جامعة الشهيد حمه لخضر – الوادي
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحماية الجنائية للتوقيع الإلكتروني

(دراسة مقارنة)

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر في الحقوق
تخصص: قانون أعمال

إعداد الطالب:
بوزيدي عبد الرزاق

لجنة المناقشة:

الاسم واللقب	الجامعة	الصفة
أ. جمال غريسي	جامعة الشهيد حمه لخضر – الوادي	رئيسا
أ. محمد نعرورة	جامعة الشهيد حمه لخضر – الوادي	مشرفا ومقررا
أ. مباركة عمامرة	جامعة الشهيد حمه لخضر – الوادي	مناقشا

السنة الجامعية: 2018/2017


بسم الله الرحمن الرحيم

الإهـــداء

أهدي ثمرة جهدي إلى أغلى ما في الوجود إلى روح من ربتني
من بحر فضلها و أفاضت عليا بالحب والحنان من قلبها وكانت
بدعواتها تساعدني وبروحها تغذيني إلى من شدني الحنين إلى ذكراها.
إليك نفسي ايتها الحنونة طيب الله ثراك وأسكنك فسيح جنانه
أمي الحنون مباركة بن الجموعي.
إلى الشعلة التي أنارت لي طريق حياتي ولا زال ضوئها النور الذي استهدي

به أبي الغالي * محمد*

إلى زوجتي الفاضلة بن الجموعي حسيبة التي شجعتني ووقفت معي لإكمال دراستي الجامعية .
لك مني زوجتي الغالية كل الإحترام و التقدير .
الى ربيع عمري وبهجة قلبي ونور عيني ابنائي *محمد الأمين – ملاك لوجين ومرام

و إلى كل إخوتي و أخواتي و أخص بالذكر أخي عبد الجبار وجميع أصدقائي وزملائي في العمل و الدراسة . و بالخصوص زملائي في المجلس الشعبي البلدي لبلدية المرارة،

شكروعرفان

اللهم لك الحمد كله ولك الشكر كله وإليك يرجع الأمر كله علانيته

وسره فأهل أنت أن تحمد و أهل أن تعبد .

وليس هناك أفضل مما قال خير الورى سيدنا محمد عليه الصلاة والسلام

* من لا يشكر الناس لا يشكر الله * حديث صحيح*

فنشكر الله عز وجل على الصحة والقوة التي وهبنا لانجاز هذا البحث الذي

وجهتنا الكثير من الصعاب في انجازه . فالحمد لله رب العالمين.

ونتقدم بالشكر إلى :

- الأستاذ الفاضل المشرف :" محمد نعرورة "

على توجيهاته ومساعدته لنا في انجاز هذا العمل المتواضع.

- كل أساتذتنا على مجهوداتهم المبذولة من أجل إهدائنا بالعلم النافع

- إلى كل زملائي موظفي وموظفات مجلس قضاء الوادي و المحكمة الادارية بولاية

مقدمـــة

مقدمـــــــــــة

يطالعنا تطور تكنولوجيا المعلومات والاتصال الحديث في كل يوم بأوضاع جديدة، أصبحت معه الوسائل الإلكترونية العصب المحرك للمعاملات الالكترونية فظهرت ماتسمى بالحكومة الالكترونية، أين أصبحت معظم المعاملات المالية والتجارية تتم إلكترونيا، وبالتالي لم تعد الوسيلة التقليدية في إثبات التصرفات القانونية " التوقيع التقليدي" ملائمة للتعاقدات الحديثة التي تتم في الشكل الإلكتروني، لذا ظهر التوقيع الإلكتروني ليكون بديلا عن التوقيع التقليدي، ليتوافق وطبيعة التعاقدات القانونية التي تتم باستخدام الوسائل والأجهزة الإلكترونية الحديثة.

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية و لإيجاد حلول لها كان لابد من البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فانه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية.

إنّ التطور التكنولوجي الذي شهده العالم خاصة بعد الانتشار الواسع لاستخدام التقنية الحديثة في جميع مجالات الحياة السياسية والاقتصادية والاجتماعية والثقافية أدى إلى زيادة التعاملات والنشاطات المختلفة في هذه المجالات، مما نتج عنه كما هائلا من المعلومات والبيانات، التي لم تعد الطرق التقليدية قادرة على استيعابها وحفظها واسترجاعها بالسرعة المطلوبة، مما اضطر إلى البحث عن أساليب جديدة تحقق الغاية وتسهل على الأفراد المعاملات والتبادلات وإبرام العقود، فظهر التوقيع الإلكتروني الذي يعد أهم الأساليب الحديثة على الإطلاق 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 رقم 23/06 المؤرخ في20 ديسمبر 2006 المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وكذا

القانون رقم :04/15 المؤرخ في :2015/02/01 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين الذي حاول من خلاله المشرع وضع البنية القانونية للتوقيع الالكتروني، وكذلك بث الثقة فيه عن طريق وضع نظم للمصادقة عليه من أجل التأكد من صحتها مع فرض الجزاءات والمسؤوليات في حالة عدم مراعاتها.

أهمية الدراسة:

ترجع أهمية هذا الموضوع الى تبيان مدى أهمية وجود التوقيع الالكتروني على السند الالكتروني لإضفاء الحجية عليه وزيادة الثقة بين المتعاملين خاصة في مجال التجارة الالكترونية لذلك لابد من وجود تشريعات جنائية حامية للتوقيع الالكتروني حتى يكون هناك جزاء لكل من تسول له نفسه العبث بالتوقيع الالكتروني و المحررات الالكتروني بصفة عامة.

أهداف الدراسة:

نسعى من خلال هذه الدراسة الى تحقيق الأهداف مختلفة أهمها تسليط الضوء على الإطار المفاهيمي للتوقيع الالكتروني، وكذا تبيان خصائصه وصوره، مع توضيح شروطه ووظائفه وأهم تطبيقاته ودراسة بعض التشريعات الجنائية الغربية و العربية الحامية للتوقيع الالكتروني من خلال تبيان صور الاعتداء على التوقيع الالكتروني والعقوبات المقررة لها .

أسباب اختيار الموضوع:

تعود أسباب اختيارنا لهذا الموضوع لنوعين من الأسباب، منها ذاتية وأخرى عملية موضوعية.

فأما عن الأسباب الذاتية، فيعود اختيارنا لهذا الموضوع إلى رغبتنا وميولنا للبحث في هذا النوع من المواضيع المرتبطة بعالم الانترنت و الاتصالات الحديثة ودراسته، وذلك نظرا لقلة الأبحاث القانونية و الدراسات الأكاديمية التي تتناول هذه التجربة التي تدرس الحماية الجنائية بصفة خاصة، وكذلك لكوني موظف كأمين ضبط بمجلس قضاء الوادي وقد كانت لنا تجربة مع التوقيع الالكتروني لان وزارة العدل قد قامت بتوزيع مفاتيح التوقيع الالكتروني على جميع الموظفين و العمل بالتوقيع الالكتروني هو ساري المفعول الآن لذلك كان التساؤل لدي هل

التوقيع الالكتروني له حماية قانونية و تقنية و خاصة الحماية الجنائية لذلك كان لدي الفضول للبحث في هذا الموضوع من ناحية الحماية الجنائية.

أما من الناحية العلمية والموضوعية، فاغلبها تتلخص فيما يطرحه الموضوع من إشكاليات قانونية، أحاول طرحها ومناقشها و الإجابة عليها و التي تشكل سببا قويا وباعثا كافيا لاختيار الموضوع، فقد حاولنا من خلال هذه الدراسة إثراء الموضوع ببعض الآراء و الحقائق التي تعكس واقع وحقيقة الحماية الجنائية للتوقيع الالكتروني، خاصة وأن مسألة التوقيع الإلكترونيتعتبر من المستجدات الحديثة في الجزائر التي قامت بسن تشريع خاص بالتوقيع الالكتروني إلا في سنة 2015.

كما أن هناك دوافع أخرى كان لها أثرها في اختيار الموضوع، و التي تنطلق من نقص الكتابات في هذا الموضوع خاصة الجزائرية منها، لحداثة قانون التوقيع الالكتروني إلى جانب قلة الأحكام و الاجتهادات القضائية في هذا المجال، وكذا الرغبة في معرفة القواعد القانونية لهذا الموضوع التي عززها المشرع الجزائري في هذا المجال.

إشكالية الدراسة:

إنطلاقا من الأهمية التي أصبح يكتسبها التوقيع الالكتروني في مختلف المعاملات والتصرفات الالكترونية بين الدول، المؤسسات و الأفراد، حيث أنه إزداد دوره و مجال إستعماله ضمن مختلف التصرفات القانونية التي تتم عبر الوسائل الالكترونية، و ذلك لعدم ملائمة التوقيع التقليدي بحكم طبيعته المادية للمعاملات الإلكترونية.

و أمام هذا فإن التوقيع الإلكتروني يعد عنصرا أساسيا لصحة و سلامة مختلف المحررات الإلكترونية التي تتجدد فيها التصرفات و المعاملات القانونية المنجزة بوسائل إلكترونية.

و يمكن طرح الاشكالية على الشكل التالي:

- **مامدى فعالية التشريعات المختلفة في حماية التوقيع الإلكتروني جنائيا؟**

و تتضمن هذه الاشكالية مجموعة من التساؤلات نوجزها على الشكل التالي:

- **مامفهوم التوقيع الالكتروني؟وماهي أهم تطبيقاته؟**
- **مامدى حجية التوقيع الالكتروني في الاثبات؟**

– ماهي أهم صور الاعتداءات على التوقيع الالكتروني و العقوبات المقررة لها في التشريعات الغربية و العربية؟

منهج الدراسة:

طبيعة موضوع البحث تقتضي استخدام مناهج علمية معينة وسوف يتم إيرادها بالترتيب حسب أهمية الاستخدام.

المنهج الغالب والأكثر استخداما في هذه الدراسة هو المنهج التحليلي كطريقة عملية لوصف وتحليل الظاهرة عن طريق جمع المعلومات وتصنيفها الذي يعتبر طريقة من الطرق المرتبطة بالظواهر الإنسانية لبحث أكاديمي يتميز بالأسلوب العلمي والتحليلي وهذا المفهوم يتلاءم مع طبيعة هذه الدراسة، التي تعتمد أساسا على التسلسل المنطقي للأفكار وتحليلها وعرض الأفكار، انطلاقا من معطيات ومبادئ قانونية يمكن البرهنة على صحتها ومن ثم يتسم توظيفه في تحليل النصوص القانونية،والأحكام المتعلقة بالجرائم الالكترونية عامة و جرائم الاعتداء على التوقيع الالكتروني خاصة ، و تفسيرها وتحليلها للوصول إلى نتائج تتماشى مع العقل و المنطق.

إضافة إلى استخدام المنهج المقارن، الذي يستخدم المقارنة كأداة معرفية، ويتم إعماله أساسا عند مقارنة بين ما هو معمول به في القوانين الوضعية، والأنظمة القانونية واستخراج أوجه التشابه والاختلاف فيما بينهما، ومقارنتهما بما أخذ به المشرع الجزائري، ويظهر هذا المنهج بصورة جلية عند مقارنة النصوص القانونية المتعلقة بمحاربة الجرائم الالكترونية عامة و جرائم الاعتداء على التوقيع الالكتروني خاصة مع ما جاءت به القوانين الغربية و كذا العربية التي سبقت الجزائر في هذا المجال .

صعوبات الدراسة:

أما بخصوص صعوبات الدراسة فترجع أساسا إلى العناء في تجميع المراجع المتعلقة ببعض المواضيع و الأفكار التي تطرحها الدراسة خصوصا الجزئية منها باعتبار الدراسة تتعرض إلى الكثير من المواضيع و الأفكار التفصيلية المتسلسلة، إلى جانب كثرة المراجع في بعض جوانب الدراسة مقابل شحها في جوانب أخرى، حيث أن جانب الكثرة جعل توظيفها واستغلالها أكثر في تحقيق أهداف الدراسة، وهو ما أضاف على أعباء الدراسة العبء الموضوعي المتعلق

بالحجم الموضوعي للدراسة قصد استيعاب جميع أفكار الدراسة ومواضيعها، أما بخصوص ندرتها في بعض جوانب الدراسة، فرض على الباحث أن يكون في بحث مستمر إلى غاية أخر يوم من كتابة الموضوع، لتغطية جميع الجوانب ولاسيما الفرعية والجزئية منها، مما أضاف العبء الزمني الذي كان من المفترض أن تستغرقه الدراسة.

إلى جانب أن أكثر المراجع المتوفرة عن الموضوع تركز على جانب وتهمل الجوانب الأخرى، ولاسيما الجزئية و التفصيلية إضافة إلى قلة المراجع المتخصصة التي تتناول أحكام قانون04/15 المتضمن التوقيع و التصديق الالكترونيين نظرا لحداثة القانون وقلة الأحكام القضائية في هذا المجال، وهي الصعوبات التي تم التغلب عليها بهدف الوصول إلى دراسة شاملة ومتكاملة للموضوع.

خطة الدراسة:

للاجابة على الاشكالية الرئيسة للموضوع، مع ما ينبثق عنها من تساؤلات فرعية قمنا بتقسيم دراستنا هذه إلى مقدمة و فصلين و خاتمة .

خصصنا **الفصل الأول** لدراسة للاطار التنظيمي للتوقيع الالكتروني و مدى حجيته في الاثبات أما **الفصل الثاني** تطرقنا فيه الى القواعد الجنائية الحامية للتوقيع الالكتروني.

لننهي الموضوع **بخاتمة** تتضمن عرضا موجزا لما احتوت عليه المذكرة من أفكار، كما نوضح فيها ما تم استخلاصه من نتائج تم التوصل إليها من خلال عملية البحث وأهم التوصيات.

نتمنى أن نكون قد أصبنا في معالجة هذا الموضوع وفق ما توفر لدينا من مصادر ، فإذا أصبنا من الله و منه ، و إن كان غيره ، حسبنا صدق نيتنا و خالص جهدنا ، و التوفيق من الله وحده .

الفصل الأول

الفصل الأول
الإطار المفاهيمي للتوقيع الإلكتروني و مدى حجيته

حتى تكون هناك دراسة متكاملة لموضوع بحثنا والذي جاء عنوانه الحماية الجنائية للتوقيع الإلكتروني، لابد من تسليط الضوء على الإطار المفاهيمي للتوقيع الإلكتروني و مدى حجيته في الإثبات، لذلك خصصنا الفصل الأول من بحثنا هذا لعرض الإطار المفاهيمي للتوقيع الإلكتروني ومدى حجيته في الإثبات، التي خصصنا لها المبحث الأول لدراسة الإطار التنظيمي للتوقيع الإلكتروني، سنتعرض بالتفصيل لمفهوم التوقيع الإلكتروني من خلال تعريفه أولا التعريف الفقهي و القضائي له ثم التعريف القانوني له من خلال قانون الأونسترال و التوجيه الاوروبي و تعريفه من خلال بعض التشريعات المقارنة، كذلك سنسلط الضوء على صور التوقيع الإلكتروني و خصائصه و كذلك وظائفه ومجالات تطبيقه كل هذا سيكون في المبحث الأول، أما المبحث الثاني الذي خصصناه لحجية التوقيع الإلكتروني في الإثبات سنعرض من خلاله شروط حجية التوقيع الإلكتروني في الإثبات و موقف بعض التشريعات منه، لذلك لزم علينا رسم خطة نعرض من خلالها هذا الفصل.

و سنعرض هذا الفصل من خلال المبحثين التاليين :

المبحث الاول : الإطار المفاهيمي للتوقيع الإلكتروني.

المبحث الثاني : حجية التوقيع الإلكتروني في الإثبات.

المبحث الأول
الإطار المفاهيمي للتوقيع الإلكتروني.

أدى التطور التكنولوجي السريع الذي نعيشه الأن، والذي يطلق عليه عصر ثورة المعلومات والبيانات الى ظهور وسائل وأساليب جديدة في إبرام العقود لم تكن معروفة منذ سنوات قليلة وهذه الوسائل في تطور دائم ومستمر وسريع ، ولما كان القانون هو مرآة الواقع كان لابد للمشرع من إصدار تشريعات لمعالجة ما أستجد من وسائل وطرق لإبرام العقود.

ويعتبر التوقيع الإلكتروني من التطبيقات التي ظهرت وتوسع في إستخدامها ترتيبا على التوسع في إستخدام الحاسب الألي وتقدم تطبيقاته وتقنياته على نحو جعل الحياة اليومية للأفراد والدول تعتمد عليه بصفة شبه كلية.

وحيث أن ثورة الاتصالات قد إختصرت المسافات بين والدول، فما المانع من الاستفادة من الأثار الإيجابية لهذه التقنيات في محاولة لتحديث المفاهيم التقليدية المستقرة في الفقه القانوني التقليدي[1].

وسنعرض هذا المبحث من خلال المطلبين التاليين:

المطلب الأول : مفهوم التوقيع الإلكتروني.

المطلب الثاني: وظائف التوقيع الإلكتروني و مجالات تطبيقه.

المطلب الأول
مفهوم التوقيع الإلكتروني

إن الانتشار الواسع والمذهل للتجارة الإلكترونية واللّجوء المتنامي للعقود الإلكترونية،أدى إلى ضرورة البحث عن بديل للتوقيع التقليدي،حتى لا يكون عقبة أمام التعاملات الإلكترونية عبر الإنترنت،الأمر الذي أسفر عن إيجاد شكل جديد غير مألوف من التوقيعات وهو التوقيع الإلكتروني،الذي يختلف في شكله ومضمونه وتكنولوجيته عن التوقيع التقليدي،بإعتباره يوضع على محررات تختلف بدورها عن المحررات الورقية[2].

نتطرق في الفرع الأول لتعريف التوقيع الإلكتروني، أما الفرع الثاني فخصصناه لدراسة صور و خصائص التوقيع الإلكتروني.

الفرع الأول
تعريف التوقيع الإلكتروني .

سنعرض أولا التعريفات التي أدرجت للتوقيع الإلكتروني فقها وقضاء، ثم نتطرق بعد ذلك لأهم تعريفاته القانونية[3].

---

[1] عبد الرسول عبد الرضا ، محمد جعفر هادي ،المفهوم القانوني للتوقيع الإلكتروني ،مجلة المحقق المحلي للعلوم القانونية و السياسية ،جامعة بابل ، العراق ،العدد الأول ، السنة الثانية ،ص ص.138،137.

[2] محمد ناصر حمودي،العقد الدولي الإلكتروني المبرم عبر الإنترنت،الطبعة الأولى دار الثقافة للنشر والتوزيع،عمان،2012، ص.324.

[3] بسمة فوغالي ، إثبات العقد الإلكتروني و حجيته في ظل عالم الإنترنت،مذكرة ماجيستير في القانون الخاص ،كلية الحقوق و

أولا : التعريف الفقهي والقضائي للتوقيع الإلكتروني.

قبل أن يتم تجسيد التوقيع الإلكتروني قانونا،اختلف الفقه والقضاء في تعريفه وايجاد معنى له[1].

1/التعريف الفقهي للتوقيع الإلكتروني.

عرف بعض الفقهاء التوقيع الإلكتروني بأنه مجموعة من الإجراءات يتبع استخدامها عن طريق الرموز أو الأرقام، إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا،يجري تشفيرها باستخدام زوج من المفاتيح، واحد معلن والآخر خاص بصاحب الرسالة[2].

كما عرفه فقهاء آخرون بأنه مجموعة من الإجراءات التقنية التي تمكن من تحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بشأنه[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].

نستنتج من هذه التعريفات،بأن مسألة وضع تعريف فقهي دقيق للتوقيع الإلكتروني ارتكزت في الأساس على بعض المحاولات المستندة على تحديد الوظيفة المزدوجة المتمثلة في التحقق من الشخصية والرضا كتعبير عن الإرادة[5]، وبالتالي متى حقق التوقيع هاتين الوظيفتين اعتبر توقيعا،سواء اتخذ الشكل اليدوي أو الإلكتروني[6].

2/ التعريف القضائي للتوقيع الإلكتروني.

سلكت محكمة النقض الفرنسية في تعريفها للتوقيع الإلكتروني مسلك تعريفه على ضوء التوقيع التقليدي، فبعدما عرفت هذا الأخير بأنه:((شهادة بخط اليد تكشف عن رضاء الموقع بهذا التصرف وتمكن من التحقق من إسناد التوقيع لصاحب الوثيقة))[7] قررت بأن هذه الطريقة الحديثة للتوقيع الإلكتروني تقدم نفس الضمانات للتوقيع اليدوي الذي يمكن أن يكون مقلدا،بينما الرمز السري لا يمكن أن يكون إلا لصاحب الكارت فقط[8] .

كما كرس القضاء بعد ذلك أحكامه نحو الاعتداد بهذا النوع الجديد من التوقيعات،وبين بأنه يشكل توقيعا صحيحا معتد به قانونا،كل رمز خطي مميز وخاص يسمح بتحديد وتشخيص صاحبه دون لبس ولا غموض، وانصراف إرادته الصريحة الالتزام بمحتوى ما تم التوقيع عليه وقد أقر هذا الاتجاه للقضاء الفرنسي في حكم لمحكمة النقض المصرية في 1989/11/08 بخصوص قبول التوقيع الرقمي في حالات الوفاء بالبطاقة البنكية تطبيقا لحكم محكمة النقض الفرنسية في حكمها السابق المشهور بقضية"كريكيداس"[9].

العلوم السياسية ،جامعة محمد لمين دباغين، سطيف، ص.59.

1 الصفحة نفسها.

2 أسامة بن غانم العبيدي ، حجية التوقيع الإلكتروني في الإثبات ، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، ص.145.

3 محمد ناصر حمودي، مرجع سابق، ص. 326.

4 عادل رمضان الأبيوكي،التوقيع الإلكتروني في التشريعات الخليجية ،د.ط،دار المكتب الجامعي الحديث،الاسكندرية،2009، ص.15.

5 محمد ناصر حمودي، مرجع سابق، ص ص.327،326.

6 Alain Bensoussan et Yves le Roux, Cryptologie et signature électronique, hermes science publication ,paris, 1999, p79 .

7 محمد ناصر حمودي، مرجع سابق ،ص.327.

8 «Ce procédé moderne présente les même garanties que la signature manuscrite la quelle peut être imitée tandis que le code secret n'est connu que du seul titulaire de la carte ».

9 محمد ناصر حمودي، مرجع سابق ،ص.327.

من مجمل هذه الأحكام يتضح بأن التوقيع الإلكتروني وسيلة حديثة لتحديد هوية صاحب التوقيع ورضائه بالتصرف القانوني الموقع عليه[1]، وبالتالي يقوم بذات وظائف التوقيع التقليدي المعهود،كل ما هنالك أنه ينشأ عبر وسيط إلكتروني،استجابة لنوعية المعاملات التي تعتبر بدورها إلكترونية ووجب توقيعها إلكترونيا، كونه لا مكان فيها للإجراءات اليدوية، وأيا كانت الألفاظ أو العبارات المستعملة في تعريفه فإنّها تتحدد في المضمون وهو تحديد هوية الشخص الموقع وتمييزه عن غيره،حيث العبرة بالمساواة الوظيفية بين النوعين من التوقيعات[2].

ثانيا: التعريف التشريعي للتوقيع الإلكتروني.

اهتمت غالبية القوانين، وعلى جميع المستويات بالتوقيع الإلكتروني،فقد كان هذا الأخير محل اهتمام من قبل المنظمات سواء الدولية أو الإقليمية، لتتبعها بعد ذلك تشريعات مختلف الدول[3].

1/ تعريف التوقيع الإلكتروني وفقا للمنظمات الدولية والتوجيهات الأوروبية.

كانت الخطوة الأولى الفعلية لميلاد التوقيع الإلكتروني تشريعيا،هي صدور القانون النموذجي للتجارة الإلكترونية الدولية لسنة1996[4] وقد عرف التوقيع الإلكتروني في المادة 07 على أنه » عندما يشترط القانون وجود توقيع من شخص يستوي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

أ/ استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

ب/ كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات،في ضوء كل الظروف،بما في ذلك أي إتفاق متصل بالأمر»[5] .

هذا التعريف ركز على ضرورة قيام التوقيع الإلكتروني بالوظائف التقليدية للتوقيع وهي تمييز هوية الشخص،والتعبير عن رضائه الارتباط بالعمل القانوني،على نحو ما ورد في الفقرة ،(أ) كما ركز أيضا على أنه يتعين أن تكون طريقة التوقيع الإلكتروني،والواردة في الفقرة (ب) طريقة موثوقا بها،ولم يحدد تلك الطرق أو الإجراءات التي يتعين إتباعها، وآنما تركها لكل دولة تحددها بطريقتها ووفقا لتشريعاتها[6] .

وجاء بعد ذلك قانون اليونسترال للتوقيعات الإلكترونية لعام ،2001 وتحديدا في نص المادة2/أ التي عرفت التوقيع الإلكتروني بأنه ((بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات))[7].

---

[1] Santiago Cavanillas Mugica et autres, commerce électronique, Edition delta, beyrouth liban 2004,p57.

[2] محمد ناصر حمودي، مرجع سابق ،ص.328.

[3] بسمة فوغالي، مرجع سابق، ص.61.

[4] عبد الوهاب مخلوفي،التجارة الإلكترونية عبر الإنترنت،رسالة دكتوراه،كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر بانتة،2012/2011،ص.203.

[5] L'article 7, loi type de la CNUDCI (A/51/628)1996, « Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de donnée **: a)**Si une méthode est utilisé pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données ; et **b)**Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été crée ou communiqué, compte de tout accord en la matière ».

[6] ايمان مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته، الجوانب القانونية لعقد التجارة الالكترونية، ط 1، دار الجامعة الجديدة لنشر، الإسكندرية، 2008،ص. 249

[7] رانيا عزب،العقود الرقمية في قانون الإثبات،د.ط ،دار الجامعة الجديدة،الإسكندرية،2012، ص. 181.

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

أما التوجيه الأوروبي رقم 1999/93، فقد عرف التوقيع الإلكتروني في الفقرة الأولى من المادة الثانية بأنه ((عبارة عن معطيات ذات شكل إلكتروني مرتبطة أو مدرجة بمعطيات إلكترونية أخرى التي يمكنها أن تقوم بوظيفة التعريف))[2].

وقد ميز التوجيه الأوروبي المذكور بين نوعين من التوقيع، التوقيع الإلكتروني المتقدم أو المؤمن والتوقيع الإلكتروني البسيط أو العادي[3]، فالتوقيع الإلكتروني المؤمن هو الذي يكون معتمدا من أحد مقدمي خدمات التصديق الإلكتروني،والذي يمنح شهادة تفيد صحة هذا التوقيع، بعد التحقق من نسبة التوقيع إلى صاحبه،ويتمتع هذا التوقيع بالحجية القانونية الكاملة في الإثبات إذا توفر على شروط معينة وفقا للفقرة الثانية من المادة الثانية من التوجيه المشار إليه وهي:

أ/ أن يرتبط التوقيع بشخص الموقع حصرا.
ب/ أن يسمح بتحديد هوية الشخص الموقع.
ج/ أن يكون قد أنشئ بوسائل تبقى تحت رقابة الموقع الحصرية.
د/ أن يرتبط التوقيع بالبيانات التي يحيل إليها على نحو يسمح بكشف كل تعديل لاحق عليها[4].

أما التوقيع الإلكتروني البسيط، فيتمتع بالحجية القانونية في حالة عدم إنكاره، أما في حالة إنكاره فيقع على عاتق من أدلى به إقامة الدليل على أنه قد تم بطريقة تقنية موثوق بها[5].

وبالتالي على خلاف القانون النموذجي للجنة اليونسترال التي حاولت وضع قواعد عامة تسترشد بها الدول عند وضع قوانين وطنية متعلقة بالتوقيعات الإلكترونية وتفاديها وضع تعريفات دقيقة قد تعيق الدول في ذلك،فإن التوجيه الأوروبي وبالرغم من كونه يشكل بدوره إطارا
عاما لقوانين الدول الأعضاء في الإتحاد الأوروبي،إلاّ أنه فصل في مسألة التوقيع الإلكتروني أكثر،تعريفاً وأنواعا وشروطا،وحتى بين القيمة القانونية فيما بين أنواع التوقيعات ذاتها،وبينها وبين التوقيعات اليدوية التقليدية[6].

2/ تعريف التوقيع الإلكتروني وفقا لتشريعات بعض الدول.

إن التعريف الذي أورده التوجيه الأوروبي،أخذت به معظم التشريعات الأوروبية ففي القانون المدني الفرنسي ورد تعريف التوقيع بشكل عام والتوقيع الإلكتروني بشكل خاص في

---

1 عبد الوهاب مخلوفي،المرجع السابق، ص. 204

2 رانيا عزب، المرجع السابق، ص. 183.

3 نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، د.ط، دار الثقافة للنشر والتوزيع،عمان،2005،ص. 171.

4 L'article2/2 « On entend par signature électronique avancée, une signature électronique qui satisfait aux exigences suivantes : a)être liée uniquement au signature ; b)permettre d'identifier le signature ; c)être créée par des moyens que le signature puisse sous son contrôle exclusif ; d)être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ». Alain Bensoussan et Yves le Roux ,Cryptologie et signature électronique ,op cit , p76 .

5 إلياس ناصيف،العقد الإلكتروني في القانون المقارن،الطبعة الأولى،منشورات الحلبي الحقوقية،بيروت،2009،ص.237.

6 محمد ناصر حمودي، مرجع سابق، ص ص.331، 332.

نص المادة 1316 فقرة 4 المضافة بموجب القانون رقم 230/2000[1]، حيث تنص هذه المادة على أن:((التوقيع الإلكتروني ضروري لاكتمال التصرف القانوني وهو يحدد هوية من يحتج به عليه و يعبر عن رضا الأطراف بالالتزامات الناشئة عن هذا التصرف،وعندما يتّم بواسطة موظف عام يكتسب هذا التصرف صفة الرسمية.وعندما يكون التوقيع إلكترونيا يقتضي استخدام وسيلة آمنة لتحديد الشخص،بحيث تضمن صلته بالتصرف الذي وقع عليه،ويفترض أمان هذه الوسيلة ما لم يوجد دليل مخالف بمجرد وضع التوقيع الإلكتروني الذي يجري بموجبه تحديد شخص الموقع.

ويضمن سلامة التصرف، وذلك بالشروط التي يتم تحديدها بمرسوم يصدر عن مجلس الدولة))[2] .

وأضافت المادة الأولى من المرسوم الفرنسي رقم272/2001 الصادر في 2001/03/30 الذي جاء كتطبيق للقانون 230/2000، الشروط التي يجب توافرها في التوقيع الإلكتروني وعموما هي:

- ✓ أن يكون للتوقيع طابع متفرد يسمح بتحديد شخص الموقع عن غيره وذلك باستخدام وسيلة تقنية آمنة تسمح بذلك وتضمن صلة الموقع بالتصرف القانوني الذي وقع عليه.
- ✓ ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- ✓ سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- ✓ إمكانية كشف أي تعديل أو تبديل في بيانات المحرر أو التوقيع الإلكتروني[3].

يتضح مما تقدم، أن المشرع الفرنسي وضع مفهوما موحدا للتوقيع،من دون أن يفرق بين توقيع تقليدي وتوقيع إلكتروني فيما يتعلق بحجية كل منهما للإثبات،على أن يكون التوقيع مميزا لشخص صاحبه،ويتم بإجراءات آمنة تضمن سرية بيانات هذا التوقيع[4].

ومن بين القوانين الغربية التي عرفت التوقيع الإلكتروني،نجد القانون الأمريكي الذي نظّمه تنظّيما محكما سواء على المستوى الفدرالي أو على مستوى الولايات،غير أننا نركز على القانون

الفدرالي والذي عرف التوقيع الإلكتروني في قانون المعاملات الإلكترونية الصادر في 2000/07/30 بأنه:((أصوات أو إشارات أو رموز، أو أي إجراء آخر يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، ويقترن بتعاقد أو مستند أو محرر، ويستخدمه الشخص قاصدا التوقيع على المحرر))[5].

وتجدر الإشارة إلى أنه هناك تشريعات غربية أخرى تناولت مسألة تعريف التوقيع الإلكتروني،إلا أنها لا تخرج عن نطاق ما ورد بالقانون الفرنسي والأمريكي، التي ركزت كلّها

---

1 عبد الوهاب مخلوفي، مرجع سابق، ص. 205.

2 L'article 1316- 4 ,loi 2000 - 230 , « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose elle manifeste le consentement des parties aux obligation qui découlent de cet acte quand elle est apposée par un de officier public, elle confère l'authenticité à l'acte lorsqu'elle est électronique ,elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache la fiabilité de ce procédé est présumée du signataire assurée et l'intégrité de l'acte garantie, dans des condition fixées par décret en conseil d'état».

إلياس ناصيف، مرجع سابق ،ص.239.

3 محمد ناصر حمودي، مرجع سابق ،ص. 333.

4 إلياس ناصيف، مرجع سابق ،ص .239.

5 محمد ناصر حمودي، مرجع سابق ، ص.232.

على وظائف التوقيع الإلكتروني، بغض النظر عن الشكل الإلكتروني الذي يتخذه والوسيلة التكنولوجية التي يتّم بها[1].

أما في الدول العربية، فنجد أن غالبية التشريعات المنظمة لمعاملات التجارة الإلكترونية قد عرفت التوقيع الإلكتروني[2]، حيث عرفت المادة 2 من قانون المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة التوقيع الإلكتروني بأنه:((توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني، ملحق أو مرتبط منطقيا برسالة إلكترونية وممهور بنية توثيق أو إعتماد تلك الرسالة))[3].

بينما في مصر وبصدور القانون رقم15 لسنة 2004 الخاص بالتوقيع الإلكتروني وفي المادة 1/ج منه،عرف التوقيع الإلكتروني بأنه:((ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره))[4].

أما في الجزائر وبموجب القانون رقم 04/15 الخاص بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[5]، فقد عرف التوقيع الإلكتروني في مادته الثانية بأنه:((بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى،تستعمل كوسيلة للتوثيق)).

نلاحظ من خلال التعريف السابق،أن القانون الجزائري قد أخذ بتعريف قانون اليونسترال النموذجي،مع تغيير بعض العبارات فقط،فقد استعمل عبارة "تستعمل كوسيلة للتوثيق" والمراد بها

هو أن تستخدم لتوثيق هوية الموقع وبيان موافقته على مضمون ما وقع عليه[6]،وهو ما نصت عليه المادة السادسة من القانون 04/15 سالف الذكر((يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع واثبات قبوله مضمون الكتابة في الشكل الإلكتروني)).

كما عرفت المادة الثانية نفسها الموقع وحصرته في الشخص الطبيعي دون الشخص المعنوي، حيث تنص بأن:(الموقع: شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله))[7].

وقد ميز المشرع الجزائري على غرار معظم التشريعات الأوروبية،بين نوعين من التوقيع الإلكتروني،التوقيع الإلكتروني العادي أو البسيط والتوقيع الإلكتروني المؤمن "أو الموصوف" كما أطّلق عليه في القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين سالف الذكر،حيث عرف التوقيع الإلكتروني الموصوف بموجب المادة7 منه بأنه التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية :

- ✓ أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

---

1 عبد الوهاب مخلوفي، مرجع سابق ، ص. 205.

2 محمد ناصر حمودي، مرجع سابق ، ص.334.

3 القانون رقم 02 ، المتعلق بالمعاملات والتجارة الإلكترونية الإماراتي، المؤرخ في 2002/02/26،المنشور في الجريدة الرسمية العدد277، دبي.

4 إبراهيم بن شايع الحقيل، سليمان بن محمد بن الشدي، التوقيع الإلكتروني وأثره في إثبات الحقوق والإلتزامات بين الشريعة الإسلامية والنظم والقواعد القانونية، ورقة عمل مقدمة في ندوة التوقيع الإلكتروني، المنعقدة في الرباط، المملكة المغربية، يونيو ،2006منشورات المنظمة العربية للتنمية الإدارية، ،2008،ص.221.

5 قانون رقم 04/15،الخاص بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين،المؤرخ في 1فبراير 2015الموافق لـ 11ربيع الثاني 1436هـ،ج ر،العدد06،الصادرة في 10فبراير 2015الموافق لـ 20ربيع الثاني 1436.

6 بسمة فوغالي ، مرجع سابق ، ص.66.

7 بسمة فوغالي ، مرجع سابق ، ص.66.

- ✓ أن يرتبط بالموقّع دون سواه.
- ✓ أن يمكن من تحديد هوية الموقّع.
- ✓ أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- ✓ أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقّع.
- ✓ أن يكون مرتبطا بالبيانات الخاصة به،بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

نلاحظ من مجمل التعريفات السابقة، بأن التوقيع الإلكتروني في كافة القوانين المنظمة له والمنظمة للتجارة الإلكترونية واحدة تقريبا، مع اختلاف الألفاظ ولكن مع وحدة المضمون، فقد اختلفت الأساليب التي يتم خلعها على التعريف دونما تغيير في مضمون التعريف ذاته، والسبب في ذلك هو وحدة المصدر الذي استقت منه هذه التشريعات موضوع تنظيم التوقيع الإلكتروني[1].

كما ركزت هذه التعريفات على الصور والأشكال على سبيل المثال،حتى تتسع مستقبلا لأي صور أو أشكال قد تظهر للتوقيع الإلكتروني،وعلّة ذلك هي توفير مرونة أكثر للمتعاملين في اختيار الوسيلة التي يرونها تكفل الأمن والثقة في هذا التوقيع[2].

الفرع الثاني
صور وخصائص التوقيع الالكتروني

أدى التطور الحاصل في نطاق نظام المعلومات والاتصالات إلى ظهور العديد من الصور التي يتخذها التوقيع الإلكتروني، التي تختلف باختلاف الطريقة التي تتم بها، كما تختلف من حيث قدرتها على توفير الثقة والأمان ووسائل الحماية التي تعتمد على الوسيلة التقنية المستخدمة[3]. قمنا بمعالجة صور التوقيع الالكتروني **أولا** وخصائصه **ثانيا**.

أولا: صور التوقيع الإلكتروني.

لم يعد التوقيع الإلكتروني مقتصرا على صورة واحدة نتيجة لتقدم الهائل في التكنولوجيا بل ظهرت صور جديدة للتوقيع الإلكتروني، ومن هذه الصور مايلي:

1/ التوقيع الرقمي.

يعتبر التوقع الرقمي من أهم صور التوقيع الإلكتروني نظرا لما يتمتع به من قدرة فائقة على تحديد هوية أطراف العقد تحديدا دقيقا ومميزا ، إضافة لما يتمتع به أيضا من درجة عالية من ثقة و الأمان في استخدامه و تطبيقه عند إبرام العقود التجارية، ويمثل التوقيع الرقمي في تلك الرموز السرية و المفاتيح المتماثلة وغير متماثلة، من حيث اعتماده على اللوغاريتمات و المعادلات الرياضية المعدة من الناحية الفنية، وذلك باستخدامه برنامجا محددا، بحيث لا يمكن لأحد الكشف عن الرسالة إلا الشخص الذي يحمل مفتاح فك التشفير والتحقيق من أي تحويل الرسالة قد تم باستخدام المفتاح الخاص إضافة إلى تحققه من أن الرسالة الواردة لم يلحقها أي تغيير أو تعديل[4].

---

1 محمد حسن رفاعي العطار،البيع عبر شبكة الإنترنت، الطبعة الأولى،دار الجامعة الجديدة،الإسكندرية،،2007،ص. 172.

2 إياد محمد عارف عطا سده،مدى حجية المحررات الإلكترونية في الإثبات،مذكرة ماجستير،كلية الدراسات العليا،جامعة النجاح الوطنية،فلسطين،،2009،ص. 61.

3 طيموش عزولة، فريدة علاوات ، التوقيع الالكتروني في ظل القانون 04/15 ، مذكرة ماستر تخصص القانون الخاص الشامل، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة بجاية، الجزائر، 2015-2016، ص.10.

4 زينب غريب، إشكالية التوقيع وحجيته في الإثبات، مذكرة لنيل رسالة ماستر، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس، الرباط، 2009- 2010، ص 36.

2/ التوقيع بالقلم الإلكتروني.

هذه الطريقة تتمثل في استخدام قلم إلكتروني حساس يمكنه الكتابة على شاشة الكمبيوتر عن طريق برنامج هو المسيطر أو المحرك لكل العملية ويقوم هذا البرنامج بوظفتين أساستين لهذا النوع من التوقيعات الأولى وهي خدمة التقاط التوقيع، والثانية خدمة التحقق من صحة التوقيع[1].

و تقوم هذه الطريقة على آلية عمل معينة، تتمثل في نقل التوقيع المحرر بخط اليد بواسطة التصوير بالماسح الضوئي ونقل الصورة إلى رسالة إلكترونية يراد بها إضافة هذا التوقيع إليها لإضفاء الحجية عليها.

وبالرغم من سهولة استخدام هذه الوسيلة إلا أنها محفوفة بالمخاطر، بحيث يكون من الصعوبة في بعض الأحيان نسبة الرسالة إلى موقعها. ذلك لأنه قد يتسنى للمرسل إليه الاحتفاظ بنسخة عن صورة التوقيع التي وصلته، وإعادة وضعها على أي وثيقة محررة عبر وسيط إلكتروني ويدعى أن واضعها هو صاحب التوقيع الفعلي[2].

3/ التوقيع الكودي (البطاقات الممغنطة).

هذه الصورة من أكثر الصور شيوعا في حياتنا العملية حيث تقوم البنوك بإصدار بطاقات الائتمان ، والتي تستخدم في السحب النقدي من خلال بطاقات الصرف الآلي والتي تخول حاملها إمكانية سحب مبالغ نقدية من حسابه بحد متفق عليه بينه وبين البنك مصدر البطاقة ، إضافة إلى ما تقوم به أيضا من عمليات دفع عبر الإنترنت ، حيث تحتوي هذه البطاقة على رقم سري لا يعرفه إلا صاحبه.والذي يخول له الدخول إلى حسابه وإجراء العمليات التي يريدها، في حالة إتمام العملية من خلال الصراف الآلي لصورة صحيحة وحصول العميل في عملية السحب مثلا على المبلغ الذي أرادة فإنه يحصل على شريط ورقي يثبت فيه المبلغ الذي تم سحبه والتاريخ والساعة والمبلغ المحسوب ورصيد المتبقي ، حيث حلت هذه الإجراءات جميعها محل التوقيع التقليدي لما تميز به من الأمان و الثقة وتميز صاحب البطاقة الذي يحمل الرقم[3].

4/ التوقيع البيوميتري.

إن الإقبال على إبرام المعاملات بشكل عام وفي مجال المعاملات التجارية و البنكية بشكل خاص يتوقف على مدى ما توفره الجهات من وسائل أمان تكفل السرية و الخفة في التعامل وتحقيقا لهذا الهدف توصلت البنوك لعالمية الكبرى إلى الاعتماد على الخواص الذاتية للإنسان[4]،ويقوم هذا على أساس التحقق من شخصية المتعامل بالاعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية ، مسح العين البشرية، التعرف على الوجه البشري، خواص اليد البشرية، التحقق من نبرة الصوت، والتوقيع الشخصي، ويتم التأكد من شخصية المتعامل عن طريق إدخال معلومات للحاسب أو الوسائل الحديثة مثل

---

1 خالد ممدوح إبراهيم، إثبات العقود والمراسلات الإلكترونية، طبعة الأولى، الدار الجامعية، الإسكندرية،2010،ص.275.

2 علي أبو مارية، التوقيع الإلكتروني ومدى قوته في الإثبات (دراسة مقارنة)،مجلة جامعة الخليل للبحوث،المجلد5، العدد2،جامعة فلسطين الأهلية، بيت لحم 2010،ص111.

3 نوال تزير ، الشكلية في العقود التجارة الإلكترونية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم سياسية، جامعة خميس مليانة، 2014/2013،ص.4.

4 سعيد السيد قنديل، التوقيع الالكتروني: ماهيته، صوره، حجيته في الاثبات بين التداول والاقتباس، ط2، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص6 ومايليها.

التقاط صورة دقيقة لعين المستخدم أو صوته أو يده ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسب ليقوم بعد ذلك بالمطابقة[1].

وما يلاحظ أن هذا التوقيع يعتري العديد من الصعوبات، مثل تآكل بصمات الأصابع عبر الزمن أو بسبب ممارسة العمل في بعض المهن، وتطابق وجه التوائم، وصعوبة الاستخدام في شبكة مفتوحة كالإنترنت، مثلا جعل تطبيق هذا النوع من التوقيع في شبكة الإنترنت قاصرا على استخدامات محددة[2].

ثانيا: خصائص التوقيع الإلكتروني.

يتميز التوقيع الإلكتروني بعدة خصائص أهمها ما يلي:

1- التوقيع الإلكتروني يتم عبر وسائل إلكترونية وعن طريق أجهزة الحاسب الآلي والانترنت أو على أسطوانة[3] حيث أصبح بإمكان أطراف العقد الاتصال ببعضهم البعض والإطلاع على وثائق العقد والتفاوض بشأن شروطه وكيفية إبرامه وإفراغه في محررات إلكترونية وأخيرا إجراء التوقيع الإلكتروني عليه[4].

2- لم يشترط في التوقيع الإلكتروني صورة معينة حيث أنه يمكن أن يأتي على شكل حرف أو رمز أو رقم أو إشارة أو حتى صوت، المهم فيه أن يكون ذو طابع منفرد يسمح بتمييز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه[5].

3- الوظيفة الرئيسية للتوقيع الإلكتروني هي الحفاظ على مضمون المحرر الإلكتروني وتأمينه من التعديل بالإضافة أو الحذف، وذلك عن طريق ربط المحرر الإلكتروني بالتوقيع الإلكتروني[6].

4- التوقيع الإلكتروني يحقق الأمان والخصوصية والسرية في نسبته للموقع، وبالنسبة للمتعاملين،وخاصة مستخدمي شبكة الإنترنت، وعقود التجارة الدولية، وذلك عن طريق إمكانية تحديد هوية الموقع، ومن ثم حماية المؤسسات من عمليات تزوير التوقيعات[7].

5- التوقيع الإلكتروني يحدد شخصية الموقع ويميزه عن غيره[8].

واستناداً لهذه الخصائص توجد عدة فروق جوهرية بين التوقيع الإلكتروني والتوقيع التقليدي نوردها فيما يلي:

- ✓ أن التوقيع العادي عبارة عن رسم يقوم به الشخص بمعنى أنه فن وليس علم ومن هنا يمكن تزويره، أما التوقيع الإلكتروني فهو علم وليس فن ويصعب تزويره، بحيث يتم التوقيع الإلكتروني بواسطة برنامج كمبيوتر خاص لهذه الغاية[1].

---

1 نسرين عبد الحميد نبيه، الجانب القانوني للقانون التجاري، منشأة المعارف، الإسكندرية ،2008ص344.

2 سهيلة طمين ، الشكلية في عقود التجارة الإلكترونية، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري-تيزي وزو- 2011، ص.57.

3 عباس العبودي، تحديات إثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، ط1،منشورات الحلبي الحقوقية، لبنان،2010، ص.149.

4 بشار محمود دودين،الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، ط 2،دار الثقافة للنشر والتوزيع،الأردن،2010، ص. 247.

5 عباس العبودي، مرجع سابق، ص. 149.

6 بشار محمود دودين، مرجع سابق، ص. 248.

7 عبد الحميد ثروت، التوقيع الالكتروني:ماهيته، مخاطره وكيفيته، مدى حجيته في الاثبات، دار الجامعة الجديدة، الإسكندرية، 2007،ص.38.

8 طيموش عزولة، فريدة علاوات، مرجع سابق ،ص.17.

- ✓ أنّ التوقيع التقليدي يتخذ شكلا معينا كالإمضاء أو الختم أو بصمة الأصبع وللموقع حرية اختيار إحدى هاته الصور، أما التوقيع الالكتروني فإنه لا يشترط شكل معين فالمهم أن يكون للتوقيع طابع منفرد يسمح بتمييز الشخص الموقع وتحديد هويته[2].

- ✓ التوقيع التقليدي يوضع على دعامة مادية تكون في الغالب دعامة ورقية[3] تحاكي الشكل الذي تم التصرف به من خلال الحضور المادي للأطراف في مجلس واحد، أما التوقيع الالكتروني فيتم عبر وسيط يير مادي أي الكتروني يتم عبر شبكة الانترنت بين أشخاص لا يجمعهم مجلس واحد[4].
- ✓ التوقيع التقليدي يقوم بوظيفتين فهو يحدد هوية الشخص الموقع ويعد دليل على الحضور المادي أثناء التوقيع، أما التوقيع الالكتروني فوظائفه تنحصر في أنه يحدد هوية الشخص الموقع ويحقق الأمان والثقة في صحة التوقيع ونسبه لصاحبه ويمنح كذلك صفة المحرر الأصلي للمستند مما يجعل من هذا الأخير دليلا للإثبات[5].

---

[1] صالح عطا الله، التوقيع الإلكتروني في التجارة الإلكترونية والتحكيم الإلكتروني، مقال منشور بتاريخ 2016/06/11 ، اطلع عليه في 2018/02/05 في الموقع:
http://newssparrow.blogspot.com/2013/05/blog-post_4572.html

[2] بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الانترنت، دار الثقافة للنشر والتوزيع،2010، ص.247.

[3] بشار محمود دودين، مرجع سابق ،ص.247.

[4] رؤى الأنصاري، تعريف التوقيع الالكتروني، مقال منشور بتاريخ 2014/05/14 ، أطلع عليه بتاريخ 2018/05/02 في الموقع:
http://isdept-info.blogspot.com

[5] علي مبروك ممدوح، مدى حجية التوقيع الالكتروني في الإثبات، دار النهضة العربية القاهرة، 2009 ،ص.49.

المطلب الثاني
وظائف التوقيع الالكتروني ومجالات تطبيقه.

بعدما تعرضنا في المطلب الأول لمفهوم التوقيع الالكتروني و عرضنا معظم تعريفاته و كذلك تطرقنا لخصائصه و صوره، في هذا المطلب سنتعرض لوظائفه و بعض مجالات تطبيقه.

الفرع الأول
وظائف التوقيع الالكتروني.

من تعريف التوقيع الالكتروني في قانون الاونسترال النموذجي وقوانين الدول العربية التي أخذت به نجد أنه يحقق أكثر من وظيفة وهي تحديد هوية الشخص الملتزم بالإضافة التزامه بمضمون السند الموقع عليه وإقراره[1] ويمكن إجمال وظائف التوقيع الإلكتروني في ثلاث وظائف أساسية وهي :

أولا: تحديد هوية الموقع.

نرى أن تعريف التوقيع الالكتروني يتجه إلى لزوم أن يدقق في الشخص الموقع، واعتبرت قوانين التجارة الالكترونية إن تحديد هوية الشخص الموقع هو إعطاء حجية التوقيع الالكتروني[2].

ثانيا: التعبير عن إرادة الموقع على السند.

إن الوظيفة الثانية للتوقيع الالكتروني والتي تظهر من خلال تعريف القوانين والفقه له هي إظهار إلتزام الموقع لمحتوى العقد الذي يذيل به، ذلك لكي يظهر رضا الموقع بمضمونه كاملا ومن هنا نرى أنه وسيلة للتعبير عن الإرادة[3].

ثالثا: إثبات سلامة العقد .

تعتبر هذه الوضعية الأهم والحديثة للتوقيع الالكتروني حيث تؤدي إلى الحفاظ على مضمون محتوى العقد وتكامله لان هذه الوثيقة الالكترونية التي يتم تبادلها عبر شبكة الانترنت تكون أكثر عرضة للمخاطر لكن يتم التغلب على هذه المخاطر عن طريق التشفير وهذا ما رأيناه في التوقيع الرقمي[4].

الفرع الثاني

مجالات تطبيق التوقيع الإلكتروني.

كثير من المعاملات التي تتم عبر شبكة الانترنت لا تتم إلاّ بالاعتماد على التوقيع الالكتروني لإثبات صحتها، ومن أبرز مجالات تطبيق التوقيع الالكتروني ما يلي:

---

[1] مبروك حدة، حجية السندات الالكترونية في الإثبات (دراسة مقارنة)، مجلة العلوم القانونية و السياسية، عدد 17، جامعة حمه لخضر الوادي، جانفي 2018، ص.46.

[2] الصفحة نفسها.

[3] مبروك حدة، مرجع سابق، ص.47.

[4] محمد عبيدات لورنس، إثبات المحرر الإلكتروني، دار الثقافة، عمان 2009،ص ص.156،154.

1- بطاقة الائتمان Credit card:

تعرف بخنها بطاقة بلاستيكية ومغناطيسية يصدرها البنك لصالح عملائه بدلا من حمل النقود، لها شكل مستطيل تحمل اسم المؤسسة المصدرة لها، شعارها، توقيع واسم حاملها ورقمها وتاريخ نهاية صلاحيتها[1] ، يستطيع العميل من خلالها شراء مستلزماته ثم التسديد لاحقا، أما عن كيفية تطبيق التوقيع الالكتروني من خلال بطاقة الائتمان فإنه يتم باستخدام التوقيع الرقمي[2].

2- بطاقة الصراف الآلي ATM:

من خلالها يمكن للعميل سحب مبالغ نقدية من رصيده بحد أقصى متفق عليه[3]، كما تمكنه من الاستفسار عن رصيده أو كشف حساب مختصر أو تحويل رصيده إلى رصيد آخر وإجراء إيداعات نقدية[4].

أما عن كيفية تطبيق التوقيع الالكتروني من خلال بطاقة السحب الآلي فإنّه يتم بإدخال بطاقة السحب الآلي في المكان الخاص لها في جهاز الصراف الآلي، ثم يقوم بإدخال الرقم الخاص بالبطاقة، وأخيرا تحديد العملية المصرفية المراد القيام بها سحب أو إيداع أو تحويل[5].

3- بطاقة الدفع Debited card:

من خلالها يمكن للعميل أن يسحب منها مباشرة قيمة مشترياته وأجور الخدمات المقدمة له، وذلك بناء على السندات الموقعة منه[6]، وتعتمد هذه البطاقة على وجود رصيد للعميل لدى البنك في حساب جاري[7].

فالعميل عند قيامه بتنفيذ عملية السحب فإنه يقوم بتحويل أمواله إلى البائع التاجر، فإذا كانت البطاقة ((On-line)) أي على الخط فإنه يتم تحويل الأموال يوميا[8]، وفي هذه الحالة يقوم المشتري بتسليم بطاقته للبائع ويقوم هذا الأخير بتمريرها داخل جهاز خاص، بعدها يقوم المشتري بإدخال الرقم الخاص به ليعلن الموافقة على إتمام العملية، أما إذا كانت خارج الخط ((Offline)) فإن التحويل يتم خلال عدة أيام، وفي هذه الحالة يستخدم التوقيع التقليدي من أجل تحويل المبلغ من رصيد بطاقة المشتري إلى رصيد البائع[9].

4- البطاقة الذكية Smart card:

---

1 محمد أمين الرومي، التعاقد الالكتروني عبر الانترنت، دار المطبوعات الجامعية الاسكندرية،2004 ،ص.130.

2 عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، ط2، دار الثقافة لنشر والتوزيع،الأردن،2012،ص.102.

3 عمار لوصيف، استراتجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، مذكرة ماجستير في العلوم الاقتصادية، جامعة منتوري قسنطينة،2009/2008،ص.42.

4 ميادة بلعايش/ حياة بن اسماعين، مشروع الصيرفة الالكترونية في الجزائر، مجلة أبحاث اقتصادية وإدارية، العدد السادس عشر، ديسمبر2014،ص.74.

5 عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، المرجع السابق،ص.102.

6 معطى سيد أحمد، واقع وتأثير التكنولوجيا الجديدة للإعلام والاتصال على أنشطة البنوك الجزائرية، مذكرة ماجستير في إدارة الأفراد وحوكمة الشركات، جامعة أبو بكر بلقايد تلمسان 2012/2011 ،ص.24.

7 معطى سيد أحمد، مرجع سابق ،ص.40.

8 علاء محمد عيد النصيرات، حجية التوقيع الالكتروني في الاثبات،(دراسة مقارنة)، ط1، دار الثقافة لنشر والتوزيع، الأردن، .2001 ، ص.42.

9 عيسى غسان ربضي، مرجع سابق ، ص.100.

هي عبارة عن بطاقة بلاستيكية، تحتوي على شريحة ميكروية ((Micro-processor puce)) يمكن استخدامها في استخراج وتخزين ومعالجة ونقل البيانات الرقمية كالنقود الالكترونية أو المعلومات الطبية[1].

وتتم برمجة هذه البطاقة من قبل شركات متخصصة حيث تقوم بإدخال بعض المعلومات المهمة وتبرمج دالة جبرية فتولد الرقم السري، وعند كل استخدام يقوم العميل بإدخال البطاقة في آلة القراءة مع دخول الرقم السري المولد في البطاقة[2].

المبحث الثاني
حجية التوقيع الالكتروني في الاثبات

إن وجود التوقيع الالكتروني ضمن المحرر على وسيط الكتروني غير مادي وانفصاله عن شخص الموقع قد يثير الشك حول مصداقيته في تمييز هوية صاحبه وضمان ارتباطه بالتصرف القانوني حيث يمكن للقراصنة اختراق نظام المعلومات ومعرفة التوقيع وفك شفرته

[1] نوال بن عمارة، وسائل الدفع الالكتروني (الأفاق والتحديات)، ص.7،بحث منشور بتاريخ 2017/02/03 اطلع عليه في 2018/06/08 في الموقع:

http://dspace.univ-ouargla.dz

[2] علاء محمد نصيرات، مرجع سابق ،ص .43.

واستخدامه دون موافقة صاحبه كل ذلك بخلاف التوقيع العادي الذي يتطلب الحضور الجسماني لصاحبه مما يسهل التحقق منه ويتم الاحتفاظ بنسخة من المحرر تكون بمنأى عن العبث والتغيير، ويمكن لخبراء الخطوط كشف أي تلاعب أو تزوير في التوقيع، إن مثل هذا التخوف رغم ما ينطوي عليه من بعض الصواب لم يقف عقبة أمام استخدام الوسائل التكنولوجية الحديثة في مجال الإثبات[1] وهذا بالاستعانة بجهات التوثيق الالكترونية والمرخص لها القيام بهذه الوظيفة، حيث تقوم بمنح شهادات بصحة التوقيع الالكتروني وذلك بعد التحقق من شخصية الأطراف المتعاقدة وإتباع وسائل الأمان التقنية التي تضفي حماية وسرية لهذا التوقيع[2].

إذا استطاع التوقيع الإلكتروني تحقيق شروط معينة تؤدي إلى وصوله إلى درجة الأمان والثقة في قدرته على تحقيق الوظائف التي يحققها التوقيع التقليدي،ففي هذه الحالة فإنه سيتمتع بالحجية القانونية في الإثبات،والأثر القانوني للتوقيع الإلكتروني للتوقيع الإلكتروني يختلف بحسب اختلاف مدى تحقيقه لكل هذه الشروط من عدمه،فالتوقيع الذي يحقق كل الشروط التي حددها القانون يتمتع بأثر قانوني أعلى من التوقيع الإلكتروني الذي لا يحقق كل هذه الشروط[3]، ومنه سنقوم في هذا المطلب بإبراز الشروط التي لابد أن يتوفر عليها التوقيع ونبين موقف التشريعات حول الأخذ بحجية التوقيع الالكتروني.

وسنعرض هذا المبحث من خلال المطلبين التاليين :

المطلب الأول : شروط حجية التوقيع الإلكتروني في الإثبات.

المطلب الثاني : موقف التشريعات من التوقيع الإلكتروني.

المطلب الأول

شروط حجية التوقيع الإلكتروني في الإثبات.

حتى يتمتع التوقيع الإلكتروني بحجية في الإثبات،لابد أن يستوفي الشروط التي تمنحه الحجية القانونية في الإثبات والتي يؤدي عدم توافرها إلى عدم تحقق وصف التوقيع الإلكتروني[4]، ويشترط في التوقيع الإلكتروني عموما حتى يقوم بوظيفته مجموعة من الشروط يمكن تصنيفها إلى نوعين من الشروط،شروط قانونية والتي تتطلب في كل توقيع،وشروط تكنولوجية تقنية خاصة بالتوقيع الإلكتروني[5].

وسنعرض هذا المطلب من خلال الفرعين التاليين:

الفرع الأول : الشروط القانونية للتوقيع الالكتروني.

الفرع الثاني:الشروط التكنولوجية التقنية للتوقيع الالكتروني.

الفرع الأول
الشروط القانونية للتوقيع الإلكتروني.

---

1 محمد حسين منصور، قانون الاثبات – مبادئ الاثبات و طرقه، دار الجامعة الجديدة للنشر، طبع سنة 1998،ص .287.

2 سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية،ط2007،2،ص.23

3 بسمة فوغالي، مرجع سابق، ص.87.

4 أسامة بن غانم العبيدي، مرجع سابق ،ص 164.

5 عبد الله بن عبد العزيز بن محمد الفحام،حجية التوقيع الإلكتروني في الإثبات،رسالة ماجستير،جامعة الإمام محمد بن سعود الإسلامية،المملكة العربية السعودية،1428،ص30.

بما أن التوقيع هو شكل خاص من أشكال الكتابة،فإنه يتعين لكي يحقق وظيفته في الإثبات أن تتوفر فيه الشروط التالية: أن يكون شخصيا،أن يكون مميزا لموقع التعاقد وأن يتصل التوقيع بالمحرر الكتابي[1].

أولا/أن يكون التوقيع شخصيا.

التوقيع هو علامة شخصية، بمعنى أن يتولى الشخص بنفسه وضع التوقيع،فإذا وقّع شخص آخر باسم الموقّع فلاّ يعتد بهذا التوقيع ويكون باطلا،ولو تم ذلك برضاء صاحب التوقيع، فالعبرة هنا بأن يكون التوقيع صادرا ممن يراد أن يحتج به عليه[2].

وحتى يتسنى للتوقيع القيام بأداء وظيفته،يجب أن يكون دالا على شخصية الموقع فطريقة التعبير من خلال الوسيط الإلكتروني وجهات التصديق الإلكتروني،تسمح بالتعرف على هوية صاحب التوقيع بطريقة محسوسة كماّ في حالة التوقيع في شكله الكتابي،ومع تقدم التقنيات التي تستهدف التثبت من التوقيع الإلكتروني والتي تسمح بتحديد هوية صاحب التوقيع من خلال أنظمة فعالة تكشف عمليات التسلل والقرصنة،وحماية الأطراف في ظل تقنيات عالية وبرامج أمنية للتأكد من هوية أصحاب التوقيع بما يؤكد سلامة التوقيع ويعزز الثقة ويدل على موافقة كل طرف على المعلومات الواردة برسالة البيانات،فكل تقنية تميز صاحبها ومستوفية للشروط المطلوبة في التوقيع يعتمد عليها كدليل إثبات،وهي مسألة موضوعية تخضع لتقدير قاضي الموضوع[3].

يشترط أن يكون التوقيع دالا ومحددا لشخص الموقع ليتحقق بذلك دوره في الإثبات،

ونستطيع القول أن التوقيع الإلكتروني قادر على تحديد هوية الشخص الموقع،إذ أنه وعند استعراض صور التوقيع الإلكتروني،نرى أنه بإمكان هذه الوسائل إذا دعمت بوسائل توفر الثقة الكافية بها، تحديد هوية الشخص الموقع بصورة ممتازة ربما تفوق قدرة التوقيع العادي، فالتوقيع البيومتري يقوم أساسا على استخدام الخواص الذاتية للشخص،الأمر الذي يؤدي إلى تحديد هويته،وأما التوقيع الإلكتروني القائم على الأرقام السرية فهو قادر على تحديد هوية الموقع، مادام أن التوقيع رقم سري لا يعرفه إلا صاحبه،فالشخص لا يستطيع أن ينكر استخدامه للبطاقة المقترنة برقمه السري الذي لا يعرفه غيره ولا يتشابه مع غيره،وأما التوقيع بالقلم الإلكتروني فهو إن أحسن استخدامه فهو قادر على تحديد هوية الموقع، إذ أن هذا النظام لا يمكن استخدامه إلا من قبل الشخص الموقع وحده والدليل على ذلك أن هذا النظام لا يعمل إذا اختلف الموقع وكذلك إذا وقع الشخص بصورة غير مطابقة لما هو مخزن في ذاكرة الكمبيوتر،أما التوقيع الرقمي فهو بدوره قادر على تحديد هوية الشخص الموقع، من خلال المفاتيح العامة والخاصة كما يمكن الاستعانة بسلطة التصديق للتحقق من هوية الشخص[4].

ثانيا/أن يكون مميزا لموقع التعاقد.

حتى يقوم التوقيع بوظيفته في الإثبات لمضمون المحرر،يلزم أن يكون التوقيع دالا على شخصية صاحبه ومميزا له عن غيره، فإذا لم يكن التوقيع كاشفا عن هوية صاحبه ومحددا لذاتيته فلا يعتد به وبالتالي لا يؤدي دوره في إثبات مضمون المحرر،ومن أمثلة ذلك أن يتخذ

---

1 بسمة فوغالي، مرجع سابق، ص. 94.

2 إيمان مأمون أحمد سليمان، مرجع سابق،ص 273.

3 خالد مصطفى فهمي، النظام القانوني لتوقيع الالكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 95 .

4 علاء محمد عيد نصيرات، المرجع السابق، ص ص.68،69.

التوقيع شكل حروف معرجة أو رسم آخر،أو كان التوقيع بالحروف الأولى من الاسم واللقب أو بواسطة ختم مطموس لا يمكن قراءته[1].

وهو ما نص عليه قانون التوقيع والتصديق الإلكترونيين 04/15 طبقا للمادة 3/7 «التوقيع الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات التالية: ... أن يمكن من تحديد هوية الموقع.... [2]» .

يمكن القول أن التوقيع الإلكتروني بصوره يعد من قبيل العلامات المميزة الخاصة بالشخص وحده دون غيره ولا يشاركه بها أحد، فالتوقيع البيومتري القائم على الخصائص الذاتية أو بالرقم السري بكل مجالاته أو بالقلم الإلكتروني أو التوقيع الرقمي،كلها تتضمن علامات مميزة تميز الشخص عن غيره، فالتوقيع البيومتري يقوم على الخصائص الذاتية للشخص التي يتميز بها عن غيره، كذلك الرقم السري فلا يمكن أن يتشابه اثنان بنفس الرقم السري داخل النظام الواحد فهو يميز كل شخص عن غيره فلا يستطيع أحد استخدام الرقم السري لشخص آخر ولا يمكنه أن يعرفه بأي طريقة إلا بإهمال صاحبه في حفظه،وكذلك التوقيع بالقلم الإلكتروني فهو مثل الإمضاء العادي في قدرته على تمييز الشخص عن غيره ويتمتع بقدر من الحماية فلا يمكن إنجازه إلا إذا طابق التوقيع بالقلم الإلكتروني الإمضاء المخزن في الكمبيوتر،أما بالنسبة للتوقيع الرقمي فهو كالرقم السري خاص بصاحبه ويستطيع أن يميزه عن غيره فهو يقوم على مفتاحين عام وخاص وهذا الخاص لا يعلمه إلاّ الشخص الموقع[3].

مما سبق نخلص إلى أن التوقيع يجب أن يحمل في طياته ما من شأنه التعرف على صاحبه بأن يكون مميزا ومحددا لشخص صاحبه بغض النظر عن وسيلة إصداره أي لا يشترط أن يتم التوقيع بخط يد الموقع، بل يمكن إتمامه بأداة منفصلة عن شخصه[4].

ثالثا/ إتصال التوقيع بالمحرر.

والمقصود بهذا الشرط أن يكون التوقيع ضمن المحرر كلا لا يتجزأ، وذلك حتى يمنح المحرر قيمته القانونية، ويكون التوقيع دالا على رضاء موقعه بمضمون المحرر، ومعنى ذلك أنه لابد أن يكون هذا التوقيع متصلا اتصالا ماديا ومباشرا بالمحرر المكتوب[5].

وإذا كان المستقر هو أن يوضع التوقيع في نهاية الكتابة التي تضمنها المحرر،حتى يكون منسجما على جميع البيانات المكتوبة الواردة فيه ويعلن عن موافقة الموقع والتزامه بمضمونه إلا أن وجود التوقيع في مكان آخر لا ينفي هذه الموافقة، وان كان يخضع لتقدير قاضي الموضوع، فالمهم هو أن يدل التوقيع على إقرار صاحبه بمضمون المحرر وقبوله له، لذلك فقد ورد في حكم لِ قضاء محكمة النقض الفرنسية باعتماد التوقيع حتى وان كان الموقع قد وضعه في أعلى الصفحة مادام يدل دلالة واضحة على إقرار الموقع بمضمون المحرر[6].

وتتعلق مسألة اتصال التوقيع الإلكتروني بالمحرر الإلكتروني أساسا،بكفاءة التقنيات المستخدمة في تأمين مضمون المحرر المدون إلكترونيا،وبالتالي تأمين ارتباطه بشكل لا يقبل الانفصال عن التوقيع،ومن أهم هذه التقنيات تقنية التوقيع الرقمي الذي يعتمد على مفتاحين عام وخاص

---

1 عبد الوهاب مخلوفي، مرجع سابق ، 220.

2 سماح كحول،حجية الوسائل التكنولوجية في الاثبات ،مذكرة لنيل شهادة الماستر قسم الحقوق ،كلية الحقوق و العلوم السياسية،جامعة قاصدي مرباح ورقلة،2015/2014،ص.30.

3 علاء محمد عيد نصيرات، مرجع سابق،ص65 .

4 إيمان مأمون أحمد سليمان، مرجع سابق،ص 276.

5 عبد الوهاب مخلوفي، مرجع سابق،ص 220.

6 إيمان مأمون أحمد سليمان، مرجع سابق، ص. 276-277.

ولا يستطيع أحد أن يطلع على مضمون المحرر إلا الشخص الذي يملك المفتاح القادر على تمكين الشخص من ذلك،وبناء على ذلك فإن المحرر يرتبط بالتوقيع على نحو لا يمكن فصله ولا يمكن لأحد غير صاحب المحرر المدون على هذا النحو من التدخل بتعديل مضمونه، ويمكن توافر هذا اشرط أيضا في شتى صور التوقيع الإلكتروني الأخرى،من خلال إعتماد تقنيات تكفل توافره،كما هو الحال في التوقيع بالقلم الإلكتروني[1].

الفرع الثاني
الشروط التكنولوجية والتقنية للتوقيع الإلكتروني.

نصت مجمل القوانين التي نظمت التوقيع الإلكتروني على جملة من الشروط يجب توافرها في التوقيع الإلكتروني حتى يمكن الإحتجاج به في الإثبات أهمها الموثوقية، ونعني بالموثوقية أن يكون التوقيع الإلكتروني توقيعا آمنا،وأن يتم التأكد من صحته بشهادة تصديق معتمدة[2].

أولا/ أن يكون التوقيع الإلكتروني توقيعا آمنا.

ولكي يكون التوقيع الإلكتروني توقيعا آمنا،يجب أن يكون التوقيع الإلكتروني الخاص بالموقع، والمقصود بذلك أن تكون بيانات إنشاء التوقيع أو ما يطلق عليها القانون الفرنسي معطيات إنشاء التوقيع، وهي مثل المفتاح الخاص في التوقيع الرقمي أو بصمة الإصبع وبصمة العين في التوقيع البيومتري أو الكود السري في التوقيع الكودي،فكل هذه المعطيات يجب أن تكون خاصة بالموقع وحده، بمعنى أن تكون حصرية على شخص واحد فقط[3] وهو الموقع، وقد نص على هذا الشرط معظم القوانين التي تبنت التوقيع الإلكتروني،فنجد التوجيه الأوروبي نص على هذا الشرط في الفقرة الثانية من المادة الثانية[4] والتي تنص على جملة من الشروط التي يتعين أن تتوافر في التوقيع المؤمن من بينها ارتباط التوقيع الإلكتروني فقط بالموقع،وقد أورد قانون اليونسترال النموذجي للتوقيع الإلكتروني الصادر عام 2001،هذا الشرط أيضا في الفقرة الأولى من المادة السادسة بنصه» ...أن تكون بيانات إنشاء التوقيع مرتبطة بالموقع»[5].

ولا يكفي أن يكون التوقيع الإلكتروني هو الخاص بالموقع وحده حتى يكون هذا التوقيع توقيعا آمنا،بل يجب أن يكون الموقع مسيطرا على وسائل إنشاء التوقيع الإلكتروني وعرف المرسوم الفرنسي في الفقرة الخامسة من المادة الأولى أداة إنشاء التوقيع الإلكتروني بأنها:
«شيء مادي أو برنامج حاسب آلي لإنشاء معطيات التوقيع الإلكتروني[6]»، ونجد أن قانون اليونسترال النموذجي الخاص بالتوقيعات الإلكترونية عند تناول هذا الشرط قد نص في المادة 3/6 على«...إذا كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر» وهو بذلك قد خلط بين وسيلة إنشاء التوقيع وبين معطيات أو بيانات إنشاء التوقيع، في حين نجد كل من القانون الفرنسي والتوجيه الأوروبي قد نص على نفس العبارة «أن تكون وسائل إنشاء التوقيع تحت سيطرة الموقع»، وعبر القانون المصري عن هذا الشرط

---

1 علاء محمد عيد نصيرات، مرجع سابق،ص 66-76.
2 بسمة فوغالي، مرجع سابق، ص. 97.
3 سامح عبد الواحد التهامي، مرجع سابق،ص 458.
4 عبد الوهاب مخلوفي، مرجع سابق،ص223 .
5 وهو الشرط الذي تضمنه قانون التوقيع الإلكتروني المصري رقم 15لسنة 2004في المادة ،18وتضمنه أيضا قانون المعاملات والتجارة الإلكترونية الإماراتي لسنة 2002في المادة ،20والمرسوم التنفيذي الجزائري 123/01في المادة 3مكرر والتي أضيفت بموجب المرسوم التنفيذي 162/07سالف الذكر.
6 Dispositif de création de signature électronique « un matériel ou un logiciel destiné à mettre en application les donnée de création de signature électronique ».

في المادة18 بـ" سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني" ويقصد بالوسيط الإلكتروني الوسيلة التي يتم بها إنشاء التوقيع الإلكتروني[1].

وبالتالي يجب أن تكون وسيلة إنشاء التوقيع الإلكتروني تحت سيطرة الموقع أو يتحكم فيها وحده،بحيث لا يستطيع أن يتحكم فيها شخص آخر غيره،بحيث تكون البيانات أو المعطيات الناتجة عن هذه الوسيلة خاصة بالموقع فقط ومرتبطة به[2].

أما المشرع الجزائري فقد نص على هذا الشرط بموجب المادة10 من القانون04/15 والتي تنص على أنه:« يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة » لتضيف المادة 11 من القانون 15 / 04 على أن الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني تتوفر فيها المتطلبات الآتية:

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

أ/ ألاّ يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة،وأن يتّم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الإعتماد.

ب/ألاّ يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الإستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الإعتماد.

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

2/ يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع[3].

ثانيا/التصديق الإلكتروني.

التصديق الالكتروني هو وسيلة فنية آمنة للتحقق من صحة التوقيع أو السند، حيث يتم نسبه إلى شخص أو كيان معين عبر جهة موثوق بها أو طرف محايد يطلق عليه مقدم خدمات التصديق[4].

1 / جهات التصديق الإلكتروني.

يعبر في قانون الأونسيترال النموذجي بشأن التوقيعات الالكترونية على جهة التصديق الالكتروني بمصطلح "مقدم خدمات التصديق،" حيث عرفته المادة الثانية على أنه: "شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية".

أمّا القانون الفرنسي فقد عرف مقدم خدمة التصديق في المرسوم 272 لسنة 2001 بأنه: "أي شخص يقدم شهادات التصديق أو خدمات أخرى في مجال التوقيع الالكتروني"[5].

أما المشرع الجزائري فقد اشترط نشوء التوقيع الإلكتروني الموصوف على أساس شهادة تصديق إلكتروني موصوفة والتي تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات التصديق الإلكتروني[6]،وهذا حتى يكون له حجية في الإثبات مماثلة للتوقيع المكتوب.

---

[1] مصطفى معوان،التجارة الإلكترونية ومكافحة الجريمة المعلوماتية،الطبعة الأولى،دار الكتاب الحديث،القاهرة،2008، ص124.

[2] سامح عبد الواحد التهامي، مرجع سابق،ص ص.462،461.

[3] بسمة فوغالي، مرجع سابق،ص.99.

[4] محمد حسين منصور، مرجع سابق، ص. 29.

[5] «prestataire de service de certification ‘ tout entite personne qui délivre des certificats électroniques ou fournit d’autres services en matière de signature électronique »

[6] إياد محمد عارف عطا سده، مرجع سابق،ص. 67.

والملاحظ على هذه التعريفات أنّها وسعت من المجال الذي تقوم به جهات التصديق الالكتروني، فإضافة إلى دورها الأساسي والمتمثل في إصدار شهادات التصديق الالكتروني فهي تقوم كذلك بنشاطات أخرى لها صلة بتقنية التوقيع الالكتروني.

غير أنّه ما يعاب على هذه التعريفات أنّها ذكرت كلمة 'شخص طبيعي'، ففي الواقع العملي لا يمكن له تقديم خدمة تصديق لأنها تحتاج إلى تقنيات وأجهزة معقدة وخبرات فنية، لذا لا يمكن أن يقوم بها إلا شخص معنوي سواء كان عام أو خاص[1] .

2/ مهام جهة التصديق الإلكتروني.

يمكن أن تسأل فيما إذا كان لجوء الأطراف إلى جهات التوثيق الالكتروني إلزامي أم لا؟ إذا نظرت إلى التوجه الأوروبي السابق ذكره نرى أنه ترك حرية اللجوء إلى جهات التوثيق إلى الأطراف ولم يجعلها إلزامية، لكن بعض القوانين جعلتها إلزامية مثل قانون التجارة الالكترونية الإماراتي قض ى أنه إذا اعتمد شخص التوقيع الالكتروني لابد أن يكون معزز بشهادة التصديق ومن هنا يمكن حصر مهام جهات التوثيق في النقاط الآتية:

- ✓ التحقق من هوية الموقع.
- ✓ إثبات مضمون التبادل الالكتروني.
- ✓ تحديد لحظة إبرام العقد[2].

المطلب الثاني

موقف التشريعات من التوقيع الإلكتروني.

لقد ساهمت الكثير من الهيئات و البلدان المهتمة بسن قوانين وتشريعات تعالج قضية التوقيع الإلكتروني لتضفي عليه الصفة الإلزامية وتعطيه الحجية الكاملة في الإثبات والذي هو زمام تلك المعاملات التجارية. التي تتم عبر الوسائل التكنولوجيا[3]، وسنتعرض إلى موقف قانوني الأنسيترال والتوجيه الأوروبي وإلى موقف التشريع الفرنسي والتشريع الجزائري من خلال الفرعين التاليين:

الفرع الأول : موقف قانون التجارة الدولية الاونستيرال و التوجيه الاوروبي من التوقيع الالكتروني.

الفرع الثاني : موقف التشريع الفرنسي و الجزائري من التوقيع الإلكتروني.

الفرع الأول
موقف قانون التجارة الدولية الاونستيرال و التوجيه الاوروبي من التوقيع الالكتروني.

اولا: موقف قانون التجارة الدولية الاونستيرال.

[1] سامح عبد الواحد التهامي، التعاقد عبر الانترنت-دراسة مقارنة-، دار الكتب القانونية، مصر، 2008، ص412.
[2] محمد حسين منصور، مرجع سابق، ص .293.
[3] سماح كحول، مرجع سابق،ص.31.

جاء قانون الأونسيترال كخطوة رائدة في الاعتراف بحجية التوقيع الإلكتروني والتعاملات التجارية التي تتم عبر الإنترنت، حيث يتضح من خلال ما ورد في المادة 3/6 من هذا المشروع ((يعتبر التوقيع الإلكتروني قابلا للتعويل عليه لغرض الوفاء بالاشتراط المشار إليه في الفقرة: إذا

أ/ كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص أخر.

ب/ كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع لسيطرة الموقع دون أي شخص آخر

ج/ كان أي تغيير في التوقيع الإلكتروني، يجرى بعد حدوث التوقيع قابلا للاكتشاف.

د/ كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف))[1].

توضح المادة المذكورة أعلاه أنه لابد من وجوب توافر هذه الاشتراطات حتى يصبح التوقيع مقبولا وله الحجية الكاملة في الإثبات، فقد وردت هذه الشروط بكل تفصيل حتى لا يدعى مجال لتوضيح أكثر.

كما بينت المادة 7من نفس المشروع السلوك التي لابد أن تتوفر في الموقع والتي يجب أن يتصف بها في توقيعه.

وبينت أيضا المادة 9 من نفس المشروع الالتزامات الواقعة على عاتق مقدم خدمات التصديق أو هيئة إصدار الشهادات بحيث توفر تلك الالتزامات ضمان قيام هذه الجهة بالخدمة المطلوبة منها مما يزيد من الأمان والثقة في التوقيع الإلكتروني[2].

كما يرى كل من عبد الله مسفر الحيان وحسن عبد الله عباس في تقييمهم لهذا المشروع بأن القانون جاء مفصلا بالشكل الذي يقضي على أي شبهة للتلاعب أو التحايل باستخدام التوقيع الإلكتروني، إلا أنه أغفل عن التطور التكنولوجي السريع الذي يحدث في مجال التجارة الإلكترونية، وبتالي فإن عباراته كانت من غير ذات المرونة التي تسمح بتطبيقها على بعض الحالات قد تستجد في المستقبل[3].

ثانيا: موقف التوجيه الأوروبي.

ينص التوجيه الأوروبي على وجوب الاعتراف بالحجية القانونية للتوقيع الإلكتروني حيث نصت المادة 1/5 من التوجيه الأوروبي بشأن التوقيعات الإلكترونية على الدول الأعضاء التي تكفل أن التوقيع الإلكتروني الذي يستند إلى شهادة مؤهل والذي يتم إنشائه بواسطة أداة إنشاء آمنة لها نفس الحجية القانونية بالنسبة للتوقيع بخط اليد وتكون مقبولة كدليل في الإجراءات القانونية.

وعلى الدول الأعضاء تكفل أن التوقيع الإلكتروني لا يمنع الفعالية القانونية كدليل في الإجراءات القانونية وحدها بحجة أنه في شكل إلكتروني، أولايستند إلى شهادة مؤهل، أو لايستند إلى شهادة مؤهل صادر عن المعتمدين مقدم خدمات التصديق، أولايتم إنشاؤها بواسطة إنشاء توقيع آمنة .

---

[1] المادة 6 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع ،2001.الأمم المتحدة نيويورك2002.

[2] المادة 7 و9من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع ،2001،الأمم المتحدة نيويورك2002.

[3] عبد الله مسفر الحيان، حسن عبد الله عباس، التوقيع الإلكتروني، دراسة نقدية لمشروع وزارة التجارة والصناعة الكويتية، مجلة العلوم الإقتصادية والإدارية، المجلد التاسع عشر، العدد الأول، 2013،ص.33.

يبين مضمون المادة المذكور أعلاه أن التوجيه الأوروبي ساوى بين التوقيع العادي والتوقيع الإلكتروني، كما دعا إلى عدم رفض التوقيع الإلكتروني الذي لا يحوز على مصادقة عليه من قبل مقدمي خدمات التصديق[1].

الفرع الثاني

موقف التشريع الفرنسي و الجزائري من التوقيع الإلكتروني.

أولا : موقف التشريع الفرنسي.

كان وعى المشرع الفرنسي مبكرا بضرورة اعتماد وسائل الاتصال الحديثة في المعاملات، وعيه هذا جعله يتدخل بموجب القانون رقم 525/80 الصادر في 12يوليو1980، والذي عدل المادة 1348 من القانون المدني، لينظم وسائل إثبات التصرفات القانونية بوجه عام، بحيث تبنى مفهوما حديثا للصورة، إذ منحها حجية معينة في الإثبات.

وهكذا جاءت المادة 1348 في فقرتها الثانية باستثناء مهم، على وجوب إعداد الدليل الكتابي، إذا كان أحد الأطراف أو المودع لديه لم يحتفظ بالسند الأصلي، وقدم صورة تعد نسخة مطابقة للأصل، ويعد دائما كل نسخ للأصل ناشئا عن إحداث تغيير تصعب إزالته في مادة الدعامة[2].

والملاحظ على هذه المادة أن المشرع الفرنسي منح للصورة حجية في الإثبات متى توافرت شروط ذلك، حيث اشترط أن تكون تلك الصورة نسخة مطابقة للأصل، وهو شرط بديهي وضروري فلا يعقل أن تكون الصورة مخالفة للنسخة الأصلية، إضافة إلى شرط التطابق، نجد شرط الدوام، وهو ما عبر عنه المشرع الفرنسي في نهاية المادة بقوله: "ويعد دائما كل نسخ للأصل ناشئا عن إحداث تغيير تصعب إزالته في مادة الدعامة".2

وهكذا كان تدخل المشرع الفرنسي جزئيا، اقتصر في بداياته على بعض القطاعات المحددة مثل قانون 30أبريل1983 بشأن السماح باستخدام الوسائط الإلكترونية كبديل عن الدفاتر التجارية في تدوين حسابات التجار، وهو ما استتبع تعديل نص المادة 47 من قانون الضرائب الفرنسي، ليصبح ممكنا قبول قسائم الشراء المدونة أو المتبادلة عبر وسيط إلكتروني من قبل جهات الربط الضريبي، كما صدر مرسوم بقانون في 03ماي1999 معدلا نص المادة 289 من قانون الضرائب، وليسمح بقبول جميع المحررات المدونة على وسائط إلكترونية، لمنحها نفس الحجية المقررة للمحررات الورقية في الإثبات قبل جهات الربط الضريبي[3].

إلى جانب هذه القوانين وغيرها، وتحت ضغط الإستجابة لمتطلبات التعامل الحديث، مع ما يفرض من استعمال تقنيات إلكترونية في الاتصال، تدخل المشرع الفرنسي بتعديل مهم على القانون المدني تعلق بالإثبات خاصة، لتدخل المحررات الإلكترونية في نطاق أدلة الإثبات، وبالتالي تحظى بنفس القوة والحجية التي تتمتع بها المحررات الورقية أو التقليدية.

وهكذا كان صدور القانون رقم 2000/230 الصادر في 13مارس2000 المتعلق بتطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني، حيث جاء هذا القانون بتعديل مهم شمل خاصة المادة 1316 من القانون المدني الفرنسي، إذ جاء فيها "يشمل الإثبات عن طريق

---

1 سماح كحول، مرجع سابق، ص.33.

2 نور الدين الناصري، "المعاملات والإثبات في مجال الاتصالات الحديثة"، سلسلة الدراسات القانونية المعاصرة، العدد 12، مطبعة النجاح الجديدة، الطبعة الأولى 1428-2007، ص ص. 64،65.

3 ثروت عبد الحميد، مرجع سابق، ص. 169.

الكتابة كل تدوين للحروف أو العلامات أو الأرقام أو أي رمز أو إشارة أخرى، ذات دلالة تعبيرية واضحة ومفهومة أيا كانت الدعامة التي تستخدم في إنشائها أو الوسيط الذي تنتقل عبره"[1].

وبهذا يكون المشرع الفرنسي قد وسع من مفهوم الكتابة المعدة للإثبات، لتشمل كل أنواعها، حيث كرس هنا مبدأ مهما، حاول من خلاله عدم التمييز في نطاق الكتابة المعدة للإثبات على أساس الوسيلة المعتمدة فيها والدعامة القائمة عليها، وهو بذلك يعترف للكتابة المعتمدة عبر دعامات إلكترونية بنفس الحجية التي للكتابة عبر دعامات مادية، فالعبرة ليست في تقنية اعتماد الكتابة ولا في الوسيلة المستخدمة فيها، وإنما في قدرة تلك الطريقة على إنشاء الكتابة ونقلها بما يحفظ كمالها، ويجعلها ذات دلالة تعبيرية واضحة،وهو ما عبرت عنه نفس المادة 1316 "تتمتع الكتابة الإلكترونية بنفس الحجية المعترف بها للمحررات الكتابية في الإثبات، شريطة أن يكون بالإمكان تحديد شخص مصدرها على وجه الدقة، وأن يكون تدوينها وحفظها قد تم في ظروف تدعو إلى الثقة"، غير أن المشرع جعل الحجية الممنوحة للكتابة الإلكترونية متوقفة على شرطين: يتمثل الأول في تحديد الموقع من خلال تحديد مصدر الكتابة، بينما تمثل الثاني في إمكانية تدوين وحفظ هذه الكتابة الإلكترونية بشيء يدعو إلى الثقة والطمأنينة في استعمالها.

إلى جانب هذه المادة 1316 التي شملها التعديل، نجد بعض المواد الأخرى، وكمثال عن ذلك المادة 1326 والتي أدخل عليها المشرع الفرنسي تغييرا، فقد كانت المادة تتطلب بأن تكون الكتابة والتوقيع بخط اليد في التصرفات القانونية الملزمة من جانب واحد، وجاء التعديل فاكتفى المشرع بأن تكون الكتابة صادرة عن الشخص نفسه[2].

وبهذا يكون المشرع الفرنسي من خلال القانون رقم 2000/230، قد جعل المحررات الإلكترونية المتضمنة لتوقيع إلكتروني تتساوى مع المحررات الكتابية المختومة بتوقيع يدوي أو تقليدي، من حيث الحجية في الإثبات، وهو بذلك يستجيب للتوجيهات الأوربية التي تسعى إلى ضرورة مسايرة التشريعات الوطنية لدول الأعضاء وذلك حتى لا تكون هناك ثغرة بين الواقع والقانون.

- ✓ بعض المحررات الخاصة بإثبات اتفاقات الائتمان أو الإيجار لأغراض السكن.
- ✓ الأوراق الخاصة بإلغاء أو إنهاء التأمين على الحياة أو التأمين الصحي، أو إلغاء الاستفادة منه.

ثانيا :موقف المشرع الجزائري .

اعترف المشرع الجزائري بحجية التوقيع الإلكتروني كغيره من التشريعات الأخرى و يظهر ذلك في القانون 04/15 المتضمن التوقيع والتصديق الإلكترونيين في المادة 7[3]بقوله ((التوقيع الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

- ✓ أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.
- ✓ أن يرتبط بالموقع دون سواه.

---

[1] المرجع نفسه، ص. 174.

[2] نور الدين الناصري، مرجع سابق، ص.80.

[3] المادة 7من القانون رقم 04/15 مؤرخ في 11ربيع الثاني عام 1436الموافق أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية الجزائرية،العدد 06،المؤرخ في 2015/02/10.

- ✓ أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- ✓ أن يكون منشأ بواسطة وسائل تكون تحت التحكم للموقع.
- ✓ أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات)).

تشير المادة المذكورة أعلاه أن المشرع الجزائري وضع شروط لابد من أن تتوفر في التوقيع الإلكتروني حتى يمكن إصباغ عليه صفة الحجية في الإثبات وهو نفس الموقف الذي أخذت به التشريعات السابقة الذكر حيث نجد أنها تتفق على مبدأ واحد وهو حتى يعتد بالتوقيع الإلكتروني في الإثبات يجب أن يتحكم ذلك بشروط وإلا تسقط صفة الحجية منه في الإثبات[1].

[1] سماح كحول، مرجع سابق، ص .34

الفصل الثاني

الفصل الثاني

القواعد الجنائية الحماية للتوقيع الإلكتروني

بعد أن درسنا في الفصل الأول الإطار التنظيمي للتوقيع الإلكتروني و كذلك حجيته في الاثبات ، في هذا الفصل سنتعرض للقواعد الجنائية الحامية للتوقيع الإلكتروني في التشريعات الغربية و العربية ، لكن بما أن جريمة الاعتداء على التوقيع الإلكتروني تعتبر من الجرائم الإلكترونية لذلك كان لزاما علينا للبحث في ماهية الجريمة الالكترونية من خلال التعرض للتعريف بها و دراسة أركانها و التعرف على خصائصها و صورها هذا سيكون في المبحث الأول أما المبحث الثاني سنتعرض من خلاله لصور الحماية الجنائية التي توفرها التشريعات الغربية و العربية للتوقيع الإلكتروني.

المبحث الأول : ماهية الجريمة الالكترونية (المعلوماتية)

المبحث الثاني :صور الحماية الجنائية للتوقيع الإلكتروني في التشريعات الغربية و العربية.

المبحث الأول

ماهية الجريمة الالكترونية

عرفت البشرية في نهاية القرن الماضي اتساعا وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع ونظرا للتطور السريع لهذه التقنية فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها تسمية الجرائم المعلوماتية.

و قد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة و نظرا لجسامة أخطارها و فداحة خسائرها و سرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين و المهتمين بأمن الصرح المعلوماتي لتحديد مفهومها، و خصائصها و أركانها و تحديد صورها و التمييز بينها و بين ما يقترب منها من ظواهر[1].

سنتعرض في هذا المبحث لمفهوم الجريمة الالكترونية ثم لخصائص وصور الجريمة الالكترونية، سيكون كل هذا وفق الخطة التالية:

المطلب الأول : مفهوم الجريمة الإلكترونية (المعلوماتية).

المطلب الثاني : أنواع الجريمة الالكترونية.

[1] سفيان سوير، جرائم المعلوماتية ، مذكرة ماجستير تخصص علوم جنائية و علم الإجرام ،كلية الحقوق، جامعة بوبكر بلقايد تلمسان، 2011/2010،ص.08.

المطلب الأول

مفهوم الجريمة المعلوماتية

إن موضوع الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول العامة ولاسيما الجزائر وتزداد أهمية تلك المسألة أمام الطابع الدولي والعالمي لشبكة الإنترنت فهذه الأخيرة تعتبر سلاح ذو حدين، يعمل بين جنبيه الظلمة والنور ويعكس وجهي الخير والشر في الإنسان، فهو وسيلة للربط والاتصال والتقارب وتبادل المعلومات والمنافع بين بني الإنسان إلا أنه يمكن أن يكون أداة تزوير وتضليل، لذا ظهرت الحاجة الماسة في الحد من هذا الجانب المظل[1].

ومن خلال هذا المطلب سنحاول استعراض تعريف الجريمة المعلوماتية **الفرع الأول** و أركان و خصائص الجريمة المعلوماتية **فرع ثاني** .

الفرع الأول

تعريف الجريمة الالكترونية

إن مسألة وضع تعريف للجريمة الالكترونية كانت محلاً لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى ووضعوا تعريفات مختلفة. ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية.وتعرف الجرائم الالكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال[2].

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن تم ابتزاز الأشخاص باستخدام تلك المعلومات[3].

---

[1] سمية مزغيش،جرائم المساس بأنظمة المعلوماتية، مذكرة ماستر قانون جنائي،كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر بسكرة ص.13.

[2] دياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية- بتاريخ 04-09-2014م، ص 02.

[3] مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، بدون دار النشر، وبدون سنة.

لقد تعدت تعارف الجريمة الالكترونية فهناك من تناولها من الزاوية التقنية أو من الزاوية القانونية، وهناك من عرفها اعتمادا على وسلة ارتكاب الجريمة. كما عرفها الأستاذ جون فورستر بأنها" فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسة[1] " كما أن هناك جانب من الفقه لا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي؛ ولذلك عُرفت هذه الجريمة بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"، وبذلك عرفها الدكتور هشام فريد رستم بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات اساسية لمرتكبه[2]" .

تتكون الجريمة الالكترونية من مقطعيين هما الجريمة والالكترونية، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات؛ أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الالكترونية فهي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت[3]" .

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أن الجريمة المعلوماتية هي " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازماً من ناحية؛ وملاحقته من ناحية أخرى كما عرفها هذا الاتجاه بأنها" هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط". أما أصحاب الاتجاه الموسع يعرف الجريمة المعلوماتية بأنها " كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر[4]".

فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة 2000 تعريف الجريمة الالكترونية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي،والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[5].

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، بدون طبعة، 2011م، ص 29.

[2] عادل يوسف عبد النبي البشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، الكوفة، ص 113.

[3] ذياب موسى البدانية، مرجع سابق، ص 310.

[4] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014م، ص 118.

[5] خالد عياد الحلبي، مرجع سابق، ص 30.

أما التعريف الدولي للجريمة الالكترونية فهو يعتمد في الغالب على الغرض من استخدام المصطلح؛ فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر وأنظمة تمثل جوهر الجريمة الالكترونية. كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر[1].

ثمة اختلاف كبير بشأن المصطلحات المستخدم للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر والانترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات.فابتداء من مصطلح استخدام الكمبيوتر، مرورا بمصطلح الاحتيال بواسطة الكمبيوتر، والجريمة المعلوماتية و جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر وجرائم التقنية العالية، إلى جرائم الهاكرز أو الاختراقات فجرائم الانترنت وأخيرا السيبر كرايم[2].

من المصطلحات التي شاعت في العديد من الدراسات هو اصطلاح الجرائم الاقتصادية المرتبطة بالكمبيوتر وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال. أما عن اصطلاحي جرائم الكمبيوتر و الجرائم المرتبطة بالكمبيوتر و الجرائم الالكترونية فهذه المصطلحات تعتبر الأكثر دقة للدلالة على هذه الظاهرة بالرغم من أنهما ولدا قبل ولادة الشبكات وقبل الانترنت، تحديداً ليس لسبب إلا لكون الانترنت بالنسبة للمفهوم الشامل لنظام المعلومات مكون من مكونات هذا النظام، وأن النظام من جديد أصبح يعبر عنه باصطلاح نظام الكمبيوتر أو النظام ألمعلوماتي[3].

الفرع الثاني

أركان و خصائص الجريمة المعلوماتية

أولا: أركان الجريمة المعلوماتية.

تنهض الجريمة على ركنين رئيسيين هما الركن المادي والركن المعنوي، فلا بد للجريمة المعلوماتية إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها، ولا بد أيضا من ركن معنوي يعبر عن إرادة المجرم المعلوماتي.

[1] ذياب موسى البداينة، مرجع سابق، ص 313.
[2] محمود إبراهيم غازي، مرجع سابق، ص 120.
[3] المرجع نفسه، ص 122.

1. الركن المادي.

لا بد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما يدور في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم ، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد ، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تمامًا لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكومبيوتر. وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها (التقليدية) ، وهذا ما يدعو للتدخل التشريعي.

2. الركن المعنوي

الجريمة ليست كيانا ماديًا خالصًا قوامه الفعل وما يترتب عليه ، بل هي فوق ذلك كيان نفسي ، ذلك أن ماديات الجريمة لا تنشئ لمفردها مسؤولية ، وهذا المنطق يسري على الجرائم المعلوماتية شأنها شأن أية جريمة أخرى ، فلا بد أن ترتكب من شخص قادر على تحمل تبعة أفعاله (مسئول جزائيا) وبذلك لا يسأل عنها من لا يعترف لهم قانون العقوبات بهذه الصفة وهم من كان فاقد الإدراك أو الإرادة .والركن المعنوي بصفة عامة علاقة تربط بين ماديات الجريمة وشخصية الجاني وهذه العلاقة تكون محل لوم للقانون وتتمثل في سيطرة الجاني على سلوكه ونتائج هذا السلوك ، وجوهر هذه العلاقة الإرادة ومن ثم فهي ذات طبيعة نفسية . ومعلوم أن هناك تقسيم للجرائم يعتمد الركن المعنوي أساسا له، وبموجبه تكون الجرائم إما عمديه وإما غير عمديه[1].

ثانيا: خصائص الجريمة الالكترونية

تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى ومن بين أهم هذه الخصائص ما يلي[2].

[1] غايب نصار، الجريمة المعلوماتية، تم الاسترجاع في 17-11-2016 من الموقع :
http://www.iasj.net/iasj?func=fulltext&aId=28397

[2] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25، ص 16.

1.مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في – الغالب – شخص أمي بسيط ، متوسط التعليم.

2. مرتكب الجريمة الإلكترونية – في الغالب – يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية – غالبا – ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع.

3. تقع الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات.

4.الجريمة الإلكترونية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

5.هي جريمة ناعمة، تنفذ بسرعة وهي صعبة الإثبات:ناعمة أي أنها لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، تنفذ بسرعة أي أنها تتميز بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جداً قد لا يتجاوز الثانية الواحدة، وفي المقابل فهي صعبة الإثبات لعدم وجود الآثار المادية التقليدية(مثل بقع الدم، تكسير، خلع...الخ). وهذا ما جعل وسائل الإثبات التقليدية غير كافية، مما أدى إلى البحث عن أدلة فعالة لإثباتها، كاستخراج البصمات الصوتية أو استعمال شبكية العين ومضاهاتها باستخدام وسائل آلية سريعة[1].

[1] كامل فريد السالك، الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية 21-23 أكتوبر 2000، الجمعية السورية للمعلوماتية، حلب، سورية.

6. **الجاذبية:** نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات...الخ[1].

7. **امتناع المجني عليهم عن التبليغ:** لا يتم في غالب الأحيان الإبلاغ عن جرائم الانترنيت إما لعدم اكتشاف الضحية لها و إما خشية من التشهير، لذا نجد أن معظم جرائم الانترنيت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها[2].

8. **سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه:** يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها،أمر في غاية الصعوبة[3].

---

[1] عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها..خصائصها،دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ 2013/01/13 على الرابط :تاريخ الاطلاع 2017/02/13.

http://accronline.com/article_detail.aspx?id=7509

[2] محمد صالح العادلي، الجرائم المعلوماتية (ماهيتها وصورها)، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان،2-4 أفريل 2006، ص 7.

[3] موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص3.

المطلب الثاني

أنواع الجريمة الإلكترونية.

بعد أن تعرضنا في المطلب الأول من هذا المبحث لتعريف الجريمة الالكترونية، أركانها و خصائصها، سنتعرض في هذا المطلب لأنواع الجريمة الالكترونية .

تعددت محاولات الفقه لتحديد أنواع الجرائم المعلوماتية و ذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة و كذا عدم وجود تعريف عام متفق عليه للجريمة المعلوماتية و تحديد مجالها و كذا بالنظر للتطور التكنولوجي في كل صوره للارتباط الوثيق بينهما[1].

و نظرا لذلك تعددت تقسيمات الجرائم المعلوماتية إلى طوائف مختلفة تتميز كل منها بسمات خاصة بالنظر إلى اختلاف المعيار المعتمد في التقسيم.

فهناك من قسم الجرائم المعلوماتية إلى ثلاث طوائف تتمثل في جرائم الحاسب الآلي الاقتصادية و جرائم الحاسب الآلي التي تنطوي على الاعتداء على حرمة الحياة الخاصة و أخيرا جرائم الحاسب الآلي التي تحدد المصالح القومية أو السلامة الشخصية للأفراد[2].

كما قسمها آخرون بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية و مدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف رئيسية تتمثل الأولى في الدخول و الاستعمال غير المصرح ما لنظام الحاسب الآلي و الثانية تتمثل في طائفة الاحتيال المعلوماتي و سرقة المعلومات و الطائفة الأخيرة تتمثل في الجرائم التي يساعد الحاسب الآلي على ارتكاب و الأفعال التي تساعد على ارتكاب جرائم الحاسبات الآلية[3].

و من الملاحظ أن هذه التقسيمات أو بعضها لم تراع بعض أو كل خصائص هذه الجرائم و موضوعها و الحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخرى.

---

[1] سفيان سوير، مرجع سابق، ص.32.

[2] Sieber (Ulrich), Criminal liabijlity for the transfer of data in international computer network, New problems for German law, European journal of Crime, law and criminal justice, Vol. 34, 1997, b p 3-27.

[3] Wasik (Martin),op, cit .p41.

و يرى البعض من الفقهاء أنه يجب مراعاة في كل محاولة لتقسيم الجرائم المعلوماتية اعتباران هما:

- ✓ التطور المستمر الذي يطرأ على الجريمة المعلوماتية بصفة عامة.
- ✓ معيار الجريمة المعلوماتية أي ما يدخل في إطار هذه الجرائم و ما يخرج منها[1].

و مراعاة للاعتبارين السابقين ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين بالاعتماد على محل الجرائم المعلوماتية التي تنصب على معطيات الحاسوب و تطال الحق في المعلومات بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ يستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسب الآلي[2].

وتتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي ، و هذا ما سنتطرق له بشكل من التفصيل .

الفرع الأول

الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي.

يشتمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية ، و يعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية و مضاعفا لجسامتها.

و يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة[3]،إذ تهدف هذه الجرائم الاعتداء على أموال الغير، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة ، و منه لا يكون النظام المعلوماتي هو محل الحماية الجنائية.

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005،ط 01،ص.256.

[2] سوير سفيان، مرجع سابق،ص.33.

[3] نائلة عادل محمد فريد قورة، مرجع سابق، ص.265.

تتعدد صور الجرائم المعلوماتية المرتكبة باستخدام النظام المعلوماتي بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها ، نتعرض لهذه الأفكار بشكل من التفصيل[1].

أولا/الجرائم المعلوماتية الواقعة على الأشخاص الطبيعية.

تقع هذه الجرائم على الأشخاص و تنقسم بدورها إلى طائفتين بحسب نوع الحقوق المعتدى عليها و دور النظام المعلوماتي في اقترافه.

تتمثل الطائفة الأولى في الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية، و أما الطائفة الثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة نتناولها فيما يأتي[2]:

1/طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية و الأدبية، ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر ، أو حالة تخزين و استخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها، ذلك أن استخدام معلومة معينة دون إذن صاحبها يتضمن اعتداء على حق من الحقوق المعنوية إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية و يندرج ضمن الحقوق الفكرية كذلك براءات الاختراع إذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع[3].

و قد نص المشرع الجزائري على حقوق الملكية الفكرية و براءات الاختراع من خلال عدة نصوص قانونية نذكر من بينها:

-المادة38 :من الدستور الجزائري التي تنص على أن "حرية الابتكار الفكري و الفني و العلمي مضمونة للمواطن.
حقوق المؤلف يحميها القانون.

[1] سفيان سوير، مرجع سابق،ص.33.
[2] المرجع نفسه،ص.34
[3] أحمد خليفة الملط ، الجرائم المعلوماتية،دار الفكر الجامعي الإسكندرية، مصر،2005، ص.184.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ و الإعلام إلا بمقتضى أمر قضائي.

الأمر 05/03المؤرخ في 2003.07.19المتعلق بحقوق المؤلف و الحقوق المجاورة .

و الأمر 07/03المؤرخ في 2003.07.19المتعلق ببراءات الاختراع[1].

2/طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة.

لقد كفلت جل الدول الحياة الخاصة لمواطنيها بالحماية وقد حذا الدستور الجزائري حذو الدساتير الدولية بحرصه على حماية الحياة الخاصة للمواطنين[2]بموجب المادة39: من الدستور الجزائري والتي تنص على أنه"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

ولاشك أن الحاسبات الآلية بما لها قدرة فائقة على تخزين أكبر كم ممكن من المعلومات، أصبحت مخزنا لأهم المعلومات و أكثرها حساسية المتعلقة بالأفراد.
و لأهمية المعلومات التي تحتويها أنظمة الحسابات الآلية أصبح لهذه الحسابات دورا هاما في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة[3].

وعليه يمكن أن يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد،كأن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه ، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص اختراق معلومات تتمثل في أسرار مكتوبة و سير ذاتية و مذكرات حياة شخصية لشخص آخر[4].

ثانيا/الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى.

[1] سفيان سوير، مرجع سابق،ص.34.
[2] تنص المادة 45 من الدستور المغربي " حياة المواطنين الخاصة حرمة يحميها القانون و المراسلات و البرقيات و المحادثات التليفونية و غيرها من وسائل الإتصال لها حرمتها و سريتها مكفولة و لاتجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب و لمدة محدودة وفقا لاحكام القانون .
[3] نائلة عادل محمد فريد قورة، مرجع سابق، ص.275.
[4] أحمد خليفة الملط ، مرجع سابق، ص.187.

هذا النوع من الجرائم لا يستلزم تدخلا لإتلاف الوظائف الطبيعية للنظام المعلوماتي و لا تعديلا على المعلومات المعالجة ، بل يقتصر في غالب الأحيان على الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات و التصنت عليها لدى النظم المعلوماتية الأخرى بالإضافة إلى إساءة استخدام البطاقات الائتمانية و سوف نبين هاتين الصورتين كالآتي[1]:

1/الولوج غير المشروع للمعلومات المعالجة آليا.

تقوم هذه الصورة بوجود المجرم المعلوماتي داخل أحد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها آليا و الإطلاع عليها من دون تصريح و قد يكون هذا الولوج إما مباشرا أو غير مباشر.

فأما الولوج المباشر فيعد من أكثر الأفعال المرتكبة و أسهلها تنفيذا و يتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة المعلوماتية بعدة طرق باستخدام آلة الطباعة أو استخدام شاشة النظام أو الإطلاع على المعلومات بالقراءة على ما هو مكتوب عليها أو باستخدام مكبر الصوت[2].

و من أمثلة الولوج المباشر قيام موظف سابق بأحد البنوك الفدرالية الأمريكية الذي كان يعمل في النظام المعلوماتي الخاص بالبنك نقل المعلومات المالية المخزنة في النظام و نقلها لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له[3].

و أما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة ، لها صلة بالنظام المعلوماتي كالمعالجة عن بعد إذ أن هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج و الاستفسار عن بعد من المراكز المعلوماتية ، إذ أنه أثناء حركتها و بثها تكون مهددة للالتقاط و التسجيل غير المشروعين في كل لحظة كتوصيل خطوط تحويلية لالتقاط المعلومات المتواجدة ما بين النظام المعلوماتي و النهاية الطرفية و إرسال المعلومات

[1] سوير سفيان، مرجع سابق،ص.36.
[2] أحمد خليفة الملط، مرجع سابق، ص.190.
[3] محمد سامي الشوا،ثورة المعلومات و انعاكساتها على قانون العقوبات ،دار النهضة العربية،1994،ص.67.

المختلسة إلى النهاية الطرفية عن طريق إشارات إلكترونية أو الولوج غير المشروع عن طريق أية طرفية بعيدة عن طريق نظام معلوماتي و معرفة كلمة السر أو مفتاح الشفرة المناسب[1].

2/إساءة استخدام البطاقات الائتمانية.

أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية.

و تعد من أخطر الجرائم المعلوماتية لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور و الحداثة ، و يتخذ هذا النوع من الجرائم المعلوماتية صورتين.

تتمثل الأولى في إساءة استخدام العميل البطاقات الائتمانية و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه و بين البنك كأن يستعمل بطاقة ائتمانية انتهت مدة صلاحيتها أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها ...إلخ. و أما الصورة الثانية تتمثل في إساءة استخدام الغير البطاقات الائتمانية كأن يقوم سارق استعمال البطاقة الائتمانية للحصول على السلع و الخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة[2].

ثالثا/الجرائم المعلوماتية الواقعة على الأسرار.

تقع هذه الجرائم باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت الأسرار عامة تخص مصالح الدولة و نظام الدفاع عنها أو أسرار خاصة تتعلق بالأفراد أو المصالح الاقتصادية للمؤسسات المختلفة أو ما يطلق عليها الأسرار المهنية، و يتخذ هذا النوع من الجرائم صورتين الأولى تتعلق بالجرائم الواقعة على أسرار الدولة و الثانية تتعلق بالجرائم الواقعة على الأسرار المهنية.

و تقع هذه الجريمة لسرقة معلومات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل[3].

---

[1] أحمد خليفة الملط ، مرجع سابق، ص.192.
[2] المرجع نفسه، ص.196.
[3] سفيان سوير، مرجع سابق،ص.38.

و هذه الجرائم تسبب أضرار لأصحابها أدبية و مادية معتبرة ، لذا حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات و الجنح ضد الشيء العمومي من المادة 61إلى 96مكرر من قانون العقوبات[1] بالإضافة للمادة394 مكرر03 من قانون العقوبات التي نصت " تضاعف العقوبات المنصوص عليها في هذا القسم[2] إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام ، دون إخلال بتطبيق عقوبات أشد " ، و حذا بذلك حذو مختلف تشريعات الدول على غرار المشرع المصري الذي نص على ذلك في قانون العقوبات في الكتاب الثاني المتعلق بالجنايات و الجنح المضرة بأمن الحكومة لاسيما عندما يكون إفشاء هذه الأسرار متعلقا بأسرار الدفاع الوطني[3] .

كما أن القانون الفيدرالي للولايات المتحدة الأمريكية لجرائم الحاسبات الآلية الصادر سنة 1984 عاقب بموجب أحكام المادة 03/1040،01 كل من يقوم بالدخول غير المصرح له إلى نظام الحاسب الآلي بإفشاء معلومات توجد داخل هذا الحاسب الآلي متى كان هذا الحاسب يستعمل بواسطة حكومة الولايات المتحدة الأمريكية أو لمصلحتها و ترتب عن ذلك الإضرار بهذا الاستعمال[4] .

كما أن مختلف التشريعات حمت الأسرار المهنية ذلك أن المعلومات التي توجد داخل النظام المعلوماتي تكون ذات طبيعة سرية، و منه يفترض توافر الثقة فيمن أوكلت إليه ، فجل التشريعات ألزمت الطبيب و المحامي بالمحافظة على الأسرار التي يقرها لهما المريض أو الموكل في الدعاوى[5].

الفرع الثاني

الجرائم المعلوماتية الواقعة على النظام المعلوماتي.

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية يتمثل في الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف إما المكونات المادية للنظام

[1] الأمر 156/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل و المتمم.
[2] القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات.
[3] أحمد فتحي سرور، الوسيط في قانون العقوبات،ط4،سنة 1991،ص.47.
[4] نائلة عادل محمد فريد قورة، مرجع سابق، ص.276.
[5] أحمد خليفة الملط ، مرجع سابق، ص.200.

المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي[1].
و هذا ما سنتطرق له بشيء من التفصيل كالاتي:

أولا/جرائم الاعتداء على المكونات المادية للنظام المعلوماتي.

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات و الشرائط و الكابلات...إلخ، ونتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية[2]،كأن تكون محلا للسرقة أو خيانة الأمانة أو الإتلاف العمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد أو العبث بمفاتيح التشغيل أو خربشة الشريط و إفساد أسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف، و يترتب على هذا الإتلاف خسائر كبيرة[3].

و من أمثلة ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة و توثيق المعلومات الحسابية إلى خسائر مالية معتبرة قدرت ب 5 ملايين فرنك فرنسي[4].

و يرى البعض من الفقهاء أنه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم، و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا و ليس على الأشياء المادية بمعنى الكلمة[5].

و تجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضآلة قيمته، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

---

[1] سفيان سوير، مرجع سابق،ص.39.
[2] أحمد خليفة الملط، مرجع سابق، ص.176.
[3] ذكي ذكي أمين حسونه ،جرائم الكمبيوترو الجرائم الأخرى ،المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة ، سنة 1993 ،ص.471.
[4] Rose (philippe), OP-cit, p58,59.
[5] André Lucas, le droit de l'informatique, paris, PUF 1987, P519,521.

ثانيا/جرائم الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي.

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة ، و قد تقع هذه الجرائم إما على البرامج التطبيقية و إما على برامج التشغيل و سنتطرق لهاتين الصورتين فيما يأتي:

1/الجرائم المعلوماتية الواقعة على البرامج التطبيقية.

يقوم الجاني في هذه الصورة بتحديد البرنامج أولا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

***تعديل البرنامج** :الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات[1].

***التلاعب في البرنامج:** يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية[2] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، و يصعب اكتشاف هذا البرنامج لصغره و دقته[3].

2/الجرائم المعلوماتية الواقعة على برامج التشغيل.

تعد برامج التشغيل تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام.

و تقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[4].

[1] أحمد خليفة الملط، مرجع سابق ، ص.173.
[2] المرجع نفسه،ص.545.
[3] le rapport du conseil de l'Europe, 15,18 novembre 1976.
[4] أحمد خليفة الملط، مرجع سابق، ص.175.

ثالثا/جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي و لما لها من قيمة اقتصادية، و بهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها و هذا ما سنتناوله فيما يأتي:

1/التلاعب في المعلومات.

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطريق مباشر أو غير مباشر.

فأما التلاعب المباشر يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، و يأخذ هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لاسيما في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين و دائمي التغيير بهدف الحصول على مرتباتهم[1]، أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طريق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك و تسجيلها و إعادة ترحيلها و إرسالها لحساب آخر في بنك آخر بهدف اختلاس تلك النقود[2].

في حين التلاعب غير المباشر يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة و معرفة أرقام وشفرات الحسابات[3].

كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة، و تكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة.

[1] Escroquerie aux Assedic de paris, jugement du 2 fev 1982 TGI de paris 13 ème ch expertise n°39, avril 1982
[2] l'informatique nouvelle , mai 1976n°73.
[3] أحمد خليفة الملط، مرجع سابق، ص.179.

2/إتلاف المعلومات:

قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية إتلاف المعلومات المخزنة بالنظام المعلوماتي.

ويتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو عن طريق استبدال أو محو المعلومات.

ويشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة من الخطورة لأنه في حالة نجاحه يستمر لوقت طويل قبل اكتشافه و يتولد عنه مكاسب كبيرة بمجرد استبدال رقم بآخر أو إحلال رقم مكان آخر ، 3فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام المعلوماتي[1].

[1] محمد سامي شوا، مرجع سابق، ص.75.

المبحث الثاني

صور الحماية الجنائية للتوقيع الالكتروني في التشريعات الغربية و العربية

بعد أن تطرقنا في المبحث الأول لمفهوم الجريمة الالكترونية أو الجريمة المعلوماتية كما تسمى عند البعض من خلال دراسة التعريف بها، دراسة أركانها ، دراسة خصائصها و كذلك صورها، كان لابد من التطرق في هذا المبحث لصور الحماية الجنائية للتوقيع الالكتروني في التشريعات الغربية و العربية لأن بحثنا في الأساس يبحث في صور الحماية الجنائية للتوقيع الإلكتروني و قد أخترنا أن نبحث و ندرس صور الحماية الجنائية للتوقيع الالكتروني في عدة تشريعات غربية منها وعربية ووقع الاختيار على التشريع الامريكي و الفرنسي بالنسبة للتشريعات الغربية و التشريع المصري و الجزائري بالنسبة للتشريعات العربية .

قمنا بتقسيم هذا المبحث وفق الخطة التالية :

المطلب الأول: صور الحماية الجنائية للتوقيع الالكتروني في التشريعات الغربية.

المطلب الثاني: صور الحماية الجنائية للتوقيع الالكتروني في التشريعات العربية.

المطلب الأول

صور الحماية الجنائية للتوقيع الالكتروني في التشريعات الغربية

وفرت بعض التشريعات الغربية حماية جنائية للتوقيع الإلكتروني و من أبرزها التشريع الفرنسي في إطار قانون العقوبات، و التشريع الامريكي في إطار قانون جرائم الكمبيوتر الفدرالي.

من خلال هذا المطلب سنحاول إستعراض صور الحماية الجنائية للتوقيع الالكتروني في التشريع الفرنسي **فرع أول و** صور الحماية الجنائية للتوقيع الالكتروني في التشريع الامريكي **فرع ثاني.**

الفرع الأول

صور الحماية الجنائية للتوقيع الالكتروني في التشريع الفرنسي.

أصدر المشرع الفرنسي بتاريخ 13مارس2000 قانونا خاصا بالتوقيع الإلكتروني رقم230 سنة 2000 في شأن تعديل قانون الإثبات في مجال تكنولوجيا المعلومات والمتعلق بالتوقيع الالكتروني السالف الذكر[1]، وقد أدرج هذا التعديل في نص المادة 1316من القانون المدني الفرنسي في ست فقرات.

الملاحظ من خلال هذه النصوص أنه لم يورد قواعد خاصة بالحماية الجنائية للتوقيع الإلكتروني بل تركها للنصوص العامة، وبالرجوع إلى هذه الأخيرة تطبق عليها جرائم الإعتداء الواقعة على النظام المعلوماتي وبياناته الواردة في المواد 1/323، 7/323 من قانون العقوبات الفرنسي، وجريمة التزوير المعلوماتي في المادة 441 من نفس القانون، وفيما يلي تفصيل لهذه الجرائم[2]:

[1] عائشة بن قارة مصطفى ،الحماية الجنائية للحكومة الإلكترونية (دراسة مقارنة)،رسالة دكتوراه قانون عام ، جامعة أبوبكر بلقايد تلمسان ،2018/2017، ص. 134.

[2] الصفحة نفسها.

أولا . الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني وبياناته:

من أبرز صور الإعتداء على النظام المعلوماتي للتوقيع الالكتروني هو الدخول إلى النظام والبقاء فيه بدون إذن، فضلا عن جريمة الإعتداء العمدي على النظام المعلوماتي الخاص بالتوقيع الإلكتروني.

1. جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي للتوقيع الإلكتروني:

نص المشرع الفرنسي على هذه الجريمة في المادة 323/ف من قانون العقوبات الفرنسي، ولقيامها ينبغي توافر ركنيها، المادي يتمثّل في الدخول أو البقاء غير المشروع في قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وتصنف هذه الجريمة من جرائم الخطر حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهي ليست من جرائم الضرر التي يشترط فيها إلحاق ضرر بالمجني عليه[1].

وتعد هذه الجريمة من الجرائم العمدية، وبالتالي لا يتصور وقوعها بطريق الخطأ، وصورة الركن المعنوي فيها هو القصد الجنائي العام.

2. جريمة الإعتداء العمدي على النظام المعلوماتي للتوقيع الإلكتروني:

نص عليها المشرع الفرنسي في المادة 323/ف2، ويتمثل الركن المادي لهذه الجريمة في التعطيل والتوقيف، أو بإفساده بأي وسيلة، ويعد ذلك أمرا منطقيا بالنظر لتعدد الوسائل وتميز الصبغة التقنية عليها حيث يصعب حصرها، وهي من الجرائم العمدية يتطلب فيها الأمر توافر القصد الجنائي العام بعنصرية العلم والإرادة، وهو ما يستفاد من نص المادة 323. 2فقرة 2من قانون العقوبات الفرنسي.

وبالتالي إذا ترتب إفساد أو تدمير سير النظام عن خطأ أو إهمال، فلا وجود لجريمة، وكمثال لذلك الشخص الذي يستعمل أسطوانة تحتوي على فيروس مدمر، دون علمه بوجوده[2].

ثانيا . الإعتداء على بيانات التوقيع الإلكتروني:

نص المشرع الفرنسي على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة 2/323 من قانون العقوبات الفرنسي، ويتمثّل الركن المادي لهذه الجريمة في النشاط الإجرامي الذي يتكون من ثلاث أفعال هي الإدخال أو المحو أو تعديل بيانات التوقيع الإلكتروني.

[1] عائشة بن قارة مصطفى، مرجع سابق،ص.135.
[2] الصفحة نفسها.

أما الركن المعنوي لهذه الجريمة فيتمثل في القصد الجنائي العام، بعنصريه العلم والإرادة، ولا يشترط توافر القصد الخاص، بل يكفي القصد الجنائي العام لتحقق الركن المعنوي[1].

ثالثا . تزوير التوقيع الإلكتروني:

جاء النص على هذه الجريمة في المادة441 من قانون العقوبات التي نصت على أنه: "يعد تزويرا كل تغيير تدليسي للحقيقة، يكون من شأنه إحداث ضررا، ويقع بأي وسيلة كانت، سواء وقع في محرر أو سند أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين" [2].

لقيام هذه الجريمة لا بد من توافر ركنين مادي ومعنوي على النحو التالي:

يقوم الركن المادي لهذه الجريمة في فعل تغيير الحقيقة في توقيع إلكتروني بأي وسيلة، ومن أشهر وسائل تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة كسر الشفرة[3].

يرى بعض الفقهاء[4] أن التوقيع الإلكتروني لا يمكن تقليده، وإنما يمكن استعماله دون علم مالكه باعتباره يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه، وذلك لأن التوقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يمكن أن يكون مماثل معه[5].

أما الركن المعنوي :يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، فجريمة تزوير التوقيع الإلكتروني من الجرائم العمدية، فيجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات، ومع ذلك تتجه إرادته إلى الفعل المجرم[6].

---

1 عائشة بن قارة مصطفى، مرجع سابق، ص. 135.

2 المرجع نفسه، ص. 136.

3 صالح شنين، الحماية الجنائية للتجارة الالكترونية(دراسة مقارنة) ،رسالة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبوبكر بلقايد تلمسان كلية الحقوق، 2013/2012، ص.239.

4 منير محمد الجنبيهي، ممدوح محمد الجنيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية،2006،ص .55.

5 حنان براهمي، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة لنيل شهادة الدكتوراه في القانون الجنائي،جامعة محمد خيضر بسكرة ،كلية الحقوق و العلوم السياسية،2015/2014، ص .239.

6 عائشة بن قارة مصطفى، مرجع سابق، ص .136.

الفرع الثاني

صور الحماية الجنائية للتوقيع الالكتروني في التشريع الأمريكي

بالإضافة إلى قانون إساءة استعمال الكمبيوتر أصدر المشرع الأمريكي في 03جوان سنة 2000 قانونا اتحاديا "للتوقيع الإلكتروني والتجارة الوطنية "،وقد سبق هذا القانون جهودا تشريعية ومنها القواعد الاتحادية للتوقيع والسجلات الإلكترونية الصادرة في 20مارس سنة 1997والتي وضعت لتطبيقها في مجال شركات الأجهزة والقانون الاتحادي للغذاء والدواء ومستحضرات التجميل وقانون الخدمة الصحية العامة[1].

وقد وضعت مجموعة العمل تقريرا في يوليه سنة 1992اقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني، غير أنها في31 أوت1994 أصدرت تقريرا وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية ،كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في 20مارس سنة 1997[2].

يعد أول تشريع هو "قانون المعاملات الإلكترونية الموحد" الذي أصدرته ولاية كاليفورنيا في 16سبتمبر سنة 1999والذي دخل حيز النفاذ في 01يناير سنة ،2000وقانون المعاملات الإلكترونية الموحد الذي أصدرته ولاية نورث كارولينا والذي دخل حيز النفاذ في 01أكتوبر 2000[3] .

وقد أصدرت ولاية نيويورك تشريعا في 28سبتمبر سنة 1999للسجلات والتوقيع الإلكتروني وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات الإلكترونية وقبول التوقيع الإلكتروني في التعاملات التجارية[4] ،4كذلك أصدرت ولاية كونتكيت قانونا للمعاملات الإلكترونية في فبراير سنة 2002ودخل حيز النفاذ في الأول من أكتوبر في ذات السنة ،كما أصدرت ولاية بنسلفانيا قانونا مماثلا في 16ديسمبر سنة1999[5].

---

[1] أشرف توفيق شمس الدين ،الحماية الجنائية للمستند الإلكتروني(دراسة مقارنة) ،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر:اكادمية شرطة دبي ،مركز البحوث والدراسات رقم العدد:1 ، من 26 إلى28 نيسان 2003 ،بدبي - الإمارات العربية المتحدة.

[2] كما صدر نموذج اختياري لقانون المعاملات الإلكترونية الموحد ،وذلك بهدف توحيد قواعد المعاملات التجارية الإلكترونية بين تشريعات الولايات ،و للبيانات المخزنة إلكترونيا تضمنتها تشريعات اتحادية منها ما ينص عليه الفصل 119من القسم الأول من تقنين الولايات المتحدة والذي يحمل عنوان "اعتراض وسائل الاتصالات السلكية والإلكترونية والشفهية.

[3] عبد الحميد ثروت ،مرجع سابق ،ص. 185و مابعدها.

[4] وقد كلف المشرع في ولاية نيويورك بموجب لمادة الثالثة من الفصل الرابع من هذا القانون ،مكتب تقنيات الولاية بوضع تقرير يتضمن وضع تنظيم ودليل عمل لإنشاء واستخدام وتخزين والمحافظة على التوقيع والسجلات الإلكترونية.

[5] أشرف توفيق شمس الدين ،مرجع سابق ،ص.7.

وبالرغم من تلك النصوص المتعلقة بالتوقيع الالكتروني ،إلا أن تلك القوانين الاتحادية والولائية لم تأت بحماية جنائية خاصة ،بل تركتها للنصوص العامة لجرائم الحاسوب.

وبالرجوع للقانون الفيدرالي الأمريكي المتعلق بالاعتداء على الحاسوب لسنة ،1996 نجد أن الفصل 1030تضمن نصوصا خاصة تجرم الاعتداء الحاسوب.

حيث يجرم المشرع الدخول العمدي على البيانات الموجودة بأجهزة الكمبيوتر بدون تصريح أويتجاوز التصريح الممنوح له أيا كانت الوسيلة المستخدمة والحصول عل معلومات سرية متعلقة بالدفاع الوطني أو العلاقات الخارجية أو الطاقة النووية ،أو الحصول على معلومات موجودة في سجل اقتصادي لمؤسسة مالية ،أويخص مصدر بطاقات مالية أوتقرير يتعلق بالمستهلكين[1].

كما عاقب المشرع على الدخول في حاسوب يستخدم في التجارة أو الاتصال بين الولايات ويقوم عمدا بنقل برامج أومعلومات أوكود أونظام الكمبيوتر[2]. ويعاقب المشرع كذلك كل من يمنع أو يحرم أو يتسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدماته أو نظام أو شبكة أومعلومات أو بيانات أو برامج[3]4. كما يعاقب المشرع على نقل أي مكونات لبرامج أومعلومات أو كود أو أمر دون موافقة المسؤولين على الكمبيوتر المستقبل للبرامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسارة لشخص أو أكثر[4].

وتجدر الإشارة إلى أنه يمكن توفير حماية جنائية عامة للتوقيع الالكتروني ،لكن يلاحظ أن المشرع اهتم بالتفصيل أكثر لان القانون الأمريكي من القوانين التي تهتم بالأمن القومي والجانب الاقتصادي ،تطلب أن تتعلق المعلومات المحصل عليها متعلقة بالأمن القومي ،أو بإحدى المؤسسات الاقتصادية ،ولا يجرم الدخول إلى النظام المعلوماتي ،بل لابد أن يترتب على الدخول إتلاف المعلومات أو البرامج التي تهتم بالأمن القومي والجانب الاقتصادي[5].

[1] محمد أمين الشوابكة ،مرجع سابق ،ص.20.
[2] عبد الحليم رمضان ،مرجع سابق ،ص.42.
[3] ياسين نافذ، مرجع سابق ،ص. 348.
[4] عبد الفتاح بيومي حجازي،النظام القانوني لحماية التجارة الالكترونية، مرجع سابق،ص.356.
[5] صالح شنين، مرجع سابق،ص.166.

المطلب الثاني

صور الحماية الجنائية للتوقيع الالكتروني في التشريعات العربية

خصت بعض التشريعات العربية التوقيع الالكتروني حماية جنائية، أبرزها التشريع المصري و التشريع التونسي اللذين كان سباقين في هذا المجال و لحق بهم المشرع الجزائري سنة 2015 من خلال سنه للقانون 04/15 المؤرخ في: 2015/02/01 المتضمن التوقيع و التصديق الالكترونيين .

من خلال هذا المطلب سنحاول إستعراض صور الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري **فرع أول و** صور الحماية الجنائية للتوقيع الالكتروني في التشريع المصري **فرع ثاني.**

الفرع الاول

صور الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري

بالرجوع إلى القانون الجزائري فالمشرع من خلال القانون رقم 04/15 المؤرخ في: 2015/02/01 تدخل مرة أخرى بعد سلسة من القوانين التي حاول من خلالها التصدي لهذا النوع المستحدث من الجرائم والاعتداءات الحاصلة على مستجدات هذا العصر.

وعليه؛ يثور التساؤل عن صور الحماية الجزائية التي قررها المشرع للتوقيع والتصديق الالكترونيين وفقا للقواعد العامة المقررة في قانون العقوبات، والقانون رقم: 04/15، وعليه سوف نوضح ذلك على النحو التالي.

أولا: صور الحماية الجزائية المقررة في قانون العقوبات.

بعد أن اعتد المشرع الجزائري بالتوقيع الالكتروني طبقا للمادة 327 من القانون المدني التي تنص في الفقرة الثانية منها على أنه "يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر1 أعلاه،" وقبل صدور القانون رقم04/15 لم ينظم المشرع الجزائري التوقيع الالكتروني ولم يحض بحماية جنائية خاصة على غرار التشريع الفرنسي، مما جعل حمايته تخضع للقواعد العامة المقررة في قانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الآلية[1]وجريمة التزوير.

[1] القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 156/66 المؤرخ 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية العدد 84،المؤرخة في 24 ديسمبر 2006.

1/ جرائم الاعتداء على النظام المعلوماتي للتوقيع الالكتروني:

يتحقق الاعتداء على التوقيع الالكتروني من خلال الاعتداء على النظام المعلوماتي له، وهذا بالدخول أو البقاء غير المصرح بهما، وهي الجريمة المنصوص والمعاقب عليها بموجب المادة394مكرر من قانون العقوبات الجزائري التي تنص على أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنة (5) وبغرامة مالية من50.000 دج إلى200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة.

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 (6) أشهر إلى سنتين (2) والغرامة من50.000 دج الى 300.000 دج .

وعلى ضوء ذلك فإنّ المشرع اعتبر فعل الدخول أو البقاء غير المصرح بهما من الأفعال الجرمية التي تطال النظام المعلوماتي للتوقيع الالكتروني، مما يتطلب منا معرفة ما هي أركانها سواء المادي المتمثل في فعلي الدخول أو البقاء وركن معنوي يتمثل في القصد الجنائي.

أ/ الركن المادي: بناء على المادة 394 مكرر من قانون العقوبات الجزائري فإنّ السلوك الإجرامي للركن المادي يتخذ إما صورة الدخول المنطقي وذلك بغرض فتح باب يؤدي إلى النظام المعلوماتي للتوقيع الالكتروني أو يتخذ صورة البقاء، وعليه؛ فإنّ هذا السلوك قد يكون ايجابيا يتمثل في فعل الدخول أو سلبيا يتمثل في الامتناع عن الخروج من النظام المعلوماتي والبقاء فيه.

ويعتبر الدخول أبسط تلك الأنشطة بحيث يكون بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي[1]، وعليه؛ فإنّ مجرد الدخول للنظام المعلوماتي للتوقيع الالكتروني لا يشكل فعلا غير مشروع وإنما يستمد عدم مشروعيته من كونه تم بطريق الغش أو ضد إرادة المسؤول على النظام وبعبارة أخرى بدون تصريح منه[2]، ويتحقق أيضا فعل الدخول المعاقب عليه في الحالة التي يتجاوز فيها التصريح بالدخول إما المجال المحدد له أو الغرض الذي منح لأجله[3].

[1] عبد الحليم يعقوب، الإعلام الجديد والجريمة الالكترونية، دار العالمية، مصر، 2014 ، ط01،ص.218.

[2] محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن، دار الجامعة الجديدة، الإسكندرية، مصر،2008 ،ص. 141.

[3] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار النهضة العربية، القاهرة، مصر،2009، ص.356.

أما البقاء فهو "التواجد داخل النظام ضد إرادة صاحب النظام أو من له السيطرة عليه[1]،وعليه فإنّ البقاء يبدأ من اللحظة التي كان يجب على الشخص فيها أن يغير وضعه بالخروج من النظام، وتحديد المدة المسموح بها للخروج من المسائل الموضوعية المتروكة للسلطة التقديرية لقاضي الموضوع[2].

وإلى جانب السلوك الإجرامي قد يتطلب قيام الركن المادي تحقق نتيجة إجرامية كما هو الحال في جرائم الضرر، أو لا يستلزم قيامه تحقق هذه النتيجة كما هو الشأن في جرائم الخطر، وجريمة الدخول والبقاء غير المصرح بهما المنصوص عليها في المادة 394 مكرر من قانون العقوبات جمع فيها المشرع هذا التقسيم إذ اعتبرها من جرائم الخطر حسب الفقرة الأولى وقرر عقوبة على كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من النظام المعلوماتي دون أن يترتب أي ضرر، أما الفقرتان الثانية والثالثة من ذات المادة فشددت العقوبة إذا ما ترتب على هذا الدخول أو البقاء عن طريق الغش إما إحداث أو تغيير لبيانات النظام أو تخريب نظام اشتغال المنظومة[3].

ب/الركن المعنوي:

بالرجوع إلى المادة 394 مكرر فقرة 1 فإنّ المشرع الجزائري اعتد بجريمة الدخول والبقاء غير المصرح بهما في صورتها البسيطة كجريمة عمدية تقوم على القصد الجنائي العام بعنصريه العلم والإرادة، ويتحقق ذلك بانصراف إرادة الجاني إلى الدخول أو البقاء غير المصرح بهما، وأن يعلم الجاني بماهية السلوك الإجرامي وتهديده لمصلحة يحميها القانون، وبالتالي لا شأن للعلم والإرادة بالنتيجة لأن هذه الأخيرة تخرج عن النموذج القانوني للجريمة[4].

أما عن الركن المعنوي للجريمة في صورتها المشددة فيتضح من خلال الفقرتين 2،3 من المادة 394 مكرر قانون العقوبات أن النتيجة المشددة هي نتيجة غير عمدية وهو الأمر الذي ذهب إليه جانب من الفقه الفرنسي أن هذه الجريمة تقع عن طريق الخطأ، ولا يتطلب المشرع فيها توافر القصد الجنائي العمدي، بحيث يعد الخطأ كافيا لقيام الجريمة، ومن

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الأردن،2008،ط01،ص.161.

[2] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية- دراسة مقارنة- دار الفكر والقانون،2015، الطبعة الأولى، ص.72.

[3] لم ينص المشرع الجزائري على جريمة الاعتداء القصدي على سلامة النظام المعلوماتي، بل اكتفى بالنص على الاعتداء كظرف مشدد، على خلاف المشرع الفرنسي الذي اعتبرها جريمة قائمة بذاتها حسب أحكام المادة 757-5من قانون العقوبات الفرنسي، انظر محمد خليفة، مرجع سابق، ص ص. 163 ،164.

[4] أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)،دار الجامعة الجديدة، الإسكندرية، مصر،2007،ص.244.

هنا فهي من جرائم الإهمال، وبالتالي فبمجرد ارتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذا استطاع الجاني إثبات وجود قوة قاهرة أدت إلى حدوثها[1].

2/ جريمة إتلاف التوقيع الالكتروني :

نص المشرع الجزائري على هذا النوع من الجرائم في المادة 394 مكرر1على النحو التالي "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث(3) سنوات وبغرامة مالية من 500.000 دج إلى 4.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

يتضح من خلال نص المادة أنه لقيام جريمة إتلاف التوقيع الالكتروني لابد من توافر ركنيين هما الركن المادي والركن المعنوي على النحو التالي:

أ/ الركن المادي:

يتخذ السلوك الإجرامي الذي يرتكبه الجاني في جريمة إتلاف التوقيع الالكتروني صورة الإدخال أو التعديل أو المحو، وينصب هذا السلوك على محل معين هو التوقيع الالكتروني ويستهدف تحقيق نتيجة معينة تتمثل أساسا في تغيير الحالة التي كانت عليها بيانات أو معلومات التوقيع الالكتروني.

وعليه؛ فإنّ المقصود بالإدخال هو "تغذية النظام بالمعلومات المراد معالجتها أو بتعليمات لازمة لعملية المعالجة[2].

أو هو "إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم كان يوجد عليها معطيات من قبل".

أما التعديل فيعني "تغيير البيانات أو المعلومات الموجودة داخل النظام واستبدالها بمعلومات أخرى."

في حين أن فعل الإزالة عرف على أنه "إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة [3]".

---

[1] نائلة عادل فريد قورة، مرجع سابق، ص.437.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر،1999، ص ص.135،134.

[3] محمد خليفة، مرجع سابق، ص.188.

ب/ الركن المعنوي :

يتبين من دراسة نص المادة 394 مكرر 1 من قانون العقوبات أن جنحة إتلاف التوقيع الالكتروني من الجرائم العمدية التي يتطلب قيامها توافر الركن المعنوي الذي يتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة.

وترتيبا على ذلك فيجب أن يعلم الجاني أنه يقوم بإتلاف توقيع الكتروني عن طريق الإدخال أو المحو أو التعديل في بياناته، بالإضافة إلى اتجاه إرادته إلى ارتكاب الفعل المادي المكون للجريمة وتحقيق النتيجة الإجرامية المترتبة على ذلك النشاط وهي إلحاق الضرر بصاحب التوقيع وجعل توقيعه الالكتروني غير صالح للاستعمال أو معيبا يفقده وظيفته ويهز ثقة المتعاملين مع صاحب التوقيع في شخصه.

أمّا القصد الخاص فإن المشرع الجزائري في المادة المذكورة أعلاه لم يستخدم أي عبارات تدل على ضرورة توافره، ومن ثم فإنّ توافر القصد العام كاف لقيام هذه الجريمة، لأنّ القصد الخاص هو انصراف العلم والإرادة إلى وقائع لا تدخل ضمن عناصر الجريمة وأركانها، ولفظ الغش الذي استخدمه المشرع يدل على أن الجريمة عمدية ولا يدل على القصد الخاص[1].

3/ جريمة تزوير التوقيع الالكتروني:

يعرف التزوير بأنّه:((تغيير للحقيقة بقصد الغش بمحرر بإحدى الطرق المبينة في القانون تغييرا من شأنه أن يسبب ضررا للغير))[2].

ولجريمة التزوير ركنان، ركن مادي يقوم بتغيير الحقيقة في محرر بإحدى الطرق الواردة في القانون تغييرا من شأنه أن يسبب ضررا للغير، وركن معنوي يتمثل في انصراف نية الجاني إلى ذلك التغيير وإلى استعمال فيما غير الحقيقة من أجله.

والجدير بالذكر أن المشرع الجزائري لم ينص على جريمة التزوير المعلوماتي بصراحة كما فعل المشرع الفرنسي في المادة 441 قانون عقوبات فرنسي، ومن ثمّ فإنّه لم يتناول جريمة التزوير الواقعة على التوقيع الالكتروني، وهو ما أثار الجدل بين مؤيد لإمكانية تطبيق النصوص التقليدية وبين معارض لذلك، وكل اتجاه له أسانيده ومبرراته.

[1] رياض فتح الله بصلة،حدود الإثبات العلمي في قضايا التزييف والتزوير، منشأة المعارف،الإسكندرية، مصر،2010،الطبعة الثالثة، ص.12.

[2] أيمن عبد الله، مرجع سابق، ص.366.

فيرى الاتجاه المعارض أنّ الطرق التي حددها القانون والتي يتم بها التزوير لا تتلاءم ولا تتناسب إلاّ مع المحرر في صورته المادية وهو في الغالب من الورق المكتوب[1]، وعليه فإنّ صور التوقيع التي حددها المشرع وربط مفهومه بوجوب اعتماده على حركة اليد، وتتمثل هذه الصورة في الإمضاء، بصمة الأصبع أو الختم، وهذا الشكل ينتفي في التوقيع الالكتروني الذي يتكون من رقم أو شفرة لا علاقة لها باسم الشخص أو لقبه أو ملامح بصمته.

أما الاتجاه المؤيد لإمكانية تطبيق النصوص التقليدية فيرى أنّ مصطلح المحررات الذي استخدمه المشرع هو مفهوم واسع يمكن أن تندرج ضمنه المحررات التقليدية والمعلوماتية، إضافة إلى أنّ التوقيع الالكتروني يؤدي نفس وظائف التوقيع التقليدي حسب ما أقره المشرع في المادة 327 قانون مدني جزائري، وعليه يستوجب توفير نفس الحماية لاتحاد في الوظيفة والهدف.

إلاّ أنّ الصعوبات التي تعرض تطبق النصوص التقليدية على تزوير التوقيع الالكتروني جعل ضرورة وجود نصوص خاصة تتلاءم وطبيعته التقنية، خاصة وأنّ جريمة التزوير المعلوماتي للتوقيع الالكتروني تتحقق عندما ينقل توقيع ذلك الشخص على الأوراق الخاصة المسحوبة على الحاسب الآلي دون علم منه أو رضاه ودون ترك أي أثر يدل على وقوعه، فنجد بالتعاملات البنكية يحتفظ بالتوقيع على الحاسب الآلي للمطابقة، مما يسهل سحبه على أوراق متعددة، كذلك أصبح بالإمكان التعاقد عن بعد ونقل التوقيع بين الدول الكترونيا[2].

وبالفعل فإنّ تصديق الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي رقم 252/14 المؤرخ 08 سبتمبر 2014 والتي تنص في مادتها العاشرة على أنه "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة" يكون قد قضى على هذا الجدل وأقر بالتزوير الذي يقع بواسطة التقنية الحديثة على التوقيع الالكتروني وتطبق العقوبات المقررة في القواعد العامة.

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، 2001، ط 01، ص. 206.

[2] انظر المواد 15إلى 30 القانون 04/15 المتضمن التوقيع والتصديق الالكترونيين.

ثانيا: صور الحماية الجزائية المقررة في القانون 04/15 :

إن الانتشار الواسع والسريع لاستخدام التكنولوجيا والتقنية الحديثة جعل المشرع يتدخل مرة أخرى لأجل بسط الحماية خاصة في المعاملات التجارية لأجل الحث على الإقبال على إبرام العقود الالكترونية التي أصبحت قابلة للتوقيع والتشفير والمصادقة الالكترونية من قبل أجهزة حددت صلاحيتها وشروط اعتمادها بدقة[1].

وبالرجوع إلى القانون 04/15 في الفصل الثاني من الباب الرابع نجد أن المشرع أقر حماية من خلال تعداد مختلف الجرائم المتعلقة بالتوقيع والتصديق الالكترونيين، وطالما أن المشرع لم يعتمد أي تصنيف لهذه الجرائم إلا أنّ قراءتنا لهذه النصوص والجرائم المتضمنة لها نميز بين تلك التي تلحق مؤدي خدمات المصادقة، وبين تلك التي تجرم بعض الممارسات المرتبطة بطالبي الخدمة، كما أن الاطلاع على تلك النصوص القانونية نجد وأن الجرائم التي نظمها المشرع تتفق في أنها جرائم عمدية يتطلب قيامها توافر الركن المعنوي الذي يقوم على القصد الجنائي العام بعنصريه العلم والإرادة ولا تحتاج إلى القصد الخاص[2].

ويتمثل العلم الواجب توافره في القصد الجنائي العام في إحاطة الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، أي كل واقعة يتطلبها القانون لبناء أركان الجريمة واستكمال عناصرها، وإضافة إلى ذلك لابد أن يشمل العلم أيضا التكييف الذي تتصف به بعض هذه الوقائع من الناحية القانونية، أو بعبارة أخرى يتعين على الجاني العلم بموضوع الحق المعتدى عليه.

أما الإرادة التي يتطلبها القصد العام فهي "حالة ذهنية أو نفسية يكون عليها الجاني ساعة إقدامه على ارتكاب الجريمة، ويمكن تصور هذه الحالة بعزم الجاني على ارتكاب الجريمة واتخاذ قرار تنفيذها، ثم إصدار الأمر لأعضاء جسمه للقيام بالأفعال المكونة لها، وقيادة هذه الأعضاء إلى تحقيق النتيجة المطلوبة. وإرادة الجاني في القصد الجرمي على هذا النحو يجب أن تتجه إلى ارتكاب الفعل، ولكن في الجرائم ذات النتيجة لا يتكون القصد الجرمي إلا إذا اتجهت الإرادة أيضا إلى إحداث النتيجة[3] ، إلاّ أنّ الملاحظ على الجرائم التي قررها

[1] أنظر المادة 11/2 من القانون 04/15 المتضمن التوقيع والتصديق الالكترونيين.
[2] عزيزة لرقط، مرجع سابق، ص.118.
[3] إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر،2008 ،ص.32.

المشرع بموجب القانون 04/15 هي جرائم خطر وليست جرائم ضرر وبالتالي يكفي لقيامها توفر السلوك الإجرامي دون حاجة إلى تحقق أو عدم تحقق نتيجة معينة.

وترتيبا على ما تقدم فإنّ دراسة هذه الجرائم سوف يقتصر على الركن المادي فقط مع تبيان النص القانوني المنظم لها على النحو التالي:

1/ صور الحماية الجزائية في مواجهة مؤدي خدمات المصادقة الالكترونية :

عمل المشرع الجزائري على تعداد الجرائم المرتبطة بمؤدي خدمات التصديق الالكتروني من خلال عدة مواد يمكن إيجازها في الجرائم التالية:

أ/ جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف :

نصت على هذه الجريمة المادة67 من القانون 04/15 على أنه "يعاقب بالحبس من شهرين إلى سنة واحدة (1) وبغرامة من مائتي ألف دينار 200.000 دج إلى مليون دينار 1.000.000 دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58،59 من هذا القانون "وعليه تعدّ هذه الجريمة من جرائم السلوك(الخطر) يقوم ركنها المادي بمجرد اتخاذ مؤدي الخدمات موقف سلبي يتمثل في عدم إعلام السلطة الاقتصادية بالتوقف عن نشاطه المحدد حسب أحكام المادة 41 من ذات القانون، ومن ثم فإن السلوك الإجرامي المكون للركن المادي يتحقق بامتناع الجهة المختصة المرخص لها إصدار شهادات التصديق الالكتروني عن الاستمرار في إصدار الشهادات دون إعلام السلطة الوصية بذلك سواء في الحالات العادية أو الحالات الاستثنائية المنصوص عليها في المادتين 58،59 من ذات القانون، إلاّ أنّ المشرع من خلال المادة 67 المذكورة أعلاه نص على ضرورة القيام بذلك خلال آجال محددة إلاّ أنّه لم يحدد ذلك (مما يترك المجال مفتوحا) ويسأل عن هذه الجريمة صاحب الترخيص أي من تم منحه الترخيص بإصدار شهادات التصديق دون سائر العاملين لديه في الشركة أو الجهة[1].

[1] عزيزة لرقط، مرجع سابق،ص.119.

ب/ جنحة إفشاء بيانات شهادة التصديق الالكتروني:

تناول المشرع الجزائري هذه الجريمة في المادة 70من القانون 04/15 التي تنص على أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من مائتين ألف دينار إلى مليون دينار أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 42 من هذا القانون". يتضح من نص هذه المادة أنّ النموذج القانوني للجريمة بالإضافة إلى الركنين المادي والمعنوي الشكلية التي يكفي لقيامها السلوك الإجرامي دون الحاجة إلى تحقيق النتيجة.

1-صفة الجاني:

حتى تقوم هذه الجريمة يجب أن تتوافر لدى القائم بها صفة العمل لدى الجهة المختصة بإصدار شهادات التصديق الالكتروني وفي المقابل لا تقوم هذه الجريمة ممن لا يعمل في الهيئة أو الجهة المرخص لها بإصدار شهادات التصديق على التوقيعات الالكترونية وعلة التجريم تكمن في أنّ الجاني في هذه الجريمة قد أؤتمن على المعلومات أو البيانات بسبب وظيفته أو عمله، أي أن عمله هو السبب المباشر لاتصال الجاني بالمعلومات فمناط العقاب هو الإخلال بالتزام ناشئ عن المهنة وما يترتب عليها من واجبات التي تضمنت السير الحسن للمهنة[1].

- **الركن المادي :**

سبق القول إنّ هذا النوع من الجرائم هي من جرائم الخطر وبالتالي يكفي لقيام ركنها المادي توافر السلوك الإجرامي ولا حاجة لتحقيق النتيجة ويتمثل السلوك الإجرامي في قيام الجاني بإفشاء أو إعلام الغير بالمعلومات أو البيانات الخاصة بالتوقيع الالكتروني للموقع ويتحقق هذا النشاط الإجرامي إما بصورة ايجابية حين يتعمد الجاني إطلاع الغير على هذه المعلومات أو البيانات أو بصورة سلبية حين يسمح الجاني للغير بالاطلاع على بيانات الموقع دون مبرر وسند قانوني كما تتحقق هذه الصورة (الصورة السلبية) في حالة عدم تأمين بيانات التوقيع الالكتروني كما نصت عليه الفقرة 4 من المادة 07 من قانون 04/15 التي اشترطت أن يكون التوقيع الالكتروني مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني.

[1] عزيزة لرقط، مرجع سابق،ص.120.

والملاحظ أنّ هذه الجريمة تتشابه مع الجريمة التي نص عليها المشرع الجزائري في المادة 72من قانون 04/15 التي جاءت على النحو التالي "يعاقب بالحبس من ثلاث أشهر(3) إلى سنتين (2) وبغرامة من عشرين ألف (20.000) دج إلى مائتين ألف (200.000)دج أو بإحدى هاتين العقوبتين فقط كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق".

ويقصد بالتدقيق حسب المادة الثانية من الفصل الثاني التي تناولت التعاريف أنه "التحقق من مدى المطابقة وفقا لمرجعية ما،" كما أنّ هذا القانون حدد السلطات التي يمكنها إجراء هذا التدقيق والمتمثلة في السلطة الوطنية حسب الفقرة الخامسة من المادة 18 ويكون ذلك على مستوى السلطتين الحكومية والاقتصادية، كما خول هذه الصلاحية أيضا للسلطة الحكومية من خلال المادة 28 فقرة 06 ويكون ذلك على مستوى الطرف الثالث الموثوق، أما السلطة الاقتصادية فهي الأخرى خول لها القانون صلاحية القيام بالتدقيق من خلال مكاتب معتمدة وذلك وفقا للفقرة الثامنة من المادة 30 من ذات القانون[1].

وعليه؛ يترتب على ما تقدم أنّ هذه الجريمة لا تقوم إلا بتوافر ركنيها المادي والمعنوي وكذا صفة الجاني على النحو الذي سبق بيانه في الجريمة السابقة.

ج-جنحة جمع البيانات الشخصية للموقع واستخدامها في غير الغرض المخصص لها :

نصت المادة71" يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03)سنوات وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار(1.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 43 من هذا القانون."

يتبن من خلال نص المادة وأنّ المشرع الجزائري اشترط لقيام هذه الجريمة توافر صفة معينة في الجاني بالإضافة إلى الركنيين المادي والمعنوي وفقا لما يلي:

1/صفة الجاني:

يتطلب لقيام هذه الجنحة أن تقع من مؤدي خدمات التصديق الالكتروني أو أحد العاملين به، ويجب أن يستخدم هذه البيانات التي قام بجمعها دون رضا الموقع في غير الغرض المخصص لها، وبالتالي لا قيام لهذه الجريمة في الحالة التي يكون جمع هذه البيانات

[1] عزيزة لرقط ، مرجع سابق ،ص.121.

الشخصية بموافقة صريحة من الموقع، وكذلك استخدامها في الغرض الذي خصص لها، ومن خلال ما تقدم يتعين توافر شرطين، الشرط الأول يتمثل في كون الجاني أحد العاملين في الجهة المختصة بإصدار شهادات التصديق الالكتروني .أما الشرط الثاني فيتمثل في القيام بفعل جمع البيانات الشخصية دون الموافقة الصريحة من الموقع أو استخدام هذه البيانات في غير الغرض المخصص لها[1].

- **الركن المادي:**

يتحقق الركن المادي بإتيان الجاني فعل ايجابي يتمثل في استخدام البيانات المتعلقة بالتوقيع الالكتروني وذلك في غير الغرض المخصص لها أو جمع البيانات الشخصية للموقع أو المعنى دون الحصول على الموافقة الصريحة منه.

وبالتالي فإنّ هذه الجريمة لا تقع بفعل سلبي كما أنها لا تحتاج إلى تحقيق نتيجة فيكفي لقيام ركنها المادي قيام السلوك الإجرامي فقط[2].

هـ-جنحة إصدار شهادة التصديق الالكتروني دون ترخيص أو بسحبه :

تنص المادة 72على أنه "يعاقب بالحبس من سنة واحدة (01) إلى ثلاث سنوات(03) وبغرامة من مائتين ألف دينار(200.000 دج) إلى مليوني دينار2.000.000 دج أو بإحدى هاتين العقوبتين فقط كل ما يؤدي خدمات التصديق الالكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الالكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه.

تصادر التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعلوم به".

يتضح من خلال نص المادة أن المشرع جرم قيام أية جهة غير مرخص لها من السلطات المختصة (السلطة الإقتصادية) حسب أحكام المادة 33 من ذات القانون إصدار الشهادات التصديق الالكتروني المعرفة بموجب الفقرة السابعة من المادة 2 من ذات القانون على أنها "وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع" كما أن ذات المادة جرمت استمرار الجهة المختصة بمنح شهادات التصديق الالكتروني بالرغم من سحب هذا الترخيص وبالتالي لقيام هذه الجريمة لا بد من توافر كل من الركن المادي والمعنوي.

[1] عزيزة لرقط ، مرجع سابق،ص.122.
[2] الصفحة نفسها.

وترتيبا على ذلك فإن جريمة إصدار شهادة التصديق الالكتروني من جهة لا تملك رخصة بذلك أو تم سحب الرخصة منها من الجرائم الشكلية التي يتطلب قيامها توافر السلوك الإجرامي فقط والذي يتمثل في قيام جهة قبل الحصول على الترخيص وفق الإجراءات والشروط التي حددها القانون 04/15 خاصة المواد 33 وما يليها منه في إصدار شهادات التصديق الالكتروني أو الاستمرار في منح شهادات التصديق بالرغم من سحب الرخصة المخولة لمؤدي خدمات التصديق الالكتروني في الحالات التي حددها ذات القانون[1].

2/ صور الحماية الجزائية المرتبطة بطلب الخدمة:

تختلف هذه الجرائم باختلاف الأفعال المرتكبة وكذا بتباين مرتكبيها، فهناك انتهاكات يرتكبها طالبو الخدمة، وأخرى ترتبط باستعمال شهادات التصديق الالكتروني المسلمة[2].

أ/ جنحة الإدلاء بإقرارات كاذبة للحصول على شهادات التصديق:

نص عليها المشرع الجزائري في المادة 66 على أنه "يعاقب بالحبس من ثلاث (03)أشهر إلى ثلاث (03) سنوات وبغرامة من عشرين ألف دينار(20.000دج) إلى مائتي ألف دينار (200.000دج) أو بإحدى هاتين العقوبتين فقط، كل ما أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة".

وعليه لقيام هذه الجريمة أيضا لا بد من توافر الركنين المادي والركن المعنوي لأنّ الهدف من هذا التجريم هو حماية الأطراف المتعاقدة من الحصول على معلومات خاطئة مما يهز الثقة المفترضة في التعاملات التجارية.

ويتحقق السلوك الإجرامي في هذه الجريمة قيام الجاني بتقديم إقرارات كاذبة سواء لمؤدى الخدمات أو للطرف الثالث الموثوق[3] باعتباره المسؤول عن منح شهادة التصديق.

وتعدّ الجريمة كغيرها من الجرائم الأخرى من جرائم السلوك المجرد وليست من جرائم الضرر، وبالتالي لا يشترط المشرع لقيام الركن المادي حلول ضرر معين، أو تحقق نتيجة معينة، وإنما يكفي لقيامها تحقق النشاط أو السلوك الإجرامي وهو تقديم معلومات خاطئة أو كاذبة[4].

---

[1] عزيزة لرقط ، مرجع سابق،ص.123.
[2] الصفحة نفسها.
[3] أنظر المادة 11/2 من القانون 04/15، المتضمن التوقيع و التصديق الالكترونيين.
[4] عزيزة لرقط، مرجع سابق،ص.124.

ب-جنحة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير:

ينص المشرع في المادة68 على أنه "يعاقب بالحبس من ثلاثة(3)أشهر إلى ثلاث(3) سنوات وبغرامة من مليون دينار(1.000.000دج) إلى خمسة ملايين دينار(5.000.000دج) أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير".

يشتمل نص هذه المادة على عدة أفعال هي الحيازة والإفشاء واستعمال بيانات إنشاء توقيع الكتروني خاصة بالغير، وبالتالي يعدّ أحد هذه الأفعال كاف لقيام الجريمة وتوقيع العقوبة المقررة متى توافرت الأركان الأخرى وتعتبر هذه الجريمة أيضا من جرائم السلوك أو الجرائم الشكلية التي يعد فيها النشاط الإجرامي كاف لقيام ولا ضرورة كحدوث ضررا أو نتيجة عنها.

وعليه؛ فإنّ السلوك الإجرامي لهذه الجريمة يتمثل في قيام الجاني إما بحيازة بيانات توقيع الكتروني خاصة بالغير، وتكفي في هذه الحالة الحيازة المادية ولا يشترط الحيازة القانونية وتتحقق الجريمة أيضا في الحالة التي يقوم بها الجاني بإفشاء بيانات إنشاء التوقيع الالكتروني والعلة في التجريم أنه من وضعت لديه هذه البيانات تكون قد أؤتمن عليها لما تتمتع بها أو الاستعمال[1].

ج-جنحة استعمال شهادة التطبيق الإلكتروني الموصوفة لغير الغرض الذي منحت لأجله:

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

يتضح جليا أن هذه الجريمة من الجرائم الشكلية التي يكفي لقيامها توفر النشاط الإجرامي المتمثل في قيام الموقع الذي منحت له شهادة تصديق على توقيعه الإلكتروني في استعمال هذه الشهادة في غير الغرض الذي منحت لأجله، وأقتصر المشرع في هذه الحالة على عقوبة الغرامة دون الحبس[2].

وعلى ضوء ما تقدم يتضح أن المشرع ومن خلال النصوص القانونية المنوه عنها أعلاه حافظ على السلطة التقديرية لقاضي الموضوع فيما يتعلق بالعقوبة المقررة وأعطى له الخيار

[1] عزيزة لرقط، مرجع سابق ،ص.124.
[2] المرجع نفسه،ص.125.

بين عقوبة الحبس وعقوبة الغرامة وهو ما يستخلص من عبارة أو بإحدى هاتين العقوبتين، كما أن المشرع نص على العقوبة المقررة للشخص المعنوي طبقا للمادة 75 من القانون رقم 04/15 وحددها بالغرامة التي تساوي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي إلاّ أن هذا لا يمنع من توقيع العقوبات التكميلية المقررة وفقا للقواعد العامة[1].

الفرع الثاني

صور الحماية الجنائية للتوقيع الإلكتروني في التشريع المصري

نص المشرع المصري على جرائم التوقيع الإلكتروني في المادتين 21،23 من قانون رقم 15لسنة2004 المتعلق بتنظيم التوقيع الإلكتروني[2].

أولا/الجرائم المنصوص عليها في المادة21 من قانون التوقيع الالكتروني:

نصت المادة21 من قانون التوقيع الإلكتروني المصري على :"أن بيانات التوقيع الإلكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله[3]".

ويتضح من المادة21 من قانون التوقيع الالكتروني، أن المشرع المصري يجرم إفشاء بيانات التوقيع الالكتروني، وجريمة استخدام هذه البيانات في غير الغرض المخصص لها،على التفصيل الآتي:

1/جريمة إفشاء بيانات التوقيع الالكتروني:

يتضح من خلال المادة21 من قانون التوقيع الإلكتروني المصري، أنه يتطلب لقيام هذه الجريمة، توافر ركنين مادي يتمثل في إفشاء للغير بيانات التوقيع الإلكتروني والوسائط الالكترونية والمعلومات من قبل الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني للغير أو استخدامها في غير الغرض الذي قدمت من أجله[4].

[1] عزيزة لرقط، مرجع سابق،ص.125.
[2] صالح شنين، الحماية الجنائية للتجارة الالكترونية(دراسة مقارنة) ،رسالة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبوبكر بلقا يد تلمسان كلية الحقوق، 2013/2012 ،ص.169.
[3] الصفحة نفسها.
[4] المرجع نفسه، ص.170.

كما يتطلب فيها إلى جانب الركن المادي ركن معنوي يتخذ صورة القصد الجنائي العام دون القصد الجنائي الخاص ،على التفصيل الآتي:

***الركن المادي:**

يتمثل الركن المادي في هذه الجريمة في إفشاء بيانات التوقيع الإلكتروني ،أي نشرها واطلاع الغير عليها ،السرية بعد أن كان العلم بها قاصرا على الذين ائتمنوا عليها بحكم وظيفتهم[1].

ويتحقق الركن المادي للجريمة بمجرد انتهاك سرية البيانات وخصوصيتها حتى ولو لم يترتب على الفعل أي نتيجة ،فالجريمة سلوكية يكتفي فيها المشرع بتحقق السلوك المادي[2].

***الركن المعنوي:**

هذه الجريمة العمدية يلزم لقيامها اتجاه إرادة الجاني إلى إفشاء بيانات التوقيع الإلكتروني أو إساءة استخدامها ،مع علمه بذلك وقبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بطريق الخطأ[3].

2/جريمة إساءة استخدام بيانات التوقيع الالكتروني:

لقيام هذه الجريمة لابد من توافر ركنين مادي و معنوي ،على النحو الآتي:

***الركن المادي:**

ويتحقق الركن المادي في هذه الجريمة بإساءة استخدام بيانات التوقيع الإلكتروني وذلك باستخدامها في غرض آخر غير ما قدمت من أجله[4]، ويقتصر هنا أيضا التجريم على من قدمت إليه أو اتصل بها بحكم عمله والذي استعملها في الغرض الذي قدمت من أجله[5].

---

[1] ويلاحظ أن التجريم هنا يقتصر على من قدمت إليه أو اتصل بها بحكم عمله ،في حين كان من المفروض أن يجرم المشرع انتهاك سرية بيانات التوقيع الالكتروني بصفة عامة .أنظر أيمن رضا محمد أحمد ،مرجع سابق ،ص.142.

[2] لا يشترط المشرع المصري تحقق نتيجة معينة لتحقق الركن المادي لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات وليس تحقق نتيجة إجرامية معينة ،وبالتالي جريمة سلوكية وليست من جرائم الضرر.

[3] صالح شنين، مرجع سابق، ص.170.

[4] سليمان أحمد فضل،مرجع سابق. ،ص.161.

[5] راجع المادة 21من قانون التوقيع الالكتروني المصري.

***الركن المعنوي:**

هذه الجريمة العمدية يلزم لقيامها توافر القصد الجنائي باتجاه إرادة الجاني إلى إساءة استخدام بيانات التوقيع الالكتروني، باستعمالها في غير الغرض المخصص لها، مع علمه بذلك و قبول النتائج المترتبة على هذا السلوك الإجرامي الذي لا يتصور وقوعه بطريق الخطأ[1].

ومتى تحقق الركن المادي والركن المعنوي وجب إنزال العقوبة على الجاني دون النظر إلى الباعث الذي دفعه إلى إساءة استخدام بيانات التوقيع الالكتروني[2].

ثانيا/الجرائم المنصوص عليها في المادة 23من قانون التوقيع الإلكتروني:

تنص المادة23 من قانون15 لسنة 2004على أنه " مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في قانون آخر يعاقب بالحبس و بغرامة لا تقل عن 10 آلاف جنيه و لا تجاوز مئة ألف جنيه ،أو بإحدى هاتين العقوبتين كل من:

1- إصدار شهادة تصديق دون الحصول على ترخيص.

2 - إتلاف أو تعييب توقيعا أو وسيطا أو محررا إلكترونيا،أو تزوير شيئا من ذلك بطريق الاصطناع أو التعديل أو بأي طريق آخر.

3 - إستعمال توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك.

4- توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اختراق أو اعتراضه أو تعطيله عن أداء وظيفته، وفي حالة العود تزداد بمقدار مثل العقوبة المقرر لهذه الجرائم[3].

1/جريمة إصدار شهادة التصديق الإلكتروني بدون ترخيص:

وقد نص المشرع المصري على هذه الجريمة في المادة 23/أ من قانون التوقيع الإلكتروني، ويتطلب لقيامها توافر ركن مادي،ومعنوي.

---

[1] هذه الجريمة العمدية يلزم لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة ،وبالتالي ذا وقع السلوك الإجرامي نتيجة الخطأ والإهمال فلا يتحقق الركن المعنوي. للتفصيل راجع سليمان أحمد فضل ،مرجع سابق ،ص.161.

[2] اكتفى المشرع المصري بالقصد الجنائي العام دون الخاص في جريمة إساءة استخدام بيانات التوقيع الالكتروني وعليه لا عبرة بالباعث والغرض من ارتكاب هذه الجريمة . فمتى تحقق والركن المعنوي في صورة القصد الجنائي العام إلى جانب الركن المادي ،وجب عقاب الجاني دون النظر إلى الباعث من إساءة استخدام التوقيع الالكتروني.

[3] صالح شنين، مرجع سابق،ص ص.171،172.

***الركن المادي:**

يتمثل السلوك الإجرامي في هذه الجريمة ،في انتحال الجاني صفة مزود خدمات التصديق المرخص له بخلاف الحقيقة، و يصدر شهادات تصديق إلكتروني دون ترخيص بذلك من الهيئة العامة لتنمية صنعة تكنولوجيا المعلومات"[1].

وبالتالي تقع هذه الجريمة إذا أصدر الجاني شهادة تصديق الكتروني دون الحصول على ترخيص مخالفة للمادة19 من قانون التوقيع الالكتروني[2].

والسبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الإلكترونية في حق الغير[3]، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الإلكتروني ،أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها[4].

ويمكن القول أن هذه الجريمة من جرائم الخطر، أو جرائم السلوك المجرد حيث يتكامل قيام الركن المادي فيها بمجرد إتيان الجاني لسلوك إصدار شهادات التصديق الالكتروني بدون ترخيص ،دون تطلب حصول ضرر بجهة ما أو شخص ما[5].

***الركن المعنوي:**

وهذه الجريمة من الجرائم العمدية ،لابد فيها من توافر القصد الجنائي العام ،وذلك بأن يعلم الجاني بأن بقوم بإصدار الشهادة دون ترخيص ،وأن تتجه إرادته إلى هذا السلوك[6].

ومن ثمة فلا يتصور وقوع هذه الجريمة بطريق الخطأ بل يجب أن تنصرف الإرادة إلى هذا الفعل،انطلاقا من المادة 2/1 .

2/جريمة إتلاف أوتعييب أو تزوير التوقيع الإلكتروني:

جرم المشرع المصري هذه الأفعال في المادة 23/ب من قانون التوقيع الإلكتروني، كالآتي:

أ/جريمة إتلاف أوتعييب التوقيع الإلكتروني:

---

[1] عبد الفتاح بيومي حجازي ،حماية المستهلك عبر شبكة الأنترنت ،دار الفكر الجامعي ،الإسكندرية مصر، 2006، ص. 157.

[2] تنص المادة 19من قانون التوقيع الالكتروني على مجموعة من الالتزامات تقع على عاتق من يرغب في مزاولة نشاط إصدار شهادات صديق الكتروني ،وهي:

- ضرورة الحصول على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات قبل ممارسة النشاط المذكور.
- سداد رسم الهيئة الذكورة مقابل هذا النشاط .
- عدم جواز التوقف عن النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير ،سوى بعد الحصول موافقة كتابية من الهيئة المذكورة.

[3] عرف القانون 15لسنة 2004في مادته الأولى شهادة التصديق الالكتروني بأنها " الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.

[4] أيمن رضا محمد ،مرجع سابق ،ص.132.

[5] سليمان أحمد فضل ،مرجع سابق ،ص.167.

[6] عبد الفتاح حجازي ،التوقيع الإلكتروني ،دار الفكر الجامعي ،الإسكندرية مصر ، 2006،ص.540.

***الركن المادي:**

ويتحقق الركن المادي في هذه الجريمة بإتلاف أو تعييب التوقيع الإلكتروني ،ويتحقق فعل الإتلاف بإفقاد البرنامج المعلوماتي الخاص للتوقيع الإلكتروني قدرته على العمل[1]، إما تعييب التوقيع الإلكتروني يكون بفقده القدرة على العمل أو الصلاحية بصورة جزئية ،كأن يصدر التوقيع مشوها أو غير واضح[2].

ويتطلب لقيام هذه الجريمة ضرورة توافر الضرر ،فالضرر هو النتيجة الإجرامية المترتبة على الاعتداء و ترتبط بالفعل برابطة سببية قانونية حال توافر أركان الجريمة ،ويستوي أن يكون الضرر ضرر مادي أو معنوي[3].

***الركن المعنوي:**

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم و الإرادة ،فيجب أن يعلم الجاني بأن فعل الإتلاف أو التعييب للتوقيع الإلكتروني محظور و معاقب عليه قانونا، وأن تتجه إرادته للفعل المجرم[4]، إما إذا كان الإتلاف الإتلاف أوالتعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه فلا تقوم هذه الجريمة.

ولا تتطلب هذه الجريمة قصدا خاصا ،و إنما يكتفي بشأنها القصد العام بعنصريه العلم و الإرادة، فتقوم الجريمة بتوافر الركن المادي والقصد الجنائي العام .

ب/جريمة تزوير التوقيع الإلكتروني:

***الركن المادي:**

يتمثل الركن المادي لهذه الجريمة في تزوير التوقيع الالكتروني بتغيير الحقيقة في التوقيع الإلكتروني بطريق الاصطناع أو التعديل أو التحويل ،أو بأي طريق على نحو يضر بالغير[5].

ومن أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك ،يتم تصميمها على غرار البرامج والأنظمة المشروعة

---

[1] لم يحدد القانون المصري في المادة 23طريقة معينة لإتلاف أو تعييب التوقيع ،وعليه يتحقق الإتلاف بأي وسيلة تؤدي إلى عدم الانتفاع به مثل نشر فيروس أو سكب كوب ماء أو سائل على الوسيط.

[2] عبد الفتاح بيومي حجازي ،حماية المستهلك عبر شبكة الأنترنت ،مرجع سابق،ص.159.

[3] أيمن رضا محمد ،مرجع سابق ،ص.188.

[4] ناقد ياسين محمد المدهون ،مرجع سابق،ص. 362.

[5] يلاحظ أن طرق التزوير لم ترد على سبيل الحصر لكون المشرع أضاف عبارة) أو أي طريق آخر(لأن حصرها غير ممكن ،لتعددها و اختلافها و وتجددها ،و لذلك يتحقق تزويره بأي طريقة ووسيلة . للتفصيل راجع عبد الفتاح بيومي حجازي،حماية المستهلك عبر شبكة الإنترنت ،مرجع سابق، ص .160.

أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني ،والقيام بنسخها[1].

***الركن المعنوي:**

يمثل الركن المعنوي في هذه الجريمة في القصد الجنائي العام ،بأن يكون الجاني عالما بأنه ترتكب جريمة و أن تتجه إرادته إلى تزوير التوقيع الإلكتروني ،فمجرد إهماله في تحري الحقيقة مهما كانت درجته لا تتحقق به جريمة التزوير[2].

ويتطلب كذلك توافر القصد الجنائي الخاص لدى الجاني إلى جانب القصد الجنائي العام وهو نية استعمال التوقيع الإلكتروني فيما زور من أجله ،على خلاف جريمة الإتلاف التي اكتفى فيها المشرع المصري بالقصد الجنائي العام[3].

ب/جريمة استعمال توقيع إلكتروني معيب أو مزور:

ورد النص على هذه الجريمة في المادة 23/ج من قانون التوقيع الإلكتروني، ويقصد باستعمال توقيع الكتروني معيب أو مزور إبراز التوقيع الالكتروني المزور أو المعييب والاحتجاج به على اعتبار أنه صحيح[4].

وتقوم جريمة استعمال توقيع إلكتروني معيب أو مزور بتوافر ركنين مادي و معنوي، على التفصيل الآتي:

***الركن المادي:**

ويتمثل في استخدام الجاني للتوقيع الإلكتروني المعيب أو المزور مع علمه بذلك ،ولا يشكل المعاملات بقيمته كما لو كان صحيحا ،ويتحقق ذلك بكل سلوك إيجابي[5].

***الركن المعنوي:**

---

[1] أيمن رضا محمد ،مرجع سابق،ص.207.

[2] سليمان أحمد فضل ،مرجع سابق،ص. 164.

[3] عبد الفتاح بيومي حجازي ،حماية المستهلك عبر الإنترنت ،مرجع سابق،ص.161.

[4] ومحل جريمة استعمال توقيع إلكتروني معيب أو مزور يتمثل في التوقيع الالكتروني المزور أو المعييب . للتفصيل راجع سليمان أحمد فضل ،مرجع سابق،ص.165.

[5] وعليه لابد أن يكون السلوك الإجرامي ايجابي بإظهار التوقيع الالكتروني المعيب المزور أو المعيب الغير في المعاملات بقيمته كما لو كان صحيحا ،فالعبرة بتقديم المستند الاحتجاج به أو الاستناد إليه في المعاملات كدليل في التمسك بحق أو الحصول على حق معين ،ويستوي أن يكون هذا الاستعمال قد بوشر في مواجهة جهة رسمية أو موظف عام في معاملات الأفراد. للتفصيل راجع جميل عبد الباقي ،القانون الجنائي و التكنولوجيا الحديثة ،مرجع سابق،ص.180.

جريمة استعمال التوقيع الإلكتروني المعيب أو المزور هي جريمة عمدية ،يلزم لقيامها أن يتوافر القصد الجنائي العام بعنصريه العلم و الإرادة ،فيجب أن يعلم أو التوقيع الإلكتروني مزورا أو معيبا وفق الاستعمال ،ومع ذلك تنصرف إرادته إلى استعماله فيما أعد له.

ولا عبرة بالأغراض التي يتوخاها الجاني في الاستعمال، فيعد مرتكبا لهذه الجريمة من يستخدم توقيعا مزورا أو معيبا ،وان كان يرمي إلى الوصول إلى حق ثابتا قانونيا[1].

وبالتالي إذا انتفت نية استعمال التوقيع الإلكتروني المعيب أو المزور فيما زور من أجله ،انتفت الجريمة ،ويجب تحري القصد وقت ارتكاب الجريمة.

وتجدر الإشارة في الأخير إلى أن المشرع المصري عاقب على استعمال توقيع إلكتروني معيب أو مزور ،دون الإتلاف ،وذلك لأن هذا الأخير لا يعمل و فقاد الصلاحية، و لا أثر له من الناحيتين العملية و القانونية[2].

3/جريمة الحصول على التوقيع الإلكتروني أو اختراقه أو اعتراضه أو تعطيله:

جاء النص على هذه الجريمة في المادة 23/د، ولقيام هذه الجريمة ،لابد من توافر ركنين مادي و معنوي ،على التفصيل لآتي:

***الركن المادي:**

ويتخذ السلوك الإجرامي في هذه الجريمة صورة الحصول بغير حق على توقيع إلكتروني بأي وسيلة ،ويمكن الاستيلاء على التوقيع الإلكترونين عن طريق السرقة أو النصب أو عن طريق خيانة الأمانة[3].

---

[1] أيمن رضا محمد ،مرجع سابق،ص.219.

[2] المرجع نفسه،ص.217.

[3] لقد أحسن المشرع المصري صنعا حينما لم يحدد وسيلة على سبيل الحصر لارتكاب الفعل المجرم ،لكنه خلافا لبعض التشريعات لم يجرم محاولة الحصول على توقيع أو محرر إلكتروني.

ويتحقق أيضا باختراق التوقيع الإلكتروني بالدخول غير المشروع أو غير المصرح به للنظام المعلوماتي المتضمن للتوقيع الإلكتروني[1]، أو اعتراضه أو تعطيله عن أداء وظيفته بأي وسيلة تؤدي إلى تباطؤ النظام و جعله غير قادر على الاستعمال دائما أو مؤقتا بشكل متقطع[2].

***الركن المعنوي:**

تعتبر هذه الجريمة من الجرائم العمدية ،تتحقق بتوافر القصد الجنائي العام فلابد أن يعلم الجاني بأن حصوله على التوقيع الإلكتروني يعتبر حق ،وأنه يخترق التوقيع الإلكتروني أو يعترضه ،أو يعطله ،و أن تتجه إرادته إلى ذلك الفعل ،ولا يتطلب المشرع في هذه الجريمة قصدا جنائيا خاصا ،بل اكتفى بالقصد الجنائي العام[3].

لذلك ينتفي القصد الجنائي إذا قام الشخص الذي يتعامل مع النظام بالحصول على التوقيع الالكتروني أو اختراقه أو اعتراضه أو تعطيله نتيجة الخطأ ،فهذه الجريمة من الجرائم العمدية لا يتصور وقوعها بطريق الخطأ[4].

---

[1] عبد الحليم رمضان ،مرجع سابق ،ص.51. وانظر أيضا:
Gassin(R) op.cit.no.88.

[2] عبد القادر القهوجي ،مرجع سابق ،ص ص.140، 141،وانظر أيضا:
Gassin(R) informatique et liberté répertorie Dalloz de droit pénal ,jzniper.1987.no522.

[3] أيمن رمضان احمد ،مرجع سابق ،ص. 164.وانظر أيضا عبد الفتاح بيومي حجازي ،التوقيع الالكتروني ،مرجع سابق، ص.133.

[4] عبد الحليم مدحت رمضان ،مرجع سابق ،ص.54.

ملخص

إنّ التطور العلمي الذي شهده العالم، والاستخدام الواسع للتقنية الحديثة في جميع مجالات الحياة، واتجاه الدولة نحو ما يعرف بالحكومة الالكترونية جعل الأساليب التقليدية في إبرام العقود لا تتلاءم معها، مما اضطر إلى البحث عن أساليب جديدة تحقق الغاية وتسهل على الأفراد المعاملات والتبادلات،فتم ادخال التوقيع الالكتروني ليحل محل التوقيع التقليدي، الذي هو وسيلة الكترونية لتوثيق هذه المعاملات ، يتم من خلاله التأكد من شخصية صاحب التوقيع وموافقته على الالنزام بها وصحة الوثيقة التي تم تبادلها بين الأطراف.

نجد أن التوقيع الالكتروني يختلف عن التوقيع التقليدي من حيث طبيعته باعتباره ملفا رقميا مؤلفا من حروف أو أرقام أو رموز الكترونية، وهو ما جعل المشرع يتدخل بإنشاء عقوبات على الاعتداءات اللاحقة به، من هذا المنطلق جاءت هذه الدراسة لتسلط الضوء على الحماية الجنائية التي قررتها مختلف التشريعات الغربية و العربية.

Résumé

Le progrès scientifique que le monde a connu et l'utilisation massive des nouvelles technologies dans tous les domaines de la vie, et l'orientation de l'Etat vers ce qu'on appelle le gouvernement électronique, fait que les méthodes classiques de conclusion des contrats sont devenus incompatibles avec ce progrès, ce qui a abouti à la recherche de nouvelles méthodes pour atteindre les objectifs et faciliter aux individus les transactions et les échanges, c'est pour ce la que la signature électronique remplace la signature traditionnelle, la signature numérique est un mécanisme permettent de garantir l'intégrité d'un document électronique et authentifier l'auteur.

Pour documenter les transactions qui sont faites par l'internet, la signature électronique assure l'identité des titulaires de cette signature et leur consentement, et l'authenticité du document qui sont échangés entre les parties.

la signature électronique a vu le jour, une signature très différente de la signature« traditionnelle », selon sa nature, car c'est un dossier numérique composé de lettres, chiffres ou symboles électroniques, cela a poussé le législateur à intervenir par la création de peines en cas d'atteinte à la signature électronique. De ce point de vu, vient cette étude à fin de souligner cette protection pénale que les différents législateurs sont consacré à la signature l'électronique.

خاتمة

الخاتمـــــــــة

من خلال دراستنا لجرائم المساس بالنظام المعلوماتي للتوقيع الإلكتروني، فإنه يتبين لنا أنه من أكثر الجرائم خطورة ، و يرجع ذلك إلى ما تتصف به هذه الجرائم عن الجرائم التقليدية من اختلاف، أضف على ذلك أنها التحديات التي فرضتها على الجهات الخاصة بوضع القوانين و إنفاذها.

فجرائم المعلوماتية عامة و جرائم الإعتداء على التوقيع الإلكتروني خاصة، مشكلة من المشكلات التي أفرزتها المعلوماتية، فهذه الثورة على قدر ما قدمته من تسهيلات للأفراد والمجتمعات على حد سواء فإنها قد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التقنية والعلمية المعقدة.

بما أن التوقيع الالكتروني واقعة مستجدة فرضتها مقتضيات التجارة الالكترونية و كذلك المعاملات الالكترونية بين الدول و الافراد فقد صدرت عدة تشريعات دولية وإقليمية ووطنية نظمت أحكامه لإزالة الغموض على هذا المفهوم الحديث و المستجد على الفكر القانوني،وبينت ماهيته و اعترفت به و من بين هذه القوانين قانون الاونسترال النموذجي لعام 1996م بشأن التجارة الإلكترونية ،و قانون الأونسترال النموذجي لعام 2001م بشأن التوقيعات الإلكترونية ، كما أصدرت المفوضية الأوروبية أحكام التوجيه الأوروبي رقم 93 لسنة 1999م بشأن التوقيعات الإلكترونية و فضلا على ذلك و إسترشادا بالقوانين النموذجية و التوجيهات الدولية، صدرت العديد من التشريعات الوطنية اعترفت بالتوقيع الإلكتروني و أضفت عليه حجية قانونية مساوية لحجية التوقيع التقليدي في الإثبات.

نجد أن للتوقيع الإلكتروني صور عديدة تختلف حسب التقنية المستخدمة في تشغيل منظومة التوقيع الإلكتروني،و من هذه الصور ما يعتمد على الأرقام أو الحروف أو الرموز ...مثل التوقيع بالرقم السري المقترن بالبطاقة الممغنطة، و منها مايعتمد على الخواص الطبيعية و الفيزيائية و هو التوقيع البيومتري، كذلك منها مايعتمد على التشفير لكل صورة من هذه الصور قوة ثبوتية تختلف عن الأخرى ، يرتكز قياس مستوى القوة الثبوتية للتوقيع الالكتروني على مدى قدرة منظومة تشغيله على تحقيق وظيفتي التوقيع التقليدي و هما التعبير عن إرادة الموقع في الإلتزام بمحتوى المحرر و تحديد هويته .

نستخلص مما سبق ان جميع التشريعات المختلفة الغربية و العربية قد وضعت حماية جنائية للتوقيع الإلكتروني، نجد أن التشريع الفرنسي و الامريكي لم يخص التوقيع الالكتروني بحماية جنائية خاصة بل يمكن حمايته في اطار القواعد العامة لقانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الألية للمعطيات، جريمة التزوير و كذلك نجده في التشريع الفدرالي الامريكي من خلال جرائم الكمبيوتر.

على خلاف تلك التشريعات خصت بعص التشريعات العربية التوقيع الالكتروني بحماية حنائية خاصة كالتشريع المصري الذي سبق التعرض له في اطار القانون رقم 2004/15 المتعلق بالتوقيع الالكتروني في المادتين 23،21 و شملت تلك الحماية العديد من الجرائم ، لكن المشرع المصري لم يجرم الشروع و بالتالي لا عقاب على الشروع فيها وكذلك نجده لم يميز بين تعطيل التوقيع الالكتروني الذي يترتب عنه توقيف مصلحة خاصة او مصلحة عامة،كما لم يجرم صنع او حيازة برامج معدة للاعتداء على التوقيع الالكتروني و بالتالي لم يكرس الحماية الوقائية.

أما بالنسبة للمشرع الجزائري الذي كان التحاقه بسن قانون خاص بالتوقيع الالكتروني متأخرا نوعا ما و كان ذلك في سنة 2015 حيث تناول المشرع الجزائري التوقيع والتصديق الالكترونيين بنصوص خاصة مستقلة وهذا استجابة لمتطلبات التطور التكنولوجي الحاصل في جميع مجالات الحياة، إذ حدد المقصود بالتوقيع الالكتروني وشروطه وكذا الجهات المختصة بالتصديق الالكتروني وفي الأخير أنشأ مجموعة من الجرائم محاولا من خلالها إقرار حماية جزائية في مواجهة مؤدي خدمات التصديق الالكتروني وكذا طالبي خدمة التوقيع الالكتروني، إلاّ أنه بالرغم من الايجابيات التي أتى بها هذا القانون إلا أنه لا يخلو من السلبيات أهمها أنّ القانون 04/15 على حسب أنه قانون خاص بالتوقيع والتصديق الالكترونيين إلا أنه لم يتناول كافة الاعتداءات التي قد تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول والبقاء غير المصرح بهما، مما يلزم الرجوع إلى القواعد العامة المدرجة في قانون العقوبات والتي يعاب عليها أنها لم تتناول التزوير المعلوماتي وفقا للقانون 23/06 بالرغم من أهميته بالنسبة للتوقيع الالكتروني، إلا أن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عالج الأمر واعتد بالتزوير المعلوماتي من خلال المادة العاشرة من الاتفاقية، كما يعاب أيضا على المشرع

أنه اقتصر الحماية المقررة في مواجهة مؤدي خدمات التصديق في حالة الإخلال بالتزاماتهم وكذا طالبي الخدمة في حين أن التحايل الالكتروني قد يقع من عدة أطراف كالقراصنة مثلا، مما يتعين على المشرع الجنائي مواجهة جميع صور التحايل لأجل حماية كافة المصالح المعتدى عليها، ضف إلى ذلك أن صور التجريم المستحدثة لحماية التوقيع الالكتروني من المؤكد تزايدها في المستقبل.

قائمة المراجع

قائمة المراجع

أولا- الكتب باللغة العربية :

01- محمد ناصر حمودي،العقد الدولي الإلكتروني المبرم عبر الإنترنت،الطبعة الأولى دار الثقافة للنشر والتوزيع،عمان،2012.

02- عادل رمضان الأبيوكي،التوقيع الإلكتروني في التشريعات الخليجية ،د.ط،دار المكتب الجامعي الحديث،الإسكندرية،2009

03- إيمان مأمون أحمد سليمان، ابرام العقد الالكتروني واثباته، الجوانب القانونية لعقد التجارة الالكترونية، ط1، دار الجامعة الجديدة لنشر، الإسكندرية، 2008.

04- رانياعزب،العقود الرقمية في قانون الإثبات،د.ط،دارالجامعة الجديدة، الإسكندرية،2012.

05- نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، د.ط، دار الثقافة للنشر والتوزيع،عمان،2005.

06- إلياس ناصيف،العقد الإلكتروني في القانون المقارن،الطبعة الأولى،منشورات الحلبي الحقوقية،بيروت،2009.

07- محمد حسن رفاعي العطار،البيع عبر شبكة الإنترنت، الطبعة الأولى،دار الجامعة الجديدة،الإسكندرية،،2007.

08- خالد ممدوح إبراهيم، إثبات العقود والمراسلات الإلكترونية، طبعة الأولى، الدار الجامعية، الإسكندرية،2010.

09- سعيد السيد قنديل، التوقيع الالكتروني: ماهيته، صوره، حجيته في الاثبات بين التداول والاقتباس، ط2، دار الجامعة الجديدة للنشر، الإسكندرية، 2006.

10- نسرين عبد الحميد نبيه، الجانب القانوني للقانون التجاري، منشأة المعارف، الإسكندرية، 2008.

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

12- بشار محمود دودين،الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، ط 2،دار الثقافة للنشر والتوزيع،الأردن،2010.

13- عبد الحميد ثروت، التوقيع الالكتروني:ماهيته، مخاطره وكيفيته، مدى حجيته في الاثبات، دار الجامعة الجديدة، الإسكندرية، 2007.

14- أحمد خليفة الملط، الجرائم المعلوماتية،دار الفكر الجامعي الإسكندرية، مصر،2005.

15- ممدوح علي مبروك، مدى حجية التوقيع الالكتروني في الإثبات، دار النهضة العربية القاهرة، 2009.

16- محمد عبيدات لورنس، إثبات المحرر الإلكتروني، دار الثقافة،عمان2009.

17- محمد أمين الرومي، التعاقد الالكتروني عبر الانترنت، دار المطبوعات الجامعية الإسكندرية،2004

18- عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، ط2، دار الثقافة لنشر والتوزيع،الأردن،2012.

19- علاء محمد عيد النصيرات، حجية التوقيع الالكتروني في الاثبات،(دراسة مقارنة)، ط1، دار الثقافة لنشر والتوزيع، الأردن، .200 .

20- سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، ط2007،2.

21- خالد مصطفى فهمي، النظام القانوني لتوقيع الالكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2007.

22- مصطفى معوان،التجارة الإلكترونية ومكافحة الجريمة المعلوماتية،الطبعة الأولى،دار الكتاب الحديث،القاهرة،2008.

23- سامح عبد الواحد التهامي، التعاقد عبر الانترنت-دراسة مقارنة-، دار الكتب القانونية، مصر، 2008 .

24- نور الدين الناصري، "المعاملات والإثبات في مجال الاتصالات الحديثة"، سلسلة الدراسات القانونية المعاصرة، العدد 12، مطبعة النجاح الجديدة، الطبعة الأولى 1428- 2007 .

25- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، بدون طبعة، 2011.

26- عادل يوسف عبد النبي البشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، الكوفة.

27- محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014.

28- محمد سامي الشوا ،ثورة المعلومات و انعاكساتها على قانون العقوبات ،دار النهضة العربية،1994.

29- أحمد فتحي سرور، الوسيط في قانون العقوبات،ط4،سنة 1991.

30- منير محمد الجنبيهي، ممدوح محمد الجنيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية،2006.

31- عبد الحليم يعقوب، الإعلام الجديد والجريمة الالكترونية، دار العالمية، مصر، ط01، 2014.

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

33- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار النهضة العربية، القاهرة، مصر،2009.

34- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الأردن،ط01،2008.

35- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية- دراسة مقارنة- دار الفكر والقانون،2015،الطبعة الأولى.

36- أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)،دار الجامعة الجديدة، الإسكندرية، مصر،2007.

37- نائلة عادل فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، لبنان،ط 01، 2005.

38- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر،1999.

39- رياض فتح الله بصلة،حدود الإثبات العلمي في قضايا التزييف والتزوير، منشأة المعارف،الإسكندرية، مصر،الطبعة الثالثة،2010.

40- أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان،ط1،2001.

41- إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر،2008.

42- محمد حسين منصور، قانون الاثبات – مبادئ الاثبات و طرقه، دار الجامعة الجديدة للنشر، طبع سنة 1998.

ثانيا- المقالات :

01- عبد الرسول عبد الرضا ،محمد جعفر هادي ،المفهوم القانوني للتوقيع الإلكتروني ،مجلة المحقق المحلي للعلوم القانونية و السياسية ،جامعة بابل ، العراق ،العدد الأول ، السنة الثانية .

02- أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56.

03- الشيخ إبراهيم بن شايع الحقيل، الشيخ سليمان بن محمد بن الشدي، التوقيع الإلكتروني وأثره في إثبات الحقوق والإلتزامات بين الشريعة الإسلامية والنظم والقواعد القانونية، ورقة عمل مقدمة في ندوة التوقيع الإلكتروني، المنعقدة في الرباط، المملكة المغربية، يونيو2006، منشورات المنظمة العربية للتنمية الإدارية،2008.

04- علي أبو مارية، التوقيع الإلكتروني ومدى قوته في الإثبات (دراسة مقارنة)،مجلة جامعة الخليل للبحوث،المجلد5، العدد2،جامعة فلسطين الأهلية، بيت لحم 2010.

05- صالح عطا الله، التوقيع الإلكتروني في التجارة الإلكترونية والتحكيم الإلكتروني، مقال منشور في الموقع:
http://newssparrow.blogspot.com/2013/05/blog-post_4572.html

06- مبروك حدة، حجية السندات الالكترونية في الإثبات (دراسة مقارنة)، مجلة العلوم القانونية و السياسية، عدد 17، جامعة حمه لخضر الوادي، جانفي 2018.

07- بلعايش ميادة / بن اسماعين حياة، مشروع الصيرفة الالكترونية في الجزائر، مجلة أبحاث اقتصادية وإدارية، العدد السادس عشر، ديسمبر2014.

08- نوال بن عمارة، وسائل الدفع الالكتروني (الأفاق والتحديات)،بحث منشور في الموقع:http://dspace.univ-ouargla.dz

09- عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها..خصائصها،دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ 2013/01/13 على الرابط :تاريخ الاطلاع 2017/02/13.

http://accronline.com/article_detail.aspx?id=7509

10- عبد الله مسفر الحيان، حسن عبد الله عباس، التوقيع الإلكتروني، دراسة نقدية لمشروع وزارة التجارة والصناعة الكويتية، مجلة العلوم الإقتصادية والإدارية، المجلد التاسع عشر، العدد الأول، 2013.

11- مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، بدون دار النشر، وبدون سنة.

ثالثا- الدراسات الجامعية :

أ/- الأطروحات :

01- عبد الوهاب مخلوفي،التجارة الإلكترونية عبر الإنترنت،رسالة دكتوراه،كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر باتنة،2012/2011.

02- بن قارة مصطفى عائشة،الحماية الجنائية للحكومة الإلكترونية (دراسة مقارنة)،رسالة دكتوراه قانون عام،كلية الحقوق،جامعة ابوبكر بلقايد تلمسان ،2018/2017.

03- صالح شنين، الحماية الجنائية للتجارة الالكترونية(دراسة مقارنة) ،رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبوبكر بلقايد تلمسان،2013/2012.

04- براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة لنيل شهادة الدكتوراه في القانون الجنائي، كلية الحقوق و العلوم السياسية،جامعة محمد خيضر بسكرة،2015/2014.

ب/- رسائل الماجستير:

01-فوغالي بسمة ، إثبات العقد الإلكتروني و حجيته في ظل عالم الإنترنت،مذكرة ماجيستير في القانون الخاص،كلية الحقوق والعلوم السياسية،جامعة محمد لمين دباغين سطيف2، 2015/2014.

02- إياد محمد عارف عطا سده،مدى حجية المحررات الإلكترونية في الإثبات،مذكرة

ماجستير ،كلية الدراسات العليا،جامعة النجاح الوطنية،فلسطين،2009.

03- طمين سهيلة، الشكلية في عقود التجارة الإلكترونية، مذكرة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2012/2011.

04- لوصيف عمار، استراتجيات نظام المدفوعات للقرن الحادي والعشرين مع الإشارة إلى التجربة الجزائرية، مذكرة ماجستير في العلوم الاقتصادية، جامعة منتوري قسنطينة2009/2008.

05- معطى سيد أحمد، واقع وتأثير التكنولوجيا الجديدة للإعلام والاتصال على أنشطة البنوك الجزائرية، مذكرة ماجستير في إدارة الأفراد وحوكمة الشركات، جامعة أبو بكر بلقايد تلمسان 2012/2011.

06- عبد االله بن عبد العزيز بن محمد الفحام،حجية التوقيع الإلكتروني في الإثبات،رسالة ماجستير ،جامعة الإمام محمد بن سعود الإسلامية،المملكة العربية السعودية،1428.

07- سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير تخصص علوم جنائية وعلم الإجرام، كلية الحقوق، جامعة بوبكر بلقايد،تلمسان،2011/2010.

ج/ مذكرات الماستر

01- زينب غريب، إشكالية التوقيع وحجيته في الإثبات، مذكرة لنيل رسالة ماستر، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس، الرباط، 2009- 2010.

02- عزولة طيموش، علاوات فريدة، التوقيع الالكتروني في ظل القانون 04/15 ، مذكرة ماستر تخصص القانون الخاص الشامل، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة بجاية، الجزائر، 2016/2015.

03- ترير نوال، الشكلية في العقود التجارة الإلكترونية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم سياسية، جامعة خميس مليانة، 2014/2013.

04- كحول سماح ،حجية الوسائل التكنولوجية في الاثبات ،مذكرة لنيل شهادة الماستر قسم الحقوق ،كلية الحقوق و العلوم السياسية،جامعة قاصدي مرباح ورقلة،2015/2014.

05- سمية مزغيش،جرائم المساس بأنظمة المعلوماتية، مذكرة ماستر قانون جنائي،كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر بسكرة .

رابعا- وثائق مختلفة :

أ/ مداخلة في مؤتمر.

01- مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25.

ب/ محاضرة .

01- كامل فريد السالك، الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية 21-23 أكتوبر 2000، الجمعية السورية للمعلوماتية، حلب، سورية.

ج/ ورشة عمل.

01- محمد صالح العادلي، الجرائم المعلوماتية (ماهيتها وصورها)، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان،2-4 أفريل 2006.

د/ ملتقيات.

01- موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009.

02- ذكي ذكي أمين حسونه،جرائم الكمبيوترو الجرائم الأخرى،المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة ، سنة 1993.

03- دياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية. بتاريخ 04-09-2014.

خامسا- النصوص الرسمية :

01- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع ،2001.الأمم المتحدة نيويورك2002.

02- قانون رقم 04/15،الخاص بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، المؤرخ في 1فبراير 2015الموافق لـ 11ربيع الثاني 1436هـ،ج.ر.ج،العدد 06، الصادرة في 10فبراير 2015الموافق لـ20 ربيع الثاني 1436.

03- القانون رقم 02 ، المتعلق بالمعاملات والتجارة الإلكترونية الإماراتي، المؤرخ في 2002/02/26،المنشور في الجريدة الرسمية العدد277، دبي.

سادسا- المراجع باللغة الفرنسية :

01-Alain Bensoussan et Yves le Roux, Cryptologie et signature électronique, hermès science publication ,paris, 1999,

02-Santiago Cavanillas Mugica et autres, commerce électronique, Edition delta, beyrouth liban 2004.

03-Sieber (Ulrich), Criminal liabijlity for the transfer of data in international computer network, New problems for German law, European journal of Crime, law and criminal justice, Vol. 34, 1997.

04-André Lucas, le droit de l'informatique, paris, PUF 1987.

فهرس

الفهـــــــــــــــــرس