاشخاص أو انتحال شخصية الغير. أما المشرع الجزائري فقد عمد على الكتابة في الشكل ضمن وسائل الاثبات المدني في اثبات التزوير المادي أو المعنوي للتوقيع الالكتروني.

ومن ثم يمكن تصور أن يقع التلاعب أو التزوير على التوقيع الالكتروني والذي يعد من الوسائل الحديثة للتوقيع، حيث يمكن للقراصنة اختراق نظم المعلوماتية، ومعرفة التوقيع، وفك شفرته واستخدامه دون موافقة صاحبه، أو نقل امضاء الشخص على الاوراق المسحوبة على الحاسب الالي وتزويرها دون علم ورضا صاحبها خاصة في مجال التعاملات البنكية.

ولكن هناك من يرى أن التوقيع الالكتروني عبارة عن مخرجات ليست ورقية بل الكترونية، وتحتوي مجموعة الرموز أو الارقام أو بإخراج رسالة الكترونية تتضمن علامة مميزة في مجملها، وهي بذلك تعد بيانات تتضمن معلومات تنشا أو تندمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية أو رقمية أو ضوئية باعتبارها ومضات كهرومغناطيسية ذات طابع معنوي وعليه فكل

[1] المادة 214-216 ق.ع.ج

[2] عزت عبد القادر، جرائم التزوير والتزييف، ط 2، دار اسامة الخوري للنشر والتوزيع، القاهرة ، 2000، ص 20.

تزوير أو تحريف ينصب على بيانات الحاسب نفسه أي بيانات مخزنة في ذاكرته من قبيل التزوير المعنوي، وليس تزويرا ماديا.

مهما يكن من أمر إذا كان تغيير الحقيقة هو مناط التزوير سواء تعلق الامر بتوقيع تقليدي أو الكتروني فإن الأمر يتم بطريقة مختلفة، إذ أن التوقيع الالكتروني لا يمكن تقليده، إنما يمكن استعماله دون علم مالكه يتم بواسطة منظومة الكترونية تتخذ شكل حروف أو أرقام أو رموز أو شارات أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر، وذلك لأن توقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي.

وبالتالي لا يمكن أن يكون متماثل معه، ومن ثم فجريمة تزوير التوقيع التقليدي تختلف عن جريمة تزوير التوقيع الالكتروني سواء في طريقة التزوير أو اسلوب اكتشاف هذا التزوير فطريقة، الكشف عن التوقيع المزور تكون عن طريق الماهرات، بينما في حالة تزوير التوقيع الالكتروني لا يمكن استخدام تلك الطريقة في اكتشاف تزوير التوقيع الالكتروني، إذا كان التوقيع سليم لكنه ليس صادر من شخص مالك منظومة التوقيع[1]

3 – الضرر في جريمة التزوير على التوقيع الالكتروني

يعد الضرر الركيزة الاساسية في جريمة التزوير على التوقيع الالكتروني ويأخذ الضرر في التزوير نطاق واسعا ولا يشترط ان يحل الضرر بشخص معين يقصده المزور، بل يكفي ان يحل باي كان ولا يشترط ان يبلغ الضرر درجة معينة من الجسامة ويرجع لقاضي الموضوع تقدير وجود الضرر، والضرر يمكن ان يكون مادي أو معنوي ويمكن أن يكون الضرر محقق أو محتمل الوقوع، وقد ينتج الضرر المحتمل من طبيعة الوثيقة المزورة ذاتها، وتكون العبرة في تقدير احتمال الضرر بالوقت الذي وقع فيه تغيير الحقيقة في المحرر باعتباره الوقت الذي تتم فيه الجريمة.

[1] منير محمد الجنبيهي ومحمود محمد الجنبيهي، المرجع السابق، ص54.

ب- الركن المعنوي لجريمة التزوير على التوقيع الالكتروني:

تقتضي جريمة التزوير بصفة عامة من الجرائم العمدية التي تتطلب قصدا جنائيا عاما وقصدا جنائيا خاصا فلا يكفي القصد العام الذي يقوم على علم المتهم باركان الجريمة واتجاه ارادته إلى الفعل المكون لها وتحقيق نتيجته بل تتطلب هذه الجريمة توافر قصد جنائي خاص يتمثل في نية استعمال المزور فيما زور من أجله، [1] وعلى هذا فان القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بأنه" تعمد تغيير الحقيقة في محرر تغييرا من شانه ان يسبب ضرر وبنية استعمال المحرر فيما غيرت من أجله الحقيقة".[2]

وانطلاقا مما سبق نصل إلى نتيجة مفادها انه لا يمكن القياس على جريمة التزوير التقليدي لان هذا يتنافى مع مبدا الشرعية والنصوص التقليدية كون جريمة تزوير التوقيع الالكتروني جريمة مستحدثة لا تنسجم مع النصوص التقليدية، ما يدعو إلى ضرورة تدخل المشرع الجزائري للنص على هذه الجريمة واخذاً بما ذهب إليه المشرع المصري من خلال القانون 115 - 2004 الخاص بتنظيم التوقيع الالكتروني وأن ما قام به المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004 وادخاله لجريمة المعالجة الآلية لمعطيات الحاسوب المادة 394 مكرر إلى غاية 394 مكرر 7 وغير كاف بالنسبة لجريمة تزوير التوقيع الالكتروني.[3]

2 العقوبات المقررة لجريمة التزوير على التوقيع الالكتروني

[1] ياسر محمد الكومي، الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، رسالة لنيل شهادة الدكتوراه في القانون الجنائي، جامعة حلوان، مصر، 2016، ص 15.

[2] محمود نجيب حسني شرح قانون العقوبات، القسم الخاص، ط 02، دار النهضة العربية، القاهرة، 1994، ص 271.

[3] وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر، الوادي، المجلد 11 ، العدد 01 ، افريل 2020 ص 592.

تماشياً مع التطور التكنولوجي في مجال الاتصالات وانتشار استخدام النظم المعلوماتية أدخل المشرع الجزائري جملة العقوبات المتعلقة بالتزوير الالكتروني تزوير التوقيع الالكتروني إلى نصوص قانون العقوبات.

فعاقب المشرع الجزائري على التزوير في المحررات العرفية أو التجارية بمقتضى المادة 219 من ق.ع.ج[1] بالحبس من سنة إلى خمس سنوات والغرامة المالية من 500 دينار جزائري إلى 20.000 دج كعقوبة اصلية إضافة إلى العقوبات التكميلية وهذا حسب الفقرة 02 من المادة 219[2] من ق.ع.ج والمتمثلة في الحرمان من حق أو أكثر من الحقوق الواردة في نص المادة 14[3] من نفس القانون وبالمنع من الإقامة من سنة إلى خمسة سنوات على الأكثر "المادة 14 من قانون العقوبات الجزائري ".

ونص المادة[4]214، والمادة[5] 216 من ق.ع.ج .والتي تضمنت عقوبة الحبس والغرامة المالية لكل مرتكب لهذه الجريمة، كما عاقب المشرع الجزائري على الشروع وعليه فإنه يعاقب من بدأ في تنفيذ جريمة التزوير في المحررات المصرفية والتجارية ولم يحقق نتيجتها، ومن بدأ فيها وأتمها بنفس العقوبة التي تضمنتها المادتان 220 - 219 من ق.ع.ج [6] ذلك بالنسبة للشخص الطبيعي.

أما الشخص المعنوي فقد نص المشرع الجزائري على مسؤولية الشخص المعنوي فيما يتعلق بجرائم التزوير في المادة 253 مكرر من قانون العقوبات.[7] وتطبق على الشخص المعنوي العقوبات المنصوص عليها في المادة 18[8] مكرر، وعند الاقتضاء المنصوص عليها في المادة 18 مكرر 2[1] من

[1] المادة 219 من ق.ع. ج.
[2] الفقرة الثانية من المادة 219 من ق. ع. ج
[3] المادة 14 من ق.ع.ج.
[4] المادة 214 من ق.ع.ج.
[5] المادة 216 من ق.ع.ج.
[6] المادة 219-220 من ق.ع.ج.
[7] المادة 253 من ق.ع.ج.
[8] المادة مكرر 18 من ق.ع.ج.

هذا القانون، ويتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر.

ثانياً: الاحتيال على التوقيع الإلكتروني

يعد الاحتيال على التوقيع الالكتروني والمنظومة المعلوماتية من أكثر الجرائم المعلوماتية التي ترتكب على نطاق واسع في مختلف الدول وتسبب بخسائر اقتصادية فادحة، الأمر الذي شكل قلقاً لدى المعنيين بالأمر حيث نجد ان هذه الجريمة تزعزع كيان ثقة الافراد بالوسائل التقنية الحديثة لنقل الأموال. ويمكن أن نعرف الاحتيال الالكتروني بأنه: (الاستلاء على حيازة مال الغير الكاملة بوسيلة يشوبها الخداع وذلك عن طريق تسليم المال.)[2]

ويمكن القول بصفة عام أنه لا يوجد تعريف مقبولاً للاحتيال الالكتروني للرجوع إليه، فقد تعددت التعريفات التي تتناول الاحتيال الالكتروني، واختلفت فيما بينها من حيث العناصر التي يجب توافرها لتحقيقه، وسوف نتعرف على اهم هذه التعريفات ثم نختار التعريف الذي نراه أكثر تعبيرا عن طبيعة الاحتيال الالكتروني، لقد توسعت غالبية التعريفات في مفهوم الاحتيال حيث يرتبط الاستخدام الغير مشروع لحسابات الالية لتحقيق الربح المادي غير المشروع بصفة عامة ويبين الاحتيال الالكتروني. [3]

وجاء لدى شراح قانون العقوبات تعريفات عديدة لجريمة الاحتيال الالكتروني بانها: الاستلاء فالاحتيال الالكتروني « . على مال منقول مملوك للغير بخداع المجني عليه وحمله على تسليمه هو التلاعب العمدي بمعلومات وبيانات تمثل قيمة مادية يخترقها نظام الحاسب الالي أو الادخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الاوامر والتعليمات التي تحكم عملية البرمجة أو

[1] المادة 18 مكرر فقرة 2 من ق.ع.ج.

[2] محمد عبد الله بوبكر موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والانترنت ،د ط, دار الثقافة والتوزيع، الاردن، 2010 ، ص184.

[3] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية، ط 1، منشورات الحلبي، لبنان، 2005، ص 424.

أية وسيلة من شأنها التأثير على الحاسب الالي حتى يقوم بعملياته بناءا على هذه البيانات أو الاحتيال المعلوماتي.[1]

1-أركان جريمة الاحتيال على التوقيع الالكتروني

لقد نص المشرع الجزائري في ق.ع.ج في نص المادة 372 كل من توصل « : منه على ما يلي إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو ابراء من التزامات، أو إلى الحصول على أي منها أو شرع في ذلك وكان بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه اما باستعمال اسماء أو صفات كاذبة أو سلطة خيالية، أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أوفي وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها".[2]

يتضح من استقراء نص المادة372 من ق.ع.ج[3] أن المشرع الجزائري لم يعالج أو بالأحرى ولم يتناول جريمة الاحتيال الالكتروني بصورة مباشرة، فالإشكالية يطرح في الحالة التي يتلاعب فيها الجاني في البيانات المعالجة الية أو البرامج المعلوماتية توصلا للاستيلاء على مال الغير ومثال ذلك قيام الجاني بالتلاعب في البيانات المخزنة أو المدخلة إلى الحاسب الالي.

لقد ظهرت الحاجة إلى تجريم الاحتيال الإلكتروني في التزايد المستمر في استعمال أنظمة الحاسبات الالية وما ارتبط بذلك من تزايد في الجريمة المعلوماتية بصفة عامة وفي الاحتيال الإلكتروني بصفة خاصة باعتباره واحد من اهم صور هذه الجريمة ومع صعوبة تطبيق النصوص التقليدية كان اتجاه

[1] عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي وعلوم جنائية ، جامعة العقيد الحاج لخضر ،باتنة 1، 2012، ص 41 .

[2] الأمر رقم 66 – 156 المؤرخ في 8 يونيو سنة 1966، يتضمن قانون العقوبات، ج ر، عدد 49، الصادرة بتاريخ 11 يونيو 1966. المعدل والمتمم لاسيما بالقانون رقم 15– 19، المؤرخ في 30 ديسمبر 2015، ج.ر العدد 71، الصادرة بتاريخ 30 ديسمبر 2015

[3] المادة 372 من ق.ع.ج.

بعض التشريعات إلى افراد نصوص لتجريم الاحتيال الالكتروني سواء كان التجريم بنص عام ام كان يتناول بعض صور الاحتيال المعلوماتي دون البعض الاخر. [1]

أ – الركن المادي لجريمة الاحتيال على التوقيع الالكتروني:

يعرف الركن المادي في جريمة النصب "الاحتيال "المعلوماتي على انه الوسيلة التي يلجا اليها النصاب أو المحتال وذلك قصد استيلاءه على مال منقول مملوك للغير وتحديدا النقود ومن هنا يتبين لنا الركن المادي الذي يتكون من 03 عناصر سوف نتطرق لها فيما يلي:

1 . السلوك الاجرامي

ان السلوك الاجرامي لجريمة الاحتيال المعلوماتي عرف في عدة أنواع وصور وطبق من طرف الجنات بعدة طرق واشكال متنوعة لذلك لابد لنا ان نتعرف على هذه الصور حتى يسهل علينا معرفة السلوك الاجرامي بشكل واضح وبنطاق واسع من ذلك سنتناول صور السلوك الاجرامي على النحو التالي. فصور السلوك الاجرامي تتمثل في عدة أنواع منها الاحتيال باستخدام بطاقات الائتمان والذي يكون في مجال بطاقات الائتمان الممغنطة، وينطوي على خطورة كبيرة من حيث مقدار الخسائر الناجمة عن كل حالة على حدى الا انه يسبب التزايد الكبير في عدد القضايا المطروحة امام القضاء.

أما النوع الآخر فهو الغش باستخدام بطاقات الائتمان من قبل صاحبها أو بواسطة الغير: والذي بدوره هو الاخر ينقسم إلى قسمين هما: الغش باستخدام بطاقات الائتمان من قبل صاحبها ويقصد به حامل البطاقة أي الافراد الذين يوافق البنك المصدر على طلبهم بالحصول على البطاقة لاستخدامها في الشراء أو السحب غيره،[2] والغش باستخدام بطاقات الائتمان بواسطة الغير ويقصد بالغير في هذه الحالة أي شخص غير التاجر والذي يتعامل معه حامل البطاقة أو موظفي البنك

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص593.

[2] نائلة عادل محمد فريد قورة ،المرجع نفسه، ص 508.

المصدر للبطاقة، فهؤلاء لهم الاحكام الخاصة بهم ولذلك يعرف بأنهم الأشخاص الذين لا يدخلون ضمن هاتين الفئتين وقد تظهر مشكلة الغير فيما لو فقدت البطاقة أو سرقت أوضاع أو سرق الرقم السري الخاص بها لان العميل لا يمكن له استخدام البطاقة دون رقم سري فتستخدم البطاقة بموجبه وهذا الرقم السري بمثابة التوقيع الالكتروني. [1]

إضافة إلى أنواع الاحتيال نجد غسيل الأموال الذي تستخدم شبكة الانترنت هذه الأيام لعمليات غسيل الأموال وقد زاد ذلك ظهور التجارة الالكترونية وهناك عدد من الأساليب تستخدم فيها شبكة الانترنت في عملية غسيل الأموال.[2]

والاحتيال التجاري الالكتروني يعرف بأنه هو استخدام الكذب والخداع أو التظليل للحصول على ميزة أو مصلحة غير مستحقة وكانت من حق طرف اخر، وتشير الدراسة إلى أن الاحتيال مثله مثل كافة الجرائم الاخرى يتضمن ثلاث عناصر رئيسية، وهي الدافع من حيث وجود العامل المحرك للإرادة والذي يوجه السلوك الاحتيالي كالانتقام وغيرها ووجود الهدف أو الضحية للسلوك الاحتيالي وغياب القدرة على توفير الحماية.

2 – النتيجة تسليم المال المعلوماتي

الاستلاء على مال الغير هو النتيجة التي يتوخاها الجاني جراء الانتحال المجني عليه وقد يكون الاستيلاء على المال اما:

اما يكون تسليم مال في مجال المعالج الالية للبيانات: قد يتم تسليم المال إلى الجاني من قبل المجني عليه المالك للمال وقد يكون هذا المجني عليه مجرد حائز مؤقت كما لمستأجر أو المستعير ومعنى التسليم في جريمة الاحتيال المعلوماتي، له دلالة خاصة عن معناه التقليدي حيث غالب ما يكون عن طريق الأجهزة الالية أي يمكن ان يكون افتراضا جعل الجهاز هو الطرف الثالث

[1] عبد الفتاح بيومي، ، المرجع السابق، ص 139.

[2] أمجد سعود الخريشة ،جريمة غسيل الأموال ، ط 1، دار الثقافة للنشر والتوزيع، الأردن ، 2009 ، ص49.

أما المال المعتدي عليه في جريمة النصب والاحتيال المعلوماتي لا يختلف مدلوله عن المال في جريمة السرقة فلابد أن يكون منقولاً وأن يكون مملوكاً للغير.

.3-الضرر في جريمة الاحتيال

لا يكفي في جريمة الاحتيال ان يرتكب الجاني فعل الاحتيال وحدوث واقعة التسليم التي تعي سلب المال وإنما يلزم أن يكون التسليم وقع بطريقة من طرق الاحتيال المستخدمة من الجاني، أي أن العلاقة السببية تنص على أن الاحتيال هو السبب الفعلي والدافع على التسليم، وأن يكون التسليم لاحقا على فعل الاحتيال ونتيجة لانخداع المجني عليه وان يكون مبني على الضرر.[1]

ب الركن المعنوي

الاحتيال جريمة عمدية ويعني هذا انه يلزم بتوافر العلم والإرادة بخصوص النشاط والنتيجة.

1. القصد العام: لا يقوم القصد العام الا بتوافر العلم والإرادة والعلم ركن من اركان الجريمة وعناصر كل وإرادة ارتكاب الفعل الاجرامي وإرادة تحقيق النتيجة الاجرامية التي تتمثل في قيام المجني عليه بتسليم ماله إلى الجاني.[2]

- **العلم**: وينحصر العلم في الاحتيال في ان الجاني يأتي افعاله وادعاؤه وهو يعلم بانها كاذبة كما انه يغير الحقيقة ويأتي بأفعال مادية ومظاهره خارجية تؤيد ادعاءاته الكاذبة.[3] علم الجاني بالركن المادي للجريمة أي ان فعله ينطوي على الاستلاء مال منقول مملوك للغير دون رضا مالكه أي صاحب المال. [4]

[1] أحمد خليفة الملط، الجرائم المعلوماتية، ط 02، دار الفكر الجامعي، الإسكندرية، 2006، ص 346.

[2] أحمد خليفة الملط، المرجع نفسه، ص 319.

[3] أسامة حمدان، الرقب جرائم النصب والاحتيال، دار يافا العلمية للنشر والتوزيع، الأردن، 2009، ص 70.

[4] محمد على العريان، الجرائم المعلوماتية انعكاسات ثورة المعلومات على قانون العقوبات، د ط، منشورات الحلبي الحقوقية، لبنان، 2005، ص 128.

- **الإرادة:** ويقصد بها انصراف إرادة الجاني إلى ابيان فعل إيجابي قائم على أحد الأساليب الاحتيالية. ويجب توفر لدى الجاني بجانب العلم إرادة تحقيق الواقعة الاجرامية وهي سلب مال الغير بان فعل الاحتيال الذي يأتيه عليه خداع وايقاعه في الخطاء الذي يحمله على تسليمه ماله. في الجرائم الناشئة عن إساءة استخدام بطاقات الائتمان حيث ينصرف علم الجاني إلى انه بالرغم من علمه بعدم سماح الرصيد في حسابه الا ان ارادته تتجه إلى وجود ائتمان وهمي بقصد الحصول على أموال من البنك. [1]

2. **القصد الخاص:** يقوم القصد الخاص في جريمة الاحتيال على اتجاه نية الجاني إلى تملك الشيء الذي تسلمه من المجني عليه ويباشر عليه مظاهر السيطرة التي ينطوي عليها حق الملكية وان يجرم المجني عليه من مباشرتها ولنية التملك في الاحتيال ذات مدلولها في جريمة السرقة فاذا لم تتوافر لدى الجاني نية تملك المال الذي تسلمه فإن القصد الخاص لا يتوافر لديه فمن كان يريد تسليم الشيء مجرد فحصه ثم رده أو الانتفاع به ثم رده فان القصد الخاص لا يتوافر لديه. [2]

3. العقوبات المقررة لجريمة الاحتيال على التوقيع الالكتروني

الجزاء الجنائي هو التبعية القانونية التي يتحملها الجاني كاثر مترتب عل الجريمة التي أرتكبها وقد يتمثل في عقوبة أو تدابير احترازي، ويصدر به حكم قضائي في اعقاب محاكمة جنائية ويتم تنفيذ هذا الجزاء بواسطة السلطة العامة بطريق الاكراه.

وإذا توافرت أركان الجريمة بأن قام الجاني باستعمال إحدى وسائل الاحتيال التي حددها القانون وتوفر لديه القصد الجنائي وترتب على ذلك خداع المجني عليه وتسليمه المال إلى الجاني وقعت جريمة

[1] أحمد خليفة الملط، المرجع السابق، ص 349.

[2] أسامة حمدان الرقب، المرجع نفسه، ص 71.

الاحتيال تامة وتحتم العقاب على الجاني وتفرض العقوبة على فعل الشروع بالجريمة كما تفرض في حالة النصب التامة، فعقوبة الشروع الذي تضمنته نص المادة 30 من ق.ع.ج [1] رقم 157 لسنة 1966.

أما بالنسبة لعقوبة جريمة الاحتيال التامة والكاملة في أركانها ومحققة للضرر فان المشرع الجزائري لم يورد نص قانوني يعاقب على جريمة النصب أو الاحتيال الالكتروني والمعلوماتي لكنه أورده بنص المادة 372 من ق.ع.ج. وتنص على جريمة النصب التقليدية كما يلي: "**يعاقب بالحبس من سنة على الأقل إلى خمسة سنوات على الأكثر وغرامة من 20.000 دج إلى 100.000 دج** "[2]

الفرع الثاني: جرائم المساس بأنظمة المعالجة الإلكترونية

إن الجريمة المعلوماتية التي ترتكب في نطاق تقنية تكنولوجية متطورة ومتقدمة ومتزايدة الاستخدام في مختلف مناحي الحياة الاقتصادية والاجتماعية، وتأسيساً على ذلك فإن أضرارها تمتد وتتسع من خلال المس بأنظمة المعالجة الالية للمعطيات، ولقد كشف الاستخدام الكبير لأجهزة الكمبيوتر عن خطورة تتصل بهذا التصنيف من الاستعمال على عدة مصالح اجتماعية وفردية تهم المجتمع حمايتها، بل أكثر من ذلك فقد ازداد استخدام الحاسب الالي إلى حد يجلب من خلاله ضرورة الحاسب الالي لسير الحياة في المجتمع ، وهو ما نجم عنه ظهور قيم جديدة ترتبط بهذا الجهاز خاصة منها ضرورة ووجوب الحرص عليه وحمايته من كل اشكال الاعتداء. [3]

ويمكن القول بان المشرع الجزائري قد وضع النصوص التي تعاقب على الافعال التي تشكل جرائم معلوماتية وكان ذلك سنة 2001 المادة 144 مكرر ومكرر 1 ومكرر 2 والمادة 146 من ق ع ج ثم أصدر نصا تشريعيا سنة 2004 يشمل سبعة مواد من المادة 394 إلى المادة 394 مكرر

[1] المادة 30 من ق.ع.ج.

[2] المادة 372 من ق.ع.ج.

[3] غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الامارات العربية، 2000، ص 625.

7 وهذا تحت عنوان "المساس بأنظمة المعالجة الالية للمعطيات "القسم السابع مكرر من قانون العقوبات.

وأخيرا القانون رقم 04 – 09 المؤرخ في 05 اوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وعليه فإن الجرائم المتعلقة بالمساس بأنظمة المعالجة الالية للمعطيات في التشريع الجزائري تشمل: جريمة الدخول الغير المشروع لنظام المعلوماتي للتوقيع الالكتروني، وجريمة البقاء الغير مصرح به في النظام المعلوماتي وأخيرا جريمة اتلاف نظام المعالجة الالية للمعطيات.

أولا: جريمة الدخول الغير مشروع إلى النظام المعلوماتي للتوقيع الالكتروني

إن قانون العقوبات الجزائري تناول هذه الصورة من الجرائم حيث نصت المادة 394 مكرر 1 على "**يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من دخل عن طريق الغش في كل جزء من منظومة المعالجة الالية للمعطيات**[1]"

1 أركان جريمة الدخول الغير مشروع إلى النظام المعلوماتي للتوقيع الالكتروني

من المعروف في الجرائم ان الجريمة لها ركنين مادي ومعنوي ومن مبدا القانون الجنائي ان كل جريمة لابد لقيامها تحقق ركن مادي يتمثل في واقعة ترتب ضررا أو تشكل خطرا على المصالح المحمية قانونا. [2]

[1] المادة 394 من ق.ع.ج.

[2] أحسن بوسقيعة، الوجيز في القانون الجنائي العام، د ط، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 47.

مع ذلك فانه لا يكفي لقيام الجريمة وتقرير العقاب عنها مجرد تحقق ركنها المادي بل يجب ان يتحقق الركن المعنوي الذي يعكس اتجاه ارادیا خاطئا يستدل منه على نفسية الجاني اثناء ارتكابه للفعل. وبالعودة إلى نص المادة 394 مكرر ومن ق.ع.ج يتضح لنا أن الجريمة الدخول إلى نظام المعالجة الالية للمعطيات تقوم كسائر الجرائم على ركنين الركن المادي، والذي يلم السلوك الاجرامي الذي يترتب عنه الدخول غير المشروع إلى النظام والركن المعنوي المتمثل في القصد الجنائي.

أ- الركن المادي لجريمة الدخول الغير مشروع إلى النظام المعلوماتي للتوقيع الالكتروني

إن الركن المادي لهذه الجريمة من نشاط اجرامي يتمثل في تحقق الفعل وحيث أن السلوك الاجرامي قد يأخذ صورة ايجابية أو سلبية ويتطلب من الجاني مباشرة نشاط إيجابي ولا يمكن ان تتحقق الجريمة بنشاط سلبي، والملاحظ على هذا النوع من الجرائم أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة مثل الرشوة أو الاختلاس أو الزنا، بل تقع وترتكب عن كل شخص أياً كانت صفته سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا يفهم طريقة تشغيل النظام وسواء كان يستطيع أن يستفيد من الدخول. [1]

ويمكن القول بان مدلول كلمة الدخول ينصرف إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي أو لسيطرة على المعطيات التي يتكون منها. كما أن فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكاً غير مشروع، وإنما يتخذ هذا الوصف انطلاقاً من كونه قد تم دون وجه حق[2].

وبمعنى أدق لقيام هذه الجريمة يجب ان يتحقق اتصال فعلي من قبل الجاني بالبرنامج وعلى هذا الأساس يستحسن استخدام لفظ الاتصال بالنظام الالي، حيث أن الاتصال لا يثير الاشكال الذي يمكن أن يترتب على فعل الدخول، وعموماً فإن المعيار الذي يتم من خلاله تبيان الاتصال قد تم

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص343.

[2] محمد حمادة مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2004، ص 183.

بطريقة الغش وبالتالي تحديده، وقد تم بطريقة مشروعة أو بواسطة الغش هو انعدام حق الشخص في الاتصال بهذا النظام سواء كان هذا الانعدام يتعلق بكل النظام أو بجزء منه. [1]

وأما بخصوص طبيعة النمط من الجرائم فالأكيد انها من الجرائم الشكلية التي لا تتطلب لقيام ركنها المادي توافر نتيجة معينة وهي كذلك من الجرائم المستمرة لان سلوك الجاني يمتد فيها طالما ظل يستغل النظام بطريقة غير مشروعة.

ب- الركن المعنوي لجريمة الدخول الغير مشروع إلى النظام المعلوماتي للتوقيع الالكتروني:

لا تقوم جريمة الدخول عن طريق الغش لنظام المعالجة الالية للمعطيات في التشريع الجزائري الا بتوافر ركن القصد الجنائي ويقصد بالركن المعنوي الرابطة المعنوية أو الصلة النفسية أو العلاقة الأدبية التي تربط بين ماديات الجريمة ونفسية فاعلها وعليه لا تقوم المسؤولية الا إذا اتجهت إرادة الجاني إلى ارتكاب أفعال مجرمة في قانون العقوبات والقواعد المكملة له.

وتعد الجريمة الدخول إلى نظام الالي من الجرائم العمدية بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي المتكون من علم وإرادة، ذلك بان تتجه إرادة الجاني إلى فعل الدخول وان يعلم الجاني ان ليس له الحق في الدخول إلى النظام.[2]

والتالي يتحقق الركن المعنوي إذا كان دخول الجاني مسموحا به أو وقع في خطا في الواقع سواء كان يتعلق بمبدأ الحق في الدخول في نطاق هذا الحق كان يجهل بوجود خطر للدخول، أو كان يعتقد أنه خطأ أنه مسموح له بالدخول، وتأسيساً على ذلك فإذا توافر القصد الجنائي بعنصريه العلو والإرادة فانه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو اثبات القدرة على المهارة أو الانتصار على النظام.[3] وبالرجوع إلى نص المادة 394 مكرر

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري ق.م.ج، الجزائر، 2002، ص 321.

[2] امال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الجنائي والعموم الجنائية، جامعة الجزائر، الجزائر، 2002، ص60.

[3] محمد حمادة مرهج الهيتي، المرجع السابق، ص 187.

ق.ع.ج [1] يلاحظ أنه القصد الجنائي لا يكفي وحده وإنما يجب توافر قصد جنائي خاص وهو الغش وبهذا نكون بصدد جريمة الدخول غير المشروع للنظام الالي.

وطبقاً للقواعد العامة يجب ان يكون القصد الجنائي معاصرا للنشاط الاجرامي فتخلف القصد الجنائي لحظة بدء ذلك النشاط ينفي عن الفعل الصفة الاجرامية وبالتالي فان النشاط إذا بدا متجردا من القصد، كما لو وجد الجاني نفسه قد دخل إلى النظام أو إلى الجزء غير المسموح له بالدخول اليه عن طريق الخطأ ولطنه استحسن هذا الانتقال، ولم يقطعه مع العلم ان ليس له الحق في اجراءه فان القصد الجنائي لهذه الصورة لا يتحقق أولا يقوم لديه.

غير أن المشرع قد عالج هذه المسالة الأخيرة وذلك بتجريم البقاء الاحتيالي داخل النظام المعلوماتي من خلال جريمة البقاء غير المصرح به داخل النظام المعلوماتي.

2 العقوبة المقررة لجريمة الدخول الغير مشروع إلى النظام المعلوماتي للتوقيع الالكتروني

ان المشرع الجزائري تناول عقوبة الجنات الذين يقومون بالدخول الاحتيالي إلى النظام الالي بالحبس وغرامة مالية حددها بنص المادة 394 مكرر "يعاقب بالحبس من ثلاثة أشهر {03} إلى سنة {1} وبغرامة من { 50.000 دج إلى 100.000 } كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة {06} أشهر إلى سنتين { 02} والغرامة من { 50.000 دج إلى 150.000 دج }" يلاحظ أن المشرع الجزائري جرم الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية واعتبر هذا

[1] المادة 394 مكرر من ق.ع.ج .

التصرف في حد ذاته يشكل جريمة اذ يستخلص لأول مرة ان مجرد اختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية يعد انتهاكا للنظام المعلوماتي بطريقة غير مشروعة.[1]

ثانياً: جريمة البقاء غير المصرح به داخل النظام المعلوماتي

تطرق المشرع الجزائري هذه الجريمة من خلال نص المادة 394 مكرر من قانون العقوبات والتي تنص على ما يلي:" **أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات .....**" **وعلى ضوء هذا النص يمكن تعريف البقاء الاحتيالي في نظام المعلوماتية بانه: "كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول والنظر فيه أي في المعطيات التي يتضمنها وغيرها من التصرفات الغير مسموح بها والتي تشكل بدورها بقاء احتيالي** "[2]

أ/ الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي:

ويقصد كذلك بالبقاء التواجد داخل نظام المعالجة الالية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام وللعلم يتحقق البقاء المعاقب عليه داخل النظام المعلوماتي مستقلاً عن الدخول للنظام، أو قد يجتمعا ويكون البقاء معاقبا عليه استقلالاً عندما يكون الدخول إلى النظام مصرحا به والمثال على ذلك الدخول إلى النظام عن طريق الخطأ أو الصدفة حيث يتوجب في هذه الحالة على المتدخل قطع الاتصال والانسحاب فوراً من داخل النظام.

ولكن اذا بقي رغم ذلك فإنه يعاقب عن جريمة البقاء داخل النظام بعد المدة المحددة له للبقاء داخله اما في حالة دخول الجاني إلى النظام ضد إرادة من له الحق في السيطرة عليه. وبقائه داخل

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى، الجزائر،2011، ص 49.

[2] عبد الفتاح بيومي، المرجع السابق، ص 235.

النظام، بعد ذلك فانه في هذا يجتمع الدخول غير المصرح به والبقاء غير المشروع معاً،[1] وعلاوة على ذلك فإنه يتبين من النص السالف الذكر ان المشرع يفرض التزاماً من تحقيق الاتصال عنده يتمثل في عدم البقاء داخل النظام الذي حصل به الاتصال. بمعنى اخر يتوجب عليه الخروج من النظام وهذا خلال القيام بفعل إيجابي وقطع الاتصال وبالتالي يمكن القول بان هذه الجريمة تعد صورة من صور الجرائم الامتناع التي تتحقق بفعل إيجابي.

ويتحقق الركن المادي لجريمة الإبقاء على الاتصال الغير المشروع مع النظام الالي وهذا في الفرض الذي يجد فيه الشخص نفسه داخل النظام عن طريق الخطأ ومع ذلك يقرر البقاء داخل النظام وعدم قطع الاتصال به. و بكل بساطة هو مجرد البقاء الفعلي فيه حيث يقاس البقاء الغير مشروع بالمدة الزمنية التي يستعمل فيها الجاني النظام وبالتالي تكتمل هذه الجريمة مع اكتمال البقاء لمدة زمنية بعكس ما هو عليه الحال بالنسبة للدخول غير المشروع.

ب/ الركن المعنوي جريمة البقاء غير المصرح به داخل النظام المعلوماتي:

إن جريمة البقاء غير المشروع داخل النظام تعد من الجرائم العمدية التي يشترط فيها توافر القصد الجنائي العام المتمثل في عنصري العلم والإرادة، حيث يجب أن يعلم الجاني انه يقوم بالتجوال داخل نظام معلوماتي بطريقة غير شرعية، كما يجب أن تتجه ارادته في نفس الوقت إلى البقاء فيه وعدم قطع الاتصال مع هذا النظام، وتعد جريمة البقاء في النظام الالي لمعالجة المعطيات من الجرائم الشكلية التي لم يتطلب المشرع لتحقيقها نتيجة معينة وهي جريمة مستمرة تتطلب تدخلاً مستمراً من الجاني.

2 العقوبة المقررة لجريمة البقاء غير المصرح به داخل النظام المعلوماتي:

[1] محمد حماد مرهج الهيتي، المرجع السابق، ص 190.

بالرجوع إلى نص المادة 394 مكرر الفقرة الثانية[1] يلاحظ ان المشرع الجزائري قد شدد في العقاب بالنسبة لجريمتي الدخول والبقاء في النظام المعلوماتي حيث ضاعف من العقوبة إذا ترتب عن الدخول والبقاء حذف أو تغير لمعطيات المنظومة الالية، وكذلك في الحالة التي يتم فيها تخريب نظام اشتغال المنظومة فان العقوبة تشدد أيضا. فضلا عن ذلك تضاعف العقوبة إذا استهدف الجريمة الدفاع الوطني أو الهيئات أو لمؤسسات الخاضعة للقانون العام، وهذا حسب المادة 394 مكرر 3 [2] من قانون العقوبات الجزائري.

ثالثا: جريمة اتلاف نظام المعالجة الالية لمعطيات التوقع الالكتروني

تطرق المشرع الجزائري إلى هذا النمط من الجرائم من خلال ما جاءت به نص المادة 394 مكرر1[3] من قانون العقوبات الجزائري والتي تنص على انه:" **يعاقب بالحبس من ستة 06 أشهر إلى ثلاث سنوات وبغرامة مالية من 5000.00 دج إلى 20.000.000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الالية أو أزال أو عدل المعطيات التي يتضمنها** ".

من خلال هذا النص ومن اجل معالجة عناصر هذه الجريمة يتوجب تحديد معنى الاتلاف والوسائل التي يتحقق بها الاتلاف. ويعرف البعض الاتلاف بجعله الشيء غير الصالح للاستعمال أو بإعدام صلاحيته أو تعطيله سواء صفة كلية الجزئية، ويقصد كذلك بالإتلاف افناء مادة الشيء أو هلاكه كلياً أو جزئياً وبالتالي توقف الشيء تماماً على أن يؤدي منفعة، ولو لم تفن مادته سواء كان هذا التوقف كلياً أو جزئياً في وظيفته المرصود لها على النحو الاكمل.

1 – أركان جريمة إتلاف التوقيع الإلكتروني

أ – الركن المادي لجريمة الإتلاف

[1] الفقرة الثانية من المادة 394 من ق.ع. ج

[2] أنظر المادة 394 الفقرة الثالثة من قانون العقوبات.

[3] المادة 394 الفقرة الأولى من ق.ع.ج

وعلى ضوء هذه التعريفات يمكن القول بان الاتلاف لا يتحقق فقط في التأثير على مادة الشيء بل يتحقق كذلك حتى في حالة الانتقاص من قيمته المالية ذلك ان الفعل الذي يترتب عنه فقدان الشيء لقيمته المالية أو الانتقاص منها هو الذي يحقق الاعتداء الذي يعاقب عليه القانون على اعتبار أنه قد ذهب بأهمية الشيء بالنسبة لمالكه.

أو هو اضافة معطيات جديدة على دعامة الخاصة بها سواء كانت خالية أم كان يوجد عليها من قبل، أما التعديل فيعني "تغيير البيانات أو المعلومات الموجودة داخل النظام واستبدالها بمعطيات أخرى وذلك بإمداده بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها.[1]

أما فعل الازالة تعرف الازالة بانها محو جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2]، وعملية ازالة المعطيات هي مرحلة لاحقة على ادخال المعطيات، فالإزالة تفترض الوجود السابق لعملية الادخال وكقاعدة عامة فان صور الركن المادية في جريمة الاتلاف. يتم عن طريق برامج تتلاعب في المعطيات وذلك بمحوها كليا أو جزئياً أو بتعديلها سواء باستخدام القنبلة المعلوماتية أوعن طريق برامج الفيروسات بصفة عامة.

لا سيما أن الفيروس المعلوماتي يصممه مجرم معلوماتي على درجة عالية من الذكاء وذو قدرة عالية في تقنية المعلومات وهذه الافعال المتمثلة في الادخال والمحو والتعديل جاءت على سبيل الحصر فلا يقع تحت طائلة التجريم اي فعل اخر.[3]

- **النتيجة الاجرامية**

معظم الجرائم الواقعة على المعطيات خطر لا يشترط لوقوعها ان يترتب على السلوك الاجرامي عدوان فعلي على المعطيات وانما يكتفي فيها لقيام الجريمة بالعدوان المحتمل أو التهديد بالخطر أي

[1] عبد الفتاح بيومي، المرجع السابق، ص 44.

[2] امال قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار هومة ، الجزائر، 2007، ص 122 .

[3] بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص 189.

بخطر العدوان فعلي على المعطيات في سريتها أو اتاحتها أو سلامتها وتكاملها، فجريمة الدخول أو البقاء غبر المصرح بهما خطر في الاصل ،لكن جريمة التلاعب بالمعطيات جريمة ضرر– جريمة مادية – إذ لا يكفي أن تهدد سلامة المعطيات بخطر الازالة أو التعديل أو الادخال، وإنما لابد أن يقع ضرر فعلي على هذه المعطيات يتمثل في تغيير حالتها فالمشرع يتطلب نتيجة معينة من خلال السلوك الاجرامي في هذه الجريمة وهي تغيير حالة المعطيات .[1]

ب– الركن المعنوي

نصت المادة 394 مكرر 1 من ق.ع.ج أن جنحة اتلاف التوقيع الالكتروني من الجرائم العمدية التي يتطلب قيامها توافر الركن المعنوي الذي يتخذ صور القصد الجنائي العام بعنصريه العلم والارادة ، وترتيبا على ذلك فيجب ان يعلم الجاني انه يقوم بإتلاف توقيع الكتروني عن طريق الادخال أو المحو أو التعديل في بياناته بالإضافة إلى اتجاه ارادته إلى ارتكاب الفعل المادي المكون للجريمة وتحقيق النتيجة الاجرامية المترتبة على ذلك النشاط، وهي الحاق الضرر بصاحب التوقيع وجعل توقيعه الالكتروني غير صالح للاستعمال أو معيبا يفقده وظيفته ويهز ثقة المتعاملين مع صاحب التوقيع في شخصه.

أما القصد الجنائي الخاص فإن المشرع الجزائري في المادة 394 مكرر 1 لم يستخدم أي عبارة تدل على ضرورة توافره ومن ثمة فإن توافر القصد العام كاف لقيام هذه الجريمة لأن القصد الخاص هو انصراف العلم والارادة إلى وقائع لا تدخل ضمن عناصر الجريمة وأركانها، ولفظ الغش الذي استخدمه المشرع يدل على أن الجريمة عمدية ولا يَدَلُ على القصد الخاص.[2]

2 – العقوبات المقررة لجريمة الاتلاف

[1] محمد خليفة، المرجع السابق، ص 184-186.

[2] عزيزة لرقط، المرجع السابق، ص 115.

يقرر قانون العقوبات الجزائري في مادته 394 مكرر 1 على مرتكب جريمة الاتلاف عقوبة تتمثل في الحبس والغرامة كما تقرر عليه المادة 394مكرر 6 عقوبة تكميلية تشترك فيها مع باقي جرائم المعطيات. طبقا لنص المادة 394 مكرر 1 فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي هي الحبس من 06 أشهر إلى 03 سنوات والغرامة التي تتراوح بين 500.000 دج إلى 2.000.000 دج.

والملاحظ ان جريمة التلاعب بالمعطيات تفوق عقوبة جريمة الدخول أو البقاء غير المصرح سواء كانت الأخير في صورتها البسيطة ام المشددة لان صورتها البسيطة لا تؤدي إلى اضرار معينة تلحق بالمعطيات أو نظام معالجتها وحتى في صورتها المشددة وان أدت إلى نفس النتائج التي تؤدي اليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها أو اتلافها، فان العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر مرتكبها القصد الجنائي للتلاعب بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشدد فالموقف النفسي لكل واحد منها له اتجاه مختلف. [1]

المطلب الثاني: جرائم الاعتداء على التوقيع الإلكتروني في إطار قانون 04/15

بالرغم من ان النظم القانونية في بعض الدول توفر الحماية الخاصة للبيانات الشخصية في مجال التعاملات الالكترونية، أن أنه يتصور أن يتم التعدي على هذه البيانات والمعلومات بأي صورة، نظراً لطبيعة التعاملات الالكترونية، وإمكانية الاطلاع على البيانات والدخول اليها في أي مكان، ولهذا تفطن المشرع الجزائري لحماية هذا الاعتداء وذلك بتعديل قانون العقوبات.

كما جرم من خلال القانون 15 - 04 المتعلق بالتوقيع والتصديق الالكترونين العديد من الجرائم الماسة بالتوقيع الالكتروني وسنتطرق إلى هذا المطلب من خلال تناوله في فرعين، **الفرع الأول**

[1] محمد خليفة، المرجع السابق، ص 191.

:جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة التصديق والتوقيع الالكتروني، أما **الفرع الثاني** جريمة حيازة أو إفشاء بيانات توقيع الكتروني موصوفة خاصة بالغير.

الفرع الأول: جريمة الادلاء بإقرارات كاذبة للحصول على شهادة تصديق وتوقيع الكتروني:

تنص المادة 66 من قانون 15 /04 على انه" **يعاقب بالحبس من ثلاث {03 } أشهر ثلاث{ 03} سنوات وبغرامة من عشرين ألف دينار {20.000 دج }إلى مائتي ألف دينار { 200.000 دج} أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكترونية موصوفة**" [1].

1- اركان جريمة الادلاء بقرارات كاذبة للحصول على شهادة تصديق وتوقيع الكتروني

إن المشرع عند نصه لهذه الجريمة، كان يهدف إلى إعطاء شهادة تصديق الالكترونية موصوفة، مصداقية عند طالبها، لان مؤدي الخدمات لا يجمع الا المعلومات الصحيحة

والضرورية عنه كما يهدف إلى خلق ثقة لدى الغير المتعامل مع صاحب هذه الشهادة مما يدفعه قدما إلى التعاقد معه خاصة في مجال التجارة الالكترونية، وتقوم هذه الجريمة على ركنيين هما:

أولاً: الركن المادي

يتحقق متى قام الجاني بالتصريح بمعطيات كاذبة، وهي البيانات الضرورية للحصول على شهادة تصديق الكترونية موصوفة، إلى مؤدي خدمات التصديق الالكتروني وهو شخص الذي له ترخيص مزاولة هذه المهنة[2].

ثانياً: الركن المعنوي

[1] أنظر المادة 66 من القانون 15-04، السالف الذكر.

[2] عبد الفتاح بيومي حجازي, التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، ط 1، ودار الفكر الجامعي، الإسكندرية ، 2006 ص 70.

ان فعل إعطاء اقرارات كاذبة للحصول على شهادة تصديق الكترونية موصوفة يعتبر فعلاً عمدياً يتحدد من خلاله ماهية الركن المعنوي لهذه الجريمة، فلا يتصور اذن تحقق الجريمة بصورة غير عمدية فالإعطاء في حد ذاته يفيد معنى الإرادة والسعي والعلم معا.

2- العقوبة المقررة لجريمة الادلاء بقرارات كاذبة للحصول على شهادة تصديق الكتروني:

النص يعاقب على جريمة التصريح عمداً بمعطيات كاذبة، لأنه لا يعقل ان يحدث عن طريق الخطأ، وهذا وفق لما جاء في المادة 66 من القانون 15- 04 بنصها على انه "**:كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكترونية " والعقوبة كما حددها المشرع بنفس المادة هي الحبس من 03 أشهر إلى 03 سنوات وبغرامة مالية من 20.000 دج إلى .200 000 دج أو بإحدى هاتين العقوبتين**".

ولن يكون هناك خطا عند الإدلاء بمعطيات صحيحة وان وجدت فإن المشرع أعطى الحق لمؤدي خدمات التصديق بإلغائها كما بينته المادة 45 الفقرة الأولى من قانون 15-04 بنصها على أنه "**ويلغي مؤدي خدمات التصديق الالكتروني أيضا شهادة التصديق الالكترونية الموصوفة عندما يتبين:**

أنه قدم منحها بناء على معلومات خاطئة أو مزورة أو إذا أصبحت المعلومات الواردة في شهادة التصديق الإلكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات التوقيع الإلكتروني".[1]

إذن مما سبق نلاحظ أن المشرع قد عاقب على جريمة الإدلاء بإقرارات كاذبة بنص القانون كما ذكرنا سابقا واعتبرها جريمة عمدية وان وقعت عن طريق الخطأ وتم اكتشافها، فان المشرع أعطى صلاحية الغاء الشهادة لي مؤدي خدمات التصديق.

الفرع الثاني :جريمة حيازة أو افشاء أو استعمال بيانات انشاء توقيع الكتروني موصوفة خاصة للغير :

[1] المادة 45 الفقرة 01 من قانون 15-04 ، السالف الذكر.

يمكن أن يتم الاعتداء على التوقيع الالكتروني عندما يتم صنع أو حيازة برنامج لإعداد التوقيع الالكتروني وتقوم هذه الجريمة بتوفر كل من الركن المادي والركن المعنوي[1] .

أولاً: جريمة حيازة بيانات انشاء التوقيع الالكتروني

من بين جرائم الاعتداء على التوقيع الالكتروني جريمة حيازة بيانات انشاء التوقيع الالكتروني وهذه الجريمة معقدة ومستحدثة في القانون الجزائري وللتعرف عليها كثيرا سنتناول أركانها والعقوبة المقررة لها وفق القانون الجزائري على النحو التالي:

1- أكان الجريمة حيازة بيانات انشاء التوقيع الالكتروني

أ- الركن المادي

بما أن الحيازة هي فعل مادي يتحقق بمجرد قيام الجاني بحفظ البيانات وجعلها بحوزته دون اذن، ويتمثل ذلك في صور عديدة وهي صناعة نظام معلوماتي أو برنامج لإعداد توقيع الكتروني أو حيازتهما بغرض اعداد توقيع الكتروني دون علم أو موافقة صاحبه وهذا ما جاء به نص المادة 68 من قانون 15-04 حيث نصت على أن " ك**ل من يقوم بحيازة او.....بيانات توقيع الكتروني موصوف خاصة بالغير**[2] "، قد يكون الجاني شخص طبيعي أو اعتباري مرخص له بإعداد التوقيع الالكتروني لا مناط التجريم هنا أن يتم عمله رغما ًعن إرادة صاحبه أي الشخص المعني بالتوقيع الالكتروني ، أما الوسيلة المستعملة في الحيازة أو الافشاء أو استعمال البيانات.

فهي مجموعة أجهزة والأدوات التي يختلس بها الجاني معلومات عن التوقيع الالكتروني القائمة بالفعل، أو يقوم بصناعة برنامج جديد للقيام بعمله غير المشروع، [3]مع العلم انه لكي تقوم الجريمة يجب أن يكون للنظام القدرة على عمل التوقيع الالكتروني

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، د ط، دار الفكر الجامعي، مصر ،2002، ص607 .

[2] المادة 68 من القانون 15 - 04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين السالف الذكر.

[3] عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 161 ـ 162.

.والملاحظ ان المشرع الجزائري قد منح اختصاص انشاء التوقيع الالكتروني حكرًا لمؤدي خدمات التصديق الالكتروني، التي لا يمكنها مباشرة عملها إلا بعد الحصول على الترخيص، وفقاً للأشكال القانونية المقررة التي وردت بنص المادة 35 الفقرة 03 من القانون 15 04 التي تنص على" **لا يمكن حامل هذه الشهادة تأدية خدمات التصديق الالكتروني الا بعد الحصول على ترخيص،**[1] .

بل وأنه لا يمكنها جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة ،وهذا ما جاءت به نص المادة 43 من نفس القانون السابق التي تنص على" **لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات ،الا بعد موافقته الصريحة** ،....."[2]، أي حتى وإن كان هذا الشخص المرخص له بإعداد التوقيع الالكتروني، فاذا قام بذلك دون موافقة صاحبه عند الفعل فانه يعد جريمة.

ب . الركن المعنوي

لكي يتحقق الركن المعنوي للجريمة يستوي بأن يكون الجاني عالما بأن المعطيات متحصلة من الجرائم المنصوص عليها في القانون وان ارادته متجهة إلى فعل احتجاز هذه البيانات والاحتفاظ بها بطريقة غير مشروعة دون اذن صاحبها أو أي جهة رسمية مخولة بذلك وبهذا التصوير يتوفر القصد الجنائي حتى وان ترتب الاحتفاظ بالمعطيات عن طريق الإهمال أو النسيان اذ العبرة بمصدر البيانات والذي هو متحصل من جريمة على خلاف المشرع الفرنسي الذي يجعل الركن المعنوي منتفيا في مثل هذه الحالة على اعتبار انعدام إرادة الجاني. ومنه يمكننا القول بأن الركن المعنوي لجريمة حيازة بيانات انشاء توقيع الكتروني هي أن يكون اتجاه إرادة الجاني إلى صنع أو حيازة برنامج لإعداد التوقيع الإلكتروني، وهو الاعتداء على التوقيع الالكتروني ليحقق غرضه .[3]

2- العقوبة المقررة لجريمة حيازة بيانات انشاء التو قيع الالكتروني

[1] المادة 35 الفقرة 03 من القانون 15 -04 ، السالف الذكر.

[2] المادة 43 من القانون 15 -04 ، السالف الذكر.

[3] زيبحة زيدان، ، المرجع السابق، ص .72 .

أقرت في نص المادة 68 من قانون 15-04 لهذه الجريمة عقوبة تمثل في الحبس من ثلاثة أشهر إلى 03 سنوات وبغرامة من مليون دينار 1.000.000 دج إلى خمسة مليون دينار جزائري5.000.000 دج أو بإحدى هاتين العقوبتين فقط

[1].كما يعاقب مؤدي الخدمات الذي أخل بأحكام المادة 43 وجاءت المادة 71 من القانون نفسه بأنه يعاقب " **بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من مائتي ألف دينار 200.000دج إلى مليون دينار جزائري 1.000.000 دج أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة و 43 من هذا القانون.**"

ثانياً: جريمة إفشاء بيانات انشاء التوقيع الإلكتروني

يتضح من نص المادة 42 [2]من القانون 15- 04 والتي نصت على أنه" :**يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة"**، أي أن المشرع الجزائري اوجب على مؤدي خدمات التصديق الإلكتروني الالتزام باحترام سرية بيانات التوقيع الإلكتروني ناهيك عن نص المادة[3] 68 من قانون 15-04 التي تناولت افشاء بيانات توقيع الكتروني موصوفة خاصة بالغير، وعرفت المادة 07[4]من نفس قانون التوقيع الالكتروني الموصوف" **هو التوقيع الذي تتوفر فيه المتطلبات الاتية:**

-أن ينشأ على أساس شهادة تصديق الكترونية موصوفة

-أن يرتبط بالموقع دون سواه ان يمكن من تحديد هوية الموقع،

-أن يكون مصمما بواسطة الية مؤمنة خاصة، بإنشاء التوقيع الالكتروني

-أن يكون منشاء بواسطة وسائل تكون تحت التحكم الحصري للموقع،

[1] المادة71 من القانون 15-04 ، السالف الذكر

[2] المادة 42 من القانون 15 -04 ، السالف الذكر.

[3] المادة 68 من القانون 15 -04 ، السالف الذكر.

[4] المادة 07 من القانون 15 -04 ، السالف الذكر.

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

ناهيك عن نص المادة 08 التي جاءت بأن التوقيع الالكتروني الموصوف مماثلا للتوقيع المكتوب والمادة 09 التي تناولت عدم تجريد التوقيع الالكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب:

شكله الالكتروني، أوانه لا يعتمد على شهادة تصديق الكتروني موصوفة، أوانه لم يتم إنشاؤه بواسطة الية مؤمنة لإنشاء التوقيع الالكتروني "من خلال المواد التي تطرقنا له لاحظنا أن المشرع الجزائري أنه بين التوقيع الالكتروني وفرض السرية وعدم افشاء البيانات.

1.اركان جريمة إفشاء بيانات انشاء التوقيع الإلكتروني

سنتطرق لهذه الأركان فيما يلي

أ. الركن المادي لهذه الجريمة، يمنع أن تقوم هذه الجريمة أيضا باستعمال هذه البيانات أغراض أخرى، غير الغرض الذي قدمت من أجله .[1]كما يتطلب لقيام هذه الجريمة، إلى جانب الركن المادي.

ب . الركن المعنوي القصد العام دون الخاص، والمتمثل في اتجاه إرادة الجاني إلى إفشاء بيانات التوقيع الإلكتروني أو اساءة استخدامها مع علمه بذلك، وقبول النتائج المترتبة على هذا السلوك الإجرامي، الذي لا يتصور وقوعه بطريق الخطأ، ونظرا ًلخطورة إفشاء بيانات التوقيع الإلكتروني.

2. العقوبة المقررة لجريمة إفشاء بيانات انشاء التوقيع الإلكتروني

عاقب المشرع على القيام بهذه الجريمة بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مائتي ألف دينار إلى مليون دينار أو بإحدى هاتين العقوبتين[2]، كما يعاقب بالحبس من ثلاثة أشهر

[1] المادة 42 الفقرة 02 من القانون 15-04، السالف الذكر.

[2] المادة 72 من القانون 15-04، السالف الذكر.

إلى سنتين وبغرامة من عشرين ألف دينار إلى مائتي ألف دينار جزائري، أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق[1].

ثالثاً: جريمة استعمال بيانات إنشاء التوقيع الإلكتروني

تنشأ هذه الجريمة من خلال الفقرة 03 من نص المادة 61 من القانون 15-04 والتي تنص على أنه" **لا يجوز لصاحب شهادة التصديق الإلكتروني عند انتهاء صلاحيتها أوعن إلغائها، استعمال بيانات إنشاء التوقيع الموافقة لها، من أجل توقيع أو تصديق هذه البيانات نفسيا من طرف مؤدي آخر لخدمات التصديق الإلكتروني.**"

1. اركان جريمة استعمال بيانات انشاء التوقيع الإلكتروني

ويتطلب لقيام هذه الجريمة توفر الركن المادي والركن المعنوي اللذان سنتطرق لهما فيما يلي.

أ. الركن المادي لجريمة استعمال بيانات إنشاء التوقيع الإلكتروني

يتمثل في استعمال بيانات إنشاء التوقيع الإلكتروني من طرف صاحب الشهادة نفسه، كما أنه قد يتحقق الركن المادي باستعمال أو إساءة استعمال بيانات بإنشاء التوقيع الإلكتروني دون رضا صاحب شهادة التصديق الإلكتروني، من طرف شخص غير مرخص له باستخدام هذه البيانات، وفي الغالب يكون هذا الشخص ذو درجة عالية من العلم والحرفية في مجال المعلوماتية[2].

ب . الركن المعنوي لجريمة استعمال بيانات انشاء التوقيع الإلكتروني

إن الركن المعنوي لجريمة استعمال بيانات انشاء التوقيع الالكتروني يتمثل في القصد الجنائي العام والقصد الجنائي الخاص أي ان الجاني عند استعمال بيانات انشاء التوقيع الالكتروني يجب ان يكون له العلم الكافي بالضرر الذي قد يلحقه بغيره ناهيك عن اتجاه ارادته نحو تحقيق نتيجة السلوك الاجرامي الذي قام به وعمل على تحقيق استعمال واستغلال بيانات شخص اما ان يكون هذا الشخص لا يعرف بموضوع جريمة الاستعمال أوانه تم اغفاله في هذا الشأن.

[1] المادة 73 من القانون 15 -04 ، السالف الذكر.

[2] عامر محمود الكسواني، التجارة عبر الحاسوب دار الثقافة للنشر والتوزيع، الأردن، 2008 ، ص181 .

2. العقوبة المقررة لجريمة استعمال بيانات انشاء التوقيع الإلكتروني

عاقب على هذه الجريمة بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من مليون دينار 1.000.000دج إلى خمسة ملايين دينار 5.000.000 دج[1]. مع الإشارة إلى انه سبق وأن صدر القانون 03-15 المتعلق بعصرنة العدالة ونص في مادته17 على جريمة الاستعمال غير القانوني لعناصر الشخصية المتصلة بإنشاء التوقيع الإلكتروني والذي يتعلق بشخص آخر، وقرر له عقوبة وتنص هذه المادة على أنه" **يعاقب بالحبس من سنة 1 إلى خمسة سنوات وبغرامة تتراوح بين مائة ألف دينار 100.000 دج إلى خمسمائة ألف دينار 500.000 دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بشخص آخر**[2].

كذلك نص في مادته 18 على جريمة حيازة شهادة إلكترونية منتهية الصلاحية أوتم إلغائها، وتنص المادة على أنه" **يعاقب بالحبس من سنة 01 إلى خمس 05 سنوات وبغرامة تتراوح بين مائة ألف دينار 100.000 دج إلى خمسمائة ألف دينار 500.000 دج كل شخص حائز شهادة إلكترونية يواصل استعمالها رغم علمه بانتهاء صلاحيتها أو إلغائها.** "[3] وبالإضافة إلى هذه الجرائم هناك نصوص جزائية خاصة أخرى في مجال حماية البيانات الشخصية الإلكترونية، حيث تلزم البنوك فيما يتعلق بواجباتها المرتبطة بتحقيق الأمن في مجال أنظمة الدفع بحفظ سرية المعطيات الشخصية التي تتحصل عليها من زبائني[4].

والحقيقة أن الالتزام بحفظ السر المصرفي التزام عام يقرر على البنوك والمؤسسات المالية بموجب المادة 117 من الأمر 03-11 المتعلق بالنقد والقرض[5]، والمعدل والمتمم، وهو من الالتزامات

---

[1] المادة 68 من القانون 15 – 04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، السالف الذكر.

[2] الأمر رقم 15 –03 المؤرخ في 01 فيفري 2015، يتعلق بعصرنة قطاع العدالة، ج، ر عدد 06 ، الصادرة بتاريخ 10 فيفري 2015.

[3] المادة 18 من القانون 03 – 15 المتعلق بعصرنة العدالة، السالف الذكر.

[4] حيث تنص 10 من الأمر رقم 07 / 05 ، المؤرخ في 25 ديسمبر 2005، يتضمن امن الدفع ج .ر عدد 37 ، الصادر بتاريخ 04 جوان 2006، على انه" **يتعين على المشاركين في نظام الدفع ضمان سرية وصحة المعلومات التي تمر عبر أنظمة الدفع**".

5 الأمر رقم 03-11، المؤرخ في 26 غشت 2003، يتعلق بالنقد والقرض، ج .ر العدد 52، الصادرة بتاريخ 27 غشت 2003، الملغى بالقانون 12 يونيو 2023، يتضمن القانون النقدي والمصرفي، ج.ر العدد 43، الصادرة بتاريخ 27 يونيو 2023.

الأساسية التي تقوم عليها المهنة المصرفية، بالنظر إلى حساسية المعلومات التي قد يتحصل عليها البنك بمناسبة تقديم خدمات بنكية الكترونية.وبالرغم من ذلك فإنه فيما يتعلق بتوقيع الجزاء الجنائي أحاله قانون النقد والقرض إلى النصوص العامة الواردة في قانون العقوبات، وبالرجوع إلى المادة 303[1] و303 مكرر[2] من هذا القانون نجد المشرع يقرر عقوبة تقدر بالحبس من شهر إلى ستة أشهر، وبغرامة من 500 إلى 5000 دج.

والملاحظ أن هذه العقوبة تمتاز بالسرعة والمرونة والتطور السريع في عناصرها بصفة عامة وطبيعتها بصفة خاصة إذا ما تمت مقارنتها بالعقوبات في جرائم أخرى، وكان الأجدر بالمشرع البنكي أن يقرر نص خاص في قانون النقد والقرض، يتلاءم وخطورة الدور الذي تؤديها البنوك والمؤسسات المالية، بحيث يميز بين العقوبات المقررة على المستخدمين كشخص طبيعي، والعقوبات المقرر على البنك كشخص معنوي.

[1] المادة 303 من ق.ع.ج.

[2] المادة 303 مكرر 1 من ق.ع.ج

خلاصة الفصل الثاني

التوقيع الالكتروني مصلحة من المصالح الجديرة بالحماية لكونه عنصر أساسي تقوم عليه التجارة الإلكترونية ، بدأ الاعتماد عليه بشكل كبير في كافه المعاملات القانونية بل أصبح احدى وسائل الحماية المدنية للمعاملات المتعلقة بالتجارة الإلكترونية، وإزاء هذه الأهمية المتزايدة وجب توفر حماية تقنية وجنائية ، لبث الثقة والامان في التوقيع الالكتروني لجا التقنيون إلى استعمال التشفير لحمايته من المخاطر التي قد يتعرض له، من تزوير، تخريب، اتلاف، سرقه وتشويه والابتزاز والتلف ، والاستخدام غير المرخص وغير القانوني لذلك تم الاعتماد تكنولوجيا التشفير الذي يعتبر تقنية قديمة استعملت منذ الازل شهد تطور عبر التاريخ وما زال في تطور مستمر حتى الان.

فعندما يضع المشفرون نظام التشفير يأتي آخرون ويحاولون فك هذا النظام ومعرفة سر الشفرة فيلجا المشفرون لنظام جديد ، يعتمد على الخوارزميات الرياضية الذكية لكن التشفير وحده لا يكفي لحماية التوقيع الالكتروني، فقد حتم ذلك ضرورة تدخل طرف ثالث يكون مهمته التعريف بالأطراف وضمان صله الشخص بتوقيعه ، تسمى بجهات المختصة بإصدار شهادات التصديق الالكتروني، لكون العقود تبرم بين غائبين باختلاف الزمان والمكان عبر شبكه اتصال مفتوحة.

هذا الأمر استلزم وجود هذا الطرف الثالث المحايد يتمثل في افراد أو شركات أو جهات مستقله وتسمى بجهات التصديق أو التوثيق الالكتروني وتعمل بترخيص من السلطات المختصة في الدولة وتحت اشرافها ضمن احكام تحدد ، نظامها وماهيتها والدور الذي تقوم به من خلال تقديم شهادات الكترونيه تحدد بها هويه الموقع وتتحقق من صحة التوقيع وارتباطه بصاحبه.

فقد أصدرت العديد من التشريعات التي تناولت تنظيم هذه الجهة بأحكام خاصة تجعلها خاضعة لرقابة الدولة وتحمل مسؤولية اعمالها تلعب جهات التصديق أو التنسيق دور أساسياً، اصدار شهادات التصديق الالكتروني وذلك التحقق أولاً من هوية الشخص الموقع، وثانياً اثبات مضمون التبادل الالكتروني، وثالثاً اصدار مفاتيح التشفير ،كل خطأ في الشهادة تقوم مسؤوليه مقدم خدمات التصديق كما يجوز اثبات كما يجوز لها اثبات عدم وجود اي خطا من جهة، اذا أدت دورها في حفظ لسرية البيانات وصحتها ولا شك أن عبء الاثبات يقع عليها هو أمر في غايه التعقيد والدقة ، نظراً لأهمية شهادة التصديق لقد عرفت التشريعات هذه الشهادة ونظمتها كما اعترفت بالشهادات التصديق والتوقيعات الإلكترونية التي تصدر من جهات التصديق الأجنبية فقد نظمت المادة 12 من قانون الاونيسترال النموذجي بشأن التوقعات الإلكترونية لعام 2000.

أما في ما يخص المبحث الثاني فقد لاحظنا ان المشرع الجزائري لم يسن أي قوانين تنظم جريمة التزوير أو الاحتيال الالكتروني بل طبق قواعد ونصوص قانون العقوبات الخاصة بالتزوير والاحتيال في التوقيع التقليدي، بالرغم من أنهما يختلفان في الكثير من الجوانب منها الركن المادي من حيث المحل والركن المعنوي من حيث القصد الجنائي العام والخاص، فنجد أيضاً أن المشرع بهذه الجرائم ورغم حداثتها إلا أنه سن نصوص قانونية لا تتوافق مع تطور وسرعة ومرونة هذه الجرائم ،إذ أن هذه النصوص تعتبر غامضة غير ملائمة لهذا التطور الاجرامي الحديث في مجال التوقيع الالكتروني بصفة خاصة والتجارة الالكترونية بصفة عامة.

يجب توفير الحماية الجنائية للتوقيع الالكتروني كونه مصلحة جديرة بالحماية، لذلك وكبه تطور تشريعي ينظمه ويحدد مصداقيته، يحميه بالتجريم والعقاب، التزوير من أكثر الجرائم التي تهدده إلى جانب جرائم معلوماتية اخرى، فقد تبنت التشريعات الوطنية تجريم الاعتداء عليه لازالت الجهود الوطنية تتضافر لمكافحة الجرائم الإلكترونية.

خاتمة

خاتمة

أصبحت المعاملات الالكترونية حقيقة قائمة في العالم المعاصر، وهي أخذه في التطور السريع ولكنها تواجه إشكالية تتعلق بالإثبات في وقت هي بحاجة إلى وسائل غير تلك التقليدية المتعارف عليها حتى تتماشى مع الحلول القانونية نتيجة الاتساع المذهل لحجم تلك التجارة والمعاملات كافة، مما استوجب إدخال التوقيع الالكتروني محل التوقيع التقليدي ليتوافق مع طبيعة التصرفات القانونية وكذا إبرام العقود التي تنفذ باستعمال الوسائل التقنية الحديثة.

يعد التوقيع الالكتروني مصطلح دخيل على الفكر القانوني، مما دفع التشريعات الدولية والوطنية إلى إصدار قوانين لتنظيم التوقيع الالكتروني ولإزالة الغموض عن هذا المصطلح الحديث، حيث أصدرت أحكاما بينت ماهيته وقوته الثبوتية، ولقد اعترفت كل التشريعات التي نظمت التوقيع الالكتروني، ومن بينها التشريع الجزائري بحجية هذا الأخير في الإثبات توازي الحجية المعترف بها للتوقيع التقليدي، شريطة أن ينشأ بواسطة وسائل خاصة بالموقع وخاضعة لسيطرته وحده دون غيره، وارتباطه ببيانات المحرر الالكتروني بطريقة يكشف بها عن أي تغيير لاحق لبيانات المحرر او للتوقيع ذاته.

كما يتعين أن يعرف التوقيع الالكتروني بهوية صاحبه والتعبير عن رضاه بمحتوى المحرر الالكتروني، وأخيرا ان يتميز بشكل فريد بارتباطه بالشخص صاحب العلاقة. لكن ليس معنى ذلك ان التوقيع الالكتروني الذي لا يحقق هذه العناصر لا يتمتع بأية حجية، بل انه يتمتع بذات حجية التوقيع الالكتروني إذا ما استطاع ان يتمسك به لإقامة الدليل على كفاءة منظومة تشغيل هذا التوقيع، كما أنه يمكن للأطراف الاتفاق على تنظيم حجية التوقيع الالكتروني مالم برد في هذا الاتفاق ما يخالف النظام العام

من خلال ما تطرقنا له في هذا الموضوع نرى ان المشرع الجزائري قد وفق نسبيا عند تناوله التوقيع الالكتروني، حيث ان فكرة التوقيع الالكتروني جعلت من التوقيع التقليدي يتراجع ذلك لما يتميز به التوقيع الالكتروني من سرعة شديدة في مجالات الحياة المختلفة، وبما انه اصبح واقعة مستجدة

على الفكر القانوني، فقد صدرت العديد من التشريعات التي، تفصله وتعطيه النطاق القانوني الخاص به.

ومن هذه التشريعات نجد المشرع الجزائري، الذي نظم التوقيع الالكتروني، في قانون-04 15المتعلق بالتوقيع، والتصديق الالكترونيين فمنحه من خلاله تعريفا وحدد انواعه وخصائصه وحجيته، فالتوقيع الالكتروني يقوم على استخدام التقنيات الحديثة من حاسوب وانترنت وغيرها، لذا فهو يتخذ شكل بيانات الكترونية تنفذ عن طريق مجموعة من الإجراءات التقنية ،وهذا التوقيع يتخذ عدة صور واشكال ولا ينحصر في صورة او شكل معين، وذلك لتعدد طرق اصدار التواقيع الالكترونية التي قد تكون على شكل حروف او ارقام او رموز معتمدة على تقنيات التشفير والتكويك والترقيم وغيرها.

ولكن بالرغم من الإيجابيات التي حققتها تقنية التوقيع الالكتروني من سرعة، والمرونة في أداء المعاملات، إلا أنه ظهر معها تنامي السلوك الاجرامي مما جعل الافراد ينتابهم الخوف على مصالحهم واموالهم وقلت الثقة والامان في التعامل بهذه التقنية.

وبالرغم من وجود المنظومة القانونية التي جعلها المشرع الجزائري لمكافحة هذه الجرائم سواء من خلال قانون العقوبات او القانون الخاص بالتنظيم التوقيع والتصديق الالكترونيين الا انها تزداد يوما عن يوم، ناهيك عن الجرائم التي تقع في الخفاء دون اكتشافها او معرفتها في حق التوقيع الالكتروني وعليه من خلال دراستنا توصلنا إلى النتائج التالية:

- كثرة الاعتداء الاجرامي وتناميه السريع والمتطور في ميدان المعلوماتية الالكتروني بالأخص على التوقيع الالكتروني.
- تنوع الجرائم وتعددها حيث تمس شتى أنواع التوقيعات الالكترونية .
- عجز القانون الجنائي في الحد من جرائم الاعتداء على التوقيع الالكتروني او تقليلها.
- عدم شمولية الجرائم التي تمس التوقيع الالكتروني في النصوص القانونية الجزائية الراهنة.
- عدم اكتشاف الجرائم المستحدثة الواقعة على التوقيع الالكتروني بالرغم من خطورتها.

- غموض وعدم وضوح النصوص القانونية التي جاء بها المشرع الجزائري سواء في قانون العقوبات والقانون الخاص بالتوقيع والتصديق الالكترونيين 15-04 الصادر في 10 فبراير 2015.
- عدم التكافؤ العقابي وجسامة الضرر الناجم عن جرائم الاعتداء على التوقيع الالكتروني.
- لكي يعتد بالتوقيع الإلكتروني قانونيا وعده عنصرا في دليل الاثبات يجب أن تكون لوسائل التقنية المستخدمة في تشغيله محل ثقة وأمان.
- عدم وجود مراقبة تقنية كافية لمعرفة واكتشاف الجرائم المستحدثة في هذا المجال
- عدم وجود كفاءات وإطارات متمرسة في ميدان جرائم التكنولوجيا تابعة للهيئات القضائية والتشريعية قادرة التحكم فيها او الفصل في قضاياها.
- عدم إعادة النظر في المنظومة القانونية التي تنظم التوقيع الالكتروني وتحكم في جرائم الاعتداء على التوقيع الالكترونية.

إضافة الى ما سبق لاحظنا أن التشريعات المقارمة لم تتطرق كليا للتنظيم التقني للتوقيع الالكتروني، وفي نظرنا المتواضع لم تحبذ بسبب ما يطرأ على تقنية التوقيع الإلكتروني من تغييرات مستمرة وسريعة، خاصة في الجانب التشغيلي له لذا تركت هذه المسألة لمراسيم تنظمها.

أما الجرائم فهي تتسم بالخطورة، نظرا لخصوصيتيها وعدم إمكانية حصرها، فقد عمل المشرع الجزائري لسد الفراغ القانوني على تعديل قانون العقوبات، وقد عاقب على الشروع في الجريمة وجعل صفح الضحية جائز أمام المتابعة، إلا أن هذه الحماية متواضعة وغير كافية، فقد اقتصرت على جرائم قلة.

وفي ختام دراستنا نتقدم بمجموعة من الاقتراحات نجملها فيما يلي:

- إعادة النظر في المنظومة القانونية التي تنظم التوقيع الالكتروني وتحكم جرائم الاعتداء على التوقيع الالكترونية.
- تكوين إطارات مؤهلة من حيث اليد العاملة أو من حيث تخصص القاضي لتوسيع مداركه ومعارفه لتحدي الإشكالات الالكترونية.

- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في الجرائم المعلوماتية وجرائم عبر الانترنت والعمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية
- انشاء قانون شامل وكامل خاص بالتوقيع الالكتروني
- انشاء تكتلات عربية لدراسة ووضع استراتيجية وسياسات او إجراءات تنفيذية لمواجهة مثل هذه الجرائم.
- على رجال القانون والقضاء إدراك كل تطور في منهجية أو السياسة الالكترونية المنتهجة.
- فرض سياسة محكمة لحماية الأجهزة الالكترونية حتى تضمن الأمان والثقة في التعاملات الالكترونية وحماية بيانات الافراد الخاصة.
- العمل على نشر الوعي وثقافة التعامل الالكتروني بين الافراد والعاملين في المجال
- فرض تكوين للقضاة حتى يتم الفصل في القضايا المتغيرة والحديثة بطريقة عصرية ومتطورة، إضافة الى تشكيل هيئات تابعة للقضاء تمكنها من اكتشاف هذه الجرائم —خبراء تقنيين وفنيين– كمساعدين لهيئة القضاء.
- مراعاة المشرع الأبعاد المستقبلية لمواكبة التطورات الحاصلة، كما أن تعدد النصوص المجرمة في هذا الإطار وتناثرها قد يشكل عائقا كبيرا أمام القاضي أثناء تكييفه للأفعال المرتكب في حق التوقيع الالكتروني من جهة وفي حق المتعاملين من جهة أخرى.
- وضع تعديلات في القانون رقم 15-04 لسد الثغرات المتعلقة بالاعتداءات الواقعة على التوقيع الالكتروني على غرار النصوص المذكورة في قانون العقوبات المتضمنة المعالجة الآلية للمعطيات.
- نص القانون رقم 15-04 المتعلق بالتصديق والتوقيع الالكترونيين نص على بعض الجرائم المتعلقة بالتوقيع الالكتروني، ولم يدرج جريمة تزوير التوقيع الالكتروني، فلا بد من تضمين هذا القانون بهذه الجريمة نظراً لخطورتها.

- اشراك المتخصصين في المجال التقني في التحضير لمشاريع أو اقتراح القوانين ذات الصلة بالمجال الالكتروني أو تعديلها عند الاقتضاء، لما لذلك من أثر على تأمين وحماية المعطيات الشخصية المستعلمة في ابرام المعاملات الالكترونية.
- نهيب على المشرع الجزائري إدراج نص ضمن قانون التوقيع والتصديق الالكترونيين 15-04 لمعالجة مسألة التنازع بين التوقيع الالكتروني والتوقيع التقليدي خاصة وأنه أعتمد على مبدأ التعادل الوظيفي بين التوقيع الالكتروني والتوقيع التقليدي.

قائمة المراجع

قائمة المراجع

أولا: النصوص القانونية والتنظيمية

أ. النصوص القانونية

1. الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426 الموافق 20 يونيو سنة 2005، الجريدة الرسمية، عدد 44، الصادرة 19 جمادى الأولى عام 1426 الموافق 26 يونيو سنة 2005.

2. الأمر رقم 07 / 05 ، المؤرخ في 25 ديسمبر 2005، يتضمن امن الدفع الجريدة الرسمية, عدد 37، الصادر بتاريخ 04 جوان 2006.

3. قانون رقم 04/15، المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 10 فبراير 2015.

4. الأمر رقم 15 -03 المؤرخ في 01 فيفري 2015، يتعلق بعصرنة قطاع العدالة، الجريدة الرسمية، عدد06 ، الصادرة بتاريخ 10 فيفري 2015.

5. الأمر رقم 66 – 156 المؤرخ في 8 يونيو سنة 1966، يتضمن قانون العقوبات، ج ر، عدد 49، الصادرة بتاريخ 11 يونيو 1966. المعدل والمتمم لاسيما بالقانون رقم 15– 19، المؤرخ في 30 ديسمبر 2015، الجريدة الرسمية, العدد 71، الصادرة بتاريخ 30 ديسمبر 2015

6. الأمر رقم 03-11، المؤرخ في 26 غشت 2003، يتعلق بالنقد والقرض، ج .ر العدد 52، الصادرة بتاريخ 27 غشت 2003، الملغى بالقانون 12 يونيو 2023، يتضمن القانون النقدي والمصرفي، الجريدة الرسمية, العدد 43، الصادرة بتاريخ 27 يونيو 2023.

ب. النصوص التنظيمية

1. المرسوم التنفيذي رقم 07 -162، المؤرخ في 30 ماي 2007، المتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات بما فيه االلاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية يعدل ويتمم المرسوم التنفيذي رقم: (01 -123) مؤرخ في 09 جويلية 2001 جريدة رسمية،عدد 27 الصادرة في 13 جويلية 2001.

2. المرسوم التنفيذي رقم 135/16، المؤرخ في 17 رجب1437 الموافق ل 25 ابريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها. جريدة رسمية العدد 26، الصادرة بتاريخ 28 أفريل 2016.

3. المرسوم التنفيذي رقم 16-134،المؤرخ في 25 ابريل سنة 2016، تحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها، جريدة،رسمية، العدد 26، الصادر بتاريخ 28 أفريل 2016.

ج. النصوص القانونية العربية

1. قانون التوجيه الأوروبي رقم 93/1999 بشأن الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ 13/ 1999/12.

2. القانون رقم 83 سنة 2000، المؤرخ في 09 أوت 2000، يتعلق المبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية، العدد 64، الصادر بتاريخ 11 أوت 2000،

3. قانون الاونسيترال النموذجي بشأن التوقيعات الإلكترونية، المؤرخ بـ 05 / 06 / 2001 .

4. قانون المعاملات الإلكترونية الأردني رقم 85 سنة2001، الجريدة الرسمية رقم 4524 الصادرة بتاريخ 03 ديسمبر 2001.

5. قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، رقم 15 لسنة 2004، الجريدة الرسمية، العدد 17 الصادرة بتاريخ 22 أفريل 2004.

6. قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012، الوقائع العراقية، رقم العدد 4256، تاريخ العدد :05-نوفمبر 2011.

ثانيا: الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دون طبعة، الديوان الوطني للأشغال التربوية، الجزائر، 2002.

2. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

3. أسامة حمدان، الرقب جرائم النصب والاحتيال، دون طبعة، دار يافا العلمية للنشر والتوزيع، الأردن، 2009.

4. اسم محمد فاضل، التعويض عن إساءة استعمال التوقيع الالكتروني، دون طبعة، دار الجامعة الجديدة، مصر ، 2018 .

5. امال قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية ، دار هومة ، الجزائر، 2007،.

6. أمجد سعود الخريشة ،جريمة غسيل الأموال ، الطبعة الاولى ، دار الثقافة للنشر والتوزيع، الأردن، 2009 .

7. ايلاف فاخر كاظم علي، مخاطر العمليات المصرفية الالكترونية (دراسة مقارنة)، الطبعة الاولى، المركز العربي للدراسات والبحوث العلمية، مصر، 2019.

8. إيمان مؤمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دون طبعة، دار الجامعة للنشر، الإسكندرية، 2008.

9. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دون طبعة، دار الخلدونية، الجزائر، 2017.

10. حسان سعاد، إثبات التعاملات الإلكترونية وفقاً للقانون الجزائري والتشريعات المقارنة، الطبعة الاولى، مكتبة الوفاء القانونية، الإسكندرية، 2019.

11. خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دون طبعة، دار الجامعة الجديدة، الإسكندرية,2007.

12. خالد ممدوح إبراهيم، ابرام العقد الالكتروني (دراسة مقارنة)، الطبعة الاولى، دار الفكر الجامعي الإسكندرية، 2008.

13. د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية، الطبعة الاولى، منشورات الحلبي، لبنان، 2005.

14. زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دون طبعة, دار الهدى، الجزائر،2011.

15. سعيد السيد قنديل، التوقيع الالكتروني، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2006.

16. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دون طبعة، دار النهضة العربية، القاهرة، 2006 .

17. عامر محمود الكسواني، التجارة عبر الحاسوب، دون طبعة، دار الثقافة للنشر والتوزيع، الأردن،2008.

18. عايض الراشد المرى ، مدى حجية الوسائل التكنولوجية الحديثة في اثبات العقود التجارية ، دون طبعة، القاهرة ، 1998.

19. عبد الفتاح البيومي الحجازي، النظام القانوني لحماية التجارة الإلكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2002.

20. عبد الفتاح البيومي حجازي، مقدمة في التجارة الالكترونية والعربية، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية، 2003.

21. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، ودار الفكر الجامعي، الإسكندرية، 2006 .

22. عبد الله أحمد عبد الله غرايبة، حجية التوقيع الإلكتروني في التشريع المعاصر، الطبعة الاولى، دار الراية للنشر، الأردن،2008.

23. عبد الله سليمان، شرح قانون العقوبات الجزائري ق.م.ج، الجزائر، 2002.

24. عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات التوثيق، الطبعة الاولى، دار وائل للنشر والتوزيع ،الأردن، 2010.

25. عزت عبد القادر، جرائم التزوير والتزييف، الطبعة الثانية، دار اسامة الخوري للنشر والتوزيع، القاهرة ، 2000.

26. عصام عبد الفتاح مطر، التحكيم الإلكتروني، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009.

27. علاء محمد عبد النصيرات، حجية التوقيع الالكتروني في الاثبات(دراسة مقارنة)، الطبعة الاولى،دار الثقافة للنشر والتوزيع، الأردن، 2005.

28. عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، الطبعة الاولى، دار الثقافة للنشر والتوزيع، الاردن، 2009.

29. الغريب فيصل سعيد، توقيع الالكتروني وحجيته في الإثبات، الطبعة الاولى، المنظمة العربية للتنمية الإدارية، مصر، 2005.

30. فادي توكل عماد الدين، عقد التجارة الإلكترونية، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، 2010.

31. لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الاولى، دار هومة للطباعة والنشر والتوزيع، الجزائر ، 2012.

32. لورنس محمد عبيدات، اثبات المحرر الالكتروني، الطبعة الاولى، دار الثقافة للنشر والتوزيع، الاردن ، 2005.

33. ماجد راغب الحلو، العقد الاداري الإلكتروني دراسة تحليلية مقارنة، دون طبعة، دار الجامعة الجديدة، مصر،2007.

34. محمد ابراهيم ابو الهيجاء، عقود التجارة الإلكترونية، (اثبات العقد الالكتروني، حماية المستهلكين، وسائل الدفع الالكتروني، المنازعات العقدية وغير العقدية، الحكومة الإلكترونية، القانون الواجب التطبيق)، الطبعة الثانية، دار الثقافة، عمان ، 2011.

35. محمد الشهاوي، شرح قانون التوقيع الإلكتروني رقم 15 لسنة 2004 (دراسة مقارنة)، الطبعة الاولى، دار النهضة العربية، القاهرة، مصر،2010.

36. محمد حمادة مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الاولى، دار الثقافة للنشر والتوزيع، الأردن، 2004.

37. محمد عبد الله بوبكر موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والانترنت ،دون طبعة ,دار الثقافة والتوزيع، الاردن، 2010 .

38. محمد على العريان، الجرائم المعلوماتية انعكاسات ثورة المعلومات على قانون العقوبات، دون طبعة، منشورات الحلبي الحقوقية، لبنان، 2005.

39. محمد محمد أبو زيد ، تحديث قانون الإثبات ،دون طبعة, بدون ناشر ، 2002.

40. محمد محمد سادات، حجية المحررات الموقعة الكترونيا في الاثبات (دراسة مقارنة)، دون طبعة، دار الجامعة الجديدة، مصر،2011.

41. محمود نجيب حسني شرح قانون العقوبات، القسم الخاص، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994.

42. مصطفى كافي، النقود والبنوك الالكترونية، دون طبعة، دار رسلان، دمشق، سوريا،2011.

43. منير محمد الحنيهي وممدوح محمد الحنيهي، التوقيع الإلكتروني وحجيته في الإثبات، دون طبعة، دار الفكر الجامعي، الاسكندرية، 2004.

44. نادية ياس البياتي، التوقيع الإلكتروني عبر الأنترنت ومدى حجيته في الإثبات دراسة مقارنة بالفقه الإسلامي، الطبعة الاولى، دار البداية ناشرون وموزعون، عمان ، 2017.

45. نادية ياس بياتي، التوقيع الالكتروني عبر الانترنت ومدى حجيته في الاثبات، (دراسة مقارنة بالفقه الإسلامي)، الطبعة الاولى، دار الثقافة لنشر والتوزيع ، عمان، 2014.

46. نضال اسماعيل برهم ، احكام عقود التجارة الإلكترونية ، الطبعة الاولى، دار الثقافة للنشر والتوزيع ، الأردن، 2005،.

47. يوسف أحمد النوافلة، الاثبات الالكتروني في المواد المدنية والمصرفية، دون طبعة، دار الثقافة للنشر والتوزيع، الأردن، 2012.

48. يوسف احمد النوافلة، حجية المحررات الالكترونية في الاثبات وفق القانوني الاثبات والمعاملات الالكترونية، الطبعة الاولى، جامعة أردنية، الأردن، 2005.

ثالثاً: المقالات

1. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم إلى مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الامارات العربية المتحدة بالتعاون مع غرفة التجارة الالكترونية وصناعة دبي، في الفترة مابين10و 12 ماي 2003، المجلد الخامس.

2. حسينة عبد الحميد شرون, صونيا مقري ,دور التشفير وشهادات المصادقة الالكترونية في حماية الدفع الالكتروني ,مجلة البحوث والدراسات القانونية والسياسية, المجلد 11,العدد 02, جامعة على لونيسي، البليدة 02، الجزائر.

3. خالد ممدوح ابراهيم، الحماية الجنائية للتوقيع الالكتروني في القانون الاتحادي رقم 02 / 2006، مجلة الفكر الشرطي، مركز بحوث القيادة العامة لشرطة الشارقة، الشارقة ،2014.

4. راضية مشري، جريمة تزوير التوقيع الالكتروني في التشريع الجزائري، مجلة حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد 20، جامعة 08 ماي، قالمة، 2017.

5. رضوان قرواش، هيئات التصديق الالكتروني في ظل القانون 04/15ا لمتعلق بالقواعد العامة للتوقيع والتصديق الالكترونيين (المفهوم والالتزامات)،مجلة العلوم الاجتماعية ، العدد 24، جامعة سطيف 2 ،2017.

6. سديري نجوى، الحماية القانونية للتوقيع الالكتروني كآلية لتدعيم الثقة في المعاملات الالكترونية عبر الانترنت، مجلة الدراسات القانونية جامعة الجزائر1، يوسف بن خدة، المجلد 08، العدد 02 ، ، 2022.

7. ط. د عبان عميروش, النظام القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري والتشريعات المقارنة, مجلة الأستاذ الباحث للدراسات القانونية والسياسية, المجلد 07, العدد 01 , جامعة محمد بوضياف، المسيلة، لجزائر, 2022 .

8. عبان عميروش، النظام القانوني للتشفير كآلية للتصديق الإلكتروني في التشريع الجزائري والتشريعات المقارنة، مجلة الاستاذ الباحث للدراسات القانونية والسياسية, العدد 01 .المجلد07 , جامعة عبد الحميد بن باديس مستغانم,الجزائر,2022.

9. عبد العزيز سمية, التوقيع الالكتروني وسيلة حديثة للإثبات, دراسة مقارنة, مجلة معارف، العدد17, جامعة اكلي محند اولحاج, البويرة, 2014.

10. غازي أبو عرابي، "حجية التوقيع الالكتروني، (دراسة مقارنة في التشريع الأردني)"، مجلة دمشق للعلوم الاقتصادية والقانونية، المجلد 30 ، ط1 ،2004.

11. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الامارات العربية، 2000.

12. فرقد عبود العرضي، جريمة التزوير الإلكتروني دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، العدد 13، جامعة الكوفة، العراق،2013 .

13. فطيمة الزهراء مصدق، التصديق الالكتروني كوسيلة لحماية التوقيع الالكتروني، مجلة الدراسات والبحوث القانونية، المجلد 05، العدد01، ،جامعة محمد بوضياف، المسيلة، 2020.

14. مرابط حمزة وداودي منصور، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية، مجلة الحقوق والعلوم السياسية ،المجلد 10، العدد01، جامعة تيارت ابن خلدو ، الجزائر، 2023.

15. مسعودي يوسف، أرجيلوس رحاب، مسعودي يوسف، أرجيلوس رحاب، مدى حجية التوقيع الإلكتروني في الإثبات في التشريع الجزائري (دراسة على ضوء أحكام قانون 04/15)، مجلة الاجتهادات للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست، الجزائر،2017.

16. هشام كلو، التنظيم القانوني للتوقيع الالكتروني في القانون الجزائري، مجلة الباحث للدراسات الاكاديمية، جامعة الحاج لخضر، باتنة 01، المجلد 10، العدد01، 2023 ،ص 496 .

17. وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر، الوادي، المجلد 11 ، العدد 01 ، افريل 2020 .

رابعا: الرسائل والمذكرات

أ. رسائل الدكتوراه

1. بوعمرة اسيا، النظام القانوني للتجارة الكترونية لدراسة مقارنة، رسالة لنيل شهادة الدكتوراه في الحقوق ،تخصص قانون الملكية الفكرية، جامعة الجزائر 01 ،الجزائر، 2012.

2. ترجمان نسيمة، الحماية الجنائية للتوقيع الإلكتروني: دراسة مقارنة، رسالة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون الأعمال، جامعة ابن خلدون، تيارت، 2021 .

3. درار نسيمة, الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني, دراسة مقارنة , رسالة لنيل شهادة الدكتوراه في القانون الخاص, جامعة أبو بكر بلقايد, تلمسان, الجزائر, 2015.

4. مرزوق يوسف، وسائل الاثبات الحديثة، رسالة لنيل شهادة دكتورة في القانون الخاص، كليه الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012 ، ص62.

5. ياسر محمد الكومي، الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه في القانون الجنائي كلية الحقوق، جامعة حلوان، مصر، 2016.

ب. مذكرات الماجستير

1.امال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الجنائي والعموم الجنائية، جامعة الجزائر، الجزائر، 2002.

2.اياد "محمد عارف عطا سده، مدى حجيه المحررات الإلكترونية في الاثبات" دراسة مقارنه"، مذكرة لنيل شهادة الماجستير في القانون الخاص، جامعه النجاح الوطنية ، كليه الدراسات العليا، نابلس، فلسطين، 2009.

3.ترجمان نسيمة, الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة, رسالة لنيل شهادة الدكتوراه طور الثالث في التجريم في قانون الأعمال, جامعة ابن خلدون, تيارت, الجزائر, 2020.

4.حسن يحي يوسف فلاح، التنظيم القانوني للعقود الالكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص، جامعة النجاح الوطنية ،نابلس، فلسطين، 2007.

5.صلاح عبد الحكيم المصري، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزه، رسالة لنيل شهادة الماجستير في ادارة الأعمال، كلية التجارة، الجامعة الإسلامية غزه .

6.طارق عبد الرحمان ناجي، التعاقد عبر الأنترنت واثاره(دراسة مقارنة)،بحث لنيل دبلوم الدراسات العليا المعمقة، كلية العلوم القانونية والاقتصادية و الاجتماعية، جامعة محمد الخامس أكدال، 2006.

7.عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي وعلوم جنائية ، جامعة العقيد الحاج لخضر ،باتنة 1، 2012.

8.عمر هبطي، التوقيع الالكتروني ،رسالة لنيل دبلوم الدراسات العليا المعمقة، في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية ،كلية الحسن الثاني ، الدار البيضاء، 2007/2006.

9.فالح جلال عبد الرضا الحسيني، أثر شكلية التوقيع الإلكتروني في القرار الإداري، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط ، 2015.

10. لالوش راضية، أمن التوقيع الالكتروني، رسالة ماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو ، 2012.

11. هدار عبد الكريم، مبدأ الثبوت بالكتابة في ظل ظهور المحررات الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة الجزائر 01، 2014/2013.

ج. مذكرات الماستر

1. بودشيشة سمية، إثبات العقد الإلكتروني، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2017/2016.

2. زينب غريب، اشكالية التوقيع الالكتروني وحجيته في الاثبات، مذكرة لنيل شهادة الماستر في القانون الخاص، جامعة محمد الخامس، الرباط ،2010.

3. سيد عبد القادر جهيدة، شكرون ساسية، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية دراسة تحليلية ومقارنة، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص شامل، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2015/2014.

4. عبد الرفيق أورام، العقد الإلكتروني وحجيته في الإثبات المدني، مذكرة لنيل شهادة الماستر، وحدة الماستر القانون المدني والأعمال، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة عبد المالك السعدي، طنجة ، 2007 /2008.

5. عزولة طيموش، علاوات فريدة، التوقيع الالكتروني في ظل القانون رقم04/15، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص الشامل، جامعة عبد الرحمان ميرة، بجاية، 2015.

6. منصور عز الدين، حجية التوقيع الإلكتروني في الإثبات، مذكرة لنيل شهادة، الماستر في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016،2015.

خامسا: المواقع الالكترونية

1. قانون التوجيه الأوروبي الصادر في 13 ديسمبر 1999 المنشور على موقع www.europa.eu.int/directives ، بتاريخ 22 فيفري 2024، 10:20 سا.

2. مولود قارة، " الإطار القانوني للتوقيع والتوثيق الإلكترونيين في قانون المعاملات والتجارة الإلكترونية "، مقال منشور عبر موقع:www.minshawi.com اطلع عليه بتاريخ 08 /02/ 2024.

فَهْرس

العنوان	الصفحة
❖ الشكر والتقدير	1
❖ الاهداءات	2
❖ مقدمة	4
الفصل الأول الإطار المفاهيمي للتوقيع الالكتروني	10
المبحث الأول :ماهية التوقيع الإلكتروني	12
المطلب الأول: مفهوم التوقيع الإلكتروني	13
الفرع الأول: تعريف التوقيع الإلكتروني	14
الفرع الثاني: خصائص التوقيع الإلكتروني	23
المطلب الثاني: أهمية وأهداف التوقيع الالكتروني	25
الفرع الأول: أهمية التوقيع الالكتروني	25
الفرع الثاني: أهداف التوقيع الإلكتروني	27
المبحث الثاني: شروط الواجب توفرها في التوقيع الإلكتروني	29
المطلب الأول: شروط التوقيع الإلكتروني ووظائفه	29
الفرع الأول: شروط التوقيع الإلكتروني	30
الفرع الثاني: وظائف التوقيع الإلكتروني	34
المطلب الثاني: حجية التوقيع الالكتروني في الاثبات	37
الفرع الأول : حجية التوقيع الالكتروني في التشريع الدولي	37
الفرع الثاني حجية التوقيع الالكتروني في التشريعات الوطنية	43
خلاصة الفصل الأول	50
الفصل الثاني	51

آليات الحماية الجنائية للتوقيع الالكتروني	
المبحث الأول: الحماية التقنية والوقائية للتوقيع الالكتروني	53
المطلب الأول: تقنية التشفير كآلية تقنية لحماية التوقيع الالكتروني	53
الفرع الأول: تعريف التشفير	54
الفرع الثاني طرق نظام التشفير	59
المطلب الثاني: التصديق الإلكتروني كألية لحماية التوقيع الالكتروني	61
الفرع الأول: تعريف نظام التصديق الالكتروني	62
الفرع الثاني: دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع	68
المبحث الثاني: جرائم الاعتداء على التوقيع الالكتروني	73
المطلب الأول: جرائم الاعتداء على التوقيع الإلكتروني في إطار قانون العقوبات	74
الفرع الأول: جرائم التزوير والاحتيال	74
الفرع الثاني: جرائم المساس بأنظمة المعالجة الإلكترونية	88
المطلب الثاني: جرائم الاعتداء على التوقيع الإلكتروني في إطار قانون 04/15	98
الفرع الأول: جريمة الادلاء بإقرارات كاذبة للحصول على شهادة تصديق وتوقيع الكتروني:	99
الفرع الثاني :جريمة حيازة أو افشاء أو استعمال بيانات انشاء توقيع الكتروني موصوفة خاصة للغير :	100
خلاصة الفصل الثاني	108
❖ خاتمة	110
❖ قائمة المراجع	116
❖ الفهرس	127

الملخص

إن التطور السريع والمذهل لتكنولوجيا الثورة الرقمية أدت الى ضرورة البحث عن بديل للتوقيع التقليدي، حتى لا يكون عقبة أمام التعاملات الالكترونية عبر الانترنت، وهو ما سمح بإيجاد نوع جديد من التوقيعات يختلف في شكله ومضمونه وتكنولوجيته عن التوقيع التقليدي.

ونظرا لأن الثقة والأمان من بين المتطلبات الأمنية التي تثيرها المعاملات الالكترونية التي تتم في بيئة الكترونية افتراضية مملوءة بالمخاطر، تتعلق أساساً بانتحال هوية أطراف التعامل الالكتروني، أو اختراق البيانات الالكترونية المتداولة، مما تحتم وجود الية تدعم هذه الثقة، وهذا ما حرص عليه المشرع الجزائري من خلال تقرير حماية جنائية للتوقيع الالكتروني في قانون العقوبات، كما أكد على هذه الحماية من خلال القانون رقم 04/15 المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين.

الكلمات المفتاحية: التوقيع الالكتروني، المعاملات الالكترونية، الحماية الجنائية، البيئة الالكترونية، التصديق الالكتروني.

Abstract

The rapid and astonishing development of the technology of the digital revolution led to the necessity of searching for an alternative to the traditional signature, so that it would not be an obstacle to electronic transactions via the Internet, which allowed the creation of a new type of signature that differs in form, content and technology from the traditional signature. Given that trust and security are among the security requirements raised by electronic transactions .

that take place in a virtual electronic environment full of risks related mainly to impersonation of the parties to electronic transactions or penetration of electronic data in circulation, which necessitated the existence of a mechanism that supports this trust, and this is what the Algerian legislator has ensured through a report Criminal protection for electronic signature in the Penal Code, and this protection was also emphasized through Law No. 04/15 specifying the general rules for electronic signature and certification.

Key words: electronic signature , electronic transactions , criminal protection, electronic data, electronic certification.