جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري

مذكرة لنيل شهادة الماستر في الحقوق
تخصص: قانون جنائي وعلوم جنائية

إعداد الطلبة:
- ماني صلاح الدين
- رمضاني أنور

إشراف الأستاذة
د/ -معزوز دليلة

لجنة المناقشة

الأستاذ(ة): د/ ربيع زهية.....رئيسا
الأستاذ(ة): د/ معزوز دليلة.....مشرفا ومقررا
الأستاذ(ة): د/ والي نادية.....ممتحنا

السنة الجامعية:2021/2020

كلمة شكر:

أيام مضت من عمري بدأتها بخطوة و ها أنا ذا اليوم أقطف ثمرة مسيرة سنين كان هدفي منها واضحا و كنت أسعى كل يوم لتحقيقه و الوصول له مهما كان صعبا....وها أنا وصلت و بيدي شعلة و سأحرص كل الحرص عليها حتى لا تنطفئ وأشكر الله أولا و أخيرا على أن وفقني و ساعدني على ذلك

أتقدم بجزيل الشكر لأستاذتي الفاضلة"معزوز دليلة" على النصائح والتوجيهات المقدمة طوال مرحلة انجاز المذكرة

كما أتوجه بجزيل الشكر:

لجميع أساتذة كلية الحقوق الدين كان لهم فضل كبير علينا.

كما أتقدم:

بجزيل الشكر لعمال مكتبة "ابن سينا" خاصة "مصطفى وحسام" الذين قدموا لنا التسهيلات اللازمة

كمل لا يفوتني تقديم الشكر لكل من ساهم ومد يد العون في انجاز هذه المذكرة من قريب أو بعيد.

صلاح الدين / أنور

الإهداء

إلى التي أوصى بها الرحمان ، فكانت تحت قديمها الجنان ، فكانت جسرا أعبر منه إلى بر الأمان إلى درة الأكوان إليك **أمي الغالية**

إلى الذي علمني و رباني ، إلى الذي كان سيراجا منيرا في كل زماني ومكان إلى أغلى هدية فقي حياتي لا تقدر بمال و لا أثمان

إلى **والدي الحبيب**

إلى إخوتي من كان لهم بالغ الأثر في الكثير من العقبات والصعاب

إلى

إلى التي أنحت اسمها من ذهب ، و كانت زهرة أهدتها لي الحياة : في الأخلاق نصحتني ، و في الشدائد آزرتني و في الحياة علمتني إليك أستاذتي الغالية "معزوز دليلة"

إلى أصدقائي في المشوار الدراسي **محمد، طارق، يوسف**.

صلاح الدين

الإهداء

إلى التي أوصى بها الرحمان ، فكانت تحت قديمها الجنان ، فكانت جسرا أعبر منه إلى بر الأمان إلى درة الأكوان إليك **أمي الغالية**

إلى الذي علمني و رباني ، إلى الذي كان سيراجا منيرا في كل زماني ومكان إلى أغلى هدية فقي حياتي لا تقدر بمال و لا أثمان

إلى **روح والدي الحبيب**

إلى إخوتي من كان لهم بالغ الأثر في الكثير من العقبات والصعاب

إلى

إلى التي أنحت اسمها من ذهب ، و كانت زهرة أهدتها لي الحياة : في الأخلاق نصحتني ، و في الشدائد آزرتني و في الحياة علمتني إليك أستاذتي الغالية "معزوز دليلة"

إلى أصدقائي في المشوار الدراسي **محمد، صلاح الدين**.

أنور

مقدمـــــــة

كانت المعاملات اليومية للأشخاص تتميز بالوضوح والدقة والتحديد في مضمونها ومحتواها إلى جانب توفر قدر من الأمان والثقة تجاهها، ويعود السبب في ذلك إلى الطريقة التي كانت يتم بها تحرير تلك المعاملات، حيث تكتب في محررات يمكن الرجوع إليها كلما تطلبت الحاجة، وبالتالي لم يكن من اليسير إنكارها أو تغيير محتواها ولم يكن الأمر يقتصر على توثيق تلك المحررات، وإنما يتم تذييلها بتوقيع أصحاب الشأن (الأطراف المتعاملة) عليها بما يفيد الإقرار بصحة مضمونها ومحتواها وصدورها ممن وقعها.

أما في الوقت الراهن فإن التحولات الأساسية التي يشهدها العالم لم تعد مقتصرة على شكل النظام الدولي ومسألة توازن القوى بل تعدى الأمر ذلك إلى البيئة العلمية والتكنولوجية والقدرة على البحث والتطور، حيث يطالعنا تطور تكنولوجيا المعلومات والاتصال الحديث في كل يوم بأوضاع جديدة، أصبحت معه الوسائل الإلكترونية العصب المحرك للتجارة الإلكترونية، فمعظم المعاملات المالية و التجارية أصبحت 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 والعقود الي تتم باستخدام الوسائل والأجهزة الإلكترونية الحديثة.

وقد واكب شيوع استخدام تكنولوجيا التقنيات الحديثة في إبرام التصرفات القانونية عدة تغيرات في كثير من المفاهيم القانونية، وفي إطار هذا التطور، وتماشيا مع التعاملات الإلكترونية، وسعيا إلى تأمينها ظهر ما يسمى بالتوقيع الإلكتروني، الذي انتشر به العمل مؤخرا في المعاملات الدولية والمحلية عبر فضاءات الانترنت التي أصبحت تهيمن على النصيب الأكبر من التعاملات التجارية المحلية منها والدولية، وقد انتشر العمل بهذه التقنية في العديد من الدول، كما أن الجزائر بدورها تسعى بخطى ثابتة نحو تطبيق هذه التقنية وتفعيلها والتي أصبحت ضرورة ملحة.

إلا أن هذا التطور في مجال التعامل الإلكتروني، بات معه المشرع ملزما بمواكبته وتغطيته مدنيا وجنائيا باللازم من النصوص ضمانا لحقوق المتعاملين داخله، وعلى اعتبار أن المستهلك الإلكتروني يتعامل ضمن فضاء افتراضي، فإنه وباعتباره الطرف الضعيف الأحق بالحماية القانونية ضد أي اعتداء أو تجاوز يمس بحقوقه بفعل هذه التعاملات.

والمشرع الجزائري بدوره واكب هذا التطور وأحكم عليه سيادة القانون من خلال إحداث قسم ضمن قانون العقوبات في القسم الثالث مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، كما استجاب كذلك لهذا التطور من خلال القانون رقم 15-04 المحدد للقواعد الخاصة بالتوقيع والتصديق الإلكترونيين، ونظرا لأهمية هذا التوقيع في إبرام التصرفات كان لازما على المشرع حمايته بقواعد قانونية جديدة تتماشى مع طبيعتها الإلكترونية.

1-أهمية موضوع الدراسة

تظهر أهمية دارسة هذا الموضوع من خلال الوقوف بداية على مفهوم التوقيع الإلكتروني من حيث هو أحد أهم المظاهر الحديثة في مجال المعاملات الإلكترونية، وتسليط الضوء على مختلف صور وخصائصه، وكذا مجموع الشروط القانونية التي يتطلبها لإضفاء الحجية القانونية عليه في الإثبات وكيفية التصديق عليه.

يحتل موضوع الحماية الجنائية للتوقيع الإلكتروني موقعا هاماً في الدراسات القانونية الجنائية الحديثة فهو من موضوعات الحاضر والمستقبل وهذه الأهمية تتبلور أمامنا سواء من الناحية النظرية أو التطبيقية.

فمن الناحية النظرية يثير مفهوم الحماية الجنائية للتوقيع الإلكتروني والجرائم التي تمثل اعتداء عليه، وما يثيره من مشاكل قانونية جنائية متعلقة بفكرة العقود الإلكترونية والتجارة الإلكترونية للتحايل الذي قد يظهر من جانب العميل أو التاجر أو الغير، وصور الاعتداء المتمثلة في الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع أو تزويره.

ومن الناحية العملية التطبيقية يثير مشاكل اختراق نظم المعلومات، وعدم الأمان في استخدام شبكة الانترنت في المعاملات، وممارسة قطاع البنوك لهذه النمطية من المعاملات الإلكترونية وأساليب الحماية الإلكترونية.

2-أسباب اختيار الموضوع

كانت أسباب اختيار هذا الموضوع في ضوء بعدين موضوعي وذاتي، فالأسباب الموضوعية تمحورت حول الحداثة القانونية والتشريعية للحماية الجنائية للتوقيع الإلكتروني، مما يدفع نحو البحث في مدى انسجام النصوص القانونية لهذه المنظومة مع المستجدات الراهنة في مجال المعاملات الإلكترونية خاصة في ظل أهمية التوقيع الإلكتروني، وأهمية المصادقة على هذا التوقيع بما يضفي عليه حجية في الإثبات، فضلا عن وسائل الحماية الجنائية المعتمدة من قبل المشرع لمواجهة جرائم الاعتداء على التوقيع الإلكتروني.

أما الأسباب الذاتية فترجع إلى الشعور بأهمية وضرورة البحث في هذا الموضوع، والطموح العلمي الذي يدفع باتجاه تقصي الجديد في ميدان القانون الجنائي والعلوم الجنائية، والرغبة في المداهمة –ولو بشكل محدود–في إثراء النقاش القانوني في مثل هذه المواضيع.

3- منهج الدراسة

تعتمد الدراسات العلمية بصفة عامة والدراسات القانونية بصفة خاصة على مناهج بحث علمية لأنها تعتبر المكون الأساسي للبحوث العلمية وموضوع دراستنا يلزم استعمال مناهج بحث علمية ومن بينها المنهج التحليلي بغية تحليل واستقراء أهم النصوص القانونية المتعلقة بالتوقيع الالكتروني، إضافة إلى المنهج الوصفي الذي يقدم أهم المعطيات والالمام بجوانب الدراسة، مع التعريج على المنهج المقارن بين الدراسات المحلية والدولية للتوقيع الالكتروني

إشكالية الدراسة

وبناء على ما سبق، نحاول الإجابة في دراستنا لموضوع الحماية الجنائية للتوقيع الإلكتروني عن تساؤل مهم يمثل إشكالية الدراسة: إلى أي مدى يمكن اعتبار الوسائل والآليات القانونية التي أقرها المشرع الجزائري كفيلة بتحقيق الحماية المطلوبة للتوقيع الإلكتروني؟

تستوجب الإجابة على الإشكالية المطروحة التعرض لمدلول التوقيع للإلكتروني من الناحية الفقهية والقانونية، وبيان أهم خصائصه وصوره هذا من جهة، ومن جهة أخرى تطرقنا إلى شروطه والتصديق عليه **(الفصل الأول)**، أما **(الفصل الثاني)** تناولنا فيه الحماية الجنائية للتوقيع الالكتروني وهذا من خلال بيان أهم الجرائم المرتبطة بالتوقيع الالكتروني، وتطرقنا الى الحماية الجنائية التوقيع الالكتروني في التشريع الجزائري.

الفصل الأول

مفهوم التوقيع الإلكتروني

التوقيع بصفة عامة عبارة عن علامة أو إشارة يضعها من ينسب إليه المحرر، ويتم التوقيع عادة بالإمضاء وذلك بكتابة الاسم واللقب، وقد يكون بالختم أو بصمة الأصبع، وهذا ليكون دالا على صاحبه ويميّزه عن غيره من الأشخاص.

هذا الكلام قبل الانتقال من العالم المادي الملموس إلى العالم الافتراضي، الذي أفرز عن ظهور الكتابة الإلكترونية التي تقتضي وجود توقيع عليها كي يمكن نسبتها لصاحبها، لكن مع استحالة تطبيق التوقيع العادي عليها نظرا لطبيعتها غير المادية، ظهر بديل عرف بالتوقيع الإلكتروني الذي حل محل التوقيع العادي.

هذا ما اضطر الفقه والتشريعات المختلفة للتدخل وضبط هذه الظاهرة القانونية الجديدة وإعطاء تعريف لها.

سيتم دراسة تعريف التوقيع الإلكتروني من الناحية الفقهية والقانونية وفي إطار التشريع الجزائري وفقا لما جاء به القانون رقم 15-04[1] المؤرخ في 11 ربيع الثاني عام 1436 الموافق ل 01 فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

ومن خلال فصلنا هذا سوف نستطرق للتعريف بالتوقيع الإلكتروني (مبحث أول)، وشروط التوقيع الإلكتروني والتصديق عليه (مبحث ثاني).

المبحث الأول

التعريف بالتوقيع الإلكتروني

من المستقر عليه في الفقه والقانون أنّ الكتابة لا تعد حجة بما دون فيها ما لم تقترن بالتوقيع، فالتوقيع مناط نسبة المحرر إلى موقعه، فهو بذلك لبس عنصرا من عناصر الدليل

[1]- قانون رقم 15-04 مؤرخ في: 2015/02/01، يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06، سنة 2015.

الكتابي فحسب وإنما هو بالدرجة الأولى تعبير عن إرادة الموقع في الالتزام بمضمون الورقة وإقراره لها ووسيلة لتمييز هوية الموقع.

وقد اجتهدت أغلب التشريعات المقارنة والمنظمات الدولية والإقليمية في وضع تشريعات تنظيمية للتوقيع الإلكتروني والمسائل المتعلقة به من خلال تنظيمه والأعراف له بالحجية الكاملة في الإثبات.

وسنتطرق من خلال هذا المبحث إلى التعريف الفقهي والقانوني للتوقيع الإلكتروني (مطلب أول)، ثم نتطرق إلى خصائصه وصوره (مطلب ثاني).

المطلب الأول

التعريف الفقهي والقانوني للتوقيع الإلكتروني

ظهر التوقيع الإلكتروني كنتيجة للتزاوج الذي حصل بين التكنولوجيا الحديثة ووسائل الاتصال متخذا أشكال عديدة ومختلفة تعتمد في مجملها على رموز وأرقام وبيانات تعتمد بدورها على المعادلات الرياضية واللوغاريتمية، ومدعومة بتكنولوجيا حماية من نوع خاص لم تكن معروفة، وقبل أن يتم تجسيد هذا النوع من التوقيعات قانونا اختلف الفقه في تعريفه وإيجاد معنى له، بينما نجد القضاء قد تصدى للمسألة من قبل (بفضل محكمة النقض الفرنسية).

ومن خلال هذا المطلب سنتطرق إلى التعريف الفقهي للتوقيع الإلكتروني (فرع أول)، والتعريف القانوني للتوقيع الإلكتروني (فرع ثاني).

الفرع الأول: التعريف الفقهي للتوقيع الإلكتروني

لقد تعددت التعريفات الفقهية التي قيلت لتحديد المقصود بالتوقيع الإلكتروني ورغم تعددها فإنها تدور في محور واحد وهو عدم الخروج عن تحديد وظيفتي التوقيع ورغم ذلك يمكن القول أن الآراء الفقهية منقسمة إلى طائفتين أو فريقين فالفريق الأول من الفقه ركّز في تعريفه على الكيفية أو الطريقة التي ينشأ من خلالها أو بها التوقيع الإلكتروني، وعرف على أنّه «التوقيع

الناتج عن إتّباع إجراءات محددة تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع الإلكتروني».[1]

كما عرّفه البعض الآخر بأنّه:" عبارة عن بيانات مجزّأة عن الرّسالة يجري تشفيرها وإرسالها مع الرّسالة بحيث يتم التّثبت من صحة الرّسالة عند فك الشّفرة وانطباق محتوى التوقيع على الرّسالة".

وعرّف البعض التوقيع الإلكتروني «مجموعة من الإجراءات والوسائل التي يتبع استخدامها عن طريق الرّموز أو الأرقام إخراج رسالة إلكترونية تتضّمن علامة مميّزة لصاحب الرّسالة المنقولة إلكترونيا يجري تشفيرها باستخدام زوج من المفاتيح، واحد معلن والآخر خاص بصاحب الرسالة» يرتكز أصحاب هذا التّعريف على أحد أشكال التوقيع الإلكتروني ألا وهو التوقيع الرقمي الذي يقوم على التشّفير اللاتماثلي أي التشّفير القائم على زوج من المفاتيح العام والخاص.[2]

وهناك من عرّفه أيضا «بأنّه مجموعة من الأرقام التي تختلط أو تمتزج مع بعضها البعض بعمليات حسابية معقّدة ليظهر في النّهاية عدد أو رقم سري خاص بشخص معين»[3]

هذه التّعاريف جاءت مركزة على الطريقة التي يتم بها إنشاء التوقيع الإلكتروني كإتباع إجراءات غير تقليدية أو من خلال استخدام معادلات رياضية بمعنى أن هذه التعريفات لم تولي أدنى اهتمام لوظيفة أو للدور الذي يقوم به التوقيع الإلكتروني.

أمّا الفريق الثاني من الفقه فقد ركز على كيفية إنشاء التوقيع الإلكتروني باعتبار مجموعة من الإجراءات لكن دون تحديد هذه الإجراءات وترك الباب مفتوحا أمام أي إجراء قد يستجد

---

[1]– ربيع السعدي، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة–1–، 2016/2015، ص35.

[2]– شرف الدين أحمد، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة لمؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية، مصر، 2000، ص 03.

[3]– فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005، ص216.

ويكون قادر على تحقيق وظائف التوقيع إضافة إلى إبراز وظائف التوقيع الإلكتروني والتي يجب أن تسعى إليها الإجراءات التقنية المعترف بها وهي تحديد هوية الموقع والتّعبير عن إرادته بالموافقة على مضمون المحرر الذي تم وضع التوقيع عليه.[1]

فعرّف البعض التوقيع الإلكتروني بأنّه «بيان مكتوب في شكل إلكتروني يتمثل في حرف أو رقم أو رمز أو إشارة أو صوت أو شفرة خاصة ومميزة ينتج من إتباع وسيلة آمنة وهذا البيان يلحق أو يرتبط منطقيا ببيانات المحرر الإلكتروني (رسالة البيانات) الدالة على هوية الموقع على المحرر والرّضاء بمضمونه».[2]

كما عرّفه البعض كذلك بأنّه «إشارات أو حروف مرخّص بها من الجهة المختصة باعتماد التوقيع، ومرتبطة ارتباطا وثيقا بالتصرف القانوني تسمح بتمييز شخص صاحبها وتحديد هويته ويعبر –دون غموض–عن رضائه بهذا التّصرف القانوني».[3]

وعرّف الفقه أيضا التوقيع الإلكتروني «بأنّه مجموعة الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرّف الذي يصدر التوقيع بمناسبته».[4]

وعُرّف أيضا التوقيع الإلكتروني «بأنّه وحدة قصير من البيانات التي تحمل علاقة رياضية مع البيانات الموجودة في محتوى الوثيقة»[5].

---

[1]– ربيع السعدي، المرجع السابق، ص 36.

[2]– أبو زيد محمد محمد، تحديث قانون الإثبات مكانة المحررات الإلكترونية بين الأدلة الكتابية، دار النهضة، مصر، 2002، ص 171.

[3]–عبد الحميد ثروت، التوقيع الإلكتروني ومخاطره وكيفية مواجهتها، مدى حجيته في الإثبات مكتبة الجلاء، الطبعة الثانية، القاهرة، 2002–2003، ص 49.

[4]– عجيمي حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، سنة 2000، ص34.

[5]– نقلا عن: ربيع السعدي، أنظر:

- Wright (B) Distribution, The Risks of Electronic signatures, Practicing Law Institute-PLI order no. G4-3988-September 1996, P66.

وعرّفه جانب آخر من الفقه بأنّه «علامة أو رمز، متمايز يخص شخصا بعينه من خلاله يعبّر الشخص عن إرادته ويؤكد على حقيقة البيانات المتضمنة في المستند الذي وقعه».

وعرّفه البعض بأنّه «إجراء معين يقوم به الشخص المراد توقيعه على المحرر سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو شفرة خاصة»[1]

الفرع الثاني: التعريف القانوني للتوقيع الإلكتروني

إن التوقيع الإلكتروني يعتبر نتيجة حتمية لاستخدام الحاسب الآلي في إجراء المعاملات بين الأفراد تجارا كانوا أو أفراد عاديين، ولا يقتصر على الأفراد فقط بل يتعداه فيما بينهم وبين المؤسسات و الإدارات.

تختلف التعاريف التي أعطيت للتوقيع الإلكتروني حسب النظرة إليه، فالبعض يعرفه بناء على الوسيلة التي يتم بها، أو بحسب الوظيفة أو بناء على التطبيقات العلمية التي يتم بها.

و من خلال هذا سوف نتطرق إلى تعريف التوقيع الإلكتروني في التشريعات الدولية(أولا)، وتعريف التوقيع الإلكتروني في التشريع الجزائري(ثانيا).

أولا: تعريف التوقيع الإلكتروني في التشريعات الدولية والإقليمية

الواقع أثبت أن استخدام الأشخاص للتوقيع الإلكتروني سبق بزمن ليس باليسير كل التّشريعات الدولية والوطنية المنظمة للتجارة الدولية والتوقيع الإلكتروني، فقد عمدت هذه التّشريعات على وضع تعريف شامل للتوقيع الإلكتروني كما حرصت هذه التّشريعات على إعطاء تعريف محدد لعدد من المصطلحات المستخدمة فيه.

ومنه سوف نتطرق إلى تعريف التوقيع الإلكتروني حسب قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية باعتباره تشريعا دوليا وكذلك تعريف التوقيع الإلكتروني في التوجيه

[1]– أبو هبة نجوى، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، طبعة 2002، ص 41.

الأوربي بشأن التوقيعات الإلكترونية، بالإضافة إلى تعريف التوقيع الإلكتروني في القانون العربي الاسترشادي.

1-التوقيع الإلكتروني في قانون الأونسيترال

أ-تعريف التوقيع الإلكتروني حسب قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية

لقد وضعت لجنة الأمم المتحدة للقانون التجاري الدولي الأونسيترال في دورتها الرابعة والثلاثين قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية لعام 2001 فقد نصت المادة الأولى منه على نطاق تطبيق هذا القانون، حيثما تستخدم التوقيعات الإلكترونية في سياق الأنشطة التجارية.

ونصّت المادة الثانية من هذا القانون على تعريف التوقيع الإلكتروني وذلك بقولها: «يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنّسبة إلى رسالة البيانات ولبيان موافقته على المعلومات الواردة في رسالة البيانات».[1]

يتّضح جليا أن قانون الأونسيترال لم يحدّد الطريقة أو التقنية التي يتم بها استخدام التوقيع الإلكتروني وهذا ليس من باب السهو أو التقصير وإنّما من أجل ترك المجال مفتوح أمام أيّة تقنية للدلالة على هوية الموقع وإبراز نيته في الالتزام بمضمون المحرر، خاصّة وأن عالم المعلومات يسير بوتيرة متسارعة جدا حتى يشمل كل التقنيات من جهة ومن جهة ثانية المحافظة كذلك على دور الدول في تحديد الطريقة التي يتم بها التوقيع كل حسب التّشريع الذي يصدر وكيفية استخدام التوقيع بالدلالة على شخصية الموقع ومدى التزامه بالمحرر، ويتبين هذا الأمر من خلال ما جاءت به المادة الثالثة من ذات القانون والتي نصّت: «لا تطبق أي من أحكام هذا القانون باستثناء المادة الخامسة بما يشكل استبعادا أو تقييدا أو حرمانا من مفهوم

[1]- أنظر المادة 2 من قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 12 ديسمبر 2001، متوفر عبر الموقع: http//daccess-ods.un.org/tmp/7958533.html

قانوني لأي طريقة إنشاء توقيع إلكتروني تفي بالاشتراطات المشار إليها في الفقرة الأولى من المادة السّادسة أو تفي على أي نحو آخر بمقتضيات القانون المنطبق».[1]

كما نصّت الفقرة الأولى من المادة السّادسة: «حيثما يشترط القانون وجود توقيع من شخص، يعدّ ذلك الاشتراط مستوفي بالنّسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني موثوق به بالقدر المناسب للفرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل ذي صلة".[2]

الملاحظ أن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية في تعريفه للتوقيع ركز على الوظيفة التي يجب أن يقوم بها التوقيع وهي تعيين هوية الموقع على رسالة البيانات والتعبير عن إرادته بالموافقة والالتزام للمعلومات الواردة في الرسالة الإلكترونية (المحرر الإلكتروني).[3]

ب-تعريف التوقيع الإلكتروني في قانون الأونسيترال النموذجي بشأن التّجارة الإلكترونية

لقد وضعت لجنة الأمم المتحدة للقانون التجاري الدولي الأونسيترال في دورتها التّاسعة والعشرين القانون النموذجي للتّجارة الإلكترونية في 1996/12/16 وبالرجوع إلى هذا النّص من المادة الأولى إلى المادة السّابعة عشر والأخير لا نجده قد تضمن أي تعريف للتوقيع الإلكتروني وكل ما في الأمر أن المادة السّابعة منه اكتفت بالإشارة إلى وظائف التوقيع الإلكتروني فقد نصّت «عندما يشترط القانون وجود توقيع من شخص، يستوفى ذلك الشّرط بالنّسبة إلى رسالة البيانات إذا:

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

[1]- أنظر المادة 3 من قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية 2001، المرجع السابق.

[2]- أنظر المادة 6، المرجع نفسه.

[3]- ربيع السعدي، المرجع السابق، ص39.

ب— كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للفرض الذي أنشئت أو أبلغت من أجل رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتّفاق متّصل بالأمر".

من خلال مراجعة قانون الأونسيترال النموذجي بشأن التّجارة الإلكترونية نجده قد جاء بمفهوم متطوّر للكتابة ولم يقصرها على الكتابة التقليدية بل شملت أيضا الكتابة الإلكترونية بالإضافة إلى الاعتراف بالتوقيع الإلكتروني وأهمّيته في الإثبات من خلال النّص المذكور أعلاه والذي جاء مبيّنا لوظائف التوقيع الإلكتروني بحيث نصّ على أنه وسيلة تستخدم لتعيين هويّة الشّخص الموقع والتدليل على موافقته على المعلومات الواردة في رسالة البيانات.[1]

2-تعريف التوقيع الإلكتروني من خلال توجيهات التكتّلات الإقليمية. (التوجيه الأوربي رقم 1999/93 الصّادر في 1999/12/13 في شأن التوقيع الإلكتروني)

إنّ التوقيع الإلكتروني وباعتباره من المسائل الفنّية والتقنيّة والقانونية يتطلّب إجراءات تضمن موثوقيته يكون من شأنها أن تعرف بموقع السّند والتأكّد من هويته ولتحقيق هذا الغرض فقد كان هذا النظام القانوني محل اهتمام على الصعيد الدولي وكذلك على الصعيد الإقليمي خاصّة وأنّ هذه التكتلات الإقليمية اتّجهت من خلال توجيهاته إلى تنظيم قواعد التّجارة الإلكترونية والتوقيع الإلكتروني وما يهمنا هنا التوجيهات التي أصدرها الاتّحاد الأوربي رقم 1999/93/24 الخاصّة بالتوقيعات الإلكترونية والتي اعتمدها البرلمان الأوربي بتاريخ 1999/12/13.[2]

وعمل من خلالها على تعريف التوقيع الإلكتروني من خلال التفريق بين نوعين من التوقيع الإلكتروني وذلك حسب مستويات التوقيع.

[1]- ربيع السعدي، المرجع السابق، ص ص 39-40.

[2]- التوجيه الأوربي رقم 93-1999، بشأن الإطار المشترك للتواقيع الإلكترونية، الصادر بتاريخ 1999/12/13.

المستوى الأول ويخصّ التوقيع الإلكتروني البسيط أو العادي والذي عرّفته المادّة الثّانية بأنّه «معلومة تأخذ شكلا إلكترونيا تقترن أو ترتبط بشكل منطقي ببيانات أخرى إلكترونية والذي يشكّل أساس منهج التوثيق».[1]

التّعريف الذي جاءت به المادّة الثّانية حدّد الوسائل القانونية التي بواسطتها يتم التوقيع الإلكتروني دون بيان الوظائف القانونية المرجوة.

أمّا النوع أو المستوى الثاني من التوقيع الإلكتروني فهو التوقيع المسبق أو المتقدم أو المعزز وهذا النوع من التوقيع عرّفته المادة الثانية الفقرة الثانية من التوجيه الأوربي بأنه التوقيع الذي يلبي وتتوفر فيه الشّروط التالية:

- أن يرتبط بشكل منفرد بصاحب التوقيع.
- أن يمكن ويتيح تحديد هوية الموقع.
- أن يتم إنشاؤه من خلال وسائل موضوعة تحت رقابة صاحب التوقيع.
- أن يكون مرتبط بالبيانات التي يلحق بها بشكل يجعل أي تعديل لاحق على البيانات يمكن كشفه.[2]

المشرع الأوربي عمل من هذا التعريف وضع ضوابط تقنية وقانونية يجب أن تتوفر في التوقيع الإلكتروني من أجل التحقق من صحته وسلامته وعند تحقق هذه الضوابط يكون التوقيع الإلكتروني متمتع بمزايا التوقيع العادي بينما التوقيع البسيط فحجته نسبية مقارنة بحجية التوقيع المتقدم (Electronique Signature Avancee)

---

[1]- نقلا عن: ربيع السعدي، أنظر:

Sinisi Vinenzo, digital signature legislation in Europe, International business lawyer, December 2000 Vol 28. N°11, P487.

[2]- نقلا عن: ربيع السعدي، أنظر:

Sinisi Vinenzo, op.cit, P489.

3-تعريف التوقيع الإلكتروني في القانون العربي الاسترشادي للإثبات بالطرق الحديثة:

عرّف هذا القانون الذي تبنته الجامعة العربية وصادق عليه مجلس الوزراء العدل العرب بموجب القرار رقم 24د/771 المؤرخ في 27 نوفمبر 2008، التوقيع الإلكتروني في مادته الأولى الفقرة (03) بأنه: «ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميز عن غير»[1].

بعد تعريف التوقيع الإلكتروني في ضوء التشريعات الدولية والإقليمية ممثلة في تعريف قانون الأونسيترال النموذجي دوليا، تعريف التوجيه الأوروبي، وتعريف القانون العربي إقليميا، لابد من تعريفه في ظل التشريع الجزائري للوقوف على نظرة المشرع الجزائري للتوقيع الإلكتروني[2].

ثانيا: تعريف التوقيع الإلكتروني في التشريع الجزائري

بصدور القانون 05-10 المؤرخ في 2005/06/20 المعدل والمتمّم للأمر 75-58 المتضمن القانون المدني يكون التشريع الجزائري قد قفز قفزة نوعية من خلال انتقاله من النظام الورقي للإثبات إلى النظام الإلكتروني في الإثبات حيث: أصبحت الكتابة الإلكترونية دليلا في الإثبات ليس هذا فحسب بل أن المشرع اعتمد مبدأ التكافؤ في الإثبات بين الكتابة التقليدية والكتابة الإلكترونية، وهذا ما نصّت عليه أحكام المادة 323 مكرر 1 بقولها «يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات على الورق».[3]

---

[1]- كواشي ياسمينة، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في ظل القانون، مذكرة مكملة لنيل شهادة الماستر في تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي-أم البواقي، كلية الحقوق والعلوم السياسية 2017/2016، ص09.

[2]- المرجع نفسه، ص09.

[3]- قانون رقم 05-10 المؤرخ في 2005/06/20 المعدل والمتمم للأمر 75-58 المؤرخ في 26-90-1975 المتضمن القانون المدني المعدل والمتمم، الجريدة الرسمية رقم 44، لسنة 2005.

وعرّف المشرع الجزائري في المادة 323 مكرر من القانون 05-10 الكتابة الإلكترونية بأنّها تسلسل في الحروف أو أوصاف أو أرقام أو أية علامة أو رموز ذات معنى مفهوم مهما كانت الوسيلة الإلكترونية المستعملة ومهما كانت طرق إرسالها[1].

أمّا بخصوص التوقيع الإلكتروني فإنّه يمكن القول أن التشريع الجزائري استعمل هذا المصطلح لأول مرة في أحكام المادة 2/327 من القانون 05-10 والتي نصّت على أن التوقيع الإلكتروني يضفي الحجية والقوة الثبوتية على المستند أو المحرر الإلكتروني.

وهذا بشرط أن يتم التوقيع الإلكتروني حسب الشّروط المحددة بأحكام المادة 323 مكرر 1 من القانون المدني، فقد نصّت المادة 2/327 قانون مدني «يعتدّ بالتوقيع الإلكتروني وفق الشّروط المذكورة في المادة 323 مكرر 1».

أمّا عن تعريف التوقيع الإلكتروني فإنّ أحكام المادة 03 من المرسوم التنفيذي رقم 07-162 عرّفته بأنّه: «معطى ينجم عن استخدام أسلوب عمل يستجيب للشّروط المحدّدة في المادّتين 323 مكرر323 مكرر1 من الأمر75-58 المؤرخ في 1975/09/26 والمذكور أعلاه".[2]

غير أنّ المشرع الجزائري ونظرا لأهمية التوقيع الإلكتروني في المعاملات الإلكترونية وانفتاح الاقتصاد الوطني كان من اللّازم عليه إيجاد سياسة قانونية تواجه هذه التحولات العميقة سواء على مستوى المعاملات الاقتصادية أو على مستوى الأنظمة الحديثة في التعامل ونظرا لكون المنظومة القانونية التي كانت موجودة لا تستجيب لمتطلبات اقتصاد حرّ ولا تساير عصر التكنولوجيا فقد تدخل المشرع الجزائري من أجل سدّ هذا الفراغ و أصدر قانونا خاص رقم 15-04 مؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، هذا

[1] – أنظر المادة 323 مكرر من القانون 05-10، المرجع السابق.

[2]– مرسوم تنفيذي رقم 07-162 يعدل ويتمم المرسوم01 / 123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية مؤرخ، في:2007/05/30 الجريدة الرسمية عدد 37، الموافق ل7 يونيو 2007.

القانون يهدف بالأساس إلى تحديد القواعد العامة والخاصة بالتوقيع الإلكتروني والتصديق الإلكتروني، فقد جاء في الباب الأول (الفصل الثاني) تحت عنوان التعاريف المقصود من التوقيع الإلكتروني فقد عرّفته المادة 02 بأنّه " بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية تستعمل كوسيلة توثيق"[1].

وقد نصّت كذلك المادة 06 من الباب الثاني (الفصل الأول) على أنّه «يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع وإثبات قبول ومضمون الكتابة في الشّكل الإلكتروني».[2]

من خلال استقراء نصوص المواد القانونية التي جاء بها قانون 15-04 لاسيما تلك المتعلقة بتعريف التوقيع الإلكتروني نجده قد تبنى المعيار الوظيفي للتوقيع بحيث جاء مركز، على وظيفة التوقيع دون التطرق أو تحديد الطريقة التي ينشأ بها هذا التوقيع.

كما أنّ المشرع الجزائري تبنى مفهوم التوقيع الإلكتروني الموصوف وهو التوقيع الذي يتم وفقا للمتطلبات الواردة بأحكام المادة السابعة والتي نصّت: «التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

1-أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

2-أن يرتبط بموقع دون سواه.

3-أن يمكن من تحديد هوية الموقع.

4-أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

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

6-أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات...».[3]

---

[1]- قانون رقم 15-04، المرجع السابق.

[2]- أنظر المادة 06، المرجع نفسه.

[3]- أنظر المادة 07، المرجع نفسه.

بمعنى آخر أنّ المشرع الجزائري تأثر بالتوجيه الأوربي رقم 1999/93 الصادر في: 1999/12/13 عندما نص على التوقيع البسيط والتوقيع المسبق أو المتقدم.[1]

المطلب الثاني

خصائص التوقيع الإلكتروني وصوره

من خلال التعريفات السابقة للتوقيع الإلكتروني، نلاحظ أن التوقيع الإلكتروني أيضا خصائص وصور تميزه وتجعله يتفوق بكثير عن التوقيعات العادية أو التقليدية، وهذا ما سوف نحاول التطرق إليه في هذا المطلب وذلك من خلال دراسة خصائص التوقيع الإلكتروني (فرع أول) وصور التوقيع الإلكتروني (فرع ثاني).

الفرع الأول: خصائص التوقيع الإلكتروني

يتميّز التوقيع الإلكتروني بأنّه لا يتم عبر وسيط مادي، بحيث تذيل به الكتابة، كما هو الحال بالنسبة للتوقيع الكتابي، وإنما يتم كليا أو جزئيا عبر وسيط إلكتروني من خلال أجهزة الكمبيوتر، أو عبر الانترنيت، بحيث يكون بإمكان أطراف العقد الاتصال ببعضهم البعض والاطلاع على وثائق العقد، والتفاوض بشأن شروطه وإفراغ هذا العقد في محررات إلكترونية، وأخيرا التوقيع عليها إلكتروني.[2]

لزوم تدخل طرف ثالث Tiers de confiance الذي يقوم بدور الوسيط بين أطراف العقد، حيث استلزمت ضرورة الأمن القانوني وجوب استخدام تقنية آمنة في التوقيع الإلكتروني تسمح

[1] – التوجيه الأوربي رقم 93–1999، المرجع السابق.

[2] – يونس عرب، منازعات التجارة الإلكترونية، الاختصاص والقانون الواجب التطبيق وطرق التقاضي، ورقة عمل مقدمة إلى مؤتمر التجارة الإلكترونية الذي أقامته منظمة الأمم المتحدة، بيروت، الفترة ما بين 8 و10 تشرين الثالث 2000، ص ص 17 -18، منشور على الموقع: http://www.aeab-low.com

بالتعرف على شخصية الموقع[1]، وسوف نتعرض إلى أهم خصائص التوقيع الإلكتروني في النقاط التالية:

أولا: يوفر الخصوصية.

حماية البيانات ضد الاستخدام غير المشروع، أو بمعنى أخر تحديد صلاحيات الوصول للبيانات وعدم السماح للأشخاص بتنفيذ إجراء معين على البيانات لا يمتلكون الصلاحيات الكافية لتنفيذه، وتتم هذه العملية بتفعيل صلاحية الوصول أثناء حفظ بيانات التوقيع الإلكتروني الموجود على بطاقة ذكية ولا يغادرها أبدا ومحمي برقم سري، بتشفير البيانات أثناء إرسالها وهي إحدى مزايا التوقيع الإلكتروني التي تهدف إلى التأكد من أن الشخص المقصود هو الوحيد الذي اطلع على المستند المرسل.[2]

نعني بالخصوصية أن البيانات متوفرة' فقط للأشخاص المسموح لهم الاطلاع عليها بعبارة' أخرى عدم إطلاع الآخرين غير المخول لهم الاطلاع على مضمون المستند الموقع إلكترونيا سوى الشخص المرسل له.

ثانيا: يوفر التعرف على المستخدم (Authentification)

تتم عملية التحقق من هوية الأشخاص أو التعرف على مصادر البيانات عن طريق كلمات السر والبطاقات الذكية، أو عن طريق شهادة" التصديق الإلكتروني المصدرة" من جهة تصديق إلكتروني، وكلما زادت الحاجة لدقة تحديد الهوية يتم اللجوء إلى جمع عدة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم.[3]

---

[1]– محمد بودالي، التوقيع الإلكتروني، مجلة الإدارة، العدد الثاني، الجزائر، 2003، ص 57.

[2]– لالوش راضية، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع "القانون الدول للأعمال"، كلية الحقوق والعلوم السياسية، جامعة المولود معمري، تيزي وزو، 2012، ص 37.

[3]– المرجع نفسه، ص 37.

ثالثا: يوفر وحدة البيانات: (integrite)

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

رابعا: يوفر عدم القدرة على الإنكار: (Non-Repidiation)

عدم قدرة الشخص الموقع إلكترونيا أو الشخص الذي قام بإرسال رسالة إلكترونية لوجود طرف ثالث يمكنه إثبات قيام طرف معين بفعل إلكتروني معين، وكذا عدم قدرة مستلم رسالة معينة على إنكاره استلامه لرسالة ما، حيث إن المفتاح العام يثبت استلام الرسالة من قبل المستقبل وذلك بإرسال رد (وصل تسليم) إلى المرسل فعدم الإنكار تعنى حماية المستند أو العقد الإلكتروني من الإنكار عن أحد الطرفين (المرسل أو المستقبل).[2]

خامسا: تاريخ توقيع الرسالة.

لا يستطيع مرسل الرسالة تغيير تاريخ توقيع وإرسال الرسالة وكذلك مستقبل الرسالة، حيث أن ذلك له أهمية كبيرة في مجال التجارة الإلكترونية والعقود القانونية يعني تاريخ توقيع الرسالة عدم قدرة مرسل الرسالة أو مستقبلها من إجراء أي تعديل على تاريخ إرسال أو استلام المستند فهو ملزم للطرفين خاصة في حال إبرام العقود التجارية عبر الانترنت.[3]

---

[1]– صلاح عبد الحكيم المصري، متطلبات استخدم التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، رسالة لنيل شهادة الماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2006، ص ص 24–25.

[2]– مناني فراح، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009، ص ص196–197. وكذا لنفس المؤلف، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008، ص ص 87، 145.

[3]– لالوش راضية، المرجع السابق، ص 38.

سادسا: يوفر السرعة ودقة إنجاز المعاملات.

يزيد التوقيع الإلكتروني من سرعة ودقة المعاملات الإلكترونية ويقلل من تأخر إرسال واستلام العقود والمستندات التجارية وغيره من العقود حول العالم.[1]

الفرع الثاني: صور التوقيع الإلكتروني

التوقيع الإلكتروني كما سبق تعريفه هو عبارة عن بيانات تتخذ شكل حروف أو أرقام أو رموز أو إشارة أو غيرها مدرجة في شكل إلكتروني أو رقمي أو ضوئي أو أية وسيلة مستحدثة في رسالة بيانات أو مضافة عليها أو مرتبطة بها ارتباطا منطقيا وله طابع خاص مما يسمح بتحديد هوية الموقع وتمييز عن غيره.

من خلال هذا التعريف يتضح أن التوقيع لا يأخذ صورة واحدة فكما أن التوقيع العادي يتم بعدة أشكال محددة في القانون فإن التوقيع الإلكتروني كذلك يأخذ صور مختلفة ومتعددة.

وهذه الصور تختلف فيما بينها من حيث درجة الثقة بها ومستوى ما تقدمه من ضمان لصاحبها بحسب الإجراءات المتبعة في إصدارها وتأمينها وتتفق جميع صور التوقيع الإلكتروني في اعتمادها على وسائط إلكترونية ومن تعدد أشكال التوقيع الإلكتروني يعود بالدرجة الأولى إلى تعدد واختلاف التقنية في تشغيل منظومة التوقيع الإلكتروني.

بالرجوع إلى القانون رقم 15-04 المتعلق بتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين نجده قد حدد الوظائف الواجب أن يؤديها التوقيع الإلكتروني مع التطرق إلى نوعي التوقيع الإلكتروني وهما التوقيع الإلكتروني الموصوف والتوقيع الإلكتروني البسيط، «غير أن المختصين في مجال المعلوماتية قد اتفقوا بشكل عام، على اعتبار التوقيع الإلكتروني عبارة تحمل في طياتها مفهوما عاما يشمل آليات تقنية يمكن استعمالها بهدف التوقيع على قدر ما تسمح هذه الآلية وحدها آو مجتمعة بتحقيق الوظائف الأساسية للتوقيع».[2]

---

[1]– لالوش راضية، المرجع السابق، ص 38.

[2]– ضياء أمين مشيمش، التوقيع الإلكتروني دراسة مقارنة تقديم القاضي الدكتور مروان كركبي دار، المنشورات الحقوقية، بيروت، لبنان، طبعة سنة 2003، ص126.

إن من تعدد صور التوقيع الإلكتروني هو المراحل المختلفة التي مرت بها التطورات التقنية والفنية في مجال المعلوماتية لذلك فإنه يصعب حصر هذه الصور والأشكال خاصة وأن الأبحاث العلمية في تقدم وتطور هذا التطور الذي أفرز أشكالا مختلفة للتوقيع الإلكتروني فما هي هذه الصور؟ للإجابة على هذا السؤال قسمنا هذا الفرع إلى خمس نقاط.

- التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة.
- التوقيع بالقلم الإلكتروني (Pen-Op).
- التوقيع البيومتري (La Signature biometrique)
- التوقيع بواسطة الماسح الضوئي.
- التوقيع الرقمي.

أولا: التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة.

تعتبر هذه الصورة الأكثر انتشارا في التعاملات الإلكترونية خاصة المعاملات البنكية حيث درجت البنوك على إصدار بطاقات ذكية -بطاقات بلاستيكية-[1] مصحوبة برقم سري يتمثل في أرقام أو حروف أو رموز تمنحها لعملائها لاستخدامها في سحب وإيداع النقود أو لسداد ثمن السلع والخدمات[2]، وتتم عملية سحب النقود أو إيداعها أو عملية الدفع الإلكتروني من خلال جهاز آلي تؤمنه البنوك للعملاء كجهاز الصراف الآلي (A.T.M)[3] أو جهاز الدفع

[1]- القليوبي سميحة، الأوراق التجارية (الكمبيالة، السند لأمر، الشيك، الشيك السياحي، الشيك المسطر، الشيك المعتمد وسائل الدفع الحديثة)، الطبعة الخامسة، دار النهضة العربية، القاهرة، 2006، ص547 وما بعدها.

[2]- حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، مصر، 2000، ص35.

[3]- أجهزة الصراف الآلي يرمز لها (A.T.M) اختصار لـ: Automatic Teller Machine، وقد وجدت ماكينات الصرف الآلية في أماكن مختلفة خارج البنوك في المحلات الكبرى والفنادق وشوكات الطيران وأصبح للعميل حرية التعامل مع رصيده بالسحب أو الإيداع باستعمال بطاقته من خلال جهاز الصراف الآلي (A.T.M) دون الرجوع للبنك وطوال اليوم دون التقييد بأوقات العمل الرسمية أو غيره. أنظر: لالوش راضية، المرجع السابق، ص 40.

الإلكتروني الموجود في المحلات التجارية، أي المحلات التي تقبل الدفع بهذه البطاقة بموجب اتفاق مع الجهة المصدرة لها.

استخدام البطاقة في السحب أو الإيداع من الصراف الآلي عن طريق قيام العميل صاحب البطاقة بعمليتين معاصرتين:

إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل بالوضع الصحيح على فتحة خاصة في جهاز الصراف الآلي (A.T.M).

إدخال الرقم السري[1] المخصص له (الذي يعد بمثابة التوقيع)، وذلك بكتابته بواسطة لوحة المفاتيح الموجودة على الجهاز الآلي، فإذا كان الرقم صحيحا فإن بيانات الجهاز توجه العميل إلى تحديد المبلغ المراد سحبه أو إيداعه، وذلك بالضغط على مفاتيح خاصة بذلك فيتم صرف المبلغ المطلوب، وتعاد البطاقة للعميل من نفس فتحة البداية.

في حالة استخدام البطاقة لوفاء ثمن المشتريات أو الخدمات فإن التاجر يتولى تمرير البطاقة عبر جهاز خاص يتصل بدوره بنظم المعلومات الخاصة بالبنك، وهذا لقراءة البطاقة فيعلم التاجر جميع البيانات الخاصة بالعميل وحدود التعامل معه قبل إبرام عقد البيع أو تقديم الخدمة له، فتتحدد بذلك حقوق التاجر ومسؤوليته طبقا لقراءة هذه البيانات.[2]

فإذا ما قام العميل بإدخال الرقم السري (PIN) الخاص به في الجهاز يتم سداد المستحقات عن طريق التحويل من حساب العميل لدى البنك إلى حساب التاجر لدى نفس البنك أو لدى بنك آخر.[3]

---

[1]– يطلق على الرقم السري الخاص بالبطاقة باللغة الفرنسية Numeros d'identifiacation personnel، ويرمز له بالمختصر Nip، وفي الإنجليزية personal identification number، ويرمز له بالمختصر P.I.N أنظر: لالوش راضية، المرجع السابق، ص41.

[2]– إبراهيم سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، أطروحة دكتورة الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص ص 51، 64.

[3]– ثروت عبد الحميد، ماهيته مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، دار الجامعة الجديدة، القاهرة، 2007، ص 58.

يوجد نظامان تعمل عليهما أجهزة الصرف الآلية (A.T.M): الأول يعرف بنظام الدفع غير المباشر (off-line)، وفي حالة استخدام ذلك النظام، يقوم جهاز التاجر بتسجيل العملية التي أنجزها العميل على شريط مغناطيسي، ولا يتغير موقفه المالي ويبقى كما هو حتى يتم نقل هذه الشرائح المغناطيسية إلى الجهة مصدرة البطاقة –البنك–حسب المدة" الزمنية المتفق عليها –يوميا أو أسبوعيا–، ليقوم موظف البنك في النهاية بتوثيق هذه العملية عن طريق تسجيلها في الحاسب المركزي التابع للجهة مصدرة البطاقة [1].

يعرف النظام الثاني بنظام الدفع المباشر (on-line)، وهو يقوم فورا وبمجرد انتهاء العميل من العملية بتحديد موقفه المالي.

يتميز هذا الشكل من التوقيع الإلكتروني بالإضافة إلى سهولته وبساطته— بقدر كبير من الأمان والثقة، كما أنه يتميز بقدرته على تحديد هوية شخص الموقع، فإتباع العميل الإجراءات التي ذكرناها سابقا، يؤكد أن من قام بالعملية المصرفية هو الشخص صاحب الرقم السري.[2]

في حالة فقدان البطاقة، أو سرقتها، أو نسيان الرقم السري، يتم تجميد كل التعاملات التي تتم بواسطتها بمجرد إخبار البنك بذلك، أضف إلى هذا أن عملية السحب يتم إثباتها على ثلاثة أنواع من المخرجات على شريط ورقي موجود خلف جهاز السحب وعلى أسطوانة ممغنطة، كما يتسلم العمل بدوره إيصالا يثبت قيامه بالعملية ويحدد –بالإضافة إلى بيانات أخرى–المبلغ الذي تم سحبه.[3]

يعتبر البعض أن هذا النوع من التوقيع –التوقيع بالرقم السري–لا يعادل التوقيع الخطي لأن استخدامه لا يقتضي الوجود المادي للشخص الذي ينسب إليه [4]، غير أن الفقهاء أجمعوا

---

[1]– القليوبي سميحة، المرجع السابق، ص 552.

[2]– محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص 270.

[3]– ثروت عبد الحميد، المرجع السابق، ص 58.

[4]– سعيد سيد قنديل، "التوقيع الإلكتروني"، دار الجامعة الجديدة، الإسكندرية، 2006، ص 68.

على صلاحيته[1]، لقدرته على تحديد هوية صاحبه وتمتعه بالثقة والأمان وقد فند جميع الفقهاء المأخذ السابق وذلك وفقا للآراء التالية:

1: إن الرقم السري مساوي للتوقيع التقليدي من حيث أداء الوظائف، فإتباع العميل للإجراءات المحددة–لسحب النقود أو إيداعها أو لدفع ثمن السلع أو الخدمات يشكل إقرارا منه بما يريد من بيانات بالشريط (الورقي أو الممغنط) الناتج عن الجهاز الآلي.

2: إن الحصول على البطاقة الممغنطة بأي طريقة كانت لا يعني الوصول للرقم السري، لانفصالهما عن بعضهما، إضافة إلى أن استعمال الرقم السري بطريقة غير مشروعة من قبل الغير مساوي لتزوير التوقيع التقليدي.

3: كل الأجهزة الخاصة بالسحب النقدي أو الدفع مبرمجة على رفض البطاقة بعد المحاولة الثالثة لإدخال الرقم السري، مما يعني تضيق فرصة استعمالها بالطرق غير الشرعية.[2]

اعترف القضاء الفرنسي مبكراً بالتوقيع الإلكتروني المتمثل في التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة، كونه محاط بالضمانات نفسها الموجودة في التوقيع التقليدي، واستند في إضفاء الحجية القانونية لهذا التوقيع الإلكتروني على الاتفاقات التي تبرم بين ذوي الشأن والتي تنص على ذلك صراحة.

وهذا ما قامت به محكمة النقض الفرنسية عند اعترافها للتوقيع الإلكتروني الذي يصاحب عملية السحب بحجيته الكاملة في الإثبات، فقد اكتفت بالأدلة التي قدمها البنك من واقع التسجيلات التي يقوم بها جهاز الحاسب الآلي الملحق بجهاز الصرف، وألغت قرار محكمة الموضوع التي استبعدت هذا الدليل لتعارضه مع مبدأ عدم جواز اصطناع الشخص دليلا

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الحساب الآلي والانترنت، دار الكتب القانونية، الإسكندرية، مصر، 2002، ص90.

[2]– سعيد سيد قنديل، المرجع السابق، ص 69.

لنفسه، على اعتبار أن اتفاق الإثبات الموجود بين البنك والعميل يبيح الاستناد إلى التسجيلات الموجودة لدى البنك في إثبات ما يقوم به العميل من معاملات.[1]

أيد الفقه في معظمه حكم محكمة النقض معتبرا أن التوقيع باستخدام الرقم السري لا يصدر عن جهاز الصراف الآلي وإنما من خلاله، فقيام العميل بإدخال البطاقة الممغنطة بفتحة الجهاز الآلي ثم كتابة الرقم السري، يعني أن العميل قد وقع على العملية، بواسطة الجهاز الآلي، فالجهاز يقوم بذات مهمة القلم في التوقيع، بمعنى أنه وسيلة لأداء التوقيع.

ثانيا: التوقيع بالقلم الإلكتروني (Pen-Op).

من الأشكال الأخرى للتوقيع الإلكتروني التي يمكن استخدامها في توثيق التصرفات القانونية التي يتم إبرامها على الوسائط الإلكترونية، التوقيع باستخدام قلم خاص، يعرف بالقلم الإلكتروني، وهو عبارة" عن قلم إلكتروني حساس يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي يتيح التقاط التوقيع، والتحقق من صحته حيث يتلقى البرنامج المثبت على قاعدة" بيانات الحاسوب، بيانات المستخدم عن طريق بطاقة تحقيق هوية إلكترونية خاصة تحتوي على بيانات كاملة عن هذا الشخص.[2]

ثم يظهر بعد ذلك بعض التعليمات على شاشة الحاسوب ليتبعها المستخدم حتى تظهر رسالة على الشاشة نطلب من المستخدم كتابة توقيعه باستخدام القلم الإلكتروني داخل مربع يعرض على الشاشة، وعندما يقوم المستخدم بتحريك القلم على الشاشة وكتابة توقيعه، يلتقط البرنامج حركة اليد ويظهر التوقيع مكتوبا على الشاشة بسماته الخاصة من حيث: حجم وشكل الحروف، والمنحنيات والدوائر، والخطوط والنقاط وغيرها من الصفات[3]، إضافة إلى تحديد

[1]– مشار إليه: سعيد سيد قنديل، المرجع السابق، ص 69. ثروت عبد الحميد، المرجع السابق، ص58.

[2]– ممدوح محمد على مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة بالفقه الإسلامي، دار النهضة العربية، مصر، 2005، ص14.

[3]– إبراهيم أبو الليل الدسوقي، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المتضررة، المجلد الخامس، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الإمارات، 2003، ص 161.

السرعة النسبية التي يجري بها وضع التوقيع، ثم يظهر للمستخدم ثلاثة مفاتيح الأول للموافقة على شكل هذا التوقيع، والثاني لإعادة- المحاولة والثالث لإلغاء التوقيع، وعندما يضغط المستخدم على أيقونة قبول التوقيع يقوم الحاسوب بتجميع جميع البيانات الخاصة بالمستخدم (الموقع) ويدمجها مع شكل التوقيع الموافق عليه ثم يقوم بتشفير جميع هذه البيانات[1] والاحتفاظ بها على نحو يتيح استرجاعها واستخدامها عند الضرورة.[2]

وعند حاجة الشخص لتوثيق التصرف القانوني الذي عزم على القيام به يرجع إلى البرنامج الذي تم حفظ التوقيع به، ولكي تتم عملية التوثيق يطلب الحاسب الآلي من الشخص كتابة توقيعه على الشاشة داخل مربع معين، ثم يقوم البرنامج بإجراء مقارنة بين خصائص التوقيع الموجود على الشاشة وتلك الخصائص المحفوظة على قاعدة البيانات فإذا تمت المطابقة بين خصائص التوقيع يصدر الحاسب الآلي تقريرا بالنتيجة التي تم التوصل إليها.[3]

هناك عقبات ومشاكل تواجه هذا النوع من التوقيع الإلكتروني تحد من انتشاره ومن أهم هذه المشاكل أنه لابن لإتمام التوقيع الإلكتروني من وجود حاسب آلي ذي مواصفات خاصة، كاحتوائه على وحدة القلم الإلكتروني والشاشة الحساسة، وهذا لتمكنه من أداء مهمته في التقاط التوقيع من شاشته، والتحقق من مطابقته للتوقيع المحفوظ بذاكرته[4]، إضافة إلى المشكلة السابقة هناك مشكلة أخرى لم تجد طريقا للحل حتى الآن هي مشكلة إثبات العلاقة بين التوقيع والمحرر، حيث لا توجد هناك تقنية تتيح التأكد من إثبات هذه الرابطة، إذ بإمكان المرسل إليه الاحتفاظ بنسخة من صورة التوقيع التي وصلته على احد المحررات، ثم يعيد وضعها على

---

[1]- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة-دراسة مقارنة-، دار النهضة العربية، مصر، 2006، ص 226.

[2]- تتمثل مهمة التشفير هنا في الحفاظ على أمن وسرية التوقيع وحمايته من محاولات المتطفلين والعابثين، لمزيد من التفاصيل أنظر: لالوش راضية، المرجع السابق، ص45.

[3]- عيسى غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2006، ص 68.

[4]- إبراهيم أبو الليل الدسوقي، المرجع السابق، ص 161.

وثيقة محرر عبر وسيط إلكتروني، ويدعي أن واضعها هو صاحب التوقيع الفعلي، وهو ما يخل بشروط الاعتراف بالحجية للتوقيع في الشكل الإلكتروني لانعدام الثقة والأمان في هذه الطريقة.

ثالثا: التوقيع البيومتري (La signature Biométrique)

تعتبر التكنولوجيا التي تستخدم في توثيق التعاقدات التي تتم عبر الوسائط الإلكترونية متغيرة نحو التطور، وبشكل مستمر، ومن التطورات التكنولوجية المبتكرة" حديثا في هذا المجال تقنية التوقيع البيومتري[1]، حيث يتم هذا التوقيع بواسطة استخدام الخواص الطبيعية والسلوكية والجسدية للشخص، وذلك لتمييزه وتحديد هويته[2]، نظرا لارتباط هذه الخواص الذاتية به، وهو ما يسمح باستخدامها في إقرار التصرفات القانونية التي تبرم عبر وسيط إلكتروني.

تعتمد هذه الصورة من صور التوقيع الإلكتروني على حقيقة علمية، هي أن لكل شخص صفات ذاتية خاصة به تختلف من شخص إلى أخر تتميز بالثبات النسبي، الذي يجعل لها قدر كبير من الحجية في التوثيق والإثبات.

تتعدد الصفات الجسدية أو البيومترية التي يعتمد عليها التوقيع البيومتري أهمها: البصمة الشخصية، بصمة شبكية العين، بصمة الصوت، خواص اليد البشرية، وغير ذلك من طرق أخرى.

تبدأ طريقة تشغيل التوقيع البيومتري بأن يسند لجهة معينة مهمة أخذ صورة دقيقة لصفة ذاتية للشخص الذي يريد استخدام الإمضاء البيومتري، وذلك عن طريق تقنية مخصصة لهذه المهمة، وبعد ذلك يتم حفظ هذه الصور بطريقة مشفرة في ذاكرة الحاسب الآلي، وعندما يدخل

---

[1]– يسمى هذا بعلم البيومترولوجي (biometriologie) الذي يهتم بدراسة الخواص المميزة لكل إنسان، وهناك من يرى إنها طريقة توفر الثقة والأمن للمعاملات الإلكترونية التي تعتمد هذا النوع من التوقيع، أنظر في ذلك: حسن عبد الباسط جميعي، المرجع السابق، ص ص40—41. وثروت عبد الحميد، المرجع السابق، ص ص60—61، وكذا: سعيد السيد قنديل، المرجع السابق، ص ص 70—71.

[2]– إبراهيم أبو الليل الدسوقي، المرجع السابق، ص 159.

الشخص في تعاقدات عبر وسائط إلكترونية، ويراد التحقق من شخصيته فليس على الجهة المختصة إلا التأكيد من مطابقة سماته بالسمات المسجلة والمحفوظة عنه من قبل، وذلك عن طريق استخدام البرنامج الخاص الذي يقوم بإجراء مقارنه بين السمات الذاتية للمتعاقد والتي يلتقطها جهاز الحاسب الآلي وبين السمات المميزة" لنفس الشخص والمخزنة من قبل بقاعدة" بيانات الجهة المختصة، ليخلص البرنامج إلى تحديد ما إذا كانت سمات الشخص المتعاقد مطابقة لسماته المسجلة من قبل فيكون التوقيع صحيحا، أو غير مطابق فيكون التوقيع غير صحيح، أي أنه لا يسمح للمتعاقد باسل إلا في حالة المطابقة الكاملة.[1]

مما لا شك فيه أن ارتباط هذه الخصائص والسمات الذاتية بالإنسان يسمح بتميزه عن غيره بشكل موثوق به، ولذلك يمكن استخدام هذه الطريقة في التوقيع على التصرفات القانونية المبرمة عبر الوسائط الإلكترونية.[2]

يؤخذ على هذا التوقيع أنه بالرغم من الدقة والأمان والثقة المتوافرة فيه، إلا أنه ليس بعيد عن التزوير، فيمكن أن تخضع الذبذبات الحاملة للصوت أو صورة بصمة الإصبع للنسخ وإعادة الاستعمال بالإضافة إلى إمكانية إدخال تعديلات عليها، كذلك الشأن لبصمة العين، فيمكن تزويرها بتقليدها عن طريق بعض أنواع العدسات اللاصقة المصنوعة من رقائق السليكون والتي تحمل نفس اللون والشكل والخصائص المخزنة على الحاسب الآلي، خصوصا إذا أخذنا في الاعتبار سرعة التطور التقني المذهل في عالم الإلكترونيات.[3]

يضاف إلى ما سبق أيضا الخواص أو السمات الجسدية لجسم الإنسان متغيرة مع تقدم السن أو المرض وعوامل أخرى، فقد تمنع الإصابة أو المرض الموقع من إمكانية إجراء مقارنة ومطابقة خواصه وسماته الذاتية التي يلتقطها جهاز الحاسب الآلي، ومن المآخذ الأخرى التي تؤخذ على هذا التوقيع، التكلفة العالية للتقنية التي يتطلبها صنع نظام آمن في شبكات

[1]– سعيد السيد قنديل، المرجع السابق، ص 70.

[2]– حسن عبد الباسط جميعي، المرجع السابق، ص 41.

[3]– سعيد السيد قنديل، المرجع السابق، ص 71.

المعلومات باستخدام السمات البيومترية، مما أدى إلى الحد من انتشار هذا النوع من التوقيع، وجعله قاصرا على بعض الاستخدامات المحدودة.[1]

وفي المقابل يرى جانب من الفقه، أن الخواص الطبيعية المميزة" لكل إنسان تستطيع أن تميزه عن غيره، وبالتالي فإن التوقيع البيومتري يعتبر وسيلة موثوق بها لتمييز الشخصي وتحديد هويته، نظرا لارتباط الخصائص الذاتية به، وهو ما يمكن معه استخدام هذه الوسيلة في إقرار المعاملات الإلكترونية[2]، ورغم قابلية هذه الوسائل للتزوير أو التقليد فإن ذلك لا يجب أن ينال منها، لأن التزوير فيها مهما بلغ لن يصل إلي ما وصل إليه التقليد والتزوير في مجال الكتابة التقليدية والتوقيع التقليدي، فكل ما هو مطلوب في التوقيع أن يعلم نسبته لصاحبه، كما أن كل وسيلة تقوم بوظيفتي التوقيع، من تعيين صاحبه وتبيان انصراف إرادته نهائيا إلى الالتزام بمضمون ما وقع عليه، تعد بمثابة توقيع.

ومع هذا نوافق الرأي الفقهي القائل بأن استخدام هذا النوع من التوقيع الإلكتروني –التوقيع البيومتري– يعتمد في المقام الأول على مدى قدرته على توفير الثقة والأمان القانونيين، وعلى مدى قدرة التقنية المستخدمة على منع الغير من التلاعب به أو نسخه أو تزويره.

ويمكن أن يتحقق ذلك عن طريق تأمينه من خلال التصديق عليه من جهات معتمدة، مرخص لها بممارسة هذا العمل، وتخضع لرقابة الدولة، بحيث تكفل التحقق على نحو دقيق من شخصية الموقع والحفاظ على سرية هذا التوقيع، وحمايته وتوفير وسائل الأمان له مما يضفي عليه مزيدا من الثقة لدى المتعاملين في إبرام التصرفات القانونية عبر الوسائط الإلكترونية، خاصة تلك المعاملات التجارية التي تتم عبر شبكة الاتصال الحديثة (الإنترنت).[3]

---

[1]– يقتصر استخدام التقنية حاليا على بعض البنوك العالمية وعلى أجهزة الأمن والمخابرات كوسيلة التحقق من الشخصية وتحديد الاستخدام المرخص لها. أنظر: لالوش راضية، المرجع السابق، ص 48.

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

[3]– أنظر: سمير حامد عبد العزيز الجمال، المرجع السابق، ص 225. حسن عبد الباسط جميعي، المرجع السابق، ص41.

رابعا: التوقيع بواسطة الماسح الضوئي.

يتم هذا النوع من التوقيع بواسطة استخدام جهاز يطلق عليه (سكانر)، حيث يقوم الشخص عن طريق هذا الجهاز بنقل التوقيع المحرر بخط اليد إلى المستند المراد إرساله ويتم تذييله بالتوقيع ومن ثم إرساله إلى الطرف الآخر عن طريق الوسيط الإلكتروني.

غير أن هذه الطريقة لم تلق رواجا في الاستعمال بسبب ضعف الثقة في قدرتها على تفادي قيام أي شخص بتصوير هذا التوقيع ووضعه على أي مستند غريب عن الموقع نفسه، وبالتالي لا يمكن بواسطتها التحقق على وجه اليقين بوجود صلة قطعية بين التوقيع وصاحبه وما يفيد الالتزام بما هو موقع عليه.

خامسا: التوقيع الرقمي.

يعرف التوقيع الرقمي بأنه: "بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة (كود)، والذي يسمح للمرسل إليه إثبات مصدرها والإستيثاق من سلامة مضمونها، وتأمينها ضد أي تعديل أو تحريف"، وهو صورة أخرى للتوقيع الإلكتروني تستخدم في إبرام التصرفات القانونية عبر الوسائط الإلكترونية[1]، حيث يعتبر الأوسع نطاقا والأكثر استخداما نظرا لطابع الأمان والثقة الذي يوفرهما، لذا حاز على أعراف وثقة العديد من الدول بشكل عام والشركات والبنوك بشكل خاص، ويعتمد هذا التوقيع على نظام التشفير (CRYPTOLOGIE)، لذا يسمي بالتوقيع الرقمي القائم على التشفير.

لا يمكن فهم التوقيع الرقمي دون التطرق إلى التشفير، إذ أن التوقيع بالمفاتيح العمومية والخصوصية يرتكز على وسائل التشفير كآلية تقنية لحماية التوقيع الإلكتروني.

ترتكز طريقة تشغيل منظومة التوقيع الرقمي على فكرة اللوغاريتمات والمعاملات الرياضة المعقدة من الناحية الفنية، وذلك بتحويل المحرر المكتوب والتوقيع الوارد عليه من نمط الكتابة

[1]– يطلق على التوقيع الرقمي بالعربية ويسمى أيضا ب "التوقيع الكودي" بالفرنسية: signature numerique وبالانجليزية: Signature Digital

العادية إلى معادلة رياضية، باستخدام مفاتيح ورموز سوية وطرق حسابية معقدة "لوغاريتمات"، ومؤدي ذلك تحويل المستند الإلكتروني من صورته المقروءة والمفهومة إلى صورة "رسالة رقمية غير مقروءة" وغير مفهومة، ولا يكون بإمكان أي شخص إعادة" هذه المعادلة اللوغاريتمية إلى صورتها المقروءة إلا الشخص الذي لديه المعادلة الخاصة بذلك والتي تتمثل في المفتاح، فالشخص المالك لمفتاح التشفير هو الذي يمكنه فقط فك هذا التشفير.[1]

ويرى البعض أن تشفير البيانات يعني "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها".[2]

وعرفه البعض الآخر بأنه "عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة".[3]

هذا وينقسم التشفير إلى نوعين:

التشفير بالمفتاح المتماثل والتشفير بالمفتاح غير المتماثل –المزدوج–وسوف نتناول هذين النوعين من التشفير على النحو التالي:

1: التشفير بالمفتاح المتماثل.

يسمى أيضا بالنظام السيمتري، ويتمثل هذا النوع من التشفير باستخدام كل من المرسل والمستقبل نفس المفتاح السري للتشفير، فطريقة تشغيل هذا النظام تعتمد على مفتاح واحد يستخدمه المرسل في عملية تشفير بيانات الرسالة –المحرر الإلكتروني– كما يستخدمه المرسل إليه في عملية فك هذا التشفير، حيث يحرر المرسل الرسالة ثم يقوم بتشفيرها بالمفتاح المتماثل،

[1]– حسن عبد الباسط جميعي، المرجع السابق، ص 42. وثروت عبد الحميد، المرجع السابق، ص 62.

[2]– محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2003، ص 180.

[3]– لالوش راضية، المرجع السابق، ص 51.

وذلك بتحويل الرسالة من صورتها المقروءة والمفهومة إلى صور رسالة رقمية غير مقروءة تتخذ أشكال ورموز وعلامات غير مفهومة، ثم يقوم بإرسال الرسالة وكذلك المفتاح المتماثل الذي شفر به بيانات المحرر الإلكتروني إلى المرسل إليه، ليتمكن هذا الأخير من فك شفرة هذه الرسالة وإعادتها إلى حالتها الأصلية.

تتميز هذه الطريقة بالبساطة ومن ثمة بالسرعة والسهولة في إجراء التشفير، حيث لا تحتاج إلى حاسب آلي ذو تقنية متطورة' أو وقت طويل في فك التشفير، ما يعاب عليها هو عملية تبادل المفتاح المتماثل بين المرسل والمرسل إليه، فعملية التبادل تشكل خطورة' على بيانات المحرر الإلكتروني المرسلة، بالتالي عدم توفر الأمان والثقة في هذا النوع من التشفير وهو ما أدى إلى تراجع استخدامه.[1]

هذا ما أوجب اللجوء إلي وسيلة اتصال آمنه يتم من خلالها إبلاغ المرسل إليه مفتاح فك التشفير، لذلك فإن التعامل بالنظام السيمتري–التشفير بالمفتاح المتماثل–مقصور على الأشخاص التي تربطهم علاقة تعارف مسبقة، وأيضا هذا النظام فعال في الشبكات المختلفة، كشبكة الانترانت (RANETINTE) وشبكة (EXTRANET).[2]

2: التشفير بالمفتاح غير المتماثل.

يعتبر نظام التشفير بالمفتاح غير المتماثل أو كما يسمى أيضا بالنظام "Asymetrique" الصورة الحديثة المعمول بها لإجراء التوقيع الرقمي، فهو نظام يعتمد على خلق وإنشاء مفتاحين

[1]– لالوش راضية، المرجع السابق ، ص 52.

[2]– شبكة الانترانت INTERANET: هي عبارة عن سلسلة من شبكات المعلومات يمتلكها مشروع أو مؤسسة واحدة وهذه الشبكات قد تكون شبكات داخلية محدودة النطاق تتصل بعضها البعض داخل نفس المكان أو تكون شبكات واسعة النطاق تتصل يبعضها البعض في أماكن مختلفة ومتعددة.

شبكة الإكسترانت EXTRANET: هي شبكة خاصة مملوكة لمنشأة معينة تلتزم بذات البروتوكولات التي تستخدمها شبكة الانترنت في إجراء عملية الاتصال وتبادل البيانات والمعلومات بين المنشأة وموزعيها أو مورديها أو شركائها أو حتى عملائها بصورة آمنة، إذ أن هذه البيانات تتعلق في غالب الأمر بصفقات وعقود ومعاملات تجارية وعروض وكذلك بيانات سوية تخص العملاء وغير ذلك وقد أمعن من خلال استخدام شبكة الإكسترانت إتمام العديد من صفقات التجارة الإلكترونية، أنظر: المرجع نفسه، ص ص 380—381.

لكل متعامل أحدهما يسمي بالمفتاح الخاص (Clé Privé)، يكون سريا لدى صاحبه لاستخدامه في التشفير والتوقيع الإلكتروني على المحررات الإلكترونية المرسلة، والمفتاح الآخر يسمي المفتاح العام "Clé publique"، وهذا المفتاح يكون معروفا للمرسل إليه بحيث يمكن استخدامه لفك التشفير، وللتحقق من شخصية الموقع علي المحرر الإلكتروني والتأكد من صحة وسلامة المحرر الإلكتروني وبالتالي فالمفتاح العام يتميز عن المفتاح الخاص كونه معروفا ومتاح إلكترونيا لطرفين أو أكثر، غير أن هذا التمييز الذي يخص المفتاح العام لا يفصله عن المفتاح الخاص لأنهما مترابطان في عملهما، ويكمل كل منهما الآخر، وهذا لوجود رابطة مباشرة بينهما، فإذا أستعمل المفتاح الخاص لتشفير الرسالة، فلا يمكن فك التشفير إلا بالمفتاح العام والعكس صحيح[1]، كما أنه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر حسابيا.[2]

فمن يرغب في التعامل إلكترونيا كالتاجر أو البائع مثلا عندما يعرض سلعته من خلال الانترنت في شكل رسالة بيانات، فإنه يتيح لأي شخص مهتم القيام بقراءة رسالة البيانات عبر الانترنت دون أن يتمكن من إجراء أي تعديل عليها لأنه لا يملك المفتاح الخاص بها، وهو المفتاح الخاص بصاحب الرسالة –البائع–، فإذا وافق المشتري عليها فإنه يقوم بالتوقيع عليها إلكترونيا باستخدام مفتاحه الخاص، وتمريرها من خلال برنامج خاص بالتشفير في الحاسب الآلي ليتم تشفيرها، ثم يعيد رسالة البيانات إلى مصدرها مرفقا بها توقيعه في ملف لا يمكن للتاجر إجراء أي تعديل به لأنه لا يملك المفتاح الخاص بصاحب التوقيع.[3]

حتى يتمكن البائع من قراءة الرسالة المرسلة إليه يجب عليه أولا فك شفرتها ولا يتم ذلك إلا عن طريق المفتاح العام لمرسل الرسالة، والذي يقوم بإرساله إلى مستلم الرسالة، وعن طريق

---

[1]– وسيم شفيق الحجار، الإثبات الإلكتروني، المنشورات الحقوقية، الصادرة ببيروت، 2002، ص190.

[2]– إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، جامعة المنصورة، مصر، 2006/2005، ص167.

[3]– ثروت عبد الحميد، المرجع السابق، ص63.

هذا المفتاح العام وباستخدام برنامج التشفير الخاص بالحاسب الآلي يتمكن المرسل إليه – البائع–من فك شفرة الرسالة وتحويلها من صورتها الرقمية إلى صورتها الأصلية المقروءة.

ولا شك أن التوقيع الرقمي على هذا النحو يحقق أعلى درجات الثقة والأمان لدى المتعاقدين به، حيث أنه يضمن تحديد هوية موقعه ويعبر عن إرادته بالارتباط بالتصرف القانوني وقبول مضمونه بصورة' واضحة لا لبس فيها، كما أنه يحافظ على التصرف القانوني بصورته الأولى ويحول دون التعديل أو العبث والتحريف بمحتوياته، فتتوفر فيه بذلك الشروط والضمانات التي يتطلبها المشرع في المحررات لكي تصلح لأن تكون دليلا كاملا في الإثبات.[1]

لضمان الأمان في عملية التشفير الخاصة بالتوقيع الرقمي، وجدت الحاجة إلى طرف ثالث، يكون محل ثقة طرفي العقد والذي يتمثل في هيئة متخصصة يكون لها سلطة توثيق التوقيع الإلكتروني، يتم تسجيل التوقيع الرقمي لديها بناء على طلب العملاء، كما تمنح هذه الجهات شهادات إلكترونية موثقة تفيد بموجبها صحة توقيع العملاء.[2]

اقترح البعض في سبيل تحقيق أقصى درجة من الأمان، أن يمتلك الشخص زوج من المفاتيح الخاصة بدلا من واحد، فإنه في حالة وجود زوج من المفاتيح الخاصة، يقوم الشخص من خلال المفتاح الأول بالتوقيع على الرسالة، ومن خلال المفتاح الثاني يتم تشفيرها، فهذا يحقق أقصى درجات الأمان. أدتا إذا كان الشخص لديه مفتاح خاص واحد يجري كلتا العمليتين به–التوقيع والتشفير–فإنه يسهل توصل شخص ما إلى ذلك المفتاح الخاص، فيتمكن بذلك من تغيير التوقيع وتعديل الرسالة.[3]

[1]– ثروت عبد الحميد، المرجع السابق، ص63.

[2]– لالوش راضية، المرجع السابق، ص55.

[3]– ثروت عبد الحميد، المرجع السابق، ص65.

المبحث الثاني

شروط التوقيع الإلكتروني والتصديق عليه

تتفق جميع التشريعات التي اعترفت بالتوقيع الإلكتروني وأضفت عليه الحجية القانونية في الإثبات، على ضرورة توافر شروط معينة تعزز من هذا التوقيع وتوفر فيه الثقة، حيث يمكن رد هذه الشروط إلى الدور أو الوظيفة التي يؤديها التوقيع، وهي تحديد هوية الموقع الذي يسند إليه الدليل أو المستند والتعبير عن إرادة الموقع في الالتزام بما أوقع عليه، وتعتمد التجارة الإلكترونية في إجراءاتها على شبكة اتصال مفتوحة، كما أن غالبية العقود التي تتم بين أطرافها تعتبر من العقود المبرمة بين غائبين، وذلك بسبب اختلاف زمان ومكان التعاقد، وغياب الحضور المادي للمتعاقدين، مما استلزم وجود طرف ثالث محايد يتمثل في أفراد أو شركات أو جهات مستقلة، تقوم بإصدار شهادات تسمى "شهادات التصديق الإلكتروني" تؤكد فيها صحة هوية وتوقيعات الأطراف المتعاقدة إلكترونيا، تسمى هذه الجهات "بجهات التصديق أو التوثيق الإلكتروني".

ومن خلال هذا المبحث سوف نستعرض شروط التوقيع الإلكتروني (مطلب أول)، والتصديق على التوقيع الإلكتروني (مطلب ثاني).

المطلب الأول

شروط التوقيع الإلكتروني في التشريع الدولي والوطني (الجزائري)

أثار العديد من القوانين تساؤلات حول مدى استيفاء التوقيع الإلكتروني للشروط القانونية التي تمنحه الحجية الكاملة في الإثبات، والإجابة على هذه التساؤلات جاءت من خلال عدة إصدارات لقوانين المعاملات الإلكترونية، التي جاءت بهدف تعزيز الثقة في مدى حجية التوقيع الإلكتروني حتى يؤدي الدور الذي أنشأ من أجله على غرار دور ووظيفة التوقيع التقليدي، ويجعل منه في مستوى واحد معه في الإثبات.

وفي هذا المطلب سوف نتطرق إلى شروط التوقيع الإلكتروني في التشريع الدولي (فرع أول)، وشروط التوقيع الإلكتروني في التشريع الجزائري (فرع ثاني).

الفرع الأول: شروط التوقيع الإلكتروني في التشريع الدولي.

الفرع الحالي، جاء لاستعراض شروط التوقيع الإلكتروني في ضوء مجموعة من القوانين الدولية إذ اشتملت هذه الشروط على ثلاثة عناصر محورية هي: أن يكون التوقيع مميز لصاحبه، سيطر الموقع على التوقيع، وعدم قابلية هذا التوقيع للتعديل أو التغيير.

أولا: أن يكون التوقيع مميزا لصاحبه

يقصد بهذا الشرط أن "يدل التوقيع الموجود علي المحرر الإلكتروني أنه ينسب إلى شخص معين، فحتى يقوم هذا التوقيع بوظيفته بالإثبات يجب أن يكون دالا على شخصية صاحبه ومميزا له عن غير من الأشخاص"[1]، فإذا لم يكن كاشفا عن هوية صاحبه ومحددا لذاتيته فلا يجب الأخذ أو الاعتداد به.

وليس فقط الفقه القانوني هو الذي اشترط هذا الشرط، بل إن غالبية القوانين الدولية والوطنية اشترطت هذا أيضا".[2]

أما في القوانين الدولية، فقد أشار القانون النموذجي الأونسيترال للتجارة الدولية الصادر سنة 1996 بنص المادة (07) منه إلى أنه: «عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

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

[1]– آلاء أحمد محمد الحاج علي، التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، فلسطين، 2013، ص49.

[2]– محمد مأمون سليمان، التحكيم الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2011، ص230.

– كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للفرض الذي أنشأت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر...»[1]

كما ذكر التوجيه الأوروبي رقم 93 لسنة 1999 أن هذا الشرط من بين الشروط الواجب توفرها في التوقيع الإلكتروني، حيث أوضح من خلال الفقرة (02) من المادة (02) هذه الشروط، أين اشترط أن يكون التوقيع الإلكتروني يسمح بتحديد شخصية الموقع.

من خلال استعراض هذه التشريعات الدولية التي تضمنت شروط التوقيع الإلكتروني نلمس شبه اتفاق بين هذه النصوص حول الشروط الواجب توفرها في التوقيع ا لإلكتروني بصفة عامة والشرط المتعلق بضرورة أن يكون هذا التوقيع مميزا لصاحبه بصفة خاصة، فالتوقيع عبارة عن علامة مميزة لشخصية الموقع تحدد هويته وتعرفه تعريفا دقيقا ومميزا.

ثانيا: سيطرة الموقع على التوقيع

من بين الشروط الأساسية للتوقيع الإلكتروني أن يكون هذا التوقيع تحت سيطرة الموقع سيطر كاملة سواء عند إنشائه أو استعماله، بحيث لا يمكن لأحد أن يقلد رموزه إلا الموقع ولإ يستطيع أحد التوقيع بدلا منه، وبالتالي فإن التوقيع الإلكتروني يجب أن يتم عبر وسائل تخضع بشكل كامل للسيطرة المباشرة لصاحب التوقيع.

وحتى تتحقق سيطرة الموقع على التوقيع لابد من إمكانية السيطرة على الوسيط الإلكتروني المتضمن هذا التوقيع، وذلك لضمان أن يكون صاحب التوقيع متفردا به سواء عند التوقيع أو استعماله بأي شكل من الأشكال".[2]

[1]– مصطفى معوان، الإثبات في المعاملات الإلكترونية في التشريعات الدولية: التوقيعات والبصمات الإلكترونية، دار الكتاب الحديث، الجزائر، 2010، ص ص 79–80.

[2]– براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة، 2015، ص155.

وقد أقر هذا الشرط من شروط التوقيع الإلكتروني أيضا القانون النموذجي للأونسيترال بشأن التوقيعات الإلكترونية الصادر سنة 2001 لاسيما المادة (06) الفقرة (03)، والتي جاء فيها: «يعتبر التوقيع الإلكتروني موثوقا به لغرض الوفاء بالاشتراط المشار إليه في الفقرة (01) إذا:

- كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.
- كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف.
- كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف».[1]

بالإضافة إلى ذلك "يجب على صاحب التوقيع الإلكتروني أن يمتلك البيانات الخاصة بإنشاء التوقيع الإلكتروني وأن يكون تحت سيطرته، ويجب عليه المحافظة عليه وأن يحرص على عدم وصوله إلى الغير لكي لا يتم التلاعب به والتحريف من أجل تحقيق مصداقية لتوقيع الإلكتروني".[2]

كما تجدر الإشارة إلى أن "القانون الفرنسي لم يتطرق إلى شروط التوقيع الإلكتروني صراحة، سوى الإشارة إلى أنه إذا كان التوقيع إلكترونيا فيتمثل في استخدام وسيلة آمنة لتحديد هوية الشخص تضمن صلته بالمستند الذي وضع توقيعه عليه، مع سلامة هذا المستند بالشروط التي يحددها مرسوم يصدر من مجلس الدولة....".[3]

ثالثا: عدم قابلية التوقيع الإلكتروني للتعديل أو التغيير

يقصد "بعدم القابلية للتعديل (Irreversible) عدم القدرة على التغيير في بيانات المحرر إلا عن طريق إتلافه أو ترك أثر مادي عليه، والحال كذلك فانه يسهل الكشف عما حدث

[1]– أنظر المادة 3 من قانون الأونيسترال بشأن التوقيعات الإلكترونية 2001، المرجع السابق.

[2]– إبراهيم إسماعيل الربيع، علاء موسى علي نالي، التوثيق الإلكتروني–قرارات التحكيم في التوثيق الإلكتروني–: (دراسة مقارنة)، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد رقم 01، بابل، العراق، 2012، ص163.

[3]– المرجع نفسه، ص161.

للمحرر من تغيير، سواء تم ذلك الكشف بمجرد نظر الشخص العادي أو بالاستعانة بأهل الخبرة".[1]

فعدم القابلية للتعديل أو التغيير أو التبديل في المحرر يعود بنفس المعنى على التوقيع، سواء العادي (التقليدي) أو الإلكتروني.

إذ يلزم لتحقيق الأمان والثقة في التوقيع الإلكتروني أن تتم "كتابة المحرر الإلكتروني والتوقيع عليه باستخدام نظم أو وسائل من شأنها المحافظة على صحة وسلامة المحرر الإلكتروني المشتمل على التوقيع وتضمن سلامته، وتؤدي إلى كشف أي تعديل أو تغيير في بيانات المحرر الإلكتروني الذي تم التوقيع عليه إلكترونيا".[2]

ونظرا لارتباط التوقيع الإلكتروني بالكتابة الإلكترونية، "فهو أيضا يواجه ذات المخاطر التي تحاصر هذه الكتابة، وهي عدم الثقة والأمان لإمكانية التعديل أو التغيير، ونتيجة لهذا فقد أصبح التوقيع الإلكتروني يشترط فيه عدة مواصفات فنية وتقنية عالية، والتي تجعل من الصعب على الغير تزوير أو تعديله أو التلاعب فيه دون أن يترك أثر يكشف به هذا التلاعب، وبذلك أصبح التوقيع الإلكتروني متفوقا على التوقيع التقليدي ذاته في هذا المجال من حيث توفير الأمن والثقة بين أطراف العقود".[3]

وقد نص على هذا الشرط في المادة (06-03-ج) من القانون النموذجي للتوقيع الإلكتروني لسنة 2001، حيث جاء فيها: «إذا كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف»

---

[1]– عابد فايد عبد الفتاح فايد، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني: دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني، دار الجامعة الجديدة، الإسكندرية، 2004، ص65.

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

[3]– محمد مأمون سليمان، المرجع السابق، ص237.

الفرع الثاني: شروط التوقيع الإلكتروني في التشريع الوطني (الجزائري)

يرى المشرع الجزائري أن التوقيع الإلكتروني الموصوف وحده يكون مساوي للتوقيع الكتابي، ومشمولا بالحماية القانونية.[1] والتوقيع الإلكتروني الموصوف هو ذلك التوقيع الإلكتروني الذي تتوفر فيه مجموعة من الشروط التي نص عليها المادة 07 من القانون رقم 15-04 سالف الذكر، وتتمثل هذه الشروط فيما يلي:

1- أن يرتبط بالموقع دون سواه ويحدد هويته:

ألزم المشرع ارتباط التوقيع الإلكتروني بالموقع وحده دون سواه تحقيقا للوظيفة القانونية للتوقيع، وهي تحديد هوية صاحب التوقيع وتمييزه عن غيره من الأشخاص، والتعبير عن إرادته في الالتزام بمضمون المحرر الإلكتروني الذي وقع عليه.[2]

2- أن يكون مصمم بآلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني:

الآلية المؤمنة لإنشاء التوقيع الإلكتروني تتمثل في جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني[3]. والتي تتوفر فيها المتطلبات التالية:[4]

- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.
- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محي من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.
- عدم تعديل البيانات محل التوقيع، وأن تعرض البيانات على الموقع قبل عملية التوقيع.

---

[1]- تنص المادة 8 من القانون 15-04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين على أنه "**يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي**".

[2]- أنظر المادة 7 الفقر 2 و3 من القانون 15-04، المرجع السابق.

[3]- أنظر المادة 2 الفقرة 5، المرجع نفسه.

[4]- أنظر المادة 11، المرجع نفسه.

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

3- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع:

حدد المشرع هذا الشرط حتى يتمتع التوقيع الإلكتروني بالحجية الكاملة في الإثبات بأن يكون للموقع وحده –دون غيره–سيطرة على الوسائل التي أنشأ بواسطتها.[1]

فحيازة الموقع لبيانات إنشاء التوقيع الإلكتروني تجعله مسيطرا عليها كحيازة الموقع لأداة حفظ المفتاح الشفري الخاص متضمنة البطاقة الذكية المؤمنة والكود السري المقترن بها، أما إذا فقد الموقع سيطرته على هذه البيانات أصبحت غير سرية، بحيث يعلمها أشخاص آخرون غير الموقع، فإن التوقيع الإلكتروني لا يعتبر حجة في الإثبات، لأن تحديد شخصية الموقع وهويته بالرجوع إلى هذا التوقيع يكون مشكوكا فيه.[2]

4- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات:

لم يبين المشرع في المادة 07 من قانون 15-04 سالف الذكر الوسائل التي يمكن الكشف من خلالها على التغييرات اللاحقة على بيانات التوقيع الإلكتروني، ولكن يمكن أن أهم وسيلة للكشف بها على التعديلات والتبديلات التي تقع على هذه البيانات في استخدام تقنية شفرة المفاتيح العام والخاص. ولكن يبقى السؤال عن كيفية كشف أي تعديل أو تبديل في بيانات المحرر أو التوقيع؟

هنا يظهر دور جهة التصديق الإلكتروني في المعاملات الإلكترونية، وهي الجهة التي يناط بها تسجيل التوقيع الإلكتروني لديها وتصدر أنماط مختلفة من هذه التوقيعات، وتمنح شهادات

[1]– أنظر المادة 5/7، من القانون 15–04، المرجع السابق.

[2]– محمد نصر محمد، حجية الدليل الإلكتروني أمام القضاء الجنائي والمدني، مكتبة القانون والاقتصاد، الرياض، السعودية، 2013، ص ص 94–95.

تفيد صحة توقيع العميل أو صحة نسبة التوقيع إلى صاحبه، كتوثيق هوية الأشخاص المستخدمين للتوقيع الإلكتروني وتأكيد نسبة المفتاح العام المستخدم إلى صاحبه، وأن الموقع يملك المفتاح الخاص، فضلا من أنها تقوم بإصدار شهادات تصديق إلكتروني تثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.[1]

ونظرا لأهمية شهادة التصديق الإلكتروني فقد جعل المشرع ضرورة استصدارها شرط من شروط التوقيع الإلكتروني الموصوف، وهو ما يعرف بالتصديق الإلكتروني.

المطلب الثاني:

التصديق الإلكتروني

يتطلب استخدام التوقيع الإلكتروني بطريقة آمنة وموثوق بها تدخل شخص ثالث، يسمى (سلطة التصديق) لإعطاء التوقيع الإلكتروني فعاليته الكاملة. فهذه السلطات تصدر شهادات إلكترونية للمصادقة على صحة التوقيع الإلكتروني ومعرفة صاحب التوقيع، ومنع التلاعب به أو بمحتوى البيانات الإلكترونية. وعليه سنبين مفهوم شهادة التصديق الإلكتروني وبياناتها (فرع أول) الجهة المختصة بإصدارها (فرع ثاني)

الفرع الأول: شهادة التصديق الإلكتروني وبياناتها

يتطلب استخدام التوقيع الإلكتروني بطريقة آمنة وموثوقة بها تدخل شخص ثلث، يسمى سلطة التصديق لإعطاء التوقيع الإلكتروني فعاليته الكاملة، فهذه السلطات تصدر شهادة إلكترونية للمصادقة على صحة التوقيع الإلكتروني ومعرفة صاحب التوقيع، ومنع التلاعب به أو بمحتوى البيانات الإلكترونية.

وعليه سوف نتناول تعريف شهادة التصديق الإلكتروني(أولا) وبيانات شهادة التصديق الإلكتروني(ثانيا).

[1]– محمد نصر محمد، المرجع السابق، ص97.

أولا: تعريف شهادة التصديق الإلكتروني

عرف قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 شهادة التصديق الإلكتروني بأنها: «رسالة بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع».

كما عرف التوجيه الأوروبي في المادة (03) شهادة التصديق الإلكتروني بأنها: «تلك التي تربط بين أداة التوقيع وبين شخص معين وتؤكد شخصية الموقع.

وقد عرفها جانب من الفقه بأنها: «الشهادات التي تصدرها جهات التوثيق المرخص لها من قبل الجهات المسؤولة في الدولة لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره، ويستوفي كافة الشروط والضوابط المطلوبة فيه كونه دليل إثبات يعول عليه».[1]

أما على الصعيد العربي، فنذكر التعريف الذي أورده قانون التوقيع الإلكتروني المصري في مادته الأولى الفقر (و)، أن شهادة التصديق الإلكتروني «هي الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع»، و"أحال القانون في شأن البيانات التي يجب أن تشتمل عليها شهادة التصديق الإلكتروني إلى اللائحة التنفيذية للقانون (المادة 20)".[2]

كما ميز المشرع الجزائري بين الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة، وعرف الأولى في المادة 2 فقرة 7 من قانون 15-04 بأنها وثيقة في شكل إلكتروني تثبت الصلة بين بيانات من التوقيع الإلكتروني والموقع. أما الشهادة الثانية فقد عرفها في المادة 15 على أنها هيا شهادة تصديق إلكتروني تتوفر فيها المتطلبات المنصوص عليها في هذه المادة.

---

[1]– حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013، ص104.

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

ونستخلص من خلال هذا التعريف أن شهادة التصديق الإلكتروني تعمل على تأكيد نسبة التوقيع الإلكتروني إلى الشخص الموقع، وتقدم هذه الشهادة من جهة محايدة موثوق بها تؤكد هوية من ينسب إليه التوقيع. وهكذا تنشئ شهادة التصديق الإلكتروني علاقة ثلاثية بين كل من جهة التصديق، والموقع والمرسل إليه.[1]

ثانيا: بيانات شهادة التصديق الإلكتروني

أغلب التشريعات المقارنة أعطت أهمية جد بالغة لشهادة التصديق الإلكتروني خاصة في مجال الإثبات وذلك من حيث تحديد بياناتها بدقة، إذ اشترطت مختلف التشريعات المنظمة للتوقيع والتصديق الإلكتروني بيانات أساسية وأخرى ثانوية.

حيث اشترط المشرع الجزائري أن تتضمن شهادة التصديق الإلكتروني مجموعة من البيانات حتى تكون معتمدة أو كما أطلق عليها تسمية الموصوفة حيث تؤدي وظيفتها في التصديق وبث الأمان والثقة للمتعاملين، وتتمثل هذه البيانات في:[2]

- الإشارة إلى ما يدل أن هذه الشهادة منحت على أساس أنها شهادة تصديق إلكتروني موصوفة.
- مدة صلاحية الشهادة.
- حدود استخدام الشهادة وقيمة المعاملات المالية.
- الرقم التسلسلي للشهادة التصديق الإلكتروني.
- هوية صاحب التوقيع الإلكتروني وصفته.
- بيانات تتعلق بالتحقيق من صحة التوقيع الإلكتروني.
- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي أخر عند الاقتضاء.
- هوية مقدم خدمات التصديق الإلكتروني.

[1]– حجازي عبد الفتاح بيومي، التوقيع الإلكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، 2005، ص295.

[2]– المادة 15/ 3 من القانون 04/15، المرجع السابق.

- التوقيع الإلكتروني الموصوف للجهة المرخص لها إصدار شهادة التصديق الإلكتروني.

الفرع الثاني: الجهة المختصة بإصدار شهادة التوقيع الإلكتروني

حدد المشرع الجزائري الجهة المختصة بإصدار شهادات التصديق الإلكتروني وأطلق عليها تسمية مؤدي خدمات التصديق الإلكتروني[1]. وكذا الشروط التي يجب أن تتوفر فيهم من خلال قانون 15-04المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين.

أولا: تعريف مؤدي خدمات التصديق الإلكتروني

عرف المشرع الجزائري بموجب المادة 02/11 من قانون 15-04 مؤدي خدمات التصديق الإلكتروني على أنه كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني.[2]

وعليه فإن مؤدي خدمات التصديق الإلكتروني هو الشخص المسؤول عن إصدار شهادة تتضمن تحديد هوية الموقع وتثبت صلته بالتوقيع الإلكتروني، إذ يعد بمثابة حلقة وصل في مجال المعاملات القانونية الإلكترونية بين المرسل والمرسل إليه، وقد يكون شخصا طبيعيا أو اعتباريا.[3]

ثانيا: شروط ممارسة نشاط مؤدي خدمات التصديق الإلكتروني

قام المشرع الجزائري بموجب المادة 33 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، بإدراج نشاط التصديق الإلكتروني في المجال الاقتصادي ضمن نظام الترخيص الذي نصت عليه المادة 39 من القانون رقم 2000-03 المؤرخ في 05 أوت 2000 المتعلق بتحديد القواعد العامة المرتبطة بالبريد و المواصلات السلكية و اللاسلكية التي تتم إنشاءها بموجب المادة 10 منه، وذلك باعتبارها كسلطة تصديق فرعية في المجال الاقتصادي تابعة للسلطة الرئيسة على مستوى مرفق المفتاح العمومي الهرمي

---

[1]- أنظر المادة 15/ 1، من القانون 15-04، المرجع السابق.

[2]- جفالي حسين، الحماية الجنائية لتوقيع المستهلك الإلكتروني في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 01، العدد الثالث، الجزائر، د.س.ن، ص267.

[3]- المرجع نفسه، ص267.

في الجزائر، مكلفة بمتابعة ورقابة نشاطات مؤدي خدمات التصديق الإلكتروني المتعلقة بالتوقيع الإلكتروني وبالتالي تمنح هاته السلطة الترخيص، بعد موافقة السلطة الوطنية للتصديق الإلكتروني لأي شخص طبيعي أو معنوي يلتزم باحترام الشروط التي تحددها في مجال إنشاء و استغلال خدمات التصديق الإلكتروني، لذا عرفت المادة 02/10 من القانون 504-1الترخيص على أنه نظام استغلال خدمات التصديق الإلكتروني و الذي يتجسد في وثيقة رسمية ممنوحة لمؤدي الخدمات بطريقة شخصية، تسمح له بالبدء الفعلي في توفير خدماته.[1]

كما ألزم المشرع طالب الترخيص بموجب المادة 34 من نفس القانون بمجموعة من الشروط الفنية والتقنية، كأن يكون خاضع للقانون الجزائري في حالة ما إذا كان شخص معنوي أو يتمتع بالجنسية الجزائرية إذا كان شخص طبيعي، والتمتع بقدرة مالية كافية وبمؤهلات وخبرة ثابتة في ميدان تكنولوجيا الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي، وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاطه.[2]

[1]- جفالي حسين، المرجع السابق، ص267.

[2]- المادة 34 من القانون 15-04، المرجع السابق.

الفصل الثاني

الحماية الجنائية المقررة للجرائم المرتبطة بالتوقيع الإلكتروني

إن بيئة المعاملات الإلكترونية وعلى الرغم من الإيجابيات التي حملتها وساهمت في تطور هذه المعاملات، لا تخلو من بعض السلبيات التي قد تقوض جهود الأطراف المعنية وتحول دون خلق بيئة آمنة وموثوقة لكافة المتعاملين، خاصة مع تنامي ظواهر مثل القرصنة والتزوير الإلكتروني وهو ما استدعى تدخل المشرعين لسن القوانين الكفيلة بوضع آليات ووسائل الحماية الجنائية للتوقيع الإلكتروني.

من هذه المنطلقات، يتناول الفصل الحالي أهم الجرائم الواقعة على التوقيع والتصديق الإلكترونيين ووسائل الحماية الجنائية المعتمدة في التشريع الجزائري في هذا الإطار.

وقد تم تقسيمه إلى مبحثين سنستعرض في (المبحث الأول) الجرائم المرتبطة بالتوقيع الإلكتروني، وفي (المبحث الثاني) الحماية الجنائية لجرائم التوقيع الإلكتروني في ظل التشريع الجزائري.

المبحث الأول

الجرائم المرتبطة بالتوقيع الإلكتروني

يأخذ موضوع الحماية الجنائية للتوقيع الإلكتروني جانبا هاما ضمن الدراسات القانونية الجنائية الحديثة، وذلك بسبب المشاكل التي بات يثيرها اختراق نظم المعلومات، وتهديد عنصر الأمان بخصوص المعاملة الإلكتروني ضمن فضاءات الإنترنت، خاصة وأن أغلب البنوك تتعامل إلكترونيا مما يتطلب تزويدها بأساليب الحماية الأزمة، ومنها الحماية الجنائية منعا من الإضرار بمصالحها والتأثير على وضعها المالي.

سوف نستعرض في هذا المبحث الجرائم الماسة ببعض المصالح (مطلب أول) والجرائم الواقعة على التوقيع الإلكتروني (مطلب ثاني).

المطلب الأول

جرائم ماسة ببعض المصالح

إن المشرع عند تدخله لحماية التوقيع الإلكتروني يواجه في ذلك جملة من الجرائم وأنماط الغش والتحايل، وهو في نفس الوقت يستهدف حماية العديد من المصالح.

ومن جملة المصالح التي يستهدف المشرع حمايتها بخصوص التوقيع الإلكتروني والتي سوف نتطرق إليها من خلال مطلبنا هذا حيث تنقسم إلى: شرعية تداول البيانات وخصوصيتها (فرع أول) والتعامل الإلكتروني" من الغش والتحايل «وحماية الثقة في التوقيع الإلكتروني (فرع ثالث).

الفرع الأول: تداول البيانات وخصوصيتها

الفرع الحالي، سنتناول فيه بعض المصالح التي يسعى المشرع لحمايتها، (أولا) شرعية تداول البيانات، (ثانيا) سرية البيانات وخصوصيتها.

أولا: شرعية تداول البيانات

تداول البيانات الإلكترونية، يقصد بذلك أن يتم تداول البيانات الإلكترونية بشكل مشروع، وأن يتم التداول لمن له حق التداول والاستخدام. ويشترط بأن يتم التداول عن طريق مزود الخدمة الإلكترونية المصرح له بذلك.

وقد عبر القانون النموذجي للتجارة الإلكترونية عن ذلك بنص المادة 2/ب[1] وقد جرم المشرع التونسي في المادة 46 من قانون التجارة الإلكترونية التعامل في البيانات بدون ترخيص.

ويشترط أن يتم تداول البيانات عن طريق مزود الخدمة الإلكترونية المصرح له بذلك. وهذا التداول يتم سواء في عملية التعاملات المصرفية أو العقود الإلكترونية أو التجارة

[1]– قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996، متوفر عبر الموقع: http//www.uncitral.org/pdf/arabic…

الإلكترونية[1]. ويتم تبادل المعلومات عن طريق شبكة الانترنت أو الاكسترانت.

2-سرية البيانات وخصوصيتها

التعامل بالتعاقد الإلكتروني يقتضي الأمان في المعاملات الإلكترونية، إذ أن أكبر المخاطر التي يكون عرضة لها هو عدم الأمان الذي يعد أكبر المخاطر التي يتخوف منها أغلب العملاء، لذلك تتجه أغلب البنوك إلى نظام التشفير من خلال حيازة العميل لرقم مشفر لا يعرفه إلا العميل للجد من التحايل الإلكتروني.[2]

وذلك يتطلب الاعتراف للمستهلك بحقه في سرية البيانات والمعلومات وتجريم الاعتداء عليها، ولذلك فإن كل اعتداء على البيانات المرسلة بين ظرفي العقد عبر فضاءات الانترنت يشكل اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بينهما، على اعتبار أن تلك البيانات تتمتع بالسرية والخصوصية وتعبر عن إرادة طرفي العقد بالقيام بتصرف قانوني. وبالتالي فإن الاطلاع على هذه البيانات أو المعلومات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة وانتهاك خصوصيتهما عن طريق فك التشفير.[3]

وقد نص مشروع قانون التجارة الإلكترونية المصري على ضرورة احترام الحق في سرية البيانات الخاصة بالعملاء واحترام الحق في الخصوصية. فأهم المخاطر التي تتعرض لها الشبكة هو عدم الأمان security وهي أعلى الأسباب التي يتخوف منها العميل بنسبة 53% بالمقارنة ببقية الأسباب الأخرى -ثم يأتي عامل صعوبة التجول عبر الشبكة بنسبة 35%- ثم عدم وجود اختيارات كافية بنسبة 27%- ثم عدم الثقة no trust بنسبة 24%- ثم ارتفاع الأسعار بنسبة 20%.[4]

---

[1]- هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، د. س. ن، ص580.

[2]- طيب موفق شريف، التوقيع الإلكتروني وحمايته جنائيا في القانون الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد01، العدد01، جامعة أحمد دراية، أدرار-الجزائر، 2017، ص83.

[3]- المرجع نفسه، ص83.

[4]- هدى حامد قشقوش، المرجع السابق، ص ص 580-581.

لذلك وضعت البنوك بالتعاون مع منظمتي الفيزا والماستر كارد نظام إلكتروني يتسم بحماية عالمية عن طريق رقم مشفر لا يعرفه إلا العميل وذلك للحد من التحايل الإلكتروني.

الفرع الثاني: التعامل الإلكتروني (الحماية من الغش والتحايل)

من أبرز المصالح التي يستهدف المشرع حمايتها جنائيا بخصوص التوقيع الإلكتروني حماية المتعاملة من الغش والتحايل، سعيا إلى إحاطة المستهلك إلكترونيا بكافة الشروط الجوهرية للمعاملة قبل الإقدام على توقيعها إلكترونيا.[1]

وهي من أهم المصالح التي يحميها القانون في المعاملات الإلكترونية ليكون المستهلك المعلوماتي على علم تام بكافة الشروط الجوهرية للمعاملة قبل توقيعه إلكترونياً وهذا ما اهتم به مشروع قانون التجارة الإلكترونية المصري وأفرد الباب السابع لحماية المستهلك من التحايل.

وقد نص القانون التونسي[2] في الباب الخامس منه على حق المستهلك في الحماية الضرورية بتوفير البيانات الجوهرية للبائع وتحديد شروط التعاقد والسحب والدفع الإلكتروني.

الفرع الثالث: حماية الثقة في التوقيع الإلكتروني

يعتبر عامل الثقة عنصرا ضروريا للإقدام على التعامل الإلكتروني، والتوقيع الإلكتروني له نفس حجية التوقيع العادي بما يبعث على الارتياح والثقة والأمان في نفس المتعامل.

وهي من أهم المصالح محل الحماية الجنائية في نطاق جرائم المعلوماتية، وقد اهتم المشرع الفرنسي بالتوقيع الإلكتروني ونص على مساواته في الحجية مع التوقيع التقليدي[3]. وذلك في نص المادة 1/1316، وأعقب هذا النص نص المادة 3/1316 والتي قررت أن الكتابة على محتوى إلكتروني لها نفس القوة في الإثبات كالكتابة على محتوى ورقي، وقد

---

[1]– طيب موفق شريف، المرجع السابق، ص83.

[2]– قانون عدد 83، مؤرخ في 09 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية التونسي، المنشور بالرائد الرسمي للجمهورية التونسية، بتاريخ 11 أوت 2000.

[3]– هدى حامد قشقوش، المرجع السابق، ص581.

حسم بذلك جدلاً فقهياً استمر لسنوات لم يحسم بعد في مصر.

المطلب الثاني

جرائم مستحدثة واقعة على التوقيع الإلكتروني

التوقيع الإلكتروني وانطلاقا من أنه مجموعة من البيانات في شكل إلكتروني، فإنه توجد خطورة الاعتداء عليه بجرائم تأخذ أشكالا وصور متعددة، ونظر لهذه الخطورة وضعت مختلف التشريعات الدولية والوطنية وسائل حماية جنائية للتوقيع الإلكتروني، وعلى هذا الأساس سوف نستعرض في هذا المطلب مختلف الجرائم المستحدثة الواقعة على التوقيع الإلكتروني، جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني (فرع أول)، جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية (فرع ثاني)، جريمة التزوير المعلوماتي (فرع ثالث)، وجريمة إتلاف وتعييب التوقيع الإلكتروني (فرع رابع).

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

عند تناول هذه الجريمة، لابد من التفرقة بين الدخول والبقاء غير المصرح به، فالأول يتحقق باختراق نظم معلومات التوقيع الإلكتروني، أما البقاء فقد يترتب على الدخول غير المصرح به أو أن يكون الدخول قد تم بشكل قانوني مصرح به إلا أن القائم بالدخول استمر داخل النظام متجاوزا الحد المسموح به للبقاء داخله فأصبح بذلك مرتكبا لجريمة رغم أن الدخول في بداية الأمر كان مشروعا.[1]

أولا-الركن المادي للجريمة

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص137.

به[1]، ودائما ما يثار التساؤل بشأن هذا الفعل وكيف يمكن تحديد ما إذا كان الفعل الذي ارتكبه الجاني هو ذاته الفعل المؤثم قانونا.[2]

1- فعل الدخول:

لم تحدد التشريعات المقارنة المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات ويتمكن تعريفه بأنه الدخول إلى المعطيات المخزنة داخل نظام الحاسوب دون رضا المسؤول عن هذا النظام.[3]

"لقد رصد الفقه الإنجليزي مشكلة بشأن تحديد معنى الدخول في القانون حيث تطلب هذا التحديد التمييز بين المشروعية وعدم المشروعية في فعل الدخول، حيث انتهى القانون الإنجليزي لتقرير ضرورة أن يكون الدخول غير مصرح به تطبيقا للمادة (05) من القسم (17) وكذا بين الدخول المباشر من الحاسب الذي يحوي البيانات ومنها بيانات التوقيع الإلكتروني والدخول عن بعد".[4]

وفكرة الدخول وفقا للتشريع الأمريكي تتمثل في مجرد فعل الدخول دون تطلب تحقق الضرر وعلى ذلك فإن الدخول غير المصرح به يتضمن عنصرين هامين هما: عنصر المكان، والذي يتمثل في الدخول إلى النظام أو المرور بداخله، والثاني عنصر الزمان وهو الزمان الذي يستغرقه التواجد داخل نظام المعلومات.[5]

وهذا معناه أن الفقه القانوني يشهد اختلافات حول تحديد طبيعة الفعل المجرم قانونا نتيجة فعل الدخول إلى نظام معلومات التوقيع الإلكتروني، بين مشروعية الفعل في حد ذاته ثم تجاوز هذه المشروعية إلى فعل مجرم قانونا يتمثل إما في دخول مشروع نظام المعلومات

---

[1]– صالح شنين، الحماية الجنائية للتجارة الإلكترونية –دراسة مقارنة–، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان، 2013، ص74.

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

[3]– صالح شنين، المرجع السابق، ص69.

[4]– حسام محمد نبيل الشنراقي، المرجع السابق، ص143.

[5]– المرجع نفسه، ص145.

في بداية الأمر، لكن الاستمرار فيه وتجاوز المدة | المحددة يجعل منه فعلا مجرما.

وجاء في اتفاقية بودابست (المادة 02) أن: «على كل طرف تبني التدابير التشريعية وغيرها من التدابير حيثما كان ذلك لازما لاعتبار الدخول إلى كل أو جزء من نظام حاسب دون وجه حق جريمة طبقا لقانونه الداخلي إذا ما ارتكب عمدا".[1]

وقد يتطلب الطرف الموقع أن يكون الفعل المقترف قد تم بمخالفة تدابير الأمن، وذلك بنية الحصول على بيانات حاسب أو لغاية أخرى غير شريفة أو أن تكون اقترفت نظرا للصلة بنظام حاسب آخر.[2]

أما المشرع الأمريكي فقد قرر في قانون تزييف آليات الدخول والإساءة والاحتيال عبر، الحاسب الآلي اعتبار كل دخول غير مصرح به المعلومات في حاسب آلي جناية، أما إذا كان الدخول قاصدا المعلومات مالية أو الثمانية أو انتهاك حرمة حاسب فدرالي فإن الجريمة تعد جنحة، وقد تم تعديل القانون الأمريكي في القسم (1030) عدة مرات وتناول تعليل 1996الأفعال التي تعد أشكال الاختراق من خلال حاسب مستخدم في مؤسسة مالية أو حكومة أو مؤسسة اقتصادية أو الاتصالات في الولايات المتحدة أو خارجها.[3]

ومن بين هذه الأشكال التوصل للدخول بشكل غير مشروع إلى حاسب حكومي، ومن ثم يكشف معلومات يفترض بقاؤها سرية سواء قام المخترق بإنشاء هذه المعلومات لمن لا يملك صلاحية استلامها أو حيازتها.[4]

إذ أدان القضاء الأمريكي أحد الأشخاص بتهمة الدخول غير المشروع إلى سجلات المحاكم الاتحادية وهي تحتوي على سجلات إلكترونية خاصة، تضم أحكاما وقررت ومستندات خاصة بدعاوى عرضت على المحكمة أو صدر فيها قرار...، حيث أن نظام

[1]– براهمي حنان، المرجع السابق، ص46.

[2]– المرجع نفسه، ص46.

[3]– حسام محمد نبيل الشنراقي، المرجع السابق، ص 144.

[4]– المرجع نفسه، ص144.

حفظ هذه المعلومات مفتوح للجمهور، إلا أن حق النسخ أو الإنزال مقيد بسداد مقابل نقدي، لكن الجاني تمكن من نسخ الملايين من الصفحات باستخدام برنامج خاص لوضع ملفات إلكترونية خفية في النظام حتى لا يتم احتساب نفقات النسخ.[1]

ويلاحظ في هذا الإطار أن المشرع التونسي استعمل عبارة النفاذ عوضا عن عبارة الدخول، ليؤكد الخاصية المادية لهذه الجريمة، فعبارة الدخول قد يكون لها مدلول مادي في حين أن النفاذ له محلول الحماية، أو عن طريق إدخال برنامج فيروس أو باستخدام الرقم الكودي لشخص آخر أو تجاوز نظام الحماية إذا كان ضعيفا، ويستوي أن يتم الدخول مباشرة أو بطريقة غير مباشرة كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلفونية.[2]

2-عدم التصريح بالدخول:

نصت المادة 23 من القانون 15 لسنة 2004 على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته».[3]

على هذا الأساس نجد أن المشرع المصري يرى أن فعل الدخول لنظام معاملات التوقيع الإلكتروني يستمد عدم مشروعيته من حدوثه دون التصريح به، ومعيار عدم المشروعية هو انعدام سلطة الفاعل في الدخول للنظام مع العلم بذلك، وعلى ذلك يعد من الحالات التي بعد الدخول فيها غير مصرح به وهي:

أ -إذا كان دخول الفاعل للنظام المعلوماتي للتوقيع الإلكتروني دون تصريح من المسؤول عنه.

---

[1]- براهمي حنان، المرجع السابق، ص48.

[2]- صالح شنين، المرجع السابق، ص74.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص151

ب –إذا كان دخول الفاعل لأماكن من النظام لم يصرح له بدخولها".[1]

أما التشريع الأمريكي ووفقا للقانون الفدرالي المتعلق بالاعتداء على الحاسوب لسنة 1996، نجد أن الفصل 1030 تضمن نصوصا خاصة تجرم الاعتداء على الحاسوب، حيث يجرم المشرع الدخول العمدي على البيانات الموجودة بأجهزة الكومبيوتر بدون تصريح أو يتجاوز التصريح الممنوح له أيا كانت الوسيلة المستخدمة والحصول على معلومات سرية،...".[2]

وتلخيصا لما ورد حول جريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني فإنه "لقيام هذه الجريمة لابد وأن الركن المادي المتمثل في الدخول غير المشروع قد وقع على أنظمة معلوماتية أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني".[3]

كما أن هذه الجريمة تصنف من جرائم الخطر، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه".[4]

ثانيا–الركن المعنوي:

إن جريمة الدخول غير المصرح به في نظم معلومات التوقيع الإلكتروني من الجرائم العمدية التي يتمثل الركن المعنوي فيها في القصد الجنائي العام بركنيه العلم والإرادة، ولا تتطلب قصدا جنائيا خاصا وذلك لكونها من جرائم الخطر التي يعاقب المشرع فيها على مجرد إتيان الفعل المجرم، وعلى ذلك يعاقب المشرع بعقوبة الجريمة التامة على إتيان الفعل المادي مع توافر القصد الجنائي دون اشترط تحقق النتيجة المتوخاة من الجريمة ".[5]

---

[1]– حسام محمد نبيل الشنراقي، المرجع السابق، ص151.

[2]– صالح شنين، المرجع السابق، ص165.

[3]– عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، 2004، ص302.

[4]– حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدراسات والبحوث، سلطنة عمان، 2006، ص18.

[5]– حسام محمد نبيل الشنراقي، المرجع السابق، ص167.

وانطلاقا من أن الركن المعنوي لجريمة الدخول غير المصرح به القاعدة بيانات تتعلق بالتوقيع الإلكتروني يتخذ صودر القصد الجنائي، وعليه فإن معظم التشريعات التي جرمت هذا الدخول غير المصرح به قد تطلبت القصد العام، إلا أن بعض التشريعات تطلبت قصدا خاصا في الجريمة.[1]

1- القصد الجنائي العام:

"عبر القانون الفرنسي عن القصد العام المتطلب في جرائم الدخول والبقاء غير المصرح به بتطلبه أن يكون الدخول لنظام المعلومات قد تم بطريقة الغش أو الخداع، وهذا المصطلح يعني أن مرتكب الدخول يعلم بكون دخوله النظام المعلومات غير مصرح به.[2]

أما القانون الأمريكي فقد تطلب فقط أن يكون الدخول دون تصريح، وتطلب القانون الإنجليزي أن يكون الدخول للنظام على نحو غير مصرح به مع العلم بذلك.[3]

في حين لم يتطلب المشرع المصري في القانون رقم 15 لسنة 2004 قصدا في جريمة الدخول غير المشروع داخل النظام المعلوماتي للتوقيع الإلكتروني، ومن ثم فإن القواعد العامة بشأن القصد الجنائي تسرب على هذه الجريمة.[4]

من هذه المنطلقات، تستخلص أن القصد العام في جريمة الدخول غير المشروع القاعدة بيانات تتعلق بالتوقيع الإلكتروني يتطلب أن يكون مرتكب هذا الدخول على علم بما يرتكبه، وأن أفعاله هذه مخالفة للقانون وتمثل جريمة، وأن ذلك سوف يعرضه لعقوبة ينص عليها القانون جزاء دخوله غير المشروع.

2- القصد الجنائي الخاص:

هذا القصد لم تتطلبه التشريعات بوجه عام مثلما تمت الإشارة إلى ذلك سابقا، غير أن

---

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص169.

[2]- المرجع نفسه، ص169.

[3]- المرجع نفسه، ص170.

[4]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص569.

بعض التشريعات تطلبته بجوار القصد العام.

مثلا نجد أنه في القانون النرويجي تشدد العقوبة إذا ارتكب فعل الدخول غير المصرح به بنية الحصول للفاعل أو لغيره على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الاطلاع على المعلومات التي يحوزها النظام.

وفي المملكة المتحدة تضمن قانون إساءة استخدام الحاسبات الآلية في المادة (02) منه تجريم الدخول غير المصرح به متى توافر للفاعل قصد خاص هو نية ارتكاب جريمة لاحقة على هذا الدخول كالسرقة أو النصب أو غيرها.[1]

ثالثا-عقوبة الجريمة:

جاءت عقوبة جريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني مختلفة من تشريع لآخر، بناء على توصيف كل تشريع لهذه الجريمة من ناحية الضرر الممكن أن تلحقه سواء بالمعلومات التي تتضمنها قاعدة البيانات، أو بشخص صاحب هذه البيانات.

فقد جاء في القانون العربي النموذجي الموحد لمكافحة جرائم إساءة استعمال أنظمة تقنية المعلومات على: «أن كل من توصل بطريق غير مشروع لاختراق نظام المعالجة الآلية للبيانات، يعاقب بالحبس والغرامة (تترك لتقدير كل دولة)، وإذا نتج عن هذا الفعل محو أو تعديل البيانات المخزنة بالحاسب الآلي أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غير من الأساليب المعلوماتية، تكون عقوبته الحبس الذي لا تزيد مدته (تترك لتقدير كل دولة) والغرامة (تترك لتقدير كل دولة) ...[2]

كما تضيف المادة نفسها: إذا ضبط الشخص داخل نظام المعالجة الآلية للبيانات دون وجه حق يعاقب بالحبس والغرامة (تترك لتقدير كل دولة)، وإذا ترتب على الفعل انتهاك

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص ص173-174.

[2]- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، المرجع السابق، ص 325.

لسرية البيانات المخزنة بالحاسب يعاقب بالحبس الذي لا تقل مدته عن (تترك لتقدير كل دولة)، والغرامة (تترك لتقدير كل دولة)».[1]

أما في التشريع الفرنسي، فقد جاءت عقوبة هذه الجريمة في قانون العقوبات المادة (323/1:7) من القانون الجديد الباب الثالث القسم الثاني، وهي التي كان منصوصا عليها في المادة (462/2:9) من القانون الفرنسي القديم.

حيث نصت هذه المادة على: «عقاب الدخول أو البقاء بطريقة ما كليا أو جزئيا داخل نظام لمعالجة المعلومات، يعاقب بالحبس الذي لا يقل عن شهرين والغرامة التي لا تزيد عن خمسين ألف يورو أو بإحدى العقوبتين، وإذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل في المعطيات المخزنة في النظام سواء بالإتلاف أو غير تكون العقوبة الحبس الذي لا يقل عن شهرين ولا يزيد عن سنتين، والغرامة التي لا تقل عن عشرة آلاف يورو ولا تزيد عن مائة ألف يورو».[2]

من خلال ما سبق نستخلص أن مختلف التشريعات تعتبر الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني جريمة يعاقب عليها القانون كونها تشتمل على فعل الدخول غير المرخص لشخص الجاني، وبقائه في نظام المعلومات بشكل غير مشروع من جهة، وقد يحصل وأن ينتج عن هذا الدخول غير المشروع إلى إتلاف بيانات نظام المعلومات أو تحريفها أو سرقتها، مما يتسبب إما في تعطيل هذا النظام عن تأدية وظائفه، أو في إلحاق ضرر بصاحب هذه البيانات سواء كان شخصا طبيعيا أو معنويا.

الفرع الثاني: الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية

بعد الوقوف على جريمة الدخول غير المشروع القاعدة بيانات تتعلق بالتوقيع الإلكتروني، هناك جريمة أخرى لا تقل خطورة عن هذه الأخيرة متمثلة في الحصول على

[1]– عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، المرجع السابق، ص 325.

[2]– حسام محمد نبيل الشنراقي، المرجع السابق، ص175.

التوقيع الإلكتروني بطرق الاحتيال.

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

أولا-تعريف الاحتيال التقليدي والإلكتروني

1. الاحتيال التقليدي:

يعرف الاحتيال على أنه: «الاستيلاء على مال مملوك للغير بخداعه وحمله على تسليم ذلك المال».[2]

ويرى البعض أن مصطلح الاحتيال يمكن تعريفه على أنه: «الاستيلاء بطريق الاحتيال على شيء مملوك للغير بنية تملكه، ولذلك يستعمل الجاني أساليب احتيالية قصد الاستيلاء على مال الغير».[3]

والمشرع المصري لم يعرف الاحتيال في القانون، وإنما الذي عرفه هو الفقه حيث ذهب بعض الفقه إلى أنه: «كل سلوك ينطوي على خداع المجني عليه بفرض الاستيلاء على أمواله، وهو ما سيفترض إتيان الجاني أسلوبا من أساليب الاحتيال ويعد وفقا لهذا التعريف إحدى عناصر الركن المادي لجريمة النصب».[4]

والمشرع الأردني لم يورد تعريفا للاحتيال، فعرفه الفقه على أنه «استيلاء على مال مملوك للغير باستعمال وسائل الخداع التي تؤدي إلى إيقاع المجني عليه في الغلط فيقوم

---

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص179.

[2]- محمد هشام صالح عبد الفتاح، جريمة الاحتيال -دراسة مقارنة-، رسالة الماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، نابلس، فلسطين، 2008، ص08.

[3]- براهمي حنان، المرجع السابق، ص57.

[4]- حسام محمد نبيل الشنراقي، المرجع السابق، ص182.

بتسليم المال الذي في حيازته».

ويعرف الاحتيال أيضا بأنه: «توصل الشخص إلى تسليم أو نقل حيازة مال منقول مملوك للغير إلى حيازته أو حيازة شخص آخر، وذلك باستعمال طرق احتيالية أو باتخاذ اسم كاذب أو حمل اسم آخر على تسليم أو نقل أو حيازة سند موجود لدين أو إبراء».[1]

2. الاحتيال الإلكتروني (المعلوماتي):

نصت المذكرة التفسيرية للاتفاقية الأوروبية لمكافحة جرائم المعلومات الموقعة في بودابست عام 2001 في المادة (8 ف/ب) على أن: «التلاعب في المكونات المادية للحاسب والتلاعبات المعلوماتية الاحتيالية تكون مجرمة إذا سببت ضرر اقتصاديا أو ماديا للغير، أو أن يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، ومصطلح الضرر يشمل النقود والأشياء غير المادية».[2]

وعرف مكتب التحقيقات الفدرالي الأمريكي الاحتيال عبر الانترنيت بأنه: «أي مخطط احتيالي عبر الانترنيت، يلعب دورا هاما في عرض السلع أو الخدمات غير الموجودة أصلا أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة العنكبوتية»؛ أما وزارة العدل الأمريكية فعرفته بأنه: «شكل من التخطيط الاحتيالي الذي يستخدم محتويات الانترنيت مثل الدردشة والبريد الإلكتروني والمواقع الإلكترونية لتقديم صفقات احتيالية أو لإرسال نتائج الاحتيال إلى المؤسسات المالية».[3]

كما عرف الاحتيال المعلوماتي بأنه «التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناء على هذه الأوامر أو التعليمات،

[1]– محمد هشام صالح عبد الفتاح، المرجع السابق، ص08.

[2]– حسام محمد نبيل الشنراقي، المرجع السابق، ص186.

[3]– المرجع نفسه، ص186.

من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير».[1]

وذهب البعض إلى أن الاحتيال في نطاق المعلومات، هو «حث الحاسب الآلي على تغيير الحقائق بأي وسيلة كانت بهدف الحصول على ربح غير مشروع على حساب شخص آخر، وتتمثل وظيفة الحاسب الآلي في مساعدة الجاني على إتمام فعل الاحتيال، وذهب بعض الفقه إلى أنه الاستعمال غير المصرح به لنظام الحاسب الآلي بنية الحصول على ممتلكات أو خدمات عن طريق الاحتيال».[2]

ثانيا-الركن المادي:

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

ولدراسة أعمق للركن المادي في جرائم الاحتيال على نظم معلومات التوقيع الإلكتروني، لابد من توضيح مسألة الأفعال التي يجرمها القانون، وهي استخدام الوسائل الاحتيالية لخداع المجني عليه، وهو هنا إما يكون المسؤول عن نظام معلومات التوقيع الإلكتروني أو الحاسب الآلي.

1. الوسائل الاحتيالية:

هناك خلاف فقهي بشأن تطبيق النص التقليدي للاحتيال على الاحتيال في مجال المعلومات ومدى إمكانية تصور الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط، انطلاقا من أن السائد قانونا وفقها أن السلوك الاحتيالي ينبغي أن يقع على شخص طبيعي.

---

[1]- براهمي حنان، المرجع السابق، ص ص57-58.

[2]- حسام محمد نبيل الشنراقي، المرجع السابق، ص184.

[3]- براهمي حنان، المرجع السابق، ص58.

وعلى أساس هذا الخلاف الفقهي، تنوعت الوسائل الاحتيالية المستخدمة من قبل مرتكبي الجرائم المعلوماتية بتطور استخدامات الحواسيب، وتضمنت الوسائل الاحتيالية في جريمة النصب التقليدية عدة وسائل اشترط المشرع توافرها لكي يبلغ الجرم المرتكب مبلغ الاحتيال وهي:

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

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

ويتجه الفقه الفرنسي إلى أن "غش وخداع نظم المعلومات والحاسبات لسلب المال تتحقق به الطرق الاحتيالية وفقا لنص المادة 405 عقوبات، حيث تتوافر فيه بالإضافة للكذب مظهر خارجي وهو إبراز المحررات أو المعلومات المدخلة للحاسب ونظام معلوماته.[2]

كما يمكن أن تقع جريمة الاحتيال في بيئة التوقيع الإلكتروني "باتخاذ اسم كاذب أو صفة غير صحيحة ومن ذلك الدخول إلى نظام معلومات التوقيع الإلكتروني باستخدام أسماء وشفرات مستخدميه الشرعيين بقصد الاستيلاء على التوقيعات، ومن ثم الأموال".[3]

2-تسليم معلومات التوقيع الإلكتروني (النتيجة الجرمية)

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

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص190.

[2]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص19.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص184.

المادي أو أثره.[1]

والأخذ بهذا الطرح يجعل من الاحتيال في مجال المعلومات لا يختلف عن الاحتيال التقليدي، حيث أن جوهر التسليم أن يكون المجني عليه اتجه بإرادته نحو وضع شيء مملوك له في متناول الجاني الذي اعتمد على الوسائل الاحتيالية للحصول على هذا الشيء.

3-العلاقة السببية بين طرق الاحتيال وتسليم المعلومات:

"لا يكفي لقيام جريمة الاحتيال التامة أن يصدر من الجاني فعل الاحتيال، وأن يسلم المجني عليه الشيء المملوك له إلى هذا الجاني، بل يلزم أن تتوفر صلة ما بين فعل الاحتيال وتسليم الشيء المملوك وأن يكون الثاني ثمرة أو نتيجة للأول"[2]، بمعنى لابد من توافر علاقة سببية ما بين فعل الاحتيال وفعل التسليم.

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

كذلك ليتمكن من الاستيلاء على معلومات ذات قيمة مادية بدون حق، فالوسائل الاحتمالية التي قام بها الجاني تربط بينها وتسليم المعلومات (المال) الذي حصل عليه علاقة سببية، فلولا هذه الوسائل الاحتيالية لما حدث تسليم للمعلومات، ولما وقع المجني عليه سواء كان شخصا طبيعيا أو نظام معلوماتي في الغلط المفضي إلى تسليم معلومات للجاني.[3]

---

[1]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص58.

[2]- المرجع نفسه، ص58.

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

ثالثا-الركن المعنوي

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

1-القصد الجنائي العام

يقوم القصد الجنائي العام على عنصري العلم والإرادة،" إذ ينبغي أن يعلم الجاني أن التوقيعات الإلكترونية التي يستولي عليها مملوكة للغير بأنها مملوكة للمجني عليه أو لغيره، كما ورد بالمذكرة التفسيرية للاتفاقية الأوروبية لمكافحة جرائم المعلوماتية بشأن المادة (8/ب) أن الجريمة يجب أن ترتكب عمدا، ويتمثل العنصر العام للقصد في التلاعب أو التدخل المعلوماتي الذي يسبب ضررا ماديا للغير".[1]

2 -القصد الجنائي الخاص:

يقوم القصد الخاص في جريمة الاحتيال "اتجاه نية الجاني إلى تملك الشيء الذي تسلمه من المجني عليه، ويباشر مظاهر السيطرة التي ينطوي عليها حق الملكية وأن يحرم المجني عليه من مباشرتها، ولنية التملك في الاحتيال ذات مدلولها في جريمة السرقة، فإذا لم تتوافر لدى الجاني نية تملك الشيء الذي تسلمه فإن القصد الخاص لا يتوافر لديه.[2]

أما الاحتيال على نظم معلومات التوقيع الإلكتروني فهي جريمة عمدية تتطلب توافر إرادة ارتكابها مع العلم بكون الفعل المراد ارتكابه مؤثم قانونا ومع ذلك تتجه نية الجاني لارتكابه، إذ أن الجاني يجب أن يكون عالما بان التلاعب الذي يرتكبه في النظام المعلوماتي للتوقيع الإلكتروني أو المعلومات التي يقوم بالتحايل على الحاسب الآلي بإدخالها إليه، فيجعله يستجيب لما يريده، ويسلمه المعلومات التي يرغب في الحصول عليها، هو فعل مجرم قانونا.[3]

---

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

[2]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص68.

[3]- أسامة بن غانم لعبيدي، "حجية التوقيع الإلكتروني في الإثبات"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، جامعة نايف للعلوم الأمنية، الرياض، 2012، ص365.

إذا في إطار معلومات التوقيع الإلكتروني، فإنه يجب أن تتجه إرادة الجاني إلى تحقيق ربح غير مشروع له أو لغيره، وهو ما فسرته المذكرة التفسيرية لاتفاقية بودابست الموقعة في 2001/11/23 بأن جريمة الاحتيال في مجال المعلومات تتطلب بالإضافة للقصد العام قصدا خاصا يتمثل في نية الغش أو نية الغش خاصة، أو بتعبير آخر نية غير آمنة أو غير شريفة بفرض الحصول على منفعة اقتصادية لشخص الجاني أو لغيره.[1]

4 -عقوبة الجريمة:

جاء في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 بنص المادة 23 فقرة هاء على العقاب على التوصل بأي وسيلة للحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني...، بالحبس والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، وذلك مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر.[2]

أما في التشريع السعودي، فقد نص على عقوبة كل الجرائم المتعلقة بالتوقيع الإلكتروني بما فيها جريمة الاحتيال في نظام المعاملات الإلكترونية لسنة 1428هـ والذي جاء فيه: «مع عدم الإخلال بأي عقوبة أشد ينص عليها نظام آخر، يعاقب كل من يرتكب أيا من الأعمال المنصوص عليها في المادة 23[3] من هذا النظام بغرامة لا تزيد عن خمسة ملايين رِيال أو بالسجن مدة لا تزيد عن خمسة سنوات أو بهما معا، ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في الجرائم المتصلة بالتوقيع الإلكتروني».[4]

---

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

[2]- المرجع نفسه، ص227.

[3]- نصت المادة 23 من نظام المعاملات الإلكترونية السعودي لسنة 1428هـ الفقرة 5 أن من جرائم التوقيع الإلكتروني: "إنشاء شهادة رقمية أو توقيع إلكتروني أو شهادة تصديق إلكترونية لغرض احتيالي، والفقرة رقم 8 التي جاء فيها: الدخول على منظومة توقيع إلكتروني لشخص آخر دون تفويض صحيح أو نسخها أو إعادة تكوينها أو الاستيلاء عليها".

[4]- أسامة بن غانم العبيدي، المرجع السابق، ص365.

الفرع الثالث: جريمة تزوير التوقيع الإلكتروني

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

أولا-تعريف جريمة تزوير التوقيع الإلكتروني:

1-تعريف التزوير:

يعرف التزوير لغة على أنه "إصلاح الكلام وتهيئته، وهي كلمة مشتقة من الزور ويعني الكذب والباطل فيقال كلام مزور ومموه بالكذب، أما في الفقه فيعرف على أنه كل وسيلة يستعملها شخص ليغش بها آخر".[1]

أما التزوير قانونا فهو: «عملية مادية وصورة من صور الكذب التي يقوم بها الشخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو رسمي بإحدى الطرق المحددة في القانون، ومن شأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير».[2]

والتزوير في مجال الأنظمة المعلوماتية، يعرف على أنه: «التلاعب في المعلومات المخزنة في أجهزة الحاسب المرتبطة بالشبكة أو اعتراض المعلومات بقصد تحريفها وتزورها».[3]

أما في إطار جرائم الاعتداء على التوقيع الإلكتروني، فقد عرفه قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 على أنه " تغيير الحقيقة في محرر أو توقيع أو

---

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص233.

[2]- عباس حفصي، جرائم التزوير الإلكتروني -دراسة مقارنة-، رسالة دكتوراه، جامعة أحمد بن بلة، وهران 1، 2015، ص16.

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

وسيط إلكتروني بإحدى الطرق التي حددها قانون العقوبات، مما يؤدي للإضرار بالغير بنية استعماله فيها زور من أجله".[1]

2 -التزوير الإلكتروني:

عرف الفقه التزوير الإلكتروني (المعلوماتي) بأنه: «تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها»، كما عرفه بأنه: «تغيير الحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة».[2]

وعرف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلي لعام 1994 في مقرراته وتوصياته بشأن جرائم الكومبيوتر والتزوير الإلكتروني بأنه: «المجرى الطبيعي لمعالجة البيانات التي ترتكب باستخدام الكومبيوتر، وتعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني».[3]

كما عرف التزوير المعلوماتي بأنه: «تغيير الحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب».[4]

وما يمكن استنتاجه من التعريفات السابقة هو أنه بالنظر لسهولة اكتشاف تزوير التوقيع الخطي، إلا أن تزوير التوقيع الإلكتروني لا يترك أي أثر ظاهر كونه يعتمد على الخبرة العلمية للجاني في مجال الحاسوب والمعلوماتية.

ثانيا-الركن المادي لجريمة تزوير التوقيع الإلكتروني:

يتمثل الركن المادي لجريمة تزوير التوقيعات الإلكترونية في سلوك الجاني والمتمثل

---

[1]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص294.

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

[3]- عباس حفصي، المرجع السابق، ص18.

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

في تغيير الحقيقة والتي تكون محل التوقيع الإلكتروني، ويحصل التزوير بأي وسيلة كانت كاستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك.

1-تغيير الحقيقة (سلوك الجاني):

"تغيير الحقيقة هو استبدالها بما يخالفها، أي هو إدخال تغيير على المحرر المراد تزويره على نحو يغير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته".[1]

و"تغيير الحقيقة سواء كان في محرر رسمي أو عرفي، يمكن تصور حصوله في المحررات في نطاق المعلوماتية، وفي هذه الحالة تسمى جريمة التزوير بأنها تزوير معلوماتي كتزوير التوقيع الإلكتروني وهو ينصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه".[2]

ويقصد بتغيير الحقيقة أيضا: " ليس تغيير الحقيقة الواقعية المطلقة وإنما الحقيقة النسبية كأن يثبت في المحرر المزور ما يخالف إرادة صاحب الشأن ويقوم بتزوير توقيع صاحب الشأن عليها حتى ولو صادف ذلك الواقع فعلا ".[3]

ويكون التزوير في نطاق المعلومات "بتغيير الحقيقة في الشرائط أو المحررات التي تمثل مخرجات الحاسب الآلي طالما حدث تغيير في بيانات الحاسب الآلي نفسه، وهو ما انتهجه قانون العقوبات الفرنسي الجديد، حيث نص على أن الركن المادي للتزوير هو التغيير التدليسي للحقيقة، وبذلك أصبح النص يتعامل مع حالات التزوير التقليدي للمحررات وكذا تزوير المحررات التقليدية والإلكترونية التي تكون مطبوعة على سند أو دعامة أو بأية وسيلة".[4]

---

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

[2]- خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص177.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص250.

[4]- أسامة بن غانم العبيدي، المرجع السابق، ص360.

2-محل التزوير:

لما كان محل جريمة التزوير في القانون التقليدي هو المحررات الورقية فإنه في نطاق التوقيع الإلكتروني نص القانون رقم 15 لسنة 2004 (قانون التوقيع الإلكتروني المصري) في المادة 23 منه على محل الجريمة وحددته بالمحرر أو التوقيع الإلكتروني أو الوسيط الإلكتروني".[1]

ولذلك فإن المحرر أو الوثيقة المعلوماتية التي تكون محلا للتزوير قد أثارت جدلا في الفقه في شأن شروطها أو متى يقال أن تزوير قد وقع عليها، "فهناك جانب من الفقه الفرنسي يرى ضرورة النظر إلى محل جريمة التزوير المعلوماتي بوصفه شرطا مفترض ومستقل لقيام الجريمة، بمعنى أنه يشترط في جريمة التزوير المعلوماتي بالإضافة لأركان التزوير في الجريمة التقليدية، أن يكون هناك وثيقة معلوماتية "محرر تم تغيير الحقيقة فيه.

في حين أن فقهاء القانون الجنائي غالبا ما يرون أن المحرر المزور عنصر ضمن عناصر الركن المادي لجريمة التزوير، والتي تلخص في تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون وأن يترتب على ذلك التزوير ضرر بالغير".[2]

كما نص المشرع الإنجليزي في قانون التزييف والتزوير الجديد المطبق في 28-10-1981 على تحديد المحرر الذي يعد محلا للتزوير وقرر في المادة (1/8/1/ذ) أده: «قرص أو شريط أو تسجيل صوتي أو أي أداة أخرى تسجل أو يخزن عليها أو فيها أي معلومات باستخدام الوسائل الميكانيكية أو الإلكترونية أو أي وسيلة أخرى".[3]

3- وسائل وطرق التزوير:

من أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني "استخدام برامج حاسوبية أو أنظمة معلوماتية خاصة بذلك يتم تصميمها على غرر البرامج والنظم

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

[2]- خالد بن عبد الله بن معيض العبيدي، المرجع السابق، ص178.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص254.

المشروعة أو محاولة بعض الأشخاص كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني والقيام بنسخها وإعادة استخدامها بعد ذلك".[1]

ولذلك فإن التوقيع الإلكتروني يتعرض للتزوير "ممن لديهم خبرة باستخدام الحاسب الآلي ومعرفة تقنية بالبرامج واستخدامها، إذ يستطيعون الدخول إلى منظومات التوقيع الإلكتروني باستخدام برامج خاصة والاحتيال على تلك النظم وفك شفرات التوقيع الإلكتروني ومن ثم استخدامها في أغراض احتيالية عن طريق نسخها أو تزويرها ووضعها على محرر مزور".[2]

للإشارة فإن التزوير في المعلومات والتوقيعات الإلكترونية ممر بثلاثة مرحل أساسية وهي:[3]

1- مرحلة التلاعب بالبيانات والتوقيعات عند الإدخال في النظام المعلوماتي، إذ يقوم الجاني بالتلاعب في التوقيعات الإلكترونية التي يتم إدخالها للنظام دون المساس بالبرنامج، هذا الأخير الذي يؤدي عمله بشكل عادي مما يؤدي لإخراج بيانات مزورة وغير حقيقية ولا تطابق البيانات التي يجب حفظها داخل النظام المعلوماتي.

2- مرحلة تزوير التوقيعات الإلكترونية والبيانات في مرحلة المعالجة الإلكترونية، إذ يترك الجاني البيانات والتوقيعات الإلكترونية كما هي دون تغيير، ويتدخل في البرنامج الخاص بالمعالجة الآلية لها سواء بالتعديل في البرنامج نفسه أو بوضع برنامج آخر يحقق هدف الجاني.

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

---

[1]– صالح شنين، المرجع السابق، ص360.

[2]– براهمي حنان، المرجع السابق، ص248.

[3]– حسام محمد نبيل الشنراقي، المرجع السابق، ص ص269–270.

وعليه "فالطرق المذكور في التزوير ليست على سبيل الحصر في جريمة التزوير المعلوماتي (التوقيع الإلكتروني) لأن هذه التكنولوجيا متطورة وأشكالها متغيرة بشكل سريع، ولذلك لا يناسب الصيغة التشريعية في تجريم تزوير الوثيقة المعلوماتية أن تكون دالة على حصر طرق التزوير فيها".[1]

ثالثا-الركن المعنوي:

لا تكتمل جريمة تزوير التوقيعات الإلكترونية أو الوثيقة المعلوماتية "إلا بتوافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وهذه الجريمة هي جريمة عمدية".[2]

وصورة الركن المعنوي فيها هي القصد الجنائي بنوعيه، " القصد الجنائي العام والمتمثل في علم الجاني أنه يغير الحقيقة، وأن هذا التغيير ينصب على محرر بإحدى الطرق المنصوص عليها قانونا، وأن من شأن فعله إحداث الضرر، بأن هذا الفعل هو فعل محضور ومعاقب عليه ومع ذلك يقبل القيام به، وتتجه إرادته إلى هذا الفعل ويقبل النتائج المترتبة عليه، بمعنى أنه يجب أن تتجه إرادته إلى فعل تغيير الحقيقة والأثر المترتب عليه وهو أن يشتمل المحرر على البيانات المخالفة للحقيقة ".[3]

هذا فضلا عن توافر القصد الجنائي الخاص، في جريمة تزوير التوقيع الإلكتروني، "والمتمثل في اتجاه نية الجاني إلى تحقيق غاية معينة وهي استعمال التوقيع الإلكتروني فيما زور من أجله ".[4]

و"استخلاص هذه النية من شأن قاضي الموضوع، وهو يستعين في ذلك بالقرائن والظروف المحيطة بارتكاب الفعل، وإن كان إثبات القصد أيسر في التزوير المادي منه في

---

[1]- براهمي حنان، المرجع السابق، ص216.

[2]-المرجع نفسه، ص224.

[3]- خالد بن عبد الله بن معيض العبيدي، المرجع السابق، ص190.

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

التزوير المعنوي لوجود آثاره".[1]

مع الإشارة إلى أن "المشرع المصري قد جمع بين تزوير التوقيع الإلكتروني ومصطلحي الإتلاف والتعييب داخل جريمة واحدة تحت مسمى جريمة إتلاف وتزوير وتعييب التوقيع أو الوسيط أو المحرر الإلكتروني، وقد جرم هذه الأفعال في المادة (23/ب) من القانون، حيث عاقب كل من أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر، وفصل جريمة التزوير المعلوماتي كصورة للقصد الجنائي الخاص، والإتلاف والتعييب كصورتين للقصد الجنائي العام، واعتبر هذه الجريمة جنحة معاقب عليها بالحبس أو الغرامة أو بكلاهما".[2]

4 -عقوبة الجريمة:

عاقب المشرع المصري على التزوير في مجال معلومات التوقيع الإلكتروني في المادة (23 فقرة ب) من قانون التوقيع الإلكتروني رقم 15 لسنة 2004، "والتي نصت عل أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد عن مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من أتلف أو عيب توقيعا أو وسيطا أو محرر إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر».

وما يستخلص من هذا النص هو أن عقوبة تزوير المستند الإلكتروني في مصر تختلف بحسب نوع المستند الإلكتروني المزور.[3]

كما نص نظام التعاملات الإلكترونية السعودي على العقوبات المقررة لهذه الجريمة في الفصل التاسع المادة (23 الفقرة ب/3) والتي جاء فيها: «يعد مخالفة لأحكام هذا النظام القيام بتزوير سجل إلكتروني أو توقيع إلكتروني، أو شهادة تصديق رقمي أو استعمال أي

[1]- خالد بن عبد الله بن معيض العبيدي، المرجع السابق، ص190.

[2]- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص544.

[3]- براهمي حنان، المرجع السابق، ص299.

من ذلك مع العلم بتزوير».[1]

وأعطى النظام السعودي لهذه الجريمة وصف المخالفة، ونص على عقوبة "غرامة لا تزيد عن خمسة ملايين رِيال أو بالسجن مدة لا تزيد عن خمس سنوات، أو بهما معا، ويجوز الحكم بمصادرة الأجهزة والبرامج والمنظومات المستخدمة في ارتكاب المخالفة".[2]

الفرع الرابع: جريمة إتلاف وتعييب التوقيع الإلكتروني

يعتبر إتلاف وتعييب التوقيع الإلكتروني شكلا من أشكال الغش المعلوماتي، وقد عالجت التشريعات والقوانين في دول العالم المختلفة كافة أشكال هذه الجريمة.

الفرع الحالي سنتناول فيه، تعريف الإتلاف(أولا)، الركن المادي(ثانيا)، الركن المعنوي(ثالثا) وعقوبة هذه الجريمة (رابعا).

أولا-تعريف الإتلاف:

1- الإتلاف التقليدي:

لم ينص المشرع المصري في قانون العقوبات الخاص به على تعريف محدد للإتلاف، بيد أن الفقه قام بتعريفه على أنه: «التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له».[3]

كما يعني الإتلاف: «تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كليا أو جزئيا».[4]

2- الإتلاف الإلكتروني:

يمكن تعريف الإتلاف الإلكتروني بأنه: «إتلاف أو محو تعليمات البرامج أو البيانات

---

[1]- نظام المعاملات الإلكترونية السعودي لسنة 1428هـ، المرجع السابق.

[2]- المرجع نفسه، المادة 23.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص296.

[4]- براهمي حنان، المرجع السابق، ص54.

ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواء استيلاء على أموال أو إطلاع على معلومات، ولكن إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته».[1]

وعرف جانب من الفقه الإتلاف على أنه: «محو المعلومات أو البرامج كلية أو تدميرها إلكترونيا أو أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال».[2]

ويعرف حسام الشنراقي إتلاف التوقيع الإلكتروني بأنه: «استخدام أي من الوسائل التكنولوجية أو البرامج لإحداث تعديل أو محو أو تدمير لنظم معلومات التوقيع الإلكتروني أو أي من مكوناتها المنطقية للإضرار بالمؤسسة أو الشخص صاحب التوقيع الإلكتروني بقصد جعل النظام المعلوماتي غير صالح للاستخدام».[3]

ثانيا: الركن المادي:

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

وقد "يقع الإتلاف على المعلومات المنسوخة على شرائط أو دعامات، وقد يقع أيضا على المكونات المادية والأجهزة المستخدمة في عمل التوقيع الإلكتروني مثل شاشات العرض

---

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

[2]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص547.

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

[4]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص542.

والأشرطة والأسطوانات والكابلات والمفاتيح والأقراص الممغنطة، وغيرها من المكونات المادية سواء كانت تحوي بيانات أو برامج أو مجرد أوعية فارغة، يشرط أن يؤدي الإتلاف أو التخريب إلى التقليل من قيمتها الاقتصادية أو يؤدي إلى تعطيلها أو عدم صلاحيتها للاستخدام".[1]

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

كما أن "العقاب على الجريمة هو عقاب على السلوك والقصد الإجرامي وليس على مدى الضرر المتحقق من هذا السلوك".[3]

ثالثا-الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، "يتمثل الأول في علم مرتكب الواقعة (الجاني) بأن فعل الإتلاف أو التعييب للتوقيع الإلكتروني محظور ومعاقب عليه قانونا، وأن تتجه إرادته للفعل المجرم، أما إذا كان الإتلاف أو التعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه، فلا تقوم هذه الجريمة".[4]

مع الإشارة إلى أن "هذه الجريمة لا تتطلب قصدا جنائيا خاصا، وإنما لا يكفي وجود القصد الجنائي العام بعنصريه الإرادة والعلم، فتقوم بذلك الجريمة بتوافر الركن المادي والقصد الجنائي العام".[5]

---

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

[2]- صالح شنين، المرجع السابق، ص174.

[3]- حسام محمد نبيل الشنراقي، المرجع السابق، ص323.

[4]- صالح شنين، المرجع السابق، ص174.

[5]- المرجع نفسه، ص174.

رابعا –عقوبة الجريمة:

لقد نص القانون الأمريكي على "العقاب على الإتلاف المعلوماتي في سياق المادة (1030 الفقرة 5) من القسم 18 بعد تعديلها، ويستكشف من نص هذه المادة أن الأشخاص المصرح لهم الدخول إلى النظام لا تتقرر مسؤوليتهم عن أعمال الإتلاف إلا إذا كانت قد تمت عمدا في حين أن الدخول غير المصرح به تتقرر به المسؤولية عن أعمال الإتلاف في جميع الحالات".[1]

أما المشرع الفرنسي "فقد نص في المادة (3/323) من القانون الجديد على كل من يدخل بطريق الغش بيانات في نظام معالجة آلية للبيانات أو يلغي أو يعدل بطريق الغش بيانات في النظام يعاقب بالحبس لمدة ثلاث سنوات وغرامة ثلاثمائة ألف فرنك فرنسي".[2]

أما القانون المصري رقم 15 لسنة 2004 فقد عاقب على إتلاف المعلومات في المادة 23 منه على الدخول لنظام معلوماتي بدون تصريح، ونصت هذه المادة الفقرة ب على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تريد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عيب توقيعا أو وسيطا أو محرر إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق اخر».[3]

المبحث الثاني

الحماية الجنائية لجرائم التوقيع الإلكتروني في التشريع الجزائري

في إطار توجه المشرع الجزائري لمواكبة التحولات الدولية والمحلية فيما يتعلق بخلق بيئة معاملات إلكترونية آمنة وموثوقة وتعزيز آليات الحماية الجنائية للتوقيع الإلكتروني،

[1]– حسام محمد نبيل الشنراقي، المرجع السابق، ص329.

[2]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص542.

[3]– حسام محمد نبيل الشنراقي، المرجع السابق، ص329.

تصدى للجرائم الممكن الاعتداء بها على التوقيع الإلكتروني وذلك بسنه لمواد ضمن قانون العقوبات وفي القانون رقم (15-04) الخاص بالتوقيع الإلكتروني.

ويتطرق المبحث الحالي لصور الحماية الجنائية للتوقيع الإلكتروني من منظور التشريع الجزائري، والذي قسمناه إلى مطلبين، تطرق الأول لهذه الجرائم في قانون العقوبات، والمطلب الثاني في القانون رقم (15-04) لسنة 2015.

المطلب الأول

صور الحماية الجنائية للتوقيع الإلكتروني في قانون العقوبات الجزائري

نظرا للتطور الحاصل في بيئة الأعمال الإلكترونية شرع المشرع الجزائري إلى تعديل قانون العقوبات وذلك بموجب الأمر رقم (06-23) المؤرخ في 26 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، إذ أضاف فصلا كاملا تحت عنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، غير أن المشرع لم يورد تعريفا لهذه الأنظمة المعلوماتية مما يطرح التساؤل حول اعتبار منظومة إنشاء توقيع الإلكتروني محل للحماية المقررة في هذا الفصل؟

يقصد بنظام المعالجة الآلية وفق التعريف الوارد في الفقرة (ب) من المادة 2 من القانون رقم 09-04 بشأن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ولاتصال ومكافحتهما[1] "بأنه أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

ووفقا لهذا التعريف الموسع فإن المحل الذي ينصب عليه سلوك الجاني في جرائم المساس بأنظمة المعالجة الآلية للبيانات يتسع لاستيعاب المعلومات في نظام المعالجة الآلية خلال مرحلة المعالجة و التخزين والاسترجاع، النظام الذي يتضمنها فضلا عن الشبكات

[1]- قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، الصادرة في 16 أوت 2009.

ذاتها أو المعلومات المنقولة عبرها، و بالتالي يشمل تجريم اعتراض عملية نقل المعلومات سواء من خلال الدخول إلى الشبكة الاتصالات أو من خلال التقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل التقاط إلكترونية، ويترتب على ذلك أن تصبح هذه الإشارات محلا ينصب عليه سلوك الجاني في هذه الجرائم.[1]

وعليه فإن منظومة إنشاء التوقيع الإلكترونية هيا جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني.[2] إذ يتم فيها تبادل البيانات بين طرفي (صاحب التوقيع ومؤدي خدمات التصديق الإلكتروني) من خلال الحاسب الآلي وباستخدام أنظمة وبرامج معينة، مما يجعلها منظومة معلوماتية وفق لتعريف السابق، وعليه تكون محلا للحماية الجنائية المقررة في المادة 394 مكرر والمادة 394 مكرر1 من قانون العقوبات باعتبارها أنظمة معالجة آلية.

ومن خلال هذا المطلب سوف نتطرق إلى أهم الصور المقررة لحماية التوقيع الإلكتروني في قانون العقوبات الجزائري المتمثلة في: جريمة الدخول أو البقاء على منظومة إنشاء توقيع الكتروني (فرع أول)، جريمة التلاعب في بيانات إنشاء توقيع الكتروني (فرع ثاني)، جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية (فرع ثالث). وجريمة حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها إلكترونيا (فرع رابع).

الفرع الأول: جريمة الدخول أو البقاء على منظومة إنشاء توقيع الكتروني.

يتحقق الاعتداء على التوقيع الإلكتروني بالاعتداء على النظام المعلوماتي للتوقيع الإلكتروني من خلال الدخول أو البقاء غير المشروع، وعالج المشرع الجزائري هذه الجريمة من خلال المادة 394 مكرر (ق ع ج) والتي جاء فيها: «يعاقب بالحبس من ثلاثة (3)

[1]– رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012، ص223.

[2]– أنظر المادة 4/2 من قانون 15–04، المرجع السابق.

أشهر إلى سنة (1) وبغرامة مالية من (50.000 دج) إلى (200.000دج) كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة للمعطيات أو يحاول ذلك».[1]

تصنف "هذه الجريمة من جرائم الخطر حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر المتطلب فيها حصول ضرر بالمجني عليه".[2]

أولا-الركن المادي:

على ضوء المادة 394 مكرر من قانون العقوبات المذكور آنفا،" فان السلوك الإجرامي للركن المادي يتخذ إما صورة الدخول المنطقي وذلك يفرض فتح باب يؤدي إلى النظام المعلوماتي للتوقيع الإلكتروني أو يتخذ صور البقاء، وعليه فإن هذا السلوك قد يكون إيجابيا يتمثل في فعل الدخول أو سلبيا يتمثل في الامتناع عن الخروج من النظام".[3]

ويتحقق فعل الدخول بإساءة استخدام النظام المعلوماتي للتوقيع الإلكتروني عن طريق شخص الجاني غير المرخص له باستخدامه أو الدخول إليه، وغرضه من ذلك قد يكون الحصول على المعلومات والبيانات المخربة داخل هذا النظام لاستخدامها في مصلحته أو مصلحة شخص آخر، وذلك من خلال استغلال خبرته في التحكم في الحاسب الآلي وبرامجه واختراق نظامه الأمني.

على هذا الأساس، "تعد هذه الجريمة من جرائم الخطر أو السلوك المجرد، أين لا يشترط حصول نتيجة معينة، بمعنى أده بمجرد الاتصال غير المشروع بالنظام يؤدي ذلك إلى قيامها".[4]

---

[1]- المادة 394 مكرر من أمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات الجزائري، المعدل والمتمم.

[2]- صالح شنين، المرجع السابق، ص167.

[3]- عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد 11، المركز الجامعي تمنراست(الجزائر)، جانفي 2017، ص113.

[4]- براهمي حنان، المرجع السابق، ص47.

لكن هناك من لا يوافق على هذا الطرح، "حيث طالما المصلحة المحمية في نظام معلومات التوقيع الإلكتروني هي حماية سرية المعلومات، فالدخول غير المشرع لابد وأن يؤدي إلى الوصول إلى المعلومات المخربة وإلا لا يكتمل الركن المادي للجريمة".[1]

ثانيا-الركن المعنوي:

بناء على نص المادة 394 مكرر، اعتبر المشرع الجزائري أن الدخول غير المشروع للنظام المعلوماتي للتوقيع الإلكتروني من الجرائم العمدية التي تتطلب توافر القصد الجنائي بعنصريه العلم والإرادة، حيث لابد وأن يعلم الجاني بعدم أحقيته في الدخول إلى النظام، ومع ذلك تنصرف إرادته نحو الإتيان بهذا السلوك المجرم قانونا.

وتجدر الإشارة إلى أن ذلك "لا يتأثر بالباعث من الدخول حتى لو كان الفضول أو التنزه أو إثبات القدر على الانتصار على النظام".[2]

أما عن الركن المعنوي للجريمة في صورتها المشددة، "فيتضح من خلال الفقرتين (2-3) من المادة 394 مكرر، أن النتيجة المشددة هي نتيجة غير عمدية، وهو ما 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 هنا فهي من جرائم الإهمال، فمجرد ارتكاب الفعل المادي يعد كافيا لقيامها إلا إذا أثبت الجاني وجود قوة قاهرة أدت إلى حدوثها".[3]

تعد هذه الجريمة من الجرائم العمدية التي تقوم بالقصد الجنائي العام الذي يتكون من عنصري العلم والإرادة المنصرفة إلى إتيان هذا الفعل بالمخالفة للقانون وبمخالفة لإرادة

[1]- براهمي حنان، المرجع السابق، ص47.

[2]- المرجع نفسه، ص49.

[3]- عزيزة لرقط، المرجع السابق، ص ص114-115.

صاحب النظام أو صاحب الحق فيه[1]. وعاقب عليها المشرع الجزائري بعقوبة الحبس من ثلاثة أشهر إلى سنة، والغرامة من 50.000 دج إلى 200.000دج، هذا في صورة الجريمة البسيطة على النحو الذي سبق بيانه، بينما في حالة الصورة المشددة تصبح العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 100.000دج إلى 400.000دج، والصورة المشددة هنا ما نصت عليه المادة 394 مكرر في فقرتها الثانية أنه:" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

أما إذا ترتب على الأفعال المذكورة سابقا تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.

الفرع الثاني: جريمة التلاعب في بيانات إنشاء توقيع الكتروني

انطلاقا من نص المادة 394 مكرر 1[2] من قانون العقوبات الجزائري يتضح أن الركن المادي لجريمة التلاعب الغير مصرح به بالمعلومات التي يتضمنها نظام إنشاء توقيع إلكتروني يتم بسلوك إجرامي يرتكبه الجاني ويستهدف تحقيق نتيجة معينة تتمثل في تغيير الحالة التي تكون عليها المعلومات في بيئتها التقنية. وهذا السلوك يتمثل في الإدخال أو التعديل أو الإزالة معلومات داخل نظام إنشاء توقيع إلكتروني وهو ما سنحاول توضيحه كما يلي:

1-الركن المادي:

-الإدخال: فعل الإدخال هو الفعل الذي بدأت به المادة 394 مكرر1 وهو تغذية النظام بالمعلومات المراد معالجتها. أو بتعليمات لازمة لعملية المعالجة[3]، ويعتبر إدخال البرامج

[1]- مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، مصر، 2000، ص53.

[2]- تنص المادة 394 مكرر 1 من قانون العقوبات على أنه "**يعاقب بالحبس... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها...**".

[3]- رشيدة بوكر، المرجع السابق، ص251.

الخبيثة إلى نظام إنشاء توقيع إلكتروني بهدف إتلاف المعلومات وتدميرها من أكثر الوسائل انتشارا وخطورة على المعلومات.

-الإزالة: وهو السلوك الثاني الذي نصت عليه المادة 394 مكرر1 من قانون العقوبات ويقصد به محو جزء أوكل المعطيات الموجودة داخل النظام أو تحطيم هذا النظام أو الدعامة الموجودة بداخلها المعطيات[1]. ويرى البعض أن فعل الإزالة هو عبارة عن إتلاف بيانات متعلقة بالتوقيع الإلكتروني التي يعالجها النظام آليا ويتحقق ذلك بإزالتها كلها أو جزء منها عن طريق برامج لها القدرة على ذلك.

-التعديل: وهو السلوك الأخير المكون للركن المادي لهذه الجريمة ويقصد به تغيير المعطيات الموجودة داخل النظام وتحريفها أو استبدالها بمعطيات أخرى، والتعديل بهذا المعنى قد يتم باستبدال المعلومات، أو عن طريق التلاعب في البرامج وذلك بإمدادها بمعلومات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها.[2]

ثانيا-الركن المعنوي:

بناءا على ما جاءت به المادة 394 مكرر1 المذكورة سابقا، يتضح أن "جنحة إتلاف التوقيع الإلكتروني من الجرائم العمدية التي يتطلب فيها توافر الركن المعنوي الذي يتخذ صور القصد الجنائي العام بعنصريه العلم والإرادة".[3]

وترتيبا عل ذلك يجب أن يعلم الجاني أده يقوم بإتلاف التوقيع الإلكتروني عن طريق الإدخال أو المحو أو التعديل في بياناته، إضافة إلى انصرف إرادته في ارتكاب الفعل المادي.

وتتمثل النتيجة الجرمية بهذا المعنى في إلحاق الضرر صاحب التوقيع الإلكتروني من

---

[1]- عبد الحليم بوقرين، الحماية الجنائية للمعاملات التجارية، أطروحة دكتوراه، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014، ص143.

[2]- رشيدة بوكر، المرجع السابق، ص256.

[3]- عزيزة لرقط، المرجع السابق، ص116.

خلال جعل توقيعه غير صالح للاستعمال أو معيبا يفقده وظيفته ويهز ثقة المتعاملين مع صاحب التوقيع في شخصها.[1]

هذه الجريمة كغيرها من الجرائم السابقة، تعد جريمة عمدية تتطلب قصد جنائي عام، وتقوم بمجرد توافر فعل الإدخال أو التعديل أو الإزالة[2]، سيما أن المشرع الجزائري استعمل عبارة عن طريق الغش، مما ينطوي على أن الشخص يعلم بسلوكه المجرم ويريد فعلا النتائج المترتبة.

قررت المادة 394 مكرر 1 عقوبة الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من 500.000 دج إلى 4.000.000 دج.

الفرع الثالث: جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية:

وقد نصت عليها الفقرة 1 من المادة 394 مكرر 2 من قانون العقوبات، والتي جاء فيها: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم".[3]

1-الركن المادي للجريمة:

من خلال نص الفقرة سالفة الذكر جرم المشرع مجموعة من الصور ضمن هذه الجريمة وهي:

---

[1]– عزيزة لرقط، المرجع السابق، ص116.

[2]– هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية –دراسة مقارنة–، دار الكتب القانونية، مصر، 2015، ص83.

[3]– طيب موفق شريف، المرجع السابق، ص85.

– تصميم معطيات إلكترونية مخزنة أو معالجة او مرسلة عن طريق منظومة معلوماتية،

– بحث عن معطيات إلكترونية مخزنة أو معالجة او مرسلة عن طريق منظومة معلوماتية.

– تجميع معطيات إلكترونية مخزنة أو معالجة او مرسلة عن طريق منظومة معلوماتية،

– نشر معطيات إلكترونية مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية،

– الإتجار في معطيات الكترونية مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

2-الركن المعنوي للجريمة:

وهو المتمثل في القصد الجنائي، وقد نصت عليه المادة في فقرتها الأولى بقولها: " ... كل من يقوم عمدا..."، إلا أن حيازة بعض هذه المعطيات قد يشكل في حد ذاته قرينة على القصد الجنائي.[1]

وبالتالي تعد هذه الجريمة من الجرائم العمدية التي يتطلب فيها توافر الركن المعنوي الذي يتخذ صور القصد الجنائي العام بعنصريه العلم والإرادة.

هذه الجريمة كغيرها من الجرائم سابقة الذكر، تعد جريمة عمدية تتطلب قصد جنائي عام، وتقوم بمجرد توافر فعل التصميم، البحث، التجميع، النشر والإتجار مما ينطوي على أن الشخص يعلم بسلوكه المجرم ويريد فعلا النتائج المترتبة.

جاء المشرع الجزائري في نص المادة 394 مكرر 2 فقرة 1 على عقوبة الحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش الأفعال سالفة الذكر.

[1]– طيب موفق شريف، المرجع السابق، ص ص85-86.

الفرع الرابع: جريمة حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها إلكترونيا

وهو ما نصت عليه الفقرة 2 من المادة سالفة الذكر (394) من قانون العقوبات، والتي جاء فيها: "حيازة أو إفشاء أو تشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".[1]

1-الركن المادي للجريمة:

ويتمثل في الصور الآتية:

- حيازة معطيات إلكترونية.
- إفشاء أو نشر معطيات إلكترونية.
- استعمال معطيات إلكترونية.

2-الركن المعنوي للجريمة:

أما الركن المعنوي لهذه الجريمة فتعد من الجرائم العمدية، حيث نجد أن حيازة بعض هذه المعطيات قد يشكل في حد ذاته قرينة على القصد الجنائي.

وبالتالي تكون هذه الجريمة كذلك من الجرائم العمدية التي تتوفر على القصد الجنائي، وتقوم بمجرد توافر فعل من الأفعال المذكورة سابقا في نص المادة 394 مكرر 2 في فقرتها الثانية، حيث تعاقب مرتكبها بعقوبة الحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش الأفعال سالفة الذكر.

بعد استعراض صور الحماية الجنائية التي اعتمدها المشرع الجزائري لحماية التوقيع الإلكتروني في ظل قانون العقوبات، أين لم يخص هذا المشرع التوقيع الإلكتروني بحماية

[1]- طيب موفق شريف، المرجع السابق، ص86.

جنائية في قانون خاص في بداية الأمر.

لكن مع صدور القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين يكون المشرع الجزائري قد سن تشريعا يكفل تحقيق حماية جنائية خاصة بالتوقيع الإلكتروني.[1]

المطلب الثاني

صور الحماية الجنائية للتوقيع الإلكتروني في ظل القانون 15-04

بعدما اقتصر المشرع الجزائري في حماية التوقيع الإلكتروني جنائيا على ما هو منصوص عليه في قانون العقوبات، توجه نحو إصدار قانون خاص بالتوقيع والتصديق الإلكترونيين وهو القانون رقم 15-04 المؤرخ في 01-02-2015، أين أقر في هذا القانون حماية جنائية للتوقيع والتصديق الإلكترونيين من خلال تعداده لمختلف الجرائم الواقعة عليهما.

لقد أقر القانون المذكور أعلاه حماية جنائية للتوقيع والتصديق الإلكترونيين من خلال تعداده لمختلف الجرائم الواقعة عليهما، والملاحظ من استقراء نصوص المواد التي تضمنت هذه الجرائم خلو القانون من اعتماد تصييف لهذه الجرائم على غرار ما جاءت به قوانين التوقيع الإلكتروني لعدد من التشريعات الأجنبية والعربية التي جاءت في هذا البحث.

من هذا المنطلق سيتناول المطلب الحالي مجموعة من أهم الجرائم الواقعة على التوقيع الإلكترونيين التي نص عليها هذا القانون وفق تسلسل المواد الواردة فيه.

ومن خلاله سنتطرق إلى جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير (فرع أول)، جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني (فرع ثاني)، وجريمة التصريح بمعطيات خاطئة لاستصدار شهادة تصديق إلكتروني (فرع ثالث).

[1]- طيب موفق شريف، المرجع السابق، ص86.

الفرع الأول: جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير

نصت على هذه الجريمة المادة 68 من القانون 15-04 «يعاقب بالحس من ثلاثة أشهر (3) إلى ثلاثة سنوات (3) وبغرامة من مليون دج إلى خمسة ملايين دج أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير».

يتمثل السلوك الإجرامي في هذه الجريمة في قيام الجاني بأحد الأفعال (الحيازة، الإفشاء، الاستعمال) وبالتالي يعد القيام بأحد هذه الأفعال كافيا لقيامها، فهي تعد من جرائم السلوك التي يعد فيها التقاط الإجرامي كافيا لقيامها.

1-حيازة أداة إنشاء توقيع إلكتروني موصوف خاصة بالغير:

وهي حيازة برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني خاصة بالغير دون موافقة صاحبه والحيازة المشروعة لهذا البرنامج أو النظام المعلوماتي لا عقاب عليها طالما أن الشخص مرخص له بهذه الحيازة من الجهة المتخصصة بهدف توثيق هذه التوقيعات طالما لم يثبت أن نيته قد اتجهت إلى استخراج توقيع إلكتروني رغما عن إرادة صاحبه.[1]

2-إفشاء أداة إنشاء توقيع إلكتروني موصوفة خاص بالغير:

يكون إفشاء أداة إنشاء توقيع إلكتروني بالتعدي على البيانات المشفرة أو فض المعلومات المشفرة التي تخص أداة إنشاء التوقيع الإلكتروني والتي تكون مرتبطة بأجهزة أو برامج معلوماتية.[2]

3-استعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير:

[1]- لالوش راضية، المرجع السابق، ص154.

[2]- بلحسني حمزة، الحماية القانونية والفنية للتوقيع الإلكتروني في مجال البيئة الرقمية، مجلة العلوم القانونية والإدارية، العدد 11، الجزائر، 2015، ص82.

ويقصد ببيانات إنشاء توقيع إلكتروني بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني، ووفقا لما جاء في نص المادة 02 الفقرة 03 من قانون 15-04 وغالبا ما تكون هذه البيانات التي تتعلق بالتوقيع الإلكتروني مخزنة داخل الحاسوب ألآلي أو قرص منفصلة مثل البيانات المتعلقة باسم صاحب التوقيع ومهنته وكافة بياناته الشخصية وكافة المعلومات بذلك التوقيع وإلي يفترض سريتها.

أما عن الركن المعنوي لهذه الجريمة فمي من الجرائم العمدية التي تشترط توافر القصد الجنائي العام بعنصريه العلم والإرادة.[1]

ولقد قرر المشرع عقوبات لهذه الجريمة في نص المادة 68 من القانون 15-04 حيث العقوبة بحد أدنى متمثل في الحبس بثلاثة أشهر وحد أقصى محدد بثلاثة سنوات حبس، وحدد الغرامة من 100000 دج إلى 500000 دج وأعطى الحرية للقاضي في النطق بإحدى هاتين العقوبتين فقط.

الفرع الثاني: جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني.

جرم المشرع الجزائري انتهاك سرية بيانات شهادة التصديق الإلكتروني من خلال نصي المادة 70 والمادة 73 من قانون 15-04 سابق الذكر، والملاحظ على هاتين المادتين أن المشرع حمى بموجبهما سرية بيانات شهادة التصديق الإلكتروني، إلا أن الاختلاف يكمن في صفة الجاني، فالمادة الأولى تتعلق بمؤدي خدمات التصديق الإلكتروني، أما الثانية فتتعلق بكل شخص مكلف بالتدقيق.

عدم معرفة الغير من غير المتعاقدين بيانات شهادة التصديق الإلكتروني، وتعني الخصوصية ارتباط هذه المعلومات بالمتعاقدين مما يحتم عدم اطلاع الغير عليها.[2]

[1]- بلحسني حمزة، المرجع السابق، ص84.

[2]- هبة حسين محمد زايد، المرجع السابق، ص61.

وكشف المعلومات أو البيانات هنا يعني إذاعتها أو نقلها وإطلاع الغير عليها خلافا لإرادة أصحابها وخروجها عن حيز الكتمان أو السرية إلى العلانية بعد أن كان العلم بها مقصورا فقط على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم وهم الأشخاص المكلفة بالتدقيق ومؤدي خدمات التصديق الإلكتروني.

فهذه الجريمة تعد من الجرائم السلوكية يكفي فيها المشرع مجرد تحقق السلوك الإجرامي دون اشتراط تحقق النتيجة لأن الغرض من التجريم هنا هو الحفاظ على سرية المعلومات وخصوصيتها وليس تحقيق نتيجة إجرامية.[1]

أما الركن المعنوي لهذه الجريمة فيقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، فمرتكب هذه الجريمة يسعى بمحض إرادته إلى كشف هذه المعلومات المتواجدة لديه بحكم وظيفته مع علمه بسريتها وفي غير الأحوال المصرح بها قانونا، وتتجه إرادته لإتيان هذا السلوك ويقبل الآثار المترتبة عليه.[2]

وتختلف عقوبة جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني باختلاف صفة الجاني، فإن كان مرتكب الجريمة مؤدي خدمات التصديق الإلكتروني فإن العقوبة نصت عليها المادة 70 من نفس القانون، وتتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط.[3]

أما إذا كان مرتكب الجريمة من بين الأشخاص المكلفون بالتدقيق، فإن عقوبته حددتها المادة 73 من نفس القانون، وتتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وهي نفس العقوبة السالبة للحرية المقررة لمؤدي خدمات التصديق الإلكتروني، وغرامة مالية تتراوح بين عشرين ألف دينار (20.000دج) إلى مائي ألف دينار (200.000 دج)، أو بإحدى

[1]– أسامة عبد الله فايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988، ص77.

[2]– جفالي حسين، المرجع السابق، ص273.

[3]– المرجع نفسه، ص273.

هاتين العقوبتين فقط.[1]

الفرع الثالث: جريمة التصريح بمعطيات خاطئة لاستصدار شهادة تصديق إلكتروني.

نصت المادة 66 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على أنه: "يعاقب بالحبس...، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة".

يتحقق الركن المادي في هذه الجريمة بمجرد توافر واقعة التصريح بالمعطيات الخاطئة أو الغير صحيحة من جانب الجاني، ذلك أن الجاني أو ممثله القانوني يقدمان معلومات خاطئة أو غير صحيحة كاذبة أيا كان موضوع المعلومات، سواء كانت تتعلق بهوية صاحب الشهادة أو هوية الشخص المفوض، وهي المعلومات التي تحدد شخص صاحب الشهادة تحديدا دقيقا. ويتعين كذلك الإدلاء بهذه المعلومات والبيانات الكاذبة إلى مؤدي خدمات التصديق الإلكتروني حاصل على ترخيص من الجهة المختصة، ويكون الغرض من ذلك هو استصدار شهادة التصديق الإلكتروني موصوفة.

أما ركنها المعنوي فهذه الجريمة من الجرائم العمدية يتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، فيجب على الجاني أن يعلم بحقيقة سلوكه الإجرامي وأنه يدلي بإقرارات كاذبة إلى مؤدي خدمات التصديق الإلكتروني بهدف الحصول على شهادة تصديق إلكتروني موصوفة، ويعلم أن هذا الفعل محضور قانونا، ومع ذلك تتجه إرادته إلى فعل السلوك الإجرامي المتمثل في الإدلاء بهذه المعلومات غير الصحيحة.[2]

إذ أقر المشرع لهذه الجريمة عقوبة سالبة للحرية تتمثل في الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات، وبعقوبة مالية تتمثل في غرامة تتراوح بين عشرين ألف دينار (20.000 دج) إلى مائي ألف دينار (200.000 دج)، أو إحداهما فقط.

---

[1]- جفالي حسين، المرجع السابق، ص273.

[2]- المرجع نفسه، 274.

والجدير بالذكر هنا أن المشرع أقرى مسؤولية الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القانون، وحدد له عقوبة تتمثل في غرامة تعادل (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.[1]

[1]– أنظر المادة 75 من قانون 15–04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين، المرجع السابق.

خاتمـــــــة

بما أن التوقيع الإلكتروني واقعة مستجدة فرضتها مقتضيات التجارة الإلكترونية فقد صدرت تشريعات دولية وإقليمية ووطنية نظمت أحكامها التوقيع الإلكتروني لإزالة الغموض على هذا المفهوم الحديث والمستجد على الفكر القانوني، وبينت مفهومه واعترفت به ومن بين هذه القوانين التي حددت الطبيعة القانونية للتوقيعات الإلكترونية، قانون الأونسيترال النموذجي لعام 1996م بشأن تنظيم التجارة الإلكترونية، وقانون الأونسيترال النموذجي لعام 2001م بشأن التوقيعات الإلكترونية، كما أصدرت المفوضية الأوربية أحكام التوجيه الأوربي رقم 93 لسنة 1999م بشأن التوقيعات الإلكترونية، وكذلك تعريف التوقيع الإلكتروني في القانون العربي الاسترشادي للإثبات بالطرق الحديثة، وفضلا على ذلك واسترشادا بالقوانين النموذجية والتوجيهات الدولية، صدرت العديد من التشريعات الوطنية اعترفت بالتوقيع الإلكتروني وأضفت عليه حجية قانونية مساوية لحجية التوقيع التقليدي في الإثبات.

يعتبر التوقيع الإلكتروني مجموعة من الحروف أو الأرقام، أو الرموز أو الأصوات، أو أي معالجة إلكترونية أخرى، بحيث يمكن أن يعبر عن رضا أطراف التصرف القانوني، وأن يميز ويحدد هوية شخص موقعه، كما يرتبط بمضمون المحرر على أي دعامة إلكترونية.

للتوقيع الإلكتروني صور عديدة تتلف التقنية المستخدمة في تشغيل منظومة التوقيع الإلكتروني، ومن هذه الصور ما يعتمد على الأرقام أو الأحرف أو الرموز... مثل التوقيع بالرقم السري المقترن بالبطاقة الممغنطة، ومنها ما يعتمد على الخواص الطبيعية والفيزيائية للإنسان وهو التوقيع البيومتري، كذلك منها ما يعتمد على التشفير باستخدام المفتاح المتماثل –المفتاح العام–أو المفتاح غير المتماثل–المفتاح العام والخاص–، لكل صورة من هذه الصور قوة ثبوتية تختلف عن الأخرى.

ولكي يتمتع التوقيع الإلكتروني بذات الحجية المقررة للتوقيع التقليدي يجب أن تتوافر فيه الشروط القانونية التي تجعل منه توقيعا موثوقا به أو معززا أو محميا أو جديرا بالتعويل عليه، كما عبرت التشريعات المختلفة على ذلك.

في بحثنا هذا تناولنا موضوع الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري، فبينا النظام القانوني لتوقيع الإلكتروني من خلال بيان مفهومه وكيفية التصديق عليه، ثم بحثنا صور الحماية الجنائية التي أقرها المشرع له، حيث خرجنا بجملة من النتائج:

-عرف المشرع الجزائري التوقيع الإلكتروني في قانون 15-04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين تعريفا مزدوجا بحيث عرف تعريفا عاما من جهة وأضاف تعريفا نوعيا خاصا بالتوقيع الإلكتروني الموصوف.

-إن تعريف المشرع الجزائري للتوقيع الإلكتروني لم يشر بشكل حصري لصور التوقيع الإلكتروني، بل أجاز أن يتخذ أي شكل سواء، كان في هيئة صور أو حرف أو رقم أو رمز، شريطة أن يكون له طابع منفرد يسمح بتمييز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار التصرف القانوني أو الرضا بموجبه، كما أن التعريف لم يربط التوقيع بشكل مادي محدد، تاركا المجال مفتوحا كي يتسع هذا التعريف لما يستجد من تطورات تكنولوجية قد تفرز أشكالا وصورا جديدة من التوقيعات الإلكترونية.

-أضفى المشرع الجزائري للتوقيع الإلكتروني الحجية الكاملة في الإثبات من خلال مساواته بالتوقيع التقليدي، بشرط أن يكون التوقيع الإلكتروني موصوف، وحتى يكون التوقيع الإلكتروني موصوف وجب تصديقه لدى مؤدي خدمات التصديق الإلكتروني المرخص له من السلطات العامة للدولة.

-حرص المشرع الجزائري على تقرير حماية جنائية للتوقيع الإلكتروني بموجب قانون 15-04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين، وأفرد الفصل الثاني من الباب الرابع منه للعقوبات على الجرائم الماسة بالتوقيع الإلكتروني.

-كما تتقرر الحماية الجنائية للتوقيع الإلكتروني من خلال حماية أنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، حيث يتم إنشاء التوقيع الإلكتروني من خلال

منظوم معلوماتية، وذلك حسب التعريف الموسع لها الوارد في قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال.

في ضوء هذه النتائج التي توصلت إليه الدراسة، يمكن أن نقدم المقترحات التالية:

إن صور التجريم المستحدثة لحماية التوقيع الإلكتروني من، المؤكد تزايدها في المستقبل نظرا للتوسع المتوقع في حجم التجارة الإلكترونية والعقود التجارية، مما يحتم صياغة النصوص الجنائية بشكل مرن يسمح بدخول الصور المستحدثة مستقبلا في النص، بما لا يمثل اعتداء على مبدأ الشرعية الجنائية.

ضرورة إنشاء سلطات التصديق الإلكتروني في أقرب وقت، لما لها من دور في حماية التعاملات الإلكترونية بوجه عام والتوقيع الإلكتروني بوجه خاص.

ضرورة تكوين القضاة في مجال المنازعات الإلكترونية، وتنظيم ندوات وأيام تكوينية خاصة فيما يتعلق بحماية البيانات الإلكترونية والتوقيع الإلكتروني.

قائمة المراجع

أولا: المؤلفات

1. أبو زيد محمد محمد، تحديث قانون الإثبات مكانة المحررات الإلكترونية بين الأدلة الكتابية، دار النهضة العربية، مصر، 2002.
2. أبو هبة نجوى، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، طبعة 2002.
3. أسامة عبد الله فايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988.
4. ثروت عبد الحميد، ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات، دار الجامعة الجديدة، القاهرة، 2007.
5. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013.
6. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، مصر، 2000.
7. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، ط1، دار الفكر الجامعي، مصر،2006.
8. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012.
9. سعيد سيد قنديل، "التوقيع الإلكتروني"، دار الجامعة الجديدة، الإسكندرية، 2006.
10. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة –دراسة مقارنة–، دار النهضة العربية، مصر، 2006.
11. ضياء أمين مشيمش، التوقيع الإلكتروني دراسة مقارنة تقديم القاضي الدكتور مروان كركبي دار المنشورات الحقوقية، بيروت لبنان، طبعة سنة 2003.
12. عابد فايد عبد الفتاح فايد، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني: دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني، دار الجامعة الجديدة، الإسكندرية، 2004.

13. عبد الحميد ثروت، التوقيع الإلكتروني ومخاطره وكيفية مواجهتها، مدى حجيته في الإثبات مكتبة الجلاء، القاهرة، الطبعة الثانية، 2002-2003.

14. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، 2004

15. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، 2005.

16. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الحساب الآلي والانترنت، دار الكتب القانونية، الإسكندرية، مصر، 2002.

17. فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005.

18. القليوبي سميحة، الأوراق التجارية (الكمبيالة، السند لأمر، الشيك، الشيك السياحي، الشيك المسطر، الشيك المعتمد وسائل الدفع الحديثة)، الطبعة الخامسة، دار النهضة العربية، القاهرة، 2006.

19. محمد حسين منصور: المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2003.

20. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.

21. محمد مأمون سليمان، التحكيم الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2011.

22. محمد نصر محمد، حجية الدليل الإلكتروني أمام القضاء الجنائي والمدني، مكتبة القانون والاقتصاد، الرياض، السعودية، 2013.

23. مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، مصر، 2000.

24. مصطفى معوان، الإثبات في المعاملات الإلكترونية في التشريعات الدولية: التوقيعات والبصمات الإلكترونية، دار الكتاب الحديث، الجزائر، 2010.

25. ممدوح محمد على مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة بالفقه الإسلامي دار النهضة العربية، مصر، 2005.

26. مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008.

27. مناني فراح، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009.

28. هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية –دراسة مقارنة–، دار الكتب القانونية، مصر، 2015.

29. وسيم شفيق الحجار، الإثبات الإلكتروني، المنشورات الحقوقية، الصادرة ببيروت، 2002.

ثانيا: الرسائل والمذكرات الجامعية

1- رسائل الدكتوراه

1. إبراهيم سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، أطروحة دكتورة الفلسفة في العلوم الأمنية جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

2. آلاء أحمد محمد الحاج علي، التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، فلسطين، 2013.

3. إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، جامعة المنصورة، مصر، 2006/2005.

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

5. ربيع السعدي، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة-1-، 2016/2015.

6. صالح شنين، الحماية الجنائية للتجارة الإلكترونية –دراسة مقارنة–، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان، 2013

7. عباس حفصي، جرائم التزوير الإلكتروني –دراسة مقارنة–، رسالة دكتوراه، جامعة أحمد بن بلة، وهران 1، 2015،

8. عبد الحليم بوقرين، الحماية الجنائية للمعاملات التجارية، أطروحة دكتوراه، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2014.

9. عيسى غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه كلية الحقوق، جامعة عين شمس، مصر، 2006.

2- مذكرات الماجستير

1. خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

2. صلاح عبد الحكيم المصري، متطلبات استخدم التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، رسالة لنيل شهادة الماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2006.

3. لالوش راضية، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع "القانون الدول للأعمال"، كلية الحقوق والعلوم السياسية، جامعة المولود معمري، تيزي وزو، 2012

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

3- مذكرات الماستر

- كواشي ياسمينة، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في ظل القانون، مذكرة مكملة لنيل شهادة الماستر في تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي،أم البواقي، 2017/2016.

ثالثا: المقالات والبحوث العلمية

1. إبراهيم أبو الليل الدسوقي، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المتضررة، بحث مقدم إلى مؤتمر الأعمال الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون، المجلد الخامس، جامعة الإمارات العربية المتحدة، الإمارات، مابين 10 و12 ماي 2003.

2. إبراهيم إسماعيل الربيع، علاء موسى علي نالي، التوثيق الإلكتروني–قرارات التحكيم في التوثيق الإلكتروني–دراسة مقارنة–، مجلة المحقق الحلي للعلوم القانونية والسياسية، بابل، العراق، العدد الأول، 2012.

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

4. بلحسني حمزة، الحماية القانونية والفنية للتوقيع الإلكتروني في مجال البيئة الرقمية، مجلة العلوم القانونية والإدارية، العدد 11، الجزائر، 2015.

5. جفالي حسين، الحماية الجنائية لتوقيع المستهلك الإلكتروني في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الأول، العدد الثالث، الجزائر، د.س.ن.

6. حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدراسات والبحوث، سلطنة عمان، 2006

7. شرف الدين أحمد، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة لمؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية، مصر، 2000.

8. طيب موفق شريف، التوقيع الإلكتروني وحمايته جنائيا في القانون الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد01، العدد01، جامعة أحمد دراية، أدرار–الجزائر، 2017،

9. عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد 11، المركز الجامعي تمنراست(الجزائر)، جانفي 2017.

10. محمد بودالي، التوقيع الإلكتروني، مجلة الإدارة، العدد الثاني، الجزائر، 2003.

11. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، الإمارات، د.س.ن

12. يونس عرب، منازعات التجارة الإلكترونية، الاختصاص والقانون الواجب التطبيق وطرق التقاضي، ورقة عمل مقدمة إلى مؤتمر التجارة الإلكترونية الذي أقامته منظمة الأمم المتحدة، الفترة ما بين 8 و10 تشرين الثالث 2000 بيروت؛ منشور على الموقع : http://www.aeab-low.com

رابعا: النصوص القانونية

1- النصوص القانونية الوطنية

أ- النصوص التشريعية

1. أمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات الجزائري، المعدل والمتمم.

2. قانون رقم 05-10 المؤرخ في 2005/06/20 المعدل والمتمم للأمر 75-58 المؤرخ في 26-90-1975 المتضمن القانون المدني المعدل والمتمم، الجريدة الرسمية رقم 44، لسنة 2005.

3. قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، الصادرة في 16 أوت 2009.

4. قانون رقم 15-04 مؤرخ في: 2015/02/01، يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06، سنة 2015.

ب-المراسيم التنظيمية

- مرسوم تنفيذي رقم 07-162 يعدل ويتمم المرسوم01 / 123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية مؤرخ، في:2007/05/30 الجريدة الرسمية عدد 37.

2- القوانين الأجنبية

1. قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16ديسمبر1996، متوفر عبر الموقع: .http//www.uncitral.org/pdf/arabic...

2. التوجيه الأوربي رقم 93-1999، بشأن الإطار المشترك للتواقيع الإلكترونية، الصادر بتاريخ 1999/12/13.

3. قانون عدد 83 مؤرخ في 9 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية التونسي، المنشور بالرائد الرسمي للجمهورية التونسية، بتاريخ 11 أوت 2000.

4. قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 12 ديسمبر 2001، متوفر عبر الموقع : http//daccess-ods.un.org/tmp/7958533.html.

5. نظام المعاملات الإلكترونية السعودي لسنة 1428هـ.

فهرس

المحتويات

فهرس المحتويات