جامعة 20 أوت 1955 – سكيكدة–

كلية الحقوق والعلوم السياسية

قسم: الحقوق

الحماية الجبائية للتوقيع الإلكتروني

مذكرة مكملة لنيل شهادة الماستر تخصص قانون جنائي

إعداد الطالبة:

بوعيطة وفاء

تحت إشراف الأستاذ:

أ: مقدم عبد الرحيم

" لجنة المناقشة "

1 / أ. منصور رحماني..... رئيسا.

2 / أ. مقدم عبد الرحيم..... مشرفا ومقررا.

3 / أ. شعلال نوال..... ..... مناقشا.

دورة جـوان 2016

إهداء

إلى من بكت العين و تمزق القلب لفراقها، و تألم الجسد و الروح بفقدانها، إلى من كانت تفرح لفرحتي و تحزن لحزني

إلى من كانت ستسعد و تبتهج بنجاحي

إلى من كانت سراجا ينير لي درب الحياة

إلى أمي الحبيبة رحمها الله.

إلى الذي علمني و رباني و صاحب الفضل علي بعد الله عز وجل

إلى من كان سندا و عونا لي طيلة مشواري الدراسي

إلى الغالي أبي.

إلى أختي و أخواتي و زوجة أبي

إلى زوجي و رفيق دربي

إلى التي كان لها الفضل في إكمال مشواري الدراسي بفضل تشجيعاتها و نصائحها لي بعد وفاة والدتي

إلى أمي نظيرة

إلى والدي "مصطفى"

إلى كل أفراد عائلتي و أصحاب الفضل علي من قريب أو بعيد إلى كل الأصدقاء و الزملاء.

شكر و عرفان

بعد شكر الله عز وجل الذي ألهمني الصبر و المقدرة لإتمام هذا العمل المتواضع، أتقدم بأسمى عبارات الشكر و الامتنان إلى أستاذي المشرف "الدكتور مقدم عبد الرحيم" الذي لم يبخل علي بنصائحه و توجيهاته، و لم يدخر جهدا في سبيل إعداد هذا البحث.

كما أتوجه بالشكر الجزيل إلى كل من الأستاذ "الدكتور منصور رحماني" و الأستاذة الفاضلة "شعلال نوال" أعضاء لجنة المناقشة لمساهمتهم في مناقشة مذكرة تخرجي.

كما أتقدم بالشكر إلى جميع أساتذة كلية الحقوق.

شكرا لكم جميعا

مقدمة:

ساهم التطور التكنولوجي في مجال المعلومات والاتصالات في ظهور تقنيات إلكترونية جديدة أهمها الحاسب الآلي وشبكة الأنترنيت، والتي كان لها الفضل في استحداث نوع جديد من المعاملات الإلكترونية التجارية والمالية، وبات من اللازم لإبرام العقود وإتمام التصرفات القانونية على الشبكة العالمية توافر مجموعة من الوسائل والأساليب لمسايرة السرعة في إنجاز هذه العمليات ولضمان الثقة والأمن الذي هو أساس كل التعاملات.

كل هذه المبررات كانت سببا في ظهور تقنية جديدة تعتمد عليها التجارة الإلكترونية لإتمام الصفقات التجارية، وبروز شكل جديد من أشكال التعاقد عن بعد عبر شبكة الأنترنيت تعرف بالتوقيع الإلكتروني، فقد غزت هذه التقنية مختلف جوانب الحياة وارتبطت بمختلف الأنشطة والعمليات الإلكترونية، وأصبحت مختلف القطاعات من بنوك ومؤسسات وإدارات تعتمد في أداء عملها وتقديم خدماتها للجمهور بشكل أساسي على استخدام التوقيع الإلكتروني، والذي بات قوام هذه القطاعات وركيزتها الأساسية لما يتميز به من أمن و خصوصية يعجز التوقيع التقليدي عن توفيرها.

فالتوقيع الإلكتروني باختلاف صوره يسمح بإبرام الصفقات بين طرفين لا تربطهم أية علاقة، ويساعد في تحديد هوية الشخص وتمييزها عن غيرها على عكس التوقيع التقليدي الذي يعجز عن تحقيق ذلك بالنظر إلى الشروط التي يتطلبها، والتي قد تكون تعجيزية في بعض الأحيان، من انعقاد مجلس العقد و ضرورة حضور طرفي العلاقة، والأكثر من ذلك اعتماد البنوك على بطاقات الائتمان في عمليات الدفع بدلا من حمل النقود و التي تعد أحد أهم تطبيقات التوقيع الإلكتروني.

هذا ويحقق التوقيع الإلكتروني أعلى درجات الأمان والسرية التي تتطلبها المعلومات والرسائل الإلكترونية من خلال عملية التشفير التي تضمن أمن و سلامة هذه البيانات والمعلومات من التحريف والتعديل، بحيث لا يمكن للغير الإطلاع عليها إلا من خلال التلاعب في هذه المعلومات عن طريق فض مفاتيح الشفرة أو كسر كلمة السر،

ولذلك أصبح من الضروري اللجوء إلى استخدام تقنية التوقيع الإلكتروني بدلا من التوقيع التقليدي الذي صار عقبة أمام كل هذه التطورات.

ولكن بالرغم من الدور الإيجابي الذي يحققه، والسمات والمزايا التي يتمتع بها التوقيع الإلكتروني في شتى المجالات، فإن الاستخدام المتزايد لهذه التقنية لا ينفي الأضرار والمشاكل التي يتسبب فيها نتيجة إساءة استخدامه على نحو غير مشروع، مما استتبعه ظهور أنماط جديدة من الجرائم لا حصر لها تختلف عن الجرائم التقليدية في عدة جوانب ومن أمثلتها التزوير الإلكتروني.

ومن أجل الحد من خطورة هذه الأفعال سارعت معظم التشريعات في مختلف الدول إلى تجريم هذه الاعتداءات لتوفير الحماية اللازمة للتوقيع الإلكتروني، سواء من خلال تعديل النصوص القانونية التقليدية القائمة لتنطبق على هذا النوع من الجرائم، أو من خلال استحداث نصوص تشريعية خاصة بالتوقيع الإلكتروني تجرم كافة الانتهاكات التي من شأنها زعزعت الثقة ولأمان بهذه التقنية الحديثة.

هذا وترجع أهمية البحث إلى أهمية التوقيع الإلكتروني الذي يعتبر من أهم التقنيات التي أفرزتها التطورات التكنولوجية الحديثة، بالإضافة إلى الدور الفعال الذي يلعبه من خلال تسريع العمليات والصفقات التجارية الإلكترونية بفضل الخصائص والمميزات التي يتصف بها، و تكمن أهمية الدراسة أيضا في ندرة الأبحاث والدراسات المتخصصة في الموضوع، عسى أن يكون هذا البحث المتواضع مرجعا للاستفادة منه في دراسات أخرى، وعلى هذا الأساس تتبلور إشكالية الدراسة التي يمكن طرحها كالتالي: ما مدى استيعاب واحتواء النصوص التقليدية سارية النفاد للجرائم الواقعة على التوقيع الإلكتروني؟ وهل توفر الحماية اللازمة و الضرورية لبعث الثقة والأمان في هذه التقنية الحديثة؟

وفي إطار دراسة هذا الموضوع وللإجابة على هذه الإشكالية الرئيسية تصادفنا جملة من التساؤلات الجزئية نوجزها فيما يلي:

- هل تنطبق النصوص التقليدية الخاصة بالتزوير العادي على جريمة تزوير التوقيع الإلكتروني؟
- هل تكفي النصوص الجزائية التقليدية لحماية التوقيع الإلكتروني؟
- هل الحماية الجنائية للتوقيع الإلكتروني تحتاج إلى نص خاص؟
- ما مدى انطباق جريمة التزوير العادية على التزوير الإلكتروني؟
- هل الحماية الجنائية المقررة في إطار التجريم الخاص بحماية الحق في الحياة الخاصة في إطار المعالجة الآلية كفيلة بحماية التوقيع الإلكتروني؟

ولقد كان الدافع الذي حفزني لبحث هذا الموضوع هو أهمية التوقيع الإلكتروني والذي يعتبر أحد أهم مواضيع الساعة التي يجب التطرق إليها و دراستها حاليا، خاصة مع التطورات السريعة التي تشهدها البشرية في مجال نظم الاتصالات والمعلومات، ولهذا يجب الإلمام بمختلف جوانبه، كما يعود سبب اختياري لهذا الموضوع أيضا إلى القصور الذي تعرفه التشريعات الجنائية الجزائرية فيما يتعلق بالحماية الجنائية للتوقيع الإلكتروني في إطار قانون العقوبات، ويهدف هذا البحث إلى تحقيق ما يلي:

- ❖ تحديد مفهوم التوقيع الإلكتروني من خلال تعريفه وبيان خصائصه، وأهميته ومختلف صوره.
- ❖ تمييز التوقيع الإلكتروني عن التوقيع التقليدي.
- ❖ بيان ضرورة استحداث نصوص جزائية خاصة.
- ❖ تعديل النصوص التقليدية السارية لتستوعب الصور المتطورة للجرائم التقليدية ومنها التزوير الإلكتروني.
- ❖ الوقوف عند القوانين العربية والأجنبية التي تتعلق بحماية التوقيع الإلكتروني ومعرفة مدى مسايرة التشريع الجزائري لها.

وفي إطار دراستي لهذا الموضوع واجهتني مجموعة من الصعوبات يرجع أهمها إلى ندرة الدراسات المتخصصة في هذا المجال خاصة في التشريع الجزائري، وأيضا عدم وجود قانون في الجزائر أو نص تشريعي خاص يوفر الحماية اللازمة للتوقيع الإلكتروني ماعدا

القانون رقم 15-04 المؤرخ في 1 فيفري 2015، والذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، من الصعوبات أيضا ارتباط التوقيع الإلكتروني بما يعرف بتكنولوجيا المعلومات مما أكسبه بعدا تقنيا استدعى معه ضرورة تبسيط بعض المصطلحات التقنية، مثل المعالجة الآلية للمعطيات، السرية المعلوماتية والأمن المعلوماتي وغيرها من المصطلحات.

وللإلمام بجوانب الموضوع اعتمدت في ذلك منهج يجمع بين المقارنة والتحليل، المنهج المقارن من خلال إبراز الحماية الجنائية للتوقيع الإلكتروني في الجزائر ومقارنتها بالتشريعات الأجنبية، مثل التشريع الفرنسي وبعض التشريعات العربية وأهمها التشريع المصري والتونسي، والمنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالحماية الجنائية للتوقيع الإلكتروني العربية منها والأجنبية.

وللإجابة على الإشكالية المطروحة تم تقسيم هذا البحث إلى فصلين:

حيث خصص الفصل الأول لبيان الحماية الجنائية للتوقيع الإلكتروني في إطار جرائم التزوير، وذلك من خلال تناول ماهية التوقيع الإلكتروني من خلال المبحث الأول، بينما تم التطرق إلى مدى تجريم الاعتداء على التوقيع الإلكتروني في المبحث الثاني.

أما الفصل الثاني فتم تخصيصه للحماية الجنائية للتوقيع الإلكتروني في إطار التجريم المقرر لحماية الحق في الحياة الخاصة، والمقسم بدوره إلى مبحثين، يتناول المبحث الأول نظم المعالجة الآلية للمعطيات، والثاني صور التجريم المقررة لحماية نظم المعالجة الآلية للمعطيات.

لأنهي هذا البحث في الأخير بخاتمة تتضمن بعض النتائج و الاقتراحات.

الفصل الأول: الحماية الجنائية للتوقيع الإلكتروني في إطار جرائم التزوير

مع التطور التكنولوجي وظهور ما يسمى بالتجارة الإلكترونية وبروز المعاملات الإلكترونية التي تتم عن طريق التعاقد عن بعد عبر شبكة الانترنيت، ولمواكبة هذا التقدم برز إلى الوجود تقنية إلكترونية جديدة أطلق عليها مصطلح التوقيع الإلكتروني، هذا الأخير دعت إليه الحاجة لاسيما أن التوقيع الكتابي أو التقليدي بات يعرقل سير المعاملات المالية والتجارية واستقرارها والتي أصبحت في الآونة الأخيرة تتم عبر الوسائط الإلكترونية منها الانترنيت.

ولكن نظرا للاعتداءات الكثيرة التي يمكن أن يتعرض لها التوقيع الإلكتروني وخاصة منها التزوير والتقليد، كان من الضروري توفير حماية جنائية له سواء من خلال تطبيق النصوص التقليدية العادية عليه، أو من خلال استحداث نصوص خاصة به وذلك لما له من أهمية كبيرة في حماية الأشخاص من تزوير توقيعاتهم وكذلك لاستقرار المعاملات بين الأفراد.

وللوقوف عند هذه الحماية ومعرفة مدى فعاليتها، وما إذا كان تطبيق النصوص التقليدية يكفي لمواجهة مختلف الاعتداءات التي تعترض التوقيع الإلكتروني، كان لابد من إلقاء الضوء أولا على ماهية التوقيع الإلكتروني (المبحث الأول)، لمعرفة الاعتداءات الواقعة عليه ومدى تجريمها (المبحث الثاني).

المبحث الأول: ماهية التوقيع الإلكتروني :

اختلفت معظم التشريعات في وضع مفهوم موحد للتوقيع الإلكتروني، حيث استقل كل تشريع في كل دولة أو منظمة بتعريفه سواء من خلال قوانين التجارة الإلكترونية، أو من خلال إفراده بقانون خاص هو قانون التوقيع الإلكتروني، وذلك إما استنادا إلى الوظيفة التي يقوم بها، أو بالنظر إلى تطبيقاته المختلفة، أو بالرجوع إلى الوسيلة التي يتم بها التوقيع الإلكتروني.

إلا إن كل هذا الاختلاف لا ينفي الاهتمام الذي حظي به التوقيع الإلكتروني من خلال تطرق جل هذه التشريعات إلى مفهومه وخصائصه (المطلب الأول)، وبيان صوره المختلفة (المطلب الثاني).

المطلب الأول: مفهوم التوقيع الإلكتروني و خصائصه.

أشرت فيما سبق أن هناك تعريفات مختلفة للتوقيع الإلكتروني حسب الزاوية أو المنظور الذي ينظر به إليه، ولهذا تعددت المفاهيم (الفرع الأول)، ولكن المعنى واحد واختلفت سماته ومميزاته (الفرع الثاني)، وكثرت تطبيقاته (الفرع الثالث).

الفرع الأول: مفهوم التوقيع الإلكتروني.

يتناول في هذا الفرع تعريف التوقيع الإلكتروني حسب المنظمات الدولية، والتشريعات الوطنية والفقه، وأهمية وشروط صحته، وحجيته وتميزه عن التوقيع الكتابي.

أولا- تعريف التوقيع الإلكتروني:

1- تعريف المنظمات الدولية للتوقيع الإلكتروني:

أ - تعريف قانون الأونيسترال النموذجي للتوقيع الإلكتروني:

عرف قانون الأونيسترال النموذجي التوقيع الإلكتروني من خلال المادة 2/ أ بالنص على أن "التوقيع الإلكتروني يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البينات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[1]، وكما هو

[1] أنظر: قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع، منشورات الأمم المتحدة، نيويورك، 2002.

واضح من النص السابق لم يقيد قانون الأونيسترال مفهوم التوقيع الإلكتروني، بل إن هذا يمكن أن يستوعب أية تكنولوجيا تظهر في المستقبل تفي بإنشاء توقيع إلكتروني[1].

ب- تعريف التوجيه الأوروبي للتوقيع الإلكتروني:

حددت المادة الثانية من التوجيه الأوروبي رقم 1999/93 مستويين للتوقيع الإلكتروني، الأول عرفته على انه "معلومة تأخذ شكلا إلكترونيا ترتبط منطقيا ببيانات أخرى إلكترونية، و التي هي بمثابة أسلوب المصادقة" وهو التوقيع الإلكتروني البسيط، والثاني هو التوقيع الإلكتروني المتقدم أو المسبق الذي يجب أن يستوفي شروط معينة[2].

2- تعريف التشريعات الوطنية للتوقيع الإلكتروني:

عرفت المادة 4/1316 من القانون المدني الفرنسي التوقيع الإلكتروني على أنه "التوقيع الضروري لإتمام تصرف أو عقد قانوني يكشف عن هوية الشخص الذي وضع التوقيع، كما يعلن عن رضاء الأطراف بالالتزامات الناشئة عنه، وإذا قام به موظف عام، فإنه يضفي الرسمية للعقد القانوني"[3].

من خلال هذا النص يتبين لنا أن المشرع الفرنسي لم يفرق بين التوقيع الإلكتروني والتقليدي، حيث يكتسب كل منهما نفس الحجية القانونية في الإثبات، طالما هذا التوقيع يميز صاحبه، ويتم بإجراءات آمنة تضمن سرية البيانات الخاصة بالتوقيع، وهو بذلك يكون قد وسع من مفهوم التوقيع[4].

أما بالنسبة للمشرع الجزائري فقد أصدر القانون رقم 04- 15 الصادر سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، والذي عرف فيه من خلال

---

[1] أنظر: غسان ربضي (عيسى)، **القواعد الخاصة بالتوقيع الإلكتروني**، ط 2، دار الثقافة، الأردن، 2012، ص 50.

[2] أنظر: OLIVIER D'AU ZON, le droit de commerce électronique, Héricy, France, 2004, P 68.

[3] أنظر: OLIVIER D'AUZON, ibid, P 76.

[4] أنظر: بلقاسم حامدي، **ابرام العقد الإلكتروني**، دكتوراه، كلية الحقوق، جامعة الحاج لخضر باتنة، 2014، ص211.

نص المادة الثانية التوقيع الإلكتروني على أنه :"بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق"[1].

كما تجدر الإشارة إلى أن المشرع الجزائري قبل صدور القانون رقم 15-04 الصادر سنة 2015 اكتفى في نص المادة 2/327 من القانون رقم 05-10 الصادر في 20 جوان سنة 2005 بالاعتراف بالتوقيع الإلكتروني، ولم يضع تعريف خاص به[2].

وعرفت المادة الأولى فقرة "أ" من القانون المصري رقم 04-15 لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني، التوقيع الإلكتروني بأنه: "ما يوضع على محرر إلكترون ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، و يكون له طابع متفرد يسمح بتحديد شخص صاحب التوقيع ويميزه عن غيره"[3].

ويتضح من خلال النص أن المشرع المصري لم يحدد بدقة طبيعة التوقيع الإلكتروني على عكس قانون الأونيسترال والتوجيه الأوروبي، والمشرع الجزائري الذي بين أن التوقيع الإلكتروني عبارة عن بيانات في شكل إلكتروني مضافة لرسالة المعلومات[4].

3- تعريف الفقه للتوقيع الإلكتروني:

تعددت التعريفات الفقهية للتوقيع الإلكتروني، حيث يعرفه بعض الفقهاء على أنه: "كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطا وثيقا بالتصرف القانوني، تسمح بتمييز شخص صاحبها، وتحيد هويته، و تتم دون

---

[1] أنظر: القانون رقم 04/15 المؤرخ في 1 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسمية عدد 06، المؤرخة في 10 فبراير 2015.

[2] أنظر: صالح شنين، **الحماية الجنائية للتجارة الإلكترونية**، دكتوراه، كلية الحقوق، جامعة أبو بكر بلقا يد تلمسان، 2012، ص 52.

[3] أنظر: كميني خميسة، **الإثبات بالكتابة في الشكل الإلكتروني**، مذكرة التخرج لنيل شهادة المدرسة العليا للقضاء، 2007، ص 16.

[4] أنظر: براهمي حنان، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، دكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة، 2014، ص 140.

غموض عن رضاه بهذا التصرف القانوني"[1]، وهذا التعريف يرتكز أساسا على ضرورة قيام التوقيع الإلكتروني بالوظائف التقليدية للتوقيع[2].

واتجه فريق آخر إلى تعريفه على أنه : "جزء صغير مشفر من بيانات يضاف إلى رسالة إلكترونية، فهو جزأ من الرسالة ذاتها يشفر ويرسل مع الرسالة، ليتم التوثيق من صحة الرسالة بفك التشفير وانطباق محتواه على الرسالة".

ومفاد هذا التعريف أن التوقيع الإلكتروني عبارة عن بيانات كما أشرنا سابقا، هذه البيانات تعتمد أساسا على نظام يسمى بنظام التشفير، كما تؤدي وظيفة هامة هي التوثيق[3].

ثانيا- التمييز بين التوقيع الإلكتروني و التوقيع الكتابي:

أصبح التوقيع التقليدي يقف عقبة أمام ظهور الوسائل الحديثة وانتشارها، والسبب في ذلك أنه لا يستطيع مسايرة ومواكبة السرعة الناتجة عن معالجة المعلومات معالجة إلكترونية، فلا يمكن تصوره إلا على مستند ورقي[4].

كما أن إتاحة استخدام التوقيع الإلكتروني تدعم التحول إلى عالم اللاورق يأمن فيه كل متعامل على أمواله ومصالحه، بالإضافة إلى رفع كفاءة العمل الإداري والمساعدة على الارتقاء[5].

كل هذه العوامل والأسباب أدت إلى ظهور فجوة كبيرة بين التوقيع الكتابي والتوقيع الإلكتروني، حيث يختلف كل منهما عن الآخر من عدة نواحي أهمها:

---

[1] أنظر: بن سعيد (لزهر)، **النظام القانوني لعقود التجارة الإلكترونية**، دار هومة، الجزائر، 2012، ص 156.

[2] أنظر: عبد الحميد (ثروت)، **التوقيع الإلكتروني**، دار الجامعة الجديدة، الاسكندرية، 2007، ص 50.

[3] أنظر: براهمي حنان، مرجع سابق، ص 142.

[4] أنظر: سعيد الغريب (فيصل)، **التوقيع الإلكتروني و حجيته في الإثبات**، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005، ص 213.

[5] أنظر: أمير فرج (يوسف)، **التوقيع الإلكتروني**، دار المطبوعات الجامعية، الاسكندرية، 2008، ص 9.

1. من حيث الشكل: التوقيع الإلكتروني هو نتاج حركة يد الموقع في صورة إمضاء أو بصمة عبر وسيط مادي يتم عبر وسيط إلكتروني عن طريق جهاز الحاسب الآلي.

2- من حيث الخصائص المادية: التوقيع الإلكتروني عبارة عن بيانات مدونة على وسائط إلكترونية و للقاضي سلطة واسعة في تقدير مدى قيمة الدليل الإلكتروني المقدم أمامه[1].

3- من حيث صورة التوقيع: صورة التوقيع في الشكل الكتابي تقتصر على الإمضاء وبصمة الختم و بصمة الإصبع، بينما التوقيع الإلكتروني يمكن أن يتخذ صورة حرف أو رقم أو رمز أو إشارة أو حتى أصوات، بشرط أن يكون لها طابع منفرد.

4- من حيث الوسيط أو الدعامة: فالتوقيع الكتابي يتم عبر وسيط مادي، أي دعامة ورقية، أما التوقيع الإلكتروني يتم عبر وسيط إلكتروني عن طريق أجهزة الحاسب الآلي وعبر الانترنت.

5- من حيث الوظيفة: التوقيع الكتابي يؤدي دورين أساسين وفي الغالب ثلاثة أدوار هي: تمييز شخصية صاحبه و تحديد هويته والتعبير عن قبوله، أما التوقيع الإلكتروني فيناط به خمسة وظائف تتمثل أساسا في تمييز شخصية صاحب التوقيع وتحديد هويته والتعبير عن إرادته في القبول، والثقة في مضمون المحرر الإلكتروني، ودلالته على حضور صاحب التوقيع[2].

6- من حيث إمكانية التزوير: فالتوقيع الإلكتروني علم وليس فن وبالتالي يصعب تزويره، بينما التوقيع الكتابي فهو عبارة عن رسم يقوم به الشخص، وبالتالي فهو فن وليس علم ومن هنا يسهل تزويره[3].

---

[1] أنظر: بلقا سم حامدي، مرجع سابق، ص 209.

[2] أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 51 وما بعدها.

[3] أنظر: أمير فرج (يوسف)، مرجع سابق، ص 15.

ثالثا- أهمية التوقيع الإلكتروني:

إن انعدام الثقة في المعاملات التي تتم عبر الشبكات الإلكترونية ومنها التجارة الالكترونية أدى إلى ظهور تقنية التوقيع الإلكتروني، وذلك من أجل رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين عبر شبك الانترنيت مما يصعب على أي شخص مهما بلغت قدرته من الاطلاع، أو تعديل أو تحريف الرسائل.

كما يسهم التوقيع الإلكتروني في تحديد هوية كل من المرسل والمستقبل إلكترونيا والحفاظ على سرية المعلومات والتأكد من شرعية مصدر أو مرسل المستند[1].

هذا وتظهر أهمية التوقيع الإلكتروني في عملية تحديد شخصية المتعاقدين وذلك من خلال الدور البارز الذي يلعبه في التعاقد عن بعد عبر الانترنيت، وفي هذه الحالة يتعين على صاحب الموقع تحديد الأشخاص الذين يستخدمون الموقع في حالة ما إذا كان طرفي العلاقة لا يملكان المواقع التي يتم من خلالها بث المعلومات، وذلك في تحديد شخصية طرفي العمليات العقدية[2].

كما يعتبر التوقيع الإلكتروني تعبير عن رضاء الشخص الموقع بمضمون المحرر ويؤكد التزامه بمضمونه وإقراره له[3]، ومن ناحية أخرى وسيلة تكسب المستندات والوثائق الإلكترونية قوتها في الإثبات[4].

---

[1] أنظر: العاني إيمان، **البنوك التجارية و تحديات التجارة الإلكترونية**، ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، 2006، ص 112.

[2] أنظر: بن عبد الله بن معيض العبيدي (خالد)، **الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية**، ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، 2009، ص 162.

[3] أنظر: بلقاسم حامدي، مرجع سابق، ص 222.

[4] أنظر: العاني إيمان، مرجع سابق، ص 112.

رابعا- شروط صحة التوقيع الإلكتروني:

يتطلب في التوقيع الإلكتروني لمنحه الحجية القانونية الكاملة في الإثبات توفر مجموعة من الشروط نصت عليها أغلب القوانين الخاصة بالتوقيع الإلكتروني يمكن إجمالها فيما يلي:

1- أن يكون متميزا و مرتبطا بصاحبه:

هذا الشرط يؤكد نية الشخص الموقع في قبوله لمضمون المحرر ونيته في الالتزام به، حيث أن التوقيع الإلكتروني وعلى مختلف صوره يعتبر علامة خاصة ومميزة لصاحبه وحده ودون غيره إذا ما تم إنشاؤه بصورة صحيحة[1].

2- سيطرة الموقع على التوقيع:

سيطرة الموقع على التوقيع تكون نتيجة سيطرته على الوسيط الإلكتروني المدون عليه منظومة إحداث التوقيع الإلكتروني، وذلك لضمان انفراد صاحبه به، ولمنع الغير من استعماله وفك رموزه ومن ثم التوقيع بدلا عنه[2].

3- سلامة الوثيقة من التغيير:

هذا الشرط يتناول مسألة هامة وضرورية هي سلامة الوثيقة الموقعة من أي تعديل قد يطرأ عليها بعد توقيعها[3]، فالتأكد من سلامة المحتوى يضمن الثقة خاصة في حالة انعدام تعاملات أو علاقات سابقة بين الأطراف.

---

[1] أنظر: محمد عبيدات (لورنس)، **إثبات المحرر الإلكتروني**، ط1، دار الثقافة، عمان، 2009، ص 131.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **التوقيع الإلكتروني في النظم القانونية المقارنة**، دار الفكر الجامعي، الاسكندرية، د س، ص 444.

[3] أنظر: محمد عبيدات (لورنس)، مرجع سابق، ص 131.

ونظرا لما تحمله التكنولوجيا الحديثة والانترنيت من مخاطر[1]، وعلى هذا الأساس يستلزم أن يكون من الميسور لصاحب التوقيع أن يعلم بأي تعديل أو تغيير في منظومة إحداث التوقيع الإلكتروني[2].

خامسا. حجية التوقيع الإلكتروني في الإثبات:

اعتد المشرع الجزائري بالتوقيع الإلكتروني في نطاق جميع المعاملات، فمن خلال الرجوع إلى نص المادة 327 من القانون المدني يتبين لنا أن المشرع قد أخذ بمبدأ التكافؤ الوظيفي بين الإثبات التقليدي والإثبات الإلكتروني، وبما أن القانون المدني هو الشريعة العامة فليس هناك ما يمنع قبول استعمال التوقيع الإلكتروني في شتى أنواع المعاملات المدنية والتجارية، والإدارية ما لم يوجد نص خاص يقيد ذلك[3].

الفرع الثاني: خصائص التوقيع الإلكتروني.

يتميز التوقيع الإلكتروني بسمات و مميزات تميزه عن التوقيع التقليدي، وهذا ما سيتم التطرق إليه من خلال هذا الفرع.

أولا- تحديد شخص الموقع و بيان هويته و تميزه عن غيره من الأشخاص[4]، أي أنه يعتبر علامة شخصية، مما ينبغي تجنب أي تلاعب أو تحايل لأن أي محاولة لتغيير رمز من الرموز المشكلة للتوقيع الإلكتروني على اعتبار أنه يقوم على معادلات رياضية يكون قابلا للكشف، وهذا ما يجعل التوقيع الإلكتروني أقل عرضة للتزوير من التوقيع التقليدي[5].

---

[1] أنظر: براهمي حنان، مرجع سابق، ص 156.

[2] أنظر: بيومي حجازي (عبد الفتاح)، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص 445.

[3] أنظر: بلقاسم حامدي، مرجع سابق، ص 256.

[4] أنظر: بن سيف الغافري (حسين)، الجرائم الواقعة على التجارة الإلكترونية، سلطنة عمان، 2006،ص 9، موقع المنشاوي للدراسات و البحوث www.minshawi.com.

[5] أنظر: سمية ديمش، **التجارة الإلكترونية حقيقتها و واقعها في الجزائر**، ماجستير، كلية العلوم الاقتصادية والتسيير، جامعة منتوري قسنطينة، 2010، ص 87 و ما بعدها.

ثانيا- التوقيع الإلكتروني يحقق الأمان والخصوصية والسرية[1]، فتقنية التشفير أتاحت إمكانية حماية البيانات المرسلة من أي تعديل أو تخريب ومنعت كل الأشخاص غير المخول لهم من التطفل على محتو الرسائل المتبادلة، خاصة مع انعدام الثقة في المعاملات التي تجري عن طريق الانترنيت ووسائل الاتصال الحديثة.

ثالثا- يسمح التوقيع الإلكتروني بإبرام صفقات بين طرفين متعاقدين يتواجدان على بعد آلاف الكيلومترات دون حاجة إلى انعقاد مجلس العقد وحضورهم شخصيا، وكل هذا من أجل تطوير وتسهيل التجارة الإلكترونية.

رابعا- توفر تقنية التوقيع الإلكتروني للأفراد حرية كاملة لاختيار نوع التوقيع الإلكتروني الذي يلائمه سواء كان توقيع كودي، أو باستعمال الخواص البيو مترية[2].

خامسا- التوقيع الإلكتروني يتكون من عناصر منفردة وسمات ذاتية خاصة بالموقع تتخذ شكل حروف أو أرقام أو رموز أو إشارات وغيرها[3].

الفرع الثالث: تطبيقات التوقيع الإلكتروني.

يتم التطرق من خلال هذا الفرع إلى أهم المجالات والتطبيقات التي يستخدم فيها التوقيع الإلكتروني، والتي تعود أساسا الى بطاقات الدفع الالي (الائتمان) ومعاملات التجارة الالكترونية.

أولا- بطاقة الائتمان:

ينظر إلى بطاقة الائتمان من الناحية القانونية على أنها عقد تتعهد بموجبه الجهة المصدرة لها لمصلحة شخص معين بفتح اعتماد لصالحه في حدود مبلغ معين، وذلك من

---

[1] أنظر: بن غانم العبيدي (أسامة)، **حجية التوقيع الإلكتروني في الإثبات**، المجلة العربية للدراسات الأمنية و التدريب، المجلد 28، عدد 56، ص 147.

[2] أنظر: سمية ديمش، مرجع سابق، ص 88.

[3] أنظر: بن سيفالغافري (حسين)، مرجع سابق، ص 9.

أجل الوفاء بثمن السلع و الخدمات التي يتحصل عليها حاملها من المحال التجارية والتي تربطها علاقة بالجهة المصدرة للبطاقة[1]، كما أنها بطاقة بلاستيكية ذات شكل مستطيل تحتوي على وجهين، يحمل الوجه الأول شعار واسم المؤسسة المصدرة وبيانات أخرى متعلقة بصاحب البطاقة، بينما يحتوي الوجه الثاني على التوقيع الإلكتروني الخاص بصاحب البطاقة ومجموعة من الأرقام والرموز[2].

هذا ويستعمل الرمز السري لتعريف وإمضاء العمليات الحسابية عبر شاشة الكمبيوتر من غير طبعها على الورق، ثم صبها بعد ذلك في دفاتر إلكترونية ليتم معالجتها بعد ذلك من طرف مصالح المحاسبة، ولا يتوقف الأمر عند هذا بل إن موظفو البنك يستعملون البطاقة مع الرمز السري لإمضاء أوامر الدفع العالمية للعملاء، مع العلم أن هذا الرمز يبقى مجهولا لا يعلم به سوى العميل الذي يلتزم به سرا، والذي يعتبر بديلا للتوقيع اليدوي[3].

ثانيا- التجارة الإلكترونية:

تعرف التجارة الإلكترونية على أنها أعمال مرتبطة بنشاطات تجارية يتم إنجازها باستخدام تقنيات متطورة توفرها ثروة المعلومات والاتصالات، حيث تشمل تبادل المعلومات إلكترونيا وإبرام العقود[4]، والذي يتم عن بعد دون الحضور المادي للأطراف أو تمثيلهم وذلك من خلال تبادل المعلومات عبر وسيط غير مادي.

وتدور الفكرة الرئيسية للتجارة الإلكترونية حول تجمع البائعين أو مقدمي الخدمات في معارض أو مراكز تجارية مفترضة وهي – المراكز التجارية الافتراضية– خدمة إلكترونية يتم

---

[1] أنظر: سامي حميد الجادر (عذبة)، **العلاقة التعاقدية المنبثقة عن استعمال بطاقة الائتمان**، ماجستير، كلية العلوم القانونية، جامعة الشرق الأوسط عمان، 2008، ص 28.

[2] أنظر: Mohammed Alisalem, Abbas talibrozoqi, The Legal basis For the protection of credit card Fraud ,

مجلة المحقق للعلوم القانونية و السياسية، العدد 2، 2015، ص 115.

[3] أنظر: محمد عيد نصيرات (علاء)، **حجية التوقيع الإلكتروني في الإثبات**، ط1، دار الثقافة، عمان، 2005، ص 44 و ما بعدها.

[4] أنظر: العاني إيمان، مرجع سابق، ص 52.

الدخول إليها عبر شبكة الانترنيتو تنقسم إلى قسمين، قسم عام متاح للجميع يتم الدخول إليه دون إتباع إجراءات معينة، والقسم الثاني مخصص للشراء و الذي يتم من خلال إتباع إجراءات معينة للتأكد من شخصية و جدية البائع، و التي تتمثل في إدخال رقم سري أو شفرة أو كود أو كلمة سر محددة[1].

المطلب الثاني: صور التوقيع الإلكتروني.

لمواكبة التطورات التقنية الحديثة ظهرت أشكال متعددة ومتنوعة للتوقيع الإلكتروني، يتخذ كل نوع منها شكلا معينا وفق إجراءات خاصة، و كما تتمتع كل صورة بمميزات وخصائص تميزها عن غيرها و بدرجة معينة من الثقة والأمان، لا تخلو أيضا من عيوب وصعوبات تعترض استعمالها.

ومن هذه الصورما يتم عن طريق التوقيع بخط اليد على شاشة الحاسب الآلي (الفرع الأول)، ومنها ما يقوم على تكنولوجيا البصمات والخواص الحيوية والطبيعية (الفرع الثاني)، وهناك من تعتمد على نظام التشفير (الفرع الثالث)، و البعض الآخر يعتمد على البطاقة الممغنطة المقترنة بالرقم السري (الفرع الرابع).

الفرع الأول: التوقيع بالقلم الإلكتروني.

إن التوقيع بالقلم الإلكتروني يختلف عن باقي صور التوقيع الإلكتروني من عدة زوايا سواء من خلال طريقة عمله، أو من خلال السمات التي يتصف بها، أو المشكلات التي يتسبب فيها و هذا ما سيتم التطرق إليه من خلال هذا الفرع.

أولا. طريقة عمل هذه التقنية:

التوقيع بالقلم الإلكتروني يتم بطريقتين، إما عن طريق نقل التوقيع المحرر بخط اليد بواسطة التصوير بالماسح الضوئي إلى الملفالمراد إضافة هذا التوقيع إليه لإكسابه الحجية

[1]أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 88.

اللازمة، أو عن طريق التوقيع مباشرة بخط اليد على شاشة الحاسب الآلي[1]عن طريق استخدام قلم إلكتروني حسابي يتميز بإمكانية الكتابة على شاشة الحاسب الإلكتروني، وهي نفس الخاصية التي تقوم عليها التوقيعات التقليدية الخطية[2].

وعن طريق برنامج خاص يتم التحقق من صحة التوقيع بالاستناد إلى حركة هذا القلم والأشكال التي يتخذها و غيرها من السمات الخاصة بالتوقيع الخاص بالموقع، والذي سبق تخزينه بالحاسب الآلي[3]،وهو بذلك يقوم بوظيفتين أساسيتين: تتمثل الأولى في خدمة التقاط التوقيع، والثانية خدمة التحقق من صحة التوقيع[4].

ثانيا- خصائص و عيوب التوقيع بالقلم الإلكتروني:

هذه الطريقة توفر مزايا لا يمكن إنكارها وذلك نظرا لمرونتها وسهولة استعمالها، فمن خلالها يتم تحويل التوقيع التقليدي عبر أنظمة معالجة المعلومات إلى الشكل الإلكتروني[5]، وفي مقابل ذلك تعترض التوقيع بالقلم الإلكتروني عقبات ومشاكل أبرزها ضرورة توفير جهاز كمبيوتر بمواصفات خاصة من أجل التقاط التوقيع والتأكد من صحته ومطابقته للتوقيع المخزن بالذاكرة[6]،كاحتوائه على وحدة القلم الإلكتروني والشاشة الحساسة، إضافة إلى ندرة وجوده وغلاء ثمنه[7].

كما تتسبب هذه الصورة في مشكلة أخرى تتمثل في إثبات الصلة بين التوقيع الإلكتروني ورسالة البيانات والتي تعتبر شرط جوهري للاعتراف بحجية التوقيع الإلكتروني،

---

[1]أنظر: أمين الرومي (محمد)، **النظام القانوني للتوقيع الإلكتروني**، دار الكتب القانونية، مصر، 2008، ص 45.

[2]أنظر: سعيد أحمد إسماعيل (محمد)، **أساليب الحماية القانونية لمعاملات التجارة الإلكترونية**، ط1، منشورات الحلبي الحقوقية، لبنان، 2009، ص 270.

[3]أنظر: بيومي حجازي (عبد الفتاح)، **النظام القانوني للتوقيع الإلكتروني**، دار الكتب القانونية، مصر، 2007، ص 399.

[4]أنظر: غسان ربضي (عيسى)، مرجع سابق، ص 64.

[5]أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 55.

[6]أنظر: براهمي حنان، مرجع سابق، ص 149.

[7]أنظر: غسان ربضي (عيسى)، مرجع سابق، ص 55 و ما بعدها.

وكل ذلك نتيجة غياب تقنية توفر الثقة في قيام هذه الرابطة أو الصلة، فمن السهل على المرسل إليه الاحتفاظ بنسخة من صورة التوقيع التي وصلت إليه على رسالة البيانات وإعادة وضعها على وثيقة إلكترونية أخرى مدعيا أنه صاحب التوقيع الفعلي[1].

الفرع الثاني: التوقيع البيو متري.

يتناول في هذا الفرع التوقيع البيو متري القائم على الخواص الفيزيائية والطبيعية للإنسان، وسماته ومميزاته إضافة إلى العيوب التي تعتريه.

أولا- طريقة عمل التوقيع البيو متري:

هذا النظام يعتمد بالأساس على الصفات و الخواص الفيزيائية و الطبيعية و السلوكية للإنسان، والتي يفترض اختلافها من شخص لآخر، ومن أمثلة هذه الخواص البصمة الشخصية، وبصمات قزحية العين، وخواص اليد البشرية، و بصمات أو نبرة الصوت والشفاه وغيره من الصفات الجسدية والسلوكية.

هذه الخواص يتم تخزينها على جهاز الحاسب الآلي عن طريق ما يسمى بنظام التشفير، وفي حالة التحقق من صحة التوقيع يتم فك التشفير ومطابقة صفات الشخص المستخدم للتوقيع الإلكتروني مع الصفات المخزنة على الحاسب الآلي[2].

ثانيا- مميزات التوقيع البيو متري:

يتميز التوقيع البيو متري أو كما يسميه البعض التوقيع باستخدام البصمة الإلكترونية بعدة مزايا أهمها:

---

[1] أنظر: أمين الرومي (محمد)، مرجع سابق، ص 46.

[2] أنظر: سعيد الغريب (فيصل)، مرجع سابق، ص 231.

1- أن النظام البيو متري القائم على الخصائص الشخصية لا يعتمد على المفاتيح السرية، مما يسمح بالتغلب على مشاكل الأرقام و كلمات السر مثل النسيان أو التزوير أو السرقة[1].

2- يعتبر التوقيع بالبصمة الإلكترونية أكثر أمنا و ثقة من استخدام التشفير، فهو إن كان يمنع الغير من الاطلاع على محتوى الرسالة الإلكترونية فهو بالمقابل لا يمكنه منع الغير من العبث بها.

3- التوقيع بالبصمة الإلكترونية لا يترك مجالا للمرسل للتنكر للمعلومات التي أرسلها[2].

4- اختلاف الخواص المميزة لكل شخص تجعل من التوقيع الإلكتروني وسيلة موثوق بها، مما يسمح باستخدامه في إقرار التصرفات القانونية المبرمة عبر وسيط إلكتروني[3].

ثالثا- المشاكل و العقبات التي تعترض التوقيع البيو متري:

1- التوثيق البيو متري يمكن مهاجمته و نسخه من طرف قراصنة الحاسب الآلي عن طريق فك التشفير الخاص به، بالإضافة إلى افتقاره إلى السرية والأمن بسبب توحيد الشركات القائمة على هذا النظام لنظم عملها[4].

2- هذا النوع من التوقيع يحتاج إلى استثمارات ضخمة لتمكين مستخدمي الشبكة الإلكترونية من استخدام الخصائص الذاتية لشخص الموقع في التوقيع الإلكتروني[5].

---

[1] أنظر: سعيد أحمد إسماعيل (محمد)، مرجع سابق، ص 266.

[2] أنظر: أبو مارية (علي)، **التوقيع الإلكتروني و مدى قوته في الإثبات**، مجلة جامعة الخليل للبحوث، مجلد 5، عدد 2، فلسطين،2010، ص 110 و ما بعدها.

[3] أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 61.

[4] أنظر: بيومي حجازي (عبد الفتاح)، **النظام القانوني للتوقيع الإلكتروني**، مرجع سابق، ص 399.

[5] أنظر: فرج يوسف (أمير)، مرجع سابق، ص 19.

3- هذا النوع من التوقيع يمكن تزويره عن طريق ارتداء عدسات لاصقة تصمم عن طريق الكمبيوتر، بحيث تطابق رسمة قزحية العين للشخص المراد انتحال شخصيته، كما يمكن تسجيل بصمة الصوت ثم إعادة التسجيل بعد ذلك والدخول إلى النظام بكل سهولة، أما بصمة الإصبع فيمكن تزويرها عن طريق وضع مادة بلاستيكية مطابقة تماما لبصمة أصابع الشخص صاحب التوقيع[1].

الفرع الثالث: التوقيع الرقمي

يتم التطرق في هذا الفرع إلى أهم صورة من صور التوقيع الإلكتروني وهو التوقيع الرقمي القائم على نظام التشفير.

أولا- المقصود بالتوقيع الرقمي:

التوقيع الرقمي عبارة عن أرقام مطبوعة تسمى "HASH" لمحتوى المعاملة التي يتم التوقيع عليها[2]، ولذلك يفرق البعض بينه وبين التوقيع الإلكتروني الذي يتشكل من سلسلة من الأرقام الحسابية من مجموعها يتكون التوقيع الإلكتروني الرقمي[3].

هذه الأرقام ترتبط برسالة البيانات فتحولها من رسالة مقروءة إلى رسالة غير مقروءة لا يمكن فك تشفرها إلا الشخص الذي لديه المفتاح الخاص بهذا التشفير[4]، هذ ويوجد نوعان من المفاتيح، مفتاح عام يسمح لأي شخص بقراءة البيانات عبر الانترنيت دون

---

[1] أنظر: أمين الرومي (محمد)، مرجع سابق، ص 47.

[2] أنظر: بلقاسم حامدي، مرجع سابق، ص 215.

[3] أنظر: أمين الرومي (محمد)، مرجع سابق، ص 15.

[4] أنظر: حنان مليكة، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم 4 الصادر بتاريخ 2009/2/25، مجلة جامعة دمشق للعلوم الاقتصادية و القانونية، مجلد 26، عدد 2، 2010، ص 562.

إمكانية إدخال أي تعديل عليها ومفتاح خاص بصاحب رسالة البيانات[1]، يقوم بوظيفة التشفير على عكس المفتاح العام الذي يستخدم لفك التشفير.[2]

ويجب عدم الخلط بين تشفير التوقيع و تشفير الرسالة، إذ أن كل منهما يمكن تشفيره إلا أن تشفير الرسالة الإلكترونية يشملها بأكملها بما في ذلك التوقيع.[3]

ثانيا- مزايا التوقيع الرقمي:

1- هذه الطريقة تحقق أعلى درجات الثقة والأمان[4]، كما تؤدي إلى التحقق من هوية الموقع وأن الرسالة الموقعة منه تنسب إليه ولا يمكنه إنكارها وذلك نتيجة الارتباط التام بين المفتاح العام والخاص.

2- التوقيع الرقمي يضمن عدم التدخل في مضمون التوقيع أو المستند الذي يرتبط به.

3- التوقيع الرقمي يحقق الارتباط بين المستند الكتابي و التوقيع الوارد عليه، كما يكفل سرية المعلومات التي تتضمنها المستندات الإلكترونية، حيث لا يمكن قراءتها إلا ممن أرسلت إليه وباستخدام المفتاح العام للمرسل.[5]

ثالثا- عيوب التوقيع الرقمي:

يبقى التوقيع الرقمي كغيره من صور التوقيع الإلكتروني عرضة لعمليات الاحتيال والتزوير والقرصنة والاختراق، وذلك عن طريق كسر المفتاح الخاص برسالة البيانات والذي يتم صياغة معادلاته على ضوء المفتاح العام، وبالتوصل إلى معرفة المفتاح الخاص

---

[1] أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 215.

[2] أنظر: بيومي حجازي (عبد الفتاح)، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، ص 400.

[3] أنظر: بلقاسم حامدي، مرجع سابق، ص 215.

[4] أنظر: بن غانم العبيدي (أسامة)، مرجع سابق، ص 154.

[5] أنظر: بلقاسم حامدي، مرجع سابق، ص 215.

يمكن بسهولة التغيير في مضمون رسالة البيانات، سواء من جانب مصدرها، أو من جانب صاحب التوقيع.[1]

الفرع الرابع: التوقيع بواسطة الرقم السري و البطاقة الممغنطة.

أولا-المقصود بالتوقيع السري:

انتشر التعامل بالبطاقات الممغنطة في مجال المعاملات التيتستخدم في السحب النقدي من خلال بطاقات الصرف الآلي لسداد ثمن بعض السلع والخدمات، أو للقيام بعمليات دفع عبر الانترنيت، وذلك نظرا لاحتوائها على رقم سري لا يعرفه إلا صاحبها[2]، ويستخدم هذا التوقيع في التعاملات البنكية والمراسلات الإلكترونية التي تتم بين التجار أو بين الشركات وأبرز مثال على ذلك بطاقة الائتمان[3]، التي تحتوي على بيانات عبارة عن الجهة التي أصدرتها واسم صاحبها ورموز وأرقام عند إدخالها لدى الصراف الآلي لقراءتها[4]، ويمكن لأي شخص أن يستعملها فلا تستلزم أن يمتلك الشخص جهاز حاسب آلي، أو أن يكون جهازه متصلا بشبكة الانترنيت.

هذا ويتم استخدام البطاقة عن طريق قيام حاملها بعمليتين متعاصرتين، إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل في فتحة في جهاز الصراف الآلي وإدخال الرقم السري المخصص له[5].

---

[1] أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 64.

[2] أنظر: محمد عبيدات (لورانس)، مرجع سابق، ص 149.

[3] أنظر: عبد الحميد نبيه (نسرين)، **الجانب الإلكتروني للقانون التجاري**، منشأة المعارف، الاسكندرية، 2008، ص 343.

[4] أنظر: فرج يوسف (أمير)، **بطاقة الائتمان و الحماية الجنائية لها**، دار المطبوعات الجامعية، الاسكندرية، 2008، ص 172 و ما بعدها.

[5] أنظر: عبد الحميد (ثروت)، مرجع سابق، ص 56 و ما بعدها.

ثانيا- مميزات التوقيع بواسطة الرقم السري و البطاقة الممغنطة و عيوبه:

هذا الشكل من التوقيعات الإلكترونية له القدرة على تحيد هوية شخص الموقع، ذلك أن إتباع العميل للإجراءات السابقة الذكر تؤكد أنه من قام بالعملية المصرفية وانه الشخص صاحب الرقم السري[1]، ضف إلى ذلك أن هذا النوع من التوقيعات الإلكترونية يتمتع بالثقة والأمان ويرجع ذلك إلى السرية المصاحبة لاستخدام الرقم السري، وفي حالة ضياع البطاقة أو فقدها أو نسيان الرقم السري تجمد كل العمليات بمجرد إخبار البنك، كما يتم تثبيت عملية السحب على ثلاثة أنواع من المخرجات على شريط ورقي موجود خلف جهاز السحب على أسطوانة ممغنطة.

وما يعيب على هذه الطريقة حصول شخص بطريقة معينة على هذه البطاقة الممغنطة والرقم السري الخاص بصاحبها، وإجرائه لعمليات سحب وشراء قبل تنبه صاحبها لفقدها، إذ أنه وفي هذه الحالة يتم خصم تلك المبالغ من حسابه لأن التوقيع في هذه الحالة لا يحدد الشخص القائم بالعملية إنما فقط يحدد الشخص الذي يتحمل نتائجها.[2]

المبحث الثاني: مدى تجريم الاعتداء على التوقيع الإلكتروني.

تعددت مجالات استخدام التوقيع الإلكتروني، فأصبحت ترتكز عليه معظم المعاملات الإلكترونية، فهو من جهة أحد أهم التقنيات التي تعتمد عليها التجارة الإلكترونية لإتمام الصفقات التجارية عبر شبكة الانترنيت والتعاقد عن بعد، ومن جهة ثانية أحد الركائز الأساسية التي تعتمد عليها المؤسسات المالية والمصرفية لإنجاز المعاملات المالية لما يمتاز به من ثقة وأمان.

كل هذا جعل التوقيع الإلكتروني عرضة للكثير من الاعتداءات والجرائم الإلكترونية الحديثة وخاصة منها التزوير الإلكتروني أو المعلوماتي، ونظرا لخصوصية هذه الجرائم

---

[1] أنظر: غسان ريضي (عيسى)، مرجع سابق، ص 60.

[2] أنظر: عبد الحميد(ثروت)،مرجع سابق، ص59.

والأضرار التي تتسبب فيها (المطلب الأول) سارعت معظم الدول إلى تعديل تشريعاتها الداخلية لتوفير حماية جنائية خاصة لهذا النوع من التوقيعات والتصدي لمثل هذا النوع من الجرائم، أو إخضاعها للقواعد العامة الخاصة بالتزوير العادي (المطلب الثاني).

المطلب الأول: خصائص و أضرار الاعتداء على التوقيع الإلكتروني.

يختلف التوقيع الإلكتروني عن التوقيع العادي ويتميز عنه بعدة خصائص ومميزات مما يؤدي بالضرورة إلى اختلاف جريمة تزوير التوقيع الإلكتروني عن التوقيع العادي (الفرع الأول)، وتميزها بمجموعة من الخصائص والسمات (الفرع الثاني)، وعدم خلوها من العيوب والأضرار (الفرع الثالث).

الفرع الأول: استعمال التوقيع الإلكتروني المزور.

يتناول من خلال هذا الفرع جريمة استعمال التوقيع الإلكتروني المزور والأركان المكونة لهذه الجريمة.

أولا- المقصود باستعمال توقيع إلكتروني مزور:

التوقيع الإلكتروني يعتبر جزء من الوثيقة المعلوماتية وعنصر من عناصرها[1]، وهذه الوثيقة المعلوماتية محل التزوير يمكن أن تكون دعامات أو شرائط مسجلة أو ممغنطة أو مخرجات من الطابعة وقد تم معالجتها معلوماتيا[2]، وبما أن التوقيع الإلكتروني يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها[3]، فإنه لا يمكنه تقليده بل يمكن استعماله دون علم مالكه، وهذا بخلاف تزوير التوقيعالتقليدي الذي يتم عن طريق تقليد توقيع شخص اخر مما يجعل التوقيع ذاته مختلف عن التوقيع الخاص

---

[1]أنظر: براهمي حنان، مرجع سابق، ص 208.

[2]أنظر: بيومي حجازي (عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، د م، 2009، ص261.

[3]أنظر: محمد الجنبيهي (منير)، **تزوير التوقيع الإلكتروني**، دار الفكر الجامعي، الاسكندرية، 2006، ص 54.

بصاحبه، بحيث لا يتمتع التوقيع المقلد بذات خواص التوقيع الأصلي وبالتالي لا يمكن أن يتماثل معه[1].

أي أن استعماله يتمثل في الحصول على منظومة التوقيع الإلكتروني الخاصة بشخص آخر و القيام باستخدامها في توقيع مستندات إلكترونية، وفي هذه الحالة يبقى التوقيع الإلكتروني سليم مثله مثلما لو كان مالك المنظومة هو الذي قام بالتوقيع بواسطتها وهذا ما يصعب الكشف عن جريمة التوقيع الإلكتروني المزيف[2]، هذا ويعتبر الحصول على هذه المنظومة والتوقيع بها كما لو كان التوقيع صادرا من صاحبه كثير الحدوث عندما يتعلق الأمر ببطاقة الائتمان، خاصة عندما يتعلق الأمر بالتعامل عبر شبكة الانترنيت، ذلك أن التوقيع السري المرتبط بالبطاقة يعد من صور التوقيع الإلكتروني، الذي يتكون من مجموعة من الحروف والأرقام يتم تركيبها في شكل كودي بحيث لا يعلمها إلا صاحب التوقيع ومن يبلغه بها[3].

ثانيا- أركان جريمة استعمال توقيع إلكتروني مزور:

1. فعل الاستعمال:

يفترض فعل الاستعمال قيام الجاني بإبراز المحرر و تقديمه إلى الغير، وفي حالة عدم تقديمه لا يمكن الادعاء بوجوده، ولهذا لا تقوم جريمة الاستعمال بمجرد التصرف على اعتبار أن العقد صحيح.

هذا ويتحقق الركن المادي في جريمة الاستعمال بمجرد التمسك أو الاحتجاج بالمحرر المزور حتى في حالة عدول المتهم عن التمسك به بعد ذلك أو عدم تحقق الغرض من الاحتجاج به، بل لا يتوقف الاستعمال على قبول المحرر المزور وإنما يتم وينتهي بمجرد تقديمه للاستفادة به في غرض معين حتى ولو لم يتحقق ذلك الغرض.

---

[1] أنظر: براهمي حنان، مرجع سابق، ص 239.

[2] أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 54.

[3] أنظر: براهمي حنان، مرجع سابق، ص 240.

ولا تقوم جريمة الاستعمال إلا إذا ورد الاستعمال على ورقة مزورة، أي تتوافر فيها الأركان العامة للتزوير والتي تتمثل في تغيير الحقيقة بإحدى الطرق المادية أو المعنويةوأيضا ترتيب سبب هذا التغيير[1]، كما لا تقوم هذه الجريمة إلا إذا انصب الاستعمال على البيان المزور أو الجزء الزور، أو الشق المزور[2].

وفي تطبيق قضائي حديث لمفهوم التزوير المعلوماتي واستعمال التوقيع الإلكتروني المزور تم حبس مهندس فرنسي مع وقف التنفيذ، وهذا الأخير يعمل مهندس إلكترونيات قام بصناعة البطاقات البنكية الائتمانية، وبعد ثلاثة سنوات من البحث أثبت أن نظام الأمان الذي تعتمده البنوك الفرنسية لا يوفر الحماية اللازمة لهذه البطاقات من الاختراقوالانتهاك.

كذلك التوقيع الإلكتروني وفي حالة التلاعب بأحد البيانات الخاصة بصاحب التوقيع وقدمت للاحتجاج بها حول بيانات لم يتم تزويرها، فإنه لا يسأل من قدمها عن جريمة الاستعمال إلا إذا تمسك بالبيان المزور للإفادة منه، أو كانت البيانات التي يحتج بها وهي غير مزورة مرتبطة بالبيان المزور الذي زور في ذات الوثيقة[3].

2- القصد الجنائي:

جريمة الاستعمال جريمة عمدية، سواء كان المحرر المزور تقليديا أو معلوماتيا، وهذا ما أكده القضاء الفرنسي بشأن استعمال الوثيقة المعلوماتية المزورة، ولذلك لابد من توافر العلم لدى الشخص بأن المحرر المقدم للاستعمال مزورا[4]، واتجاه إرادته إلى تقديمها والتمسك بها، أما إذا كان المستعمل هو المزور نفسه تقوم جريمة الاستعمال بمجرد الاحتجاج بالورقة.

---

[1]أنظر: بن عبد الله بن معيض العبيدي (خالد)، مرجع سابق، ص 201.

[2]أنظر: بيومي حجازي (عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 265.

[3]أنظر: بن عبد الله بن معيض العبيدي (خالد)، مرجع سابق، ص 203.

[4]أنظر: بيومي حجازي (عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 264.

هذا وينتفي القصد الجنائي لدى المزور إذا كان قد احتفظ به ولم تتجه إرادته إلى استعماله، ولكنه سرق منه و تم التعامل به من قبل السارق، فلا يسأل في هذه الحالة عن جريمة الاستعمال ولا يؤثر الباعث على استعمال المحرر.

وتعتبر جريمة استعمال التوقيع او المحرر المزور كأي جريمة يفرض لها عقوبة وذلك للحماية الجنائية منها، فقد نصت المادة السادسة في نظام مكافحة التزوير السعودي على عقوبة الاستعمال وجعلتها عقوبة تزوير بالمحررات الرسمية مضاف إليها الغرامة ويعني ذلك أن عقوبة الاستعمال أشد من عقوبة التزوير، ومرجع ذلك أن الاستعمال هو الذي يحقق الضرر من التزوير مما يبرر تشديد عقوبته[1].

الفرع الثاني: خصائص جريمة تزوير التوقيع الإلكتروني.

تتميز جريمة تزوير التوقيع الإلكتروني بسمات ومميزات تميزها عن جريمة تزوير التوقيع العادي وهذا ما سيتم تناوله من خلال هذا الفرع.

أولا- جريمة تزوير التوقيع الإلكتروني جريمة مركبة:

تعتبر جريمة تزوير التوقيع الإلكتروني جريمة مركبة وذلك نظرا لكونها تتكون من جريمتين، هما جريمة سرقة منظومة التوقيع الإلكتروني لشخص ما وجريمة استخدامها دون إذن من مالكها، هذا وتعدد طرق سرقة منظومة التوقيع الإلكتروني فقد تتم بطريقة تقليدية كالتلصص وقد تتم عبر الانترنيت عن طريق القرصنة الإلكترونية أو التجسس الإلكتروني[2]، وبما أن التوقيع الإلكتروني هو منظومة تتكون من رموز وأرقام تميز صاحبها وتحدد هويته، والتوقيع الكودي أو السري هو أحد صوره والذي يرتبط في الغالب بالبطاقات الممغنطة، فإنه يمكن تزويره بعد تعرضه للسرقة ومن ثمة استخدام الرقم والبطاقة في عملية السحب، أما التوقيع البيو متري الذي يعتمد على الخواص الذاتية للشخص كقزحية العين

---

[1] أنظر: بن عبد الله بن معيض العبيدي (خالد)، مرجع سابق، ص 203 و ما بعدها.

[2] أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 98.

وبصمة الأصبع والتي يتم تخزينها بطريقة مشفرة في ذاكرة الحاسب الآلي، فيمكن أن يتعرض للاختراق بفك تشفير هذه البيانات ونسخها[1].

أما عمليات التجسس فهي عمليات قديمة قدم البشرية فمنذ أقدم العصور كان الإنسان يتجسس على أعدائه، ولكن هذه العمليات تطورت لتواكب التطورات العلمية والتكنولوجية التي شهدها المجتمع، فمثلا تم اختراع جهاز الرادار ثم بعد ذلك الأقمار الصناعية، وفي ظل التطور التقني ظهر ما يعرف بالتجسس الإلكتروني والذي تكمن خطورته في ما إذا كان القائم به هم محترفون قصد الإضرار ببعض الأشخاص من خلال الاطلاع على ملفاتهم الشخصية، أو الاطلاع على أسرارهم التجارية بقصد الابتزاز أو التشهير أو للحصول على منظومة التوقيع الإلكتروني[2].

ثانيا- جريمة تزوير التوقيع الإلكتروني جريمة عابرة للحدود:

تعتبر جريمة تزوير التوقيع الإلكتروني من الجرائم العابرة للحدود الجغرافية والتي لا تحتاج إلى عنف جسدي أو مقاومة وهذا على خلاف الجرائم التقليدية، بل الأكثر من ذلك أنها تتطلب حرفية و إتقان في التنفيذ، والهدف الرئيسي من ارتكابها هو تحقيق الربح المالي مما يترتب عليه إلحاق ضرر كبير بأفراد المجتمع.

وبالإضافة إلى ما سبق تدل هذه الجريمة على المعرفة الفنية لمرتكبها في اختراق الحواجز الأمنية و تدميرها و الوصول إلى المعلومات والبيانات الخاصة بالأفراد والمنظمات وتغييرها، و يبقى دائما الهدف واحد و هو تحقيق أرباح ومكاسب مادية كانت أو معنوية سواء لصالح الشخص مرتكب الجريمة، أو لصالح شخص آخر غيره وعلى هذا الأساس يتوافر في هذه الجريمة القصد الجنائي العام[3].

---

[1] أنظر: براهمي حنان، مرجع سابق، ص 254.

[2] أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 98 و ما بعدها.

[3] أنظر: بن سعود محمد السراني (عبد الله)، **فاعلية الأساليب المستخدمة في جريمة التزوير الإلكتروني**، ط1، الرياض، 2011، ص 200.

ثالثا- لا عقاب على جريمة سرقة منظومة التوقيع الإلكتروني:

إن سرقة منظومة التوقيع الإلكتروني المملوكة لشخص ما وإن كانت في الأساس تعد جريمة إلا أنها غير معاقب عليها، فحتى نكون أمام جريمة تزوير التوقيع الإلكتروني وحتى يدخل الفعل في دائرة التجريم والعقاب، لابد من استخدام هذه المنظومة التي تم الحصول عليها بطريق غير مشروع، وهذا ما أكده القانون النموذجي الصادر عن لجنة الأمم المتحدة الخاص بالقانون التجاري الدولي وكافت القوانين الوطنية التي سارت على نهجه.

وقد اعتبر البعض أن هذا قصور و ثغرة في القانون النموذجي والقوانين الأخرى بينما ذهب رأي ثاني إلى تأكيد ما جاء به القانون النموذجي على أساس أن تجريم سرقة منظومة التوقيع الإلكتروني لا قيمة له، ويرجع ذلك إلى عدم إمكانية اكتشاف هذه الجريمة إلا بعد استخدام تلك المنظومة المسروقة، بالإضافة إلى أن هذه الجريمة هي جريمة مركبة تتكون من جريمتين – وهذا ما تم تناوله فيما سبق– لا قيمة للجريمة الأولى إلا بارتكاب الجريمة الثانية وعلى هذا الأساس فالتجريم يكون بعد ارتكاب الجريمتين[1].

رابعا- جريمة تزوير التوقيع الإلكتروني تجمع ما بين خصائص الجرائم التقليدية و جرائم الانترنيت:

جريمة تزوير التوقيع الإلكتروني تجمع ما بين خصائص الجرائم العادية التقليدية الخاصة بجريمة السرقة، وبين الخصائص المميزة لجرائم الانترنيت باعتبار أن الجريمة الأساسية تتم عبر استخدام التوقيع الإلكتروني، وقد تنعدم الخاصية الأولى لتبقى جريمة تزوير التوقيع الإلكتروني تتمتع فقط بالخصائص المميزة لجرائم الانترنيت والحاسب الآلي إذا لم تتم عبر إحدى الجرائم التقليدية، وإنما قامت عبر إحدى جرائم الحاسب الآلي[2].

---

[1]أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 99 و ما بعدها.

[2]أنظر: محمد الجنبيهي (منير)، المرجع نفسه، ص 101.

خامسا- استخدام أساليب تقنية في تزوير التوقيع الإلكتروني و صعوبة الكشف عنها:

من أهم خصائص جريمة تزوير التوقيع الإلكتروني عدم وجود أثر مادي ظاهر يشير إلى مرتكبها، وهذا راجع إلى طبيعة هذه الجريمة والتي تتكون من ذبذبات ونبضات كهربائية غير مرئية تجعل من الصعب اكتشافها[1]، وأيضا على اعتبار أن التوقيع الإلكتروني هو ختم إلكتروني مشفر لا يملك مفتاحه إلا صاحب التوقيع والذي يتم تزويره عن طريق تقليده بطريقة تشبه التوقيع الأصلي[2].

وارتكاب هذه الجريمة يتطلب الإلمام بمعارف ومهارات فنية متقدمة في مجال الحاسب الآلي والانترنيت ممن لهم الحق في الدخول على النظام فيستغلون الثقة الممنوحة لهم، أو من قبل خبراء لهم خبرة طويلة في استخدام تقنيات الاختراق والتعدي وعلى درجة عالية من الكفاءة في استخدام الحاسب الآلي[3]، فتزوير التوقيع الإلكتروني إذن يتطلب خبرة علمية في مجال الحاسوب والبرامج، بخلاف التوقيع العادي الذي يعتمد على تقليد الإمضاء أو الختم وبالتالي يتطلب من الجاني معرفة فنية، وكل هذا الاختلاف يرجع إلى طبيعة التوقيع الإلكتروني في حد ذاته[4].

الفرع الثالث: أضرار و مخاطر تزوير التوقيع الإلكتروني.

تتسبب جريمة تزوير التوقيع الإلكتروني بمجموعة من الأضرار والمخاطر تلحق الشخص أو المعاملات التي يقوم بها وهذا ما سيتم التطرق إليه من خلال هذا الفرع.

---

[1] أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 201.

[2] أنظر: براهمي حنان، مرجع سابق، ص 255.

[3] أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 201.

[4] أنظر: براهمي حنان، مرجع سابق، ص 257.

أولا- إلحاق الضرر بالسمعة التجارية للشخص:

يعتبر التوقيع الإلكتروني أهم الأدوات التي يبرم بها التاجر صفقاته التجارية عبر شبكة الانترنيت، ولما كان التوقيع الإلكتروني يوفر الثقة والأمان بين أطراف العمل التجاري في تنفيذ ما يلتزمون به بموجب العقد المبرم بين التجار، فإن فقدان التاجر لهذه الثقة يلحق ضررا بالسمعة التجارية، ولهذا يجب على التاجر أو أي شخص عادي يملك منظومة التوقيع الإلكتروني أن يلتزم بالالتزامات التي تم النص عليها والمحددة في القانون النموذجي للتوقيع الإلكتروني الصادر عن لجنة الأمم المتحدة، وكل ذلك في سبيل حماية منظومة للتوقيع الإلكتروني[1].

ثانيا- إضعاف الثقة لأي محرر إلكتروني موقع عليه إلكترونيا:

تؤدي جريمة التزوير إلى فقدان الثقة بالتعاملات الإلكترونية وخاصة عند قيام البعض بالاستيلاء على أرقام بطاقات الائتمان، أو تحويل مبالغ مالية من أرصدة بعض العملاء إلى أرصدتهم الشخصية، أو القيام بعمليات الشراء والتسديد من حساباتهم وذلك بعد اختراق نظم معلومات البنوك[2]، فالثقة في التوقيع الإلكتروني تكتسب ذات الثقة والحجية في الإثبات التي تكتسبها التوقيعات التقليدية العادية، وتزويره يضعف الثقة في منظومته وفي أي محررات إلكترونية متضمنة لهذا التوقيع مما يحلق أضرار بالشخص تبقى مدة من الزمن لتزول[3].

---

[1] أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 97.

[2] أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 200.

[3] أنظر: محمد الجنبيهي (منير)، مرجع سابق، ص 97 و ما بعدها.

المطلب الثاني: مدى انطباق التجريم المقرر في القواعد العامة على التوقيع الإلكتروني.

التوقيع الإلكتروني حتى وإن كان يؤدي نفس وظائف التوقيع العادي فإنه يختلف عنه من حيث طبيعته، أو من حيث البيئة التي أنشأ فيها.

فالتوقيع العادي يكون في صورة ختم أو إمضاء على عكس التوقيع الإلكتروني الذي يأخذ عدة صور مختلفة، فقد يأخذ شكل رمز أو رقم سري أو حتى خاصية فيزيولوجية مميزة من جسم الشخص، وكل هذه الاختلافات والفروقات تطرح جملة من التساؤلات حول مختلف الجرائم و الاعتداءات الواقعة على التوقيع الإلكتروني، وبالأخص جريمة تزوير التوقيع الإلكتروني ومدى خضوعها لطرق التزوير العادية (الفرع الأول)، أو عدم خضوعها للقواعد العامة وضرورة التجريم الخاص لتوفير حماية جنائية كافية وفعالة (الفرع الثاني).

الفرع الأول: التزوير العادي و التزوير الإلكتروني.

لمعرفة مدى تطبيق النصوص التقليدية الخاصة بالتزوير على التوقيع الإلكتروني لابد من تحديد مدلول كل من التزوير العادي والتزوير الإلكتروني، وهذا ما سيتم دراسته من خلال هذا الفرع.

أولا- مدلول التزوير العادي:

عرف قانون العقوبات الفرنسي التزوير بأنه "كل تغيير تدليسي للحقيقة يكون من شأنه أو من طبيعته أن يسبب ضررا للغير، ويتم بأي وسيلة مهما كانت في محرر أو سند للتعبير عن الرأي، والذي يكون موضوعه أو من الممكن أن يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية"[1].

[1] أنظر: بيومي حجازي (عبد الفتاح)، **التجارة الإلكترونية و حمايتها القانونية، الكتاب الثاني**، الحماية الجنائية لنظام التجارة الالكترونية، دار الكتب القانونية، مصر، 2007، ص 306.

وعرفه الفقه الفرنسي أيضا بأنه "تغيير للحقيقة في وقائع أعد المحرر لإثباتها، متى كان من شأنه أن يسبب ضرر وارتكب بقصد الغش"[1].

وعرف أيضا بأنه "إظهار الكذب في محرر بمظهر الحقيقة و ذلك غشا لعقيدة الغير"[2]، و في تعريف آخر عرف التزوير بأنه "تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون، ويكون من شأن هذا التغيير أن يسبب ضررا ويقترن بنية استعمال المحرر المزور فيما أعد لأجله"[3].

ومن خلال تحليل التعاريف السابقة نرى أن لكل تعريف جانب قد ارتكز عليه فمنها من ركز على المحتوى الكاذب للمحرر، وحرص البعض الآخر على إبراز عنصر الغش في المحررات أو وجوب اشتراط وقوع التزوير بالطرق المحددة قانون، وكان من الأحسن لو أن الفقه لم يحصر طرق التزوير بتلك المنصوص عليها في القانون على اعتبار أن هناك طرق حديثة أغفلها المشرع أو أنها لم تكن متوفرة أثناء قيامه بالتشريع[4]، كما يتبين من خلال هذه التعاريف أن التزوير يرتبط بوجود محرر له قيمة في مجال الإثبات وأن يقع تغيير الحقيقة فيه وهو أساس قيام جريمة التزوير[5].

1- التزوير المادي:

يقصد بالتزوير المادي تغيير الحقيقة بطريقة مادية تترك أثرا يدركه البصر ويمكن أن لا يتبين إلا بعد الاستعانة بخبير، هذا وقد حدد المشرع الجزائري اشكال وطرق التزوير

---

[1] أنظر: فوزي السقا (إيهاب)، **جريمة التزوير في المحررات الإلكترونية**، دار الجامعة الجديدة للنشر، الاسكندرية، 2008، ص 49.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 137.

[3] أنظر: بن عقون (حمزة)، **السلوك الإجرامي للمجرم المعلوماتي**، ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011، ص 169.

[4] أنظر: Mohammed Ali Salem ,Abbas talib rzoqi.

مرجع سابق، ص 124.

[5] أنظر: براهمي حنان، مرجع سابق، ص 165.

المادي في المادتين 214 و 216 من قانون العقوبات وهي على سبيل الحصر وتتمثل في التغيير والمحو، و التقليد، والاصطناع، وانتحال شخصية الغير أو الحلول محلها[1]، وفيما يخص التوقيع فهي كالآتي:

أ- وضع إمضاءات أو أختام مزورة:

ويقصد به توقيع الشخص بإمضاء غير إمضائه وليس له حق التوقيع به باعتباره رمزا للشخصية، وسواء كان هذا الإمضاء لشخص حقيقي أو خيالي.

ويعتبر الإمضاء مزورا متى وضع الجاني إمضاء شخص آخر على المحرر دون اشتراط تقليده، فيكفي التوقيع باسم صاحب الإمضاء حتى ولو كان رسمه مخالفا للإمضاء الحقيقي مادام هذا التوقيع يوهم بصدور المحرر من شخص المزور عليه.

أما بالنسبة للختم المزور فهو توقيع الشخص بختم غير ختمه بغض النظر عن مصدره سواء كان لشخص معلوم أو مجهول، وسواء كان ختما مصطنعا لختم صحيح، أو كان ختما صحيحا تم استعماله بدون رضاء صاحبه[2].

ب - تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات:

ويقصد بها كل ما يمكن إدخاله من تغيير مادي لصلب المحرر أو الإمضاء أو الختم الموضوع عليه، وتغيير المحررات يكون إما بالإضافة أو الحذف أو التعديل.

فبالنسبة للإضافة تكون بزيادة كلمات في مكان خال من المحرر، وأما التغيير فيكون بحذف كلمة أو رقم أو اسم أو عبارة سواء بالكشط أو الشطب[3].

---

[1] أنظر: صالح شنين، مرجع سابق، ص 59.

[2] أنظر: فوزي السقا (ايهاب)، مرجع سابق، ص 61 و ما بعدها.

[3] أنظر: بيومي حجازي (عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 186 و ما بعدها.

2- التزوير المعنوي:

التزوير المعنوي يكون عن طريق تغيير الحقيقة في محرر دون المساس بمادته أو شكله، بحيث لا يترك أثرا ماديا ملموسا يمكن إدراكه بالحواس أو تقع عليه العين مما يصعب إثباته على عكس التزوير المادي، هذا وقد نص المشرع الجزائري على هذه الطرق المعنوية في المادة 215 من قانون العقوبات والتي تتمثل عموما في جعل واقعة مزورة في صورة واقعة صحيحة، أو جعل واقعة معترف بها في صورة واقعة غير معترف بها[1].

ثانيا- مدلول التزوير الإلكتروني:

يعرف التزوير الإلكتروني في نطاق جرائم الحاسب الآلي على أنه "أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة مثل التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم"[2]، كما يعرف أيضا بأنه "تغيير للحقيقة في البيانات والمعلومات المعالجة عن طريق الحاسب الآلي، والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب".

هذا ويقصد بالكيان المادي لمخرجات الحاسب الآلي البيانات ولمعلومات التي تخرج من الحاسب الآلي، شرط أن تطبع على دعامة مادية مكتوبة كورقة أو قرص مرن أو مدمج، ومن خلال ما سبق يتضح أن التزوير المعلوماتي أو الإلكتروني يرتبط هو الآخر بتغيير الحقيقة في وثيقة معلوماتية، وهذه الأخيرة لا ترتبط بالشكل الورقي وإنما تكون دعامة معلوماتية حررت عليها معلومات ذات قيمة قانونية، وبالتالي فتغيير الحقيقة في هذه المعلومات يجب أن يظهر على هذه الدعامة[3].

وقد عرفت الوثيقة المعلوماتية أو المعالجة معلوماتيابأنها كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات، أو كل الوثائق التي تنشأ عن جهاز إلكتروني أو

---

[1] أنظر: صالح شنين، مرجع سابق، ص 62.

[2] أنظر: بيومي حجازي (عبد الفتاح)،**التجارة الإلكترونية و حمايتها القانونية، مرجع سابق**، ص 306.

[3] أنظر: براهمي حنان، مرجع سابق، ص 189.

كهرومغناطيسي أو طبع ممغنط، ويتحقق التزوير المعلوماتي إذا كان موضوعه التوقيع الإلكتروني والذي أحاطته معظم التشريعات بضوابط وضمانات بهدف حماية التجارة الإلكترونية وأموالها من خلال الثقة في التوقيع الإلكتروني[1].

1- مدى إمكانية خضوع التزوير الإلكتروني لطرق التزوير التقليدية:

إن التزوير الواقع في الوثيقة الإلكترونية يخرج عن المفهوم الواقع على المحررات الورقية، على اعتبار أن فكرة التزوير في المحرر تقتضي أن يعبر المحرر عن فكرة إنسانية وأن يكون وجوده ماديا ملموسا يمكن رؤيته بالعين المجردة[2]، كما لا يمكن تطبيق النصوص المتعلقة بالتزوير على تغيير الحقيقة في المعلومات المبرمجة، لأنها لا تعتبر محرر ولا يمكن مشاهدة المعلومات المخزنة على وسائط التخزين الخاصة بها عن طريق العين المجردة[3]، كما أنه لا يمكن الاعتداد بالتزوير إلا إذا تم بالطرق التي نص عليها القانون وهي على سبيل الحصر، وهذه الطرق غير محصورة إذا ما تعلق الأمر بالوثيقة المعلوماتية كما هو الحال عند تزويرها في شكلها الورقي.

هذا وتتميز أركان جريمة تزوير الوثيقة المعلوماتية بخصوصية في الأفعال المكونة لركنها المادي على اعتبار أنها تقع في بيئة افتراضية غير ملموسة[4].

كما لا تقوم جريمة التزوير بتغيير الحقيقة في الوثيقة المعلوماتية أثناء نشأة المستند وهذا على خلاف جريمة التزوير العادية[5].

وبما أن التوقيع الإلكتروني هو جزء من الوثيقة المعلوماتية فإنه يختلف تماما عن التوقيع العادي، ذلك أن التوقيع الإلكتروني هو من قبيل البيانات الإلكترونية في صورها

---

[1] أنظر: بيومي حجازي (عبد الفتاح)، **التجارة الإلكترونية و حمايتها القانونية**، مرجع سابق، ص 307.

[2] أنظر: فوزي السقا (ايهاب)، مرجع سابق، ص 55.

[3] أنظر: براهمي حنان، مرجع سابق، ص 173.

[4] أنظر: براهمي حنان، المرجع نفسه، ص 201.

[5] أنظر: صالح شنين، مرجع سابق، ص 59.

المختلفة التي تستخدم الحروف والرموز والتشفير، وهو غير الإمضاء الذي يعد كتابة يقوم بها الشخص وتتخذ شكلا معينا مميزا يعتمد عليه الشخص في التعبير عن التزاماته بوثيقة ما، كما لا يعتبر هذا التوقيع بصمة لأنه يقوم على تقنيات لا تعد جزء من جسم الإنسان باستثناء التوقيع البيو متري.

إن كل هذه الاختلافات تجعل تزوير التوقيع الإلكتروني مختلفا وصعبا مقارنة مع التزوير العادي[1]، حيث أن تزوير التوقيع الإلكتروني يتم باستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك يتم تصميمها على غرار البرامج والأنظمة المشروعة، أو عن طريق محاولة كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني[2].

هذا وتقوم جريمة تزوير التوقيع الإلكتروني بأفعال مختلفة عن تزوير التوقيع العادي من خلال الحصول على منظومة التوقيع الإلكتروني بطريقة غير مشروعة بنية استخدامهافي التوقيع على هذه الوثيقة[3]، و استخدام برامج فك التشفير و هي عبارة عن أقراص وبرامج تحتوي على لوغاريتمات، تقوم بعمليات تبادل وتوافيق بسرعات مهولة إلى غاية الحصول على الرقم السري الخاص بالنظام، كما يمكن استخدام الشبكات والبرامج المرتبطة بها التي تتيح الدخول إلى بعض المواقع وفك الشفرات الخاصة بها[4].

والحصول على منظومة التوقيع الإلكتروني والتوقيع بها كما لو كان التوقيع صادرا عن صاحبه كثير الحدوث عندما يتعلق الأمر ببطاقةالائتمان، فالتوقيع السري المرتبط بها يعتبر من صور التوقيع الإلكتروني، أما التوقيع الرقمي وهو أكثر أنواع التواقيع الإلكترونية

---

[1]أنظر: براهمي حنان، مرجع سابق، ص 255 و ما بعدها.

[2]أنظر: عبد الفتاح مطر(عصام)، **التجارة الإلكترونية في التشريعات العربية و الاجنبية**،دار الجامعة الجديدة، الاسكندرية، 2015، ص 337.

[3]أنظر: براهمي حنان، مرجع سابق، ص 289.

[4]أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 206.

انتشارا فإنه يرتبط بنظام التشفير ولذلك فإنه قد يتعرض لكسر الشفرة والوصول إلى الأرقام الخاصة به، والقيام بنسخها وإعادة استخدامها بعد ذلك[1].

2- قصور الطرق التقليدية للتزوير في المجال الإلكتروني:

التزوير لم يعد مجرد حك في مضمون الوثيقة أو تعديل لبعض الكلمات أو تزوير ختم أو إثبات واقعة كاذبة على أنها صحيحة[2]، وإنما يتجاوز ذلك إلى استخدام أساليب ووسائل أكثر تطورا.

ونظرا للطبيعة الخاصة للمواد الإلكترونية أصبحت الطرق التقليدية في التزوير غير مناسبة للتطبيق في هذا المجال[3]، وبما أنه لا يتم الاعتداد بالتزوير إلا إذا تم بالطرق التي نص عليها القانون و هي على سبيل الحصر[4]، فإنه وطبقا لمبدأ الشرعية والذي يعني أنه لا جريمة ولا عقوبة إلا بنص لا يسوغ لاحد أن يضيف إلى طرق التزوير التي جرمهاالمشرع طرق أخرى لم ينص عليها[5]، وبالتالي فجريمة التزوير العادية لا تستوعب تزوير التوقيع الإلكتروني ولا تحتمله.

الفرع الثاني: نحو تجريم خاص لحماية التوقيع الإلكتروني.

نظرا لعدم استيعاب القواعد التقليدية لجريمة التزوير وعدم انطباقها على تزوير التوقيع الإلكتروني، فإنه لابدمن وضع نصوص خاصة لمواجهة هذه الجريمة والتصدي لها على غرار ما هو معمول في أغلب التشريعات المقارنة.

---

[1] أنظر: براهمي حنان، مرجع سابق، ص 240.

[2] أنظر: براهمي حنان، المرجع نفسه، ص 216.

[3] أنظر: عبد الغني محمد عطا الله (شيماء)، **الحماية الجنائية للتعاملات الإلكترونية**، دار الجامعة الجديدة، الاسكندرية، 2007، ص 91.

[4] أنظر: براهمي حنان، مرجع سابق، ص 187.

[5] أنظر: براهمي حنان، المرجع نفسه، ص 218.

أولا- التزوير الإلكتروني في الجزائر و ضرورة التجريم الخاص:

التزوير الإلكتروني حاليا في الجزائر ليس محمي، فبالرجوع إلى النصوص التقليدية المنظمة لجريمة التزوير نرى أن كل هذه النصوص لا يمكن أن تنطبق على تغيير أو تحوير الحقيقة في البيانات الإلكترونية، حيث يعد التزوير وفقا لهذه النصوص التقليدية تغييرا في محرر بإحدى الطرق التي نص عليها القانون وهو ما جاء في المواد من 214 إلى 229 من قانون العقوبات الجزائري[1].

ونظرا للأهمية الكبيرة التي يحتلها التوقيع الإلكتروني في مجال التجارة الإلكترونية، حيث يساهم في تأكيد العقود والاتفاقيات التجارية وتحديد هوية كل من المرسل والمستقبل والتأكد من صحة وصدق البيانات، فأنه من الضروري توفير حماية جنائية خاصة لهذا النوع من التوقيعات، ذلك أن الاعتداء عليه يعد اعتداء على مضمون التجارة الإلكترونية[2]،كما ساهم أيضا التطور الاقتصادي والاجتماعي في زيادة حجم النشاط الاقتصادي للبنوك والمؤسسات والشركات، والتي باتت تعتمد على نظام التوقيع الإلكتروني بصوره المختلفة في أداء خدماتها للجمهور وذلك لمسايرته السرعة الناتجة عن معالجة المعلومات معالجة إلكترونية[3].

كما أدى أيضا التحول من العالم المحسوس إلى الرقمي، ومن الدعامة المادية إلى الدعامة الإلكترونية بظهور ما يسمى بالحاسبات الآلية والوسائط المتعددة والانترنيت، إلى ظهور نوع جديد من البطاقات الممغنطة التي تعتمد على الرقم السري أو الكودي وهو أحد

---

[1] أنظر: بن عقون(حمزة)، مرجع سابق، ص 171.

[2] أنظر: يوسف حسن (يوسف)، **العقود التجارية الإلكترونية الدولية**، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 42.

[3] أنظر: أحمد عبد الله غرايبية (عبد الله)،**حجية التوقيع الالكتروني في التشريع المعاصر**،ج1، ط1، دار الراية، عمان،2009، ص37ومابعدها.

صور التوقيع الإلكتروني، ومن أمثلة ذلك بطاقة الائتمان التي تصدرها البنوك والمؤسسات للقيام بعمليات الدفع بدلا من حمل النقود[1].

هذا ويساهمالتوقيع الإلكتروني في توفير الثقة والأمان والتي هي أساس كل التعاملات وأحد الركائز الأساسية في المجال الإلكتروني، خاصة وأنه مجال يتم بين أشخاص لا يجمعهم مجلس واحد ولا يعرفون بعضهم البعض.

وعليه وكنتيجة لكل هذا يجب إحاطة هذا النوع من التعاملات بنوع من الحماية وذلك من خلال توفير حماية جنائية أكثر فاعلية للتوقيع الإلكتروني، وضرورة التجريم الخاص[2].

ثانيا- تجريم التزوير الإلكتروني في التشريع المقارن:

1- صيغة التجريم في القانون المصري:

جرم المشرع المصري فعل تزوير التوقيع الإلكتروني من خلال نصوص قانون التوقيع الإلكتروني، حيث نص في المادة 23/ب على معاقبة كل من: "أتلف أو عيب توقيعا أو وسيطا أو محرر إلكترونيا أو زور شيئا ما بطريق الاصطناع أو التعديل أو المحو أو بأي طريق آخر".

ويتضح من خلال النص السابق أن المشرع المصري جمع عدة أنماط للسلوك الإجرامي الذي قد ينال التوقيع الإلكتروني إلى جانب التزوير في نص واحد، مثل الإتلاف والتعييب رغم أنه أشار إلى طرق الاصطناع والتعديل والتحوير وهي من طرق التزوير، كما انه جمع بين الاعتداء الواقع على التوقيع الالكتروني وكذا الوثيقة المعلوماتية، كما يتبين أن

---

[1] أنظر: عبد الحميد(ثروت)، مرجع سابق، ص 45.

[2] أنظر :بلحسيني حمزة، **الحماية القانونية والفنية للتوقيع الالكتروني في مجال البيئة الرقمية**، مجلة العلوم القانونية و الادارية، جامعة جيلالي اليابس بسيدي بلعباس، عدد 11، 2015، ص 72.

هذه الطرق التي ذكرها المشرع لم ترد على سبيل الحصر لأنه أضاف عبارة أو بأي طريق آخر [1].

كما جرم أيضا استعمال توقيع إلكتروني معيب أو مزور من خلال نص المادة 23/ج، وتجدر الإشارة إلى أن المشرع المصري عاقب على استعمال توقيع إلكتروني معيب أو مزور دون الإتلاف وذلك لأن هذا الأخير لا أثر له من الناحية العملية والقانونية[2].

هذا ويشترط للقول بوقوع التزوير في توقيع إلكتروني أن يتمتع بالحجية القانونية، فهذا شرط جوهري وخاصية أساسية ليكون مشمولا بالحماية القانونية ضد التزوير، ولذلك يجب الاعتراف بهذه الحجية قانونا وتوفير الشروط الفنية والتقنية ليؤدي التوقيع الإلكتروني الوظائف المنوطة به[3].

وعلة التجريم تتعلق بالثقة العامة في الوثائق عند تداولها بين الأفراد والتي تتحقق نظير تمتع هذه الوثائق بالقيمة القانونية عند الإثبات، ولكن رغم تجريم المشرع المصري تزوير التوقيع أو الوثيقة الإلكترونية في قانون التوقيع الإلكتروني، إلا أنه لم يوفق في صياغة النص المجرم لهذا الفعل لعدم توضيحه لأركان التزوير بدقة، وإنما اكتفى بالإشارة إلى بعض صور السلوك المادي مثل الاصطناع والتعديل، كما جاء النص خالي تماما من الإشارة إلا عنصر الضرر في جريمة التزوير[4].

2- صيغة التجريم في القانون الفرنسي:

المشرع الفرنسي لم يقصر التزوير على المحررات بمفهومها التقليدي، وإنما نص على وقوع التزوير بأي طريقة كانت فجاء النص الخاص بالتزوير عاما ليشمل أيضا التزوير

---

[1] أنظر :براهمي حنان، مرجع سابق، ص 238 و ما بعدها.

[2] أنظر : صالح شنين، مرجع سابق، ص 175.

[3] أنظر : براهمي حنان، مرجع سابق، ص 244 و ما بعدها.

[4] أنظر : براهمي حنان، المرجع نفسه، ص 179 و بعدها.

الإلكتروني[1]، حيث تنص المادة 1/441 من قانون العقوبات الفرنسي على أن التزوير "هو كل تغيير تدليسي للحقيقة من شأنه أو من طبيعته أن يسبب ضررا للغير في محرر أو سند وبأي وسيلة كانت، ويكون موضوعه أو من الممكن أن يكون له أثر في إنشاء الدليل على حق أو فعل يرتب نتائج قانونية"[2]، ومن خلال هذه المادة يتضح أن المشرع الفرنسي استوعب ضمن التزوير التقليدي حالة الغش المعلوماتي الواقع على وثيقة معلوماتية، وذلك من خلال استعماله لفظ سند أو دعامة كما أنه لم يحصر التزوير في طريقة معينة[3]، فصيغة النص المتعلق بالتزوير في قانون العقوبات الفرنسي هي صيغة موسعة تشمل كل تزوير في وثيقة ذات قيمة قانونية مهما كانت طبيعتها ورقية أو معلوماتية، ليتم بذلك تغطية كل أشكال التزوير المستحدثة والتي أفرزتها التكنولوجيا المعاصرة[4]، ولكنه يشترط إمكانية استخدام هذه الوثيقة أو الوسيط الذي تم تزويره لممارسة حق أو تصرف، أو أن يكون صالحا لإثبات حق أو تصرف تنتج عنه آثار قانونية[5].

وعلى هذا الأساس فإن الوثيقة الإلكترونية كالمحررات الورقية تحظى بحماية جنائية لاسيما من جريمة التزوير في معظم التشريعات الحديثة، سواء كان ذلك في إطار قانون العقوبات كما هو الحال بالنسبة للمشرع الفرنسي في المادة 1/441 من قانون العقوبات، أو في إطار نصوص خاصة كما هو الحال بالنسبة للمشرع المصري من خلال نص المادة 23 من قانون التوقيع الإلكتروني.

---

[1] أنظر: بيومي حجازي(عبد الفتاح)، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 164.

[2] أنظر: Article 441/1 du code civile française

[3] أنظر: بيومي حجازي(عبد الفتاح)، **التجارة الإلكترونية و حمايتها القانونية**، مرجع سابق، ص 306.

[4] أنظر: براهمي حنان، مرج سابق، ص 283.

[5] أنظر: فوزي السقا(ايهاب)، مرجع سابق، ص 56.

وهذا بخلاف المشرع الجزائري الذي لم يساير التشريعات الحديثة في هذا الإطار في انتظار تعديل نصوص جريمة التزوير لكي تحتوي التزوير المعلوماتي أو إصدار نص خاص بالتزوير المعلوماتي[1].

[1] أنظر: صالح شنين، مرجع سابق، ص 47 و ما بعدها.

خلاصة الفصل الأول:

أدى التطور في مجال المعاملات الإلكترونية و ظهور ما يسمى بالتجارة الالكترونية إلى إحداث تغيرات تزايدت معها استخدامات الإنسان للتقنيات الإلكترونية وخاصة منها الانترنيت، و هذه الأخيرة صاحبها ظهور تقنية أو شكل جديدة من أشكال التعاقد عنبعد و هو التوقيع الإلكتروني الذي حل محل التوقيع التقليدي، فأصبحت ترتكز عليه البنوك والمؤسسات وحتى الإدارات في تقديم خدماتها للجمهور، و وسيلة التجار في إبرام العقود عبر شبكة الانترنيت، وذلك نظرا لما يحققه من ثقة وأمان وسرعة في إتمام هذه المعاملات الإلكترونية.

ومن خلال هذا الفصل تم إسقاط الضوء على التوقيع الإلكتروني من خلال التطرق إلى ماهيته وأهم تطبيقاته، وعرض خصائصه ومميزاته واستعراض أهم صوره والاعتداءات الواقعة عليه، لأخلص في الأخير إلى أن الاستعمالات الكثيرة والمختلفة للتوقيع الإلكتروني أدى إلى تعرضه لجملة من الاعتداءات وبالأخص التزوير، وعدم إمكانية خضوع وانطباق هذا النوع من الجرائم للنصوص التقليدية الخاصة بتزوير التوقيع العادي، مما يوجب ضرورة التدخل لوضع نصوص خاصة والتصدي لهذه الجريمة أو تعديل نصوص التزوير العادية لتحتوي جريمة تزوير التوقيع الإلكتروني.

الفصل الثاني: الحماية الجنائية للتوقيع الإلكتروني في إطار التجريم المقرر لحماية الحياة الخاصة

تتعدد وتتنوع المفاهيم المتعلقة بالحياة الخاصة أو الخصوصية للأفراد خارج نطاق النظام المعلوماتي، إذ أنه لا يمكن وضع تعريف موحد خاص بها.

ومن المعروف أن هذه الخصوصية المرتبطة بالفرد خلال حياته اليومية، يمكن أن تتعرض لعدة انتهاكات جرمتها معظم التشريعات مثل التنصت الهاتفي وأخذ صورة خلسة وغيرها من الجرائم، وهذا يختلف عن مفهوم الحياة الخاصة في إطار النظم الآلية للمعطيات، حيث يتم استبدال كل هده الجرائم ليحل محلها نوع جديد من الجرائم المستحدثة أفرزتها النظم المعلوماتية.

فقد أدى الاستخدام الكثير والمتعدد لهذه الأنظمة الآلية إلى تعدد وسائل وطرق الانتهاك فأصبحت أكثر تطورا، وبات من السهل التلاعب بالمعطيات والمعلومات الآلية المخزنة في النظام المعلوماتي ومن ثمة الاعتداء على الحياة الخاصة للأفراد، وذلك من خلال الحصول على كلمة السر والقيام بكسرها عن طريق برامج متخصصة في ذلك، أو من خلال فض مفاتيح الشفرة.

ومن هنا ظهرت أهمية التوقيع الإلكتروني في الحفاظ على سرية هذه المعلومات الرقمية والرسائل الإلكترونية المتبادلة عبر الشبكة المعلوماتية، لذلك وفي سبيل حماية هذه الخصوصية للمعلومات والحق في الحياة الخاصة بصفة عامة، والتوقيع الإلكتروني بصفة خاصة لابد من تحديد هذه النظم الآلية لمعالجة المعطيات (المبحث الأول)، ومختلف صور التجريم المقررة لحمايتها (المبحث الثاني).

المبحث الأول: نظم المعالجة الآلية للمعطيات.

أدى تطور تقنيات الاتصال إلى ابتكار نظم المعالجة الآلية للمعطيات، والذي يتم من خلاله معالجة المعلومات آليا وتخزينها داخل النظام المعلوماتي.

وتختلف هذه النظم الآلية عن النظم القانونية القائمة التي تتناول الجرائم التقليدية من عدة جوانب سواء من خلال المفاهيم الخاصة بها(المطلب الاول)، أو من خلال خصوصية المعطيات التي تحتويها (المطلب الثاني).

المطلب الأول: مفهوم النظام الآلي لمعالجة المعطيات.

تعددت المفاهيم الخاصة بالأنظمة الآلية لمعالجة المعطيات (الفرع الأول) نظرا لما تحتويه من عناصر ومكونات تقوم عليها (الفرع الثاني).

الفرع الأول: تعريف النظام الآلي لمعالجة المعطيات.

النظام الآلي لمعالجة المعطيات شرط ضروري وركن مفترض لقيام جريمة الاعتداء عليه، بالإضافة إلى توحد العناصر المكونة له وهذا ما سيتم دراسته من خلال هذا الفرع.

أولا- المقصود بالنظام الآلي لمعالجة المعطيات :

التعريف المستخدم والمتداول هو التعريف الذي قدمه مجلس الشيوخ الفرنسي و الذي جاء فيه أن نظام المعالجة الآلية للمعطيات هو: "كل مجموع يتركب من واحدة أو أكثر من وحدات المعالجة، ذاكرة، برامج، معطيات، أجهزة إدخال و إخراج، وروابط تؤدي إلى نتيجة محددة، ويكون هذا المجموع محميا بأجهزة أمان"[1]

[1] أنظر: محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن**، دار الجامعة الجديدة، الاسكندرية، 2007، ص 26.

والملاحظ على هذا التعريف أنه ركز على العناصر المادية والمعنوية التي يتكون منها المركب، أساس نظام المعالجة الآلية للبيانات والتي وردت على سبيل المثال لا الحصر[1].

وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال، هذا ويعتبر نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة وذلك لخضوعه للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[2]، ولذلك حذا المشرع الجزائري في ذلك موقف المشرع الفرنسي في عدم تعريفه لنظام المعالجة الآلية للمعطيات وأوكل ذلك للفقه[3].

وعرف قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية في المادة الثانية النظام المعلوماتي على انه: "النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو استلامها أو تخزينها أو لتجهيزها على أي وجه آخر"[4].

ثانيا- ضرورة الوجود المتزامن للعناصر المكونة للنظام:

لا يتوفر نظام المعالجة الآلية للمعطيات ولا تقع أي جريمة من جرائم الاعتداء عليه المنصوص عليها اذا ما وقع الاعتداء على برامج معروضة للبيع، أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على الأجهزة التي مازالت في مرحلة التجربة أو حتى الأنظمة التي خرجت من الخدمة تماما[5]، وكذلك الدخول إلى برنامج من

---

[1] أنظر: بيومي حجازي (عبد الفتاح)، **الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة**، ط1، منشأة المعارف، الاسكندرية، 2009، ص 477.

[2] أنظر: آمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، ط2، دار هومة للطباعة والنشر، الجزائر، ص 101 و ما بعدها.

[3] أنظر: سعيداني نعيم، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012، ص 42.

[4] أنظر: أنور بندق (وائل)، **موسوعة القانون الإلكتروني و تكنولوجيا الاتصالات**، ط1، دار المطبوعات الجامعية، الاسكندرية، 2007، ص 19.

[5] أنظر: آمال قارة، مرجع سابق، ص 102.

أجل تعديله أو تحويله إلى استعمال آخر غير الاستعمال المخصص له لا يشكل جريمة بمفهوم قانون العقوبات، إلا إذا كان هذا البرنامج يشارك في تطبيق فعلي داخل نظام كامل، لأن البرنامج المعزول لا يأخذ حكم النظام[1].

وتقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل، كما تقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزء من أنظمة متعددة[2].

الفرع الثاني: مكونات النظام الآلي لمعالجة المعطيات.

يتم التطرق من خلال هذا الفرع إلى المكونات المادية و المعنوية أو المنطقية للنظام المعلوماتي.

أولا- المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي الأجهزة والمعدات الملحقة به، والتي تستخدم في تشغيله كالأسطوانات والشرائط ووحدات الإدخال والإخراج وغيرها، ويكون الاعتداء عليها عن طريق جرائم عادية وتقليدية كأن تكون محلا للسرقة أو الإتلاف العمدي[3]، وتتمثل هذه المكونات في:

1- وحدات الإدخال:

وهي الوحدات المصممة للقيام بإدخال المعلومات و المعطيات المطلوب معالجتها، ومن أمثلة هذه الوحدات لوحة المفاتيح، إذ من خلالها يتم إدخال المعطيات ومن أمثلتها أيضا الوحدات التي تستخدم في قراءة المعطيات مثل مشغل الأقراص المغناطيسية، أو الفأرة

---

[1] أنظر: محمد خليفة، مرجع سابق، ص28.

[2] أنظر: خشير مسعود، **الحماية الجنائية لبرامج الكمبيوتر**، دار الهدى، عين مليلة، الجزائر، 2010، ص 110.

[3] أنظر: سوير سفيان، **جرائم المعلوماتية**، ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بالقايد تلمسان، 2010 ص 40.

والماسح الضوئي[1]، الذي يتم عن طريقه إدخال صورة المستند أو الخريطة أو الإنسان إلى جهاز الحاسب الآلي[2].

2- وحدات الإخراج:

وتستخدم لعرض نتائج العمليات التي أتمها الكمبيوتر على المعطيات التي يتم إدخالها إليه عن طريق وحدات الإدخال، ومن أمثلتها الطابعات والشاشات، وكذلك وحدة تخزين البيانات على الأقراص الممغنطة أو على الشرائط الممغنطة[3].

3- وحدات المعالجة المركزية:

تقوم هذه الوحدات بتلقي الأوامر عن طريق أجزاء الإدخال ثم معالجته وإخراجها بالكيفية التي يرغبها مشغل الجهاز وتتمثل هذه الوحدات في، وحدة الذاكرة الرئيسية وهي الذاكرة التي تقوم بحفظ البيانات والنتائج مؤقتا ووحدة الحساب و المنطق ووحدة التحكم[4]، هذا وتعتبر وحدة المعالجة المركزية في الحاسب من أهم أجزائه لأنها بمثابة العقل في الجهاز فهي تعمل على إنجاز كافة العمليات الحسابية بسرعة مذهلة، بالإضافة إلى معالجة أنواع المعطيات والتنسيق بين جميع أجزاء الحاسب[5].

ثانيا- المكونات المعنوية للنظام المعلوماتي.

تتجسد المكونات المعنوية في المعلومات بكل صورها، وكما رأينا سابقا المكونات المادية للنظام لا تثير أية مشكلة قانونية كونها مشمولة بالحماية الجنائية، وعلى العكس من

---

[1] أنظر: محمد خليفة، مرجع سابق، ص 18 و ما بعدها.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنيت**، دار الكتب القانونية، مصر، 2007، ص 62.

[3] أنظر: محمد خليفة، مرجع سابق، ص 19.

[4] أنظر: بيومي حجازي (عبد الفتاح)، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنيت**، مرجع سابق، ص 62 و ما بعدها.

[5] أنظر: محمد خليفة، مرجع سابق، ص 20.

ذلك تبدو النصوص التقليدية قاصرة عن تحقيق الحماية الكافية والمتكاملة للمكونات المعنوية للنظام المعلوماتي الممثلة بالمعلومات أو البرمجيات، والتي قد تتعرض للسرقة أو الإتلاف أو التزوير [1].

وتكتسب المكونات المعنوية درجة كبيرة من الأهمية فهي روح النظام، والعدوان عليها يشكل جريمة بالمعنى الدقيق، وتنقسم هذه المكونات إلى قسمين: البرامج والمعطيات.

1- البرامج:

هناك مفهومان أحدهما ضيق والآخر موسع للبرامج، فأما المفهوم الضيق فهو ينصرف إلى مجموعة التعليمات الموجهة من الإنسان إلى الآلة لتنفيذ مهمة معينة[2]، أما التعريف الموسع فيشمل بالإضافة إلى المفهوم الضيق وصف البرامج وهو التقديم الكامل المفصل لعمليات في شكل شفوي أو خطي أو غيره، من أجل تحديد مجموعة التعليمات المشكلة للبرنامج، ويتضمن أيضا المستندات الملحقة والتي ليست ببرامج ولكنها تهدف إلى تبسيط مفهوم وتطبيق البرنامج[3].

2- المعطيات:

المعطيات هي عبارة عن معلومات تم تنظيمها ومعالجتها داخل النظام الآلي لمعالجة المعطيات وتخزينها بغية استرجاعها عند الحاجة إليها، وكونها عبارة عن نبضات إلكترونية لا يمكن لمسها فهي من المكونات المعنوية وليس المادية[4].

---

[1] أنظر: حمزة بن عقون، مرجع سابق، ص129.

[2] أنظر: محمد خليفة، مرجع سابق، ص 24 و ما بعدها.

[3] أنظر: محمد سلامة (عماد)، **الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج**، ط1، دار وائل للنشر، عمان، 2005، ص 50.

[4] أنظر: محمد خليفة، مرجع سابق، ص 25.

المطلب الثاني: خصوصية المعطيات الآلية و ضرورة الحماية.

إن الاعتداء على المعطيات أو المعلومات يشكل اعتداء على الحياة الخاصة للإنسان، وذلك من خلال إساءة استخدام هذه المعلومات والتي تربطها علاقة خاصة بالأفراد، فقد تتعرض سلامة وسرية هذه المعلومات للانتهاك من خلال الحصول على كلمة السر و كسرها، أو فض مفاتيح التشفير وكل هذا يعتبر خرقا وانتهاكا لخصوصية المعطيات الآلية (الفرع الأول) مما يستلزم ضرورة توفير حماية (الفرع الثاني).

الفرع الأول: خصوصية المعطيات الآلية.

لتتمتع المعطيات أو المعلومات بحماية خاصة لابد من توافر مجموعة من الشروط والخصوصية وهذا ما سيتم التطرق إليه من خلال هذا النوع.

أولا- مفهوم المعطيات:

1- تعريف المعطيات:

هي عبارة عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام ولتي لا تربطها علاقة مع بعضها البعض، كما أنها لم تخضع للتفسير أو التجهيز للاستخدام، وقد عرفها المشرع الجزائري في المادة الثانية من القانون رقم 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها: "أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[1]

[1] أنظر: سعيداني نعيم، مرجع سابق، ص 15 و ما بعدها.

2. الفرق بين المعطيات و المعلومات:

المعلومات تتكون من بيانات يتم تحويلها وتشغيلها لتصبح لها قيمة، فهي تمثل معرفة لها معنى وتفيد في تحقيق الأهداف[1]، كما أنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات و التي تصلح لأن تكون محلا للتبادل و الاتصال، أو التفسير أو التأويل أو المعالجة، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزأتها وجمعها أو نقلها بوسائل وأشكال مختلفة[2]، و بالتالي فإن المعلومات هي المعنى الذي يستخلص من المعطيات والتي تعتبر المواد الخام التي تستخرج منها المعلومات باستخدام معالجة آلية في عملية الاستخراج، إذ يتم تجميع و تشغيل المعطيات للحصول على المعلومات والتي تستخدم لدورها في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات، و التي يتم تجميعها ومعالجتها مرة أخرى من أجل الحصول على معلومات إضافية[3]، فهي بذلك تتميز بقابليتها للدمج فقد تضاف معلومة إلى معلومة أخرى لتكونا معا معلومة جديدة تختلف في قيمتها وأهميتها عما كانت عليه قبل الدمج[4].

ولهذا يمكن القول أن المعطيات هي المعلومات في حالة سكون وأن المعلومات هي المعطيات في حالة معالجة، كما أنها النتيجة المبدئية أو النهائية المترتبة على تشغيل المعطيات وتحليلها أو استقراء دلالتها واستنتاج ما يمكن استنتاجه منها وحدها أو مترافقة مع غيرها[5].

---

[1] أنظر: بو فروعة سوفيان، **نظام المعلومات المحاسبي و دوره في تسيير المؤسسة الاقتصادية**، ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، 2011، ص 51.

[2] أنظر: عبد القادر المومني (نهلا)، **الجرائم المعلوماتية**، ط1، دار الثقافة، عمان، 2008، ص 101.

[3] أنظر: سعيداني نعيم، مرجع سابق، ص 16.

[4] أنظر: عبد القادر المومني (نهلا)، مرجع سابق، ص 103.

[5] أنظر: سعيداني نعيم، مرجع سابق، ص 16 و ما بعدها.

ثانيا- شروط و خصائص المعلومات:

1- الشروط الواجب توافرها في المعلومة:

أ - التحديد و الابتكار:

إن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فالمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون محددة، لان التبليغ الحقيقي يفترض التحديد[1]، ولأن الاعتداء يجب أن ينصب على شيء محدد وأن يكون هذا الشيء محلا لحق محدد[2]، أما فيما يتعلق بالابتكار فينبغي أن ينصب على الرسالة التي تحملها المعلومة[3]، فالمعلومة الغير مبتكرة هي معلومة عامة ومتاحة للجميع ولا يمكن نسبتها لشخص محدد[4].

أ - السرية و الاستئثار:

كلما اتسمت المعلومات بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومة محددا بمجموعة من الأشخاص، ودون هذا التحديد لا يمكن أن تكون المعلومة محلا يعتدى عليه، فإذا انعدمت هذه السرية أصبحت المعلومة قابلة للتداول.

وتستمد المعلومة سريتها من طبيعتها أو بالنظر لرغبة صاحبها وإرادته أو للسببين معا كما هو الحال في الرقم السري لبطاقة الائتمان[5].

---

[1] أنظر: عبد القادر المومني (نهلا)، مرجع سابق، ص 103.

[2] أنظر: سعيداني نعيم، مرجع سابق، ص 24.

[3] أنظر: عبد القادر المومني (نهلا)، مرجع سابق، ص 103.

[4] أنظر: سعيداني نعيم، مرجع سابق، ص 24.

[5] أنظر: عبد القادر المومني (نهلا)، مرجع سابق، ص 104.

وتكتسب المعلومة صفة الاستئثار إذا كان الوصول اليها غير مصرح به إلا لأشخاص محددين، غالبا ما تكون لمن له سلطة على المعلومة و حق التصرف فيها، وذلك لوجود نوع من الرابطة بين هذه المعلومة ومالكها باعتبارها ملكا خاصا به[1].

2- الخصائص المميزة للمعلومة:

تتميز المعلومات بمجموعة من الخصائص التي تساعد على التعرف على طبيعتها وأهميتها ومقدار الحماية اللازمة لها، وهي تنقسم إلى قسمين:

أ - الخصائص الأساسية و الأولية للمعلومة:

تستند المعلومة في أساسها على أربعة أركان رئيسية وهي نوع المعلومة، الصورة التي توجد عليها المعلومة، وشكل المعلومة، والوسيط الذي توجد عليه هذه المعلومة.

فبالنسبة لنوع المعلومة قد تكون نوعا من المعرفة أو تكون في شكل رسم هندسي، وقد تتخذ شكل مجموعة من الأوامر والتعليمات.

وأما الصورة التي توجد عليها فهي لا تظهر في صورة واحدة بل تتعدد صورها، فقد تكون داخل نظام المعالجة الآلية أو في حالة حركة من نظام إلى آخر، هذا وقد تتوقف قيمة المعلومة والحماية اللازمة لها في كثير من الأحيان على الصورة التي تكون عليها.

أما عن شكل المعلومة فيقصد به الطريقة التي تكتسب بها المعلومات، كأسلوب كتابة البرنامج و القواعد اللغوية التي تتعلق بترتيب الكلمات والرموز وقواعد التشفير التي تحدد طريقة تمثيل المعلومات بالشفرة، بحيث يمكن فك هذه الشفرة فيما بعد لقراءة محتوى هذه

[1] أنظر: سعيداني نعيم، مرجع سابق، ص 25.

المعلومة، ولهذا لابد أن يمتد نطاق حماية المعلومات إلى القواعد المتصلة بشكلها من أجل منع التلاعب بالمعلومات[1]، والذي يكون باستخدام الجاني لكلمة السر أو مفتاح الشفرة[2].

ب - الخصائص التكميلية للمعلومات:

تساعد الخصائص التكميلية للمعلومات في التعرف على نوع الحماية اللازمة لها وهي تتمثل أساسا في، مدى أهمية المعلومة، ومقدار ما تعطيه من فائدة و ما تتمتع به من صحة ومصداقية، بالإضافة إلى معرفة و تحديد مالك المعلومة والمكان الذي توجد به.

وكل هذه الخصائص و السمات الأساسية منها أو التكميلية تساهم في التعرف على طبيعة المعلومة ومن ثم تقرير قيمتها بغية الوقوف على درجة الحماية اللازمة لها[3].

ثالثا- طبيعة المعلومات الآلية المتعلقة بالحياة الخاصة:

من المبادئ الأساسية أن تخزين المعلومات لا يعني أن هذه المعلومات انتقلت من الخصوصية إلى العلنية، وفي هذا الصدد تكمن الصعوبة في تحديد المعلومات التي تثير مسألة الخصوصية.

فالمعلومات المجهولة لا تثير أية صعوبة ذلك أن المجهول لا خصوصية له[4]، والمعلومة الموضوعية هي التي تتعلق ببيانات مجردة مثل الاسم والموطن، وهي تعتبر من مميزات الشخصية لمن تتعلق به باعتبار أنه صاحب عناصر المعلومة.

أما المعلومة الذاتية فهي تحمل رأيا ذاتيا عن الغير، وعادة ما تتعلق المعلومات الموضوعية والذاتية بالحياة العامة للأفراد، وعلى العكس من ذلك تعتبر البيانات أو

---

[1] أنظر: سعيداني نعيم، المرجع نفسه، ص 21 و ما بعدها.

[2] أنظر: سوير سفيان، مرجع سابق، ص 44.

[3] أنظر: سعيداني نعيم، مرجع سابق، ص 24.

[4] أنظر بن عقون (حمزة)، مرجع سابق، ص 95 و ما بعدها.

المعلومات الإسمية والتي يتم تجميعها ومعالجتها وتخزينها هي التي تمس الحياة الخاصة للأفراد[1].

وللحفاظ على هذه الخصوصية للمعلومات يمكن استخدام كلمات المرور، كما يمكن استخدام التوقيع الإلكتروني لضمان سلامتها عند نقلها وتخزينها لمنع تغيير محتواها بالإضافة إلى التشفير أو البرامج المضادة للفيروسات[2].

الفرع الثاني: ضرورة الحماية الفنية للنظام الآلي.

اختلفت التشريعات حول ضرورة وجود أو عدم حماية فنية للنظام الآلي كشرط مسبق لتمتعه بالحماية الجنائية وهذا ما سيتم تناوله في الفرع الثاني.

أولا- المقصود بالحماية الفنية:

يقصد بالحماية الفنية اتخاذ تدابير وإجراءات عن طريق وسائل إلكترونية تعطل عملية التعدي على البيانات والمعلومات، فضلا عن إمكانية الوصول إلى مرتكب هذه الأفعال[3]، كما يقصد بها أيضا دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة باعتبارها إجراءات وقائية لتجنب اختراق النظام المعلوماتي.

هذا ويشترط لضمان توفر الحماية الكافية للمعلومات الإلكترونية السرية أو الموثوقية التكاملية وسلامة المحتوى، واستمرارية توفر المعلومات وعدم الإنكار[4].

---

[1] أنظر: بد القادر المومني (نهلا)، مرجع سابق، ص 168.

[2] أنظر بن جامع (بلال)، **المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت**، ماجستير، كلية العلوم الإنسانية و العلوم الاجتماعية، جامعة منتوري، 2005، ص 182 و ما بعدها.

[3] أنظر: عبد القادر (محفوظ)، حورية سويقي، **انعكاسات المعلوماتية على الوظيفة القضائية**، المجلة المصرية للدراسات القانونية و الاقتصادية، العدد 3، يناير 2015، ص 135.

[4] أنظر: سعيداني نعيم، مرجع سابق، ص 71.

ويقصد بسرية المعلومات ضمان حفظ المعلومات المخزنة أو المنقولة عبر الشبكة وعدم الاطلاع عليها أو استخدامها إلا بموجب إذن، أما سلامة المعلومة فتعني عدم تغيير المعلومات المخزنة أو المنقولة[1].

كما يقصد بمصطلح الحماية الفنية للنظام أيضا ذلك الإجراء الوقائي الذي يتخذه صاحب النظام أو صانع البرنامج أثناء وضعه له للحد من الاعتداءات الخارجية التي قد تقع عليه، وفي هذا الصدد هناك طريقتين من الحماية هما: أسلوب التشفير والتحقق من شخصية المتعاقدين عن طريق استخدام شفرة المفتاح العام[2].

ثانيا- مدى تمتع الأنظمة الآلية لمعالجة المعطيات المحمية فنيا بحماية جنائية:

قسمت أنظمة المعالجة إلى ثلاثة أنواع:

- ✓ أنظمة مفتوحة للجمهور.
- ✓ أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- ✓ أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

وفي هذا الصدد ذهب البعض إلى القول بأن النوع الثالث من هذه الأنظمة هو فقط الذي يتمتع بالحماية الجنائية، دون النوع الأول والثاني لأن الحماية في نظرهم يجب أن تقتصر على الأنظمة المحمية فنيا، فمن يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم[3].

والمشرع الفرنسي لم يشترط ضرورة أن يكون النظام محميا بوسيلة من وسائل الحماية الفنية مثل كلمة السر أو وسائل أخرى للحماية[4] ،وكذلك فعل المشرع الجزائري

---

[1] أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 36.

[2] أنظر: خشير مسعود، مرجع سابق، ص 105.

[3] أنظر: آمال قارة، مرجع سابق، ص 105.

[4] أنظر: عبد الغني محمد عطا الله (شيماء)، مرجع سابق، ص 102.

حيث لم يشترط هو الآخر أسوة بالمشرع الفرنسي لتوافر جريمة الاعتداء على نظم المعالجة الآلية ضرورة توافر الحماية الفنية لهذا النظام، بل أن يكون غير مأدون له في ذلك[1].

وعدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده، فالحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا.

كما أنه من المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق أو تخصيص النص العام إلا إذا وجد نص يجيز ذلك[2].

المبحث الثاني: صور التجريم المقررة لحماية نظم المعالجة الآلية للمعطيات.

تتعرض المعلومات المخزنة داخل النظام المعلوماتي لعدة انتهاكات كغيرها من المعلومات الورقية وذلك رغم ما تتميز به من خصوصية ومميزات، ويتم ذلك من خلال اختراق النظام الآلي لمعالجة المعطيات والبقاء فيه بطريقة غير مشروعة (المطلب الأول)، أو من خلال كشف مفاتيح التشفير وفضها (المطلب الثاني).

المطلب الأول: جريمة الدخول و البقاء.

لقيام جريمة الدخول والبقاء في النظام المعلوماتي يتطلب توافر الركن المادي (الفرع الأول) بالإضافة إلى الركن المعنوي (الفرع الثاني)، ليأتي بعد ذلك تقرير الجزاءات الملائمة لهذه الجريمة (الفرع الثالث).

---

[1] أنظر: صالح شنين، مرجع سابق، ص 73.

[2] أنظر: آمال قارة، مرجع سابق، ص 105.

الفرع الأول: الركن المادي.

تقوم كل جريمة بتوافر ثلاثة أركان أساسية منها الركن المادي وهذا ما سيتم التطرق إليه في الفرع الأول.

أولا- فعل الدخول:

يرى الفقه الفرنسي أن الدخول له مدلول مادي ومدلول معنوي، فالمدلول المعنوي يشبه الدخول إلى النظام المعلوماتي والذي هو بمثابة الدخول إلى ذاكرة الإنسان، أما المدلول المادي للدخول فإنه يتمثل في أن الشخص يكون قد حاول الدخول بالفعل إلى هذا النظام.

ووفقا لفكرة الدخول المعنوي، فإن ذلك الدخول يتحقق بأي صورة من صور التعدي فيستوي أن يكون مباشرا أو غير مباشر، هذا ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام أو اختراقه[1]، وكذلك فعل المشرع الجزائري، فالدخول يكون بأية وسيلة سواء عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها، أو باستخدام برنامج أو شفرة خاصة أو عن طريق استخدام الرقم الكودي لشخص آخر، أو الدخول من خلال شخص مسموح له بالدخول[2].

ولا يشترط توافر صفة معينة فيمن يقوم بعملية الدخول، حيث أن هذه الجريمة يقوم بها كل الأشخاص رجالا ونساء، محترفين وغير محترفين[3]، أي أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام، أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، فتتوافر الجريمة في كل حالة يكون فيها الدخول مخالفا لشروط الدخول التي نص عليها القانون أو

---

[1] أنظر: بيومي حجازي (عبد الفتاح)، **مكافحة جرائم الكمبيوتر و الانترنيت في القانون العربي النموذجي**، دار الكتب القانونية، مصر، 2007، ص 355.

[2] أنظر: خشير مسعود، مرجع سابق، ص 115.

[3] أنظر: عبد الفتاح مطر (عصام)، مرجع سابق، ص 283.

الاتفاق، أو مخالفا لإرادة من له الحق في السيطرة على النظام كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة، أو السرية المتعلقة بالمعلومات الذاتية أو الإسمية أو سر المهنة، أو أسرار الأشخاص مثل أسرار الحياة الخاصة المهنية.

ويكون الدخول غير مشروع أيضا إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إليه إلا أن الجاني لم يحترم تلك القيود، أو الدخول كان يتطلب دفع مبلغ من النقود وتم الدخول دون دفعه[1].

هذا ويتحقق فعل الدخول إلى النظام متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج، وكذلك يتحقق الدخول الغير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج ولكنه تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه، ولذلك يخرج من نطاق الدخول غير المشروع الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كما لا تقوم الجريمة إذا اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام[2].

ثانيا- فعل البقاء:

ويقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على النظام، فالبقاء يتمثل في عدم قطع الفاعل اتصاله بالنظام عند إدراكه أن وجوده فيه غير مشروع، فهو يبدأ من اللحظة التي كان يجب على الشخص فيها أن يغير وضعه بالخروج من النظام أساسا.

ومن صور البقاء استمرار وجود الجاني داخل النظام بعد المدة المحددة له، أي المصرح له بها وهذا يعني أن الجاني كان يحوز تصريحا بالدخول إلى النظام لكنه تجاوز

---

[1] أنظر: آمال قارة: مرجع سابق، ص 109.

[2] أنظر خشير مسعود، مرجع سابق، ص 115 و ما بعدها.

حدود التصريح بتجاوزه الوقت الذي يسمح به[1]، فالبقاء يفترض اختلاس وقت النظام ويتخذ صورة الجريمة المستمرة[2].

ومما لا شك فيه أن البقاء داخل النظام بعد دخوله عن طريق الخطأ لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل النظام على الرغم من معرفته انه غير مصرح له بالدخول لا يختلف في جوهره عن الدخول غير المصرح به الى النظام، فالنتيجة الاجرامية واحدة وهي الوصول الى برنامج غير مصرح للدخول إليه، والمصلحة التي يحميها القانون هي حماية نظام الكمبيوتر في الحالتين.

وقد يجتمع الدخول غير المشروع و البقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني له الحق في دخول النظام، ولكنه يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، فيتحقق بذلك الاجتماع المادي لجريمتي الدخول والبقاء الغير المشروع في النظام[3].

وإذا كانت هذه الجريمة على هذه الصورة تهدف أساس إلى حماية المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق بصورة غير مباشرة أيضا حماية للمعطيات أو المعلومات ذاتها، فيمكن من خلالها تجريم الاستخدام الغير مشروع للبطاقات الممغنطة إما لسرقتها أو للتزوير ثم استخدامها، وحتى وإن استخدمها صاحبها في سحب مبالغ دون أن يكون لديه رصيد كاف، أو عند عدم وجود رصيد، وتكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب البطاقة يعلم بأنه ليس له رصيد كاف[4].

---

[1] أنظر: عبد الفتاح مطر (عصام)، مرجع سابق، ص 288 و ما بعدها.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **مكافحة جرائم الكمبيوتر و الانترنيت في القانون العربي النموذجي**، مرجع سابق، ص 361.

[3] أنظر: خشير مسعود، مرجع سابق، ص 116.

[4] أنظر: آمال قارة، مرجع سابق، ص 111.

وقد اختلف الفقه حول انتهاء جريمة الدخول وبداية جريمة البقاء، فذهب رأي منهم إلى القول بأن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج والبقاء مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء و تنتهي بانتهاء حالة البقاء.

ويذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه الجاني أن بقائه داخل النظام غير مشروع[1]، أما الرأي الراجح و الأصوب فهو الذي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، و يكفي لتحقق هذه الجريمة البقاء داخل النظام كله أو في جزء منه[2].

وتعتبر هذه الجريمة سلوك مجرد أي أنها تبدأ أو تنتهي بانتهاء السلوك المكون لها وهو الدخول أو البقاء، دون أن يتطلب المشرع في نموذجها القانوني حسب نصوص التجريم أي نتيجة إجرامية[3].

وقد نصت المادة 394 مكرر 3/2 من قانون العقوبات الجزائري على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل للمعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه[4].

فعل المحو ويقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، أما التعديل فيقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى وقد يتم التلاعب في المعطيات عن طريق استبدالها، أو عن طريق التلاعب في

---

[1] أنظر: خشير مسعود، مرجع سابق، ص 117.

[2] أنظر: آمال قارة، مرجع سابق، ص 113.

[3] أنظر: خشير مسعود، مرجع سابق، ص 118.

[4] أنظر: آمال قارة، مرجع سابق، ص 113.

البرنامج وذلك بإمداده بمعطيات مغايرة لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها[1]، وفعل الإدخال يقصد به إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خيالية، أم كان يوجد عليها معطيات من قبل ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة ليسحب بمقتضاها النقود من أجهزة السحب الآلي، وذلك حين استخدامه لرقمه الخاص والسري للدخول و كذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا أكثر من المبلغ المحدد له، وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو التزوير.

وهذا يعني أن النشاط الإجرامي في هذه الجريمة يرد على محل أو موضوع محدد وهو المعطيات أو المعلومات التي تمت معالجتها آليا، والتي أصبحت مجرد إشارات أو رموز تمثل تلك المعلومات، وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزء منه[2].

الفرع الثاني: الركن المعنوي.

بالإضافة إلى الركن المادي للجريمة لا بذ كذلك من توافر الركن المعنوي وهذا ما سيتم تناوله في الفرع الثاني.

تعتبر جريمة الدخول أو البقاء من الجرائم العمدية بحيث يكفي لقيامها توافر القصد العام بعنصريه العلم والإرادة، فيكفي أن يعلم الجاني أنه قد دخل النظام و ليس له الحق في الدخول إليه، أو تعمد البقاء فيه رغم انتهاء مدة حقه في البقاء ولو كان الدخول مشروعا، أما إذا انتفى علمه ففي هذه الحالة لا تقوم الجريمة كأن يجهل وجود حظر الدخول، أو كان يعتقد خطأ أنه مسموح له بالدخول فيه، ولا يتأثر القصد الجرمي بالباعث أو الدافع على

---

[1] أنظر: بيومي حجازي (عبد الفتاح)، **مكافحة جرائم الكمبيوتر و الانترنيت في القانون العربي النموذجي**، مرجع سابق، ص 383 و ما بعدها.

[2] أنظر: آمال قارة، مرجع سابق، ص 120 و ما بعدها.

الدخول أو البقاء حتى ولو كان الفضول أو التنزه، ونفس الشيء بالنسبة للركن المعنوي بالنسبة للصورة المشددة لجريمة الدخول إلى النظام أو البقاء فيه[1].

الفرع الثالث: الجزاءات المقررة لجريمة الدخول و البقاء.

يتناول من خلال الفرع الثالث مختلف العقوبات التي قررها المشرع الجزائري لجريمة الدخول و البقاء في النظام.

أولا- الصورة البسيطة للجريمة:

اعتمد المشرع الجزائري مبدأ الهرمية في التدرج في العقوبات، بالإضافة إلى معيار الخطورة الإجرامية فنص على جريمة الدخول أو البقاء في صورتيها البسيطة والمشددة[2].

فبالنسبة للصورة البسيطة للجريمة فالعقوبة التي قررها المشرع الجزائري هي الحبس من ثلاثة أشهر إلى سنة وغرامة من 50000 إلى 100000 وهذا حسب نص المادة 394 مكرر من قانون العقوبات الجزائري.

ثانيا- الصورة المشددة للجريمة:

ضاعف المشرع الجزائري العقوبة إذا ترتب على ذلك الحذف أو التغيير لمعطيات المنظومة، أو تخريب لنظام اشتغال المنظومة إلى الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج[3].

---

[1] أنظر: خشير مسعود، مرجع سابق، ص 118 و ما بعدها.

[2] أنظر: خشير مسعود، المرجع نفسه، ص 126.

[3] أنظر: زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري و الدولي**، دار الهدى، عين مليلة، الجزائر، ص 49.

وهذا الظرف المشددة هو ظرف مادي يكفي أن تقوم بينه و بين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره[1].

المطلب الثاني: جريمة فك التشفير.

التشفير هو أحد الوسائل و الآليات الفنية التي يمكن إتباعها للحفاظ على سرية وسلامة المعطيات وتأمينها، ولذلك لابد أن يخضع لمجموعة من الضوابط والشروط (الفرع الأول)، بغية تحقيق الأهداف المسطرة له (الفرع الثاني).

إلا ان هذا الأخير كغيره من الأساليب تتعدد طرق ووسائل انتهاكه (الفرع الثالث).

الفرع الأول: تعريف التشفير و ضوابطه.

يتناول من خلال هذا الفرع تعريف التشفير و بيان مختلف الضوابط التي يقوم عليها.

أولا- تعريف التشفير:

1 - التعريف القانوني للتشفير:

عرف القانون العربي النموذجي التشفير بأنه: "تحويل البيانات المعالجة إلكترونيا إلى رموز لعدم تمكين الغير من انتهاك سريتها"[2]، كما عرفه المشرع المصري في قانون التجارة الإلكترونية بأنه: "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو من تغيرها"، و عرفه المشرع التونسي في الفقرة الأولى من المادة الثانية من قانون المبادلات و التجارة الإلكترونية على أنه: "استعمال رموز أو إشارات غير متداولة، تصبح بمقتضاها المعلومات المرغوب تحريرها أو

---

[1] أنظر: امال قارة ، مرجع سابق، ص 49.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **مكافحة جرائم الكمبيوتر و الانترنيت في القانون العربي النموذجي**، مرجع سابق، ص 75.

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

أما المشرع الجزائري فرغم إصداره للقانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني لم يتطرق إلى تعريف التشفير، بل اكتفى بتحديد أنواعه و النص عليه كلما اقتضت ضرورة استخدامه، وهو ما يتضح من خلال نص المادة الثانية في الفقرة الثامنة والتاسعة[2].

2 -التعريف الفقهي للتشفير:

التشفير عبارة عن عملية رياضية - معادلات خوارزمية - يتم من خلالها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهمها إلا بعد القيام بفك الشفرة وتحويل الرموز والإشارات إلى نص مقروء[3]، فالتشفير يعمل باستخدام شفرة (صيغة رياضية) ومفتاح لتحويل البيانات المقروءة (نص عادي) إلى شكل لا يستطيع الآخرون فهمه، والشفرة هي الوصفة العامة للتشفير والمفتاح الخاص بالشخص هو الذي يجعل البيانات فريدة من نوعها يمكن فك تشفيرها من يعرف هذا المفتاح فقط، وعادة ما تكون المفاتيح عبارة عن سلسلة طويلة من الأرقام التي تحميها اليات المصادقة المشتركة مثل كلمات المرور، أو الرموز أو القياسات الحيوية مثل بصمة الأصبع[4]، أي أن عملية تشفير المعلومات تقوم بطريقتين هما التشفير وفك التشفير[5].

---

[1]أنظر: بن غانم العبيدي (أسامة)، مرجع سابق، ص 157.

[2]أنظر: بلحسيني حمزة، مرجع سابق، ص 77.

[3]أنظر: فواز محمد (المطالقة)، **الوجيز في عقود التجارة الإلكترونية**، دار الثقافة للنشر، جامعة البلقاء، د س، ص 159.

[4]أنظر: OUCH، **النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي**، يوليو (تموز)، 2001، على الموقع http : //WWW.Securingthehuman.org

[5]أنظر: بن جامع (بلال)، مرجع سابق، ص 149.

ثانيا- ضوابط التشفير:

تقوم تقنية التشفير بحفظ وتأمين التوقيع الإلكتروني عن طريق استخدام مجموعة من الإجراءات والضوابط والتي أشار إليها المشرع الجزائري بعد إصداره للقانون 15-04 في أكثر من مرجع وتتمثل هذه الضوابط في:

1 - تشفير المعلومات و البيانات التي يتم تدوينها عبر وسائط إلكترونية هو أمر مباح من الناحية القانونية:

أقر المشرع الجزائري هذا الشرط في القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث أشار في المادة الثانية الفقرة السادسة إلى آلية التحقق من التوقيع الإلكتروني، والتي تعتبر حسب الفقرة الخامسة من نفس المادة رموز أو مفاتيح الشفرة العمومية، وكل بيانات أخرى مستعملة للتحقق من التوقيع الإلكتروني، ولم يكتفي بذلك وإنما أشار أيضا في الفقرة الرابعة من نفس المادة إلى آلية إنشاء التوقيع الإلكتروني واعتبارها جهاز أو برنامج معلوماتي معد لتطبيق بيانات فريدة، كالرموز أو مفاتيح التشفير الخاصة المستعملة من الموقع لإنشاء التوقيع وذلك حسب ما ورد في الفقرة الثالثة، والأكثر من ذلك اعتبار المشرع الجزائري التوقيع الإلكتروني مسألة قانونية لا يمكن رفض الاعتداد بها كدليل إثبات أمام القضاء حسب نص المادة التاسعة[1].

كما أن القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية تعامل مع التشفير بشكل مباشر من خلال نصوص خاصة، وأجاز استخدامه في المراسلات الإلكترونية وفي التعاملات الإلكترونية التجارية عبر شبكة الانترنيت، وأكد أهمية حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير الشخصية وفكها من أي اعتداء عليها، سواء تم ذلك باستخدام عناصر التشفير الشخصية الخاصة بالتوقيع من غير طرفي العلاقة، أو سرقة

[1] أنظر: بلحسيني حمزة، مرجع سابق، ص 81.

مفاتيح التشفير التي تفك النص المشفر وترجعه إلى النص الأصلي باستخدام مفاتيح التشفير الخاصة[1].

2 - الحق في الحفاظ على سرية البيانات و المعلومات المشفرة:

هذا يعتبر من ثاني الضوابط المرتبطة بالتشفير، فنجد المشرع الجزائري قد عاقب في نص المادة 65 من القانون 15-04 كل من يقوم بحيازة أو إنشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير، وكل ذلك في سبيل حماية الحق في الخصوصية وقد تراوحت العقوبة بين عقوبة سالبة للحرية و هي الحبس من 3 أشهر إلى 3 سنوات والغرامة المالية من 1000000 إلى 5000000 أو بإحدى هاتين العقوبتين و هذا بالنسبة للشخص الطبيعي، أما الشخص المعنوي فعقوبته هي الغرامة والتي تضاعف إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وهذا ما نصت عليه المادة 75 من نفس القانون[2].

واعتبر مشروع قانون التجارة الإلكترونية المصري أن الاعتداء على البيانات المرسلة عبر شبكة الانترنيت هو اعتداء على خصوصية و سرية البيانات والمعلومات المرسلة بين طرفي العلاقة، لأن تلك البيانات والمعلومات تتميز بالخصوصية والسرية وتعبر عن إرادة طرفي العلاقة، وإطلاع الغير على هذه البيانات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة والاعتداء على خصوصيتهم بمعرفة البيانات التي تم كشفها بعد فك التشفير.

وقد وضع المشرع المصري نصوصا في قوانين التجارة الإلكترونية لمعاقبة كل من يقوم بانتهاك سرية هذه البيانات المشفرة وإفشائها[3].

---

[1] أنظر: بن غانم العبيدي (أسامة)، مرجع سابق، ص 158.

[2] أنظر: بلحسيني حمزة، مرجع سابق، ص 82.

[3] أنظر: بن غانم العبيدي (أسامة)، مرجع سابق، ص 159.

3- أن يكون التشفير صادرا من جهات مختصة:

وسبب ذلك يرجع إلى أن عملية التشفير ترتبط بمعلومات هامة وسرية، سواء تعلقت بالتجارة الإلكترونية أو بالأسرار الخاصة بالأفراد أو الدولة، وفي هذا الشأن أقر المشرع الجزائري في المادة 14 أن التأكد من مطابقة الآلية المؤقتة لإنشاء التوقيع الإلكتروني يتم من طرف الهيئة الوطنية المكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه[1].

الفرع الثاني: أهداف التشفير و طرقه.

يتم استخدام تقنية التشفير من أجل تحقيق مجموعة من الأهداف عن طريق إتباع عدة طرق وهذا ما سيتم دراسته من خلال الفرع الثاني.

أولا- أهداف التشفير:

يهدف التشفير إلى تحقيق عدد من مظاهر أمن المعلومات و هي:

1. **سرية المعلومات:** وذلك بالاحتفاظ بالمعلومات في صيغة مخفية من أي شخص.
2. **سلامة البيانات:** بامتلاك الإمكانية لكشف معالجة البيانات من قبل الأطراف غير المرخص لهم.
3. **التوثيق:** فهي من ناحية تعمل على تحديد هوية الأطراف، أما فيما يخص والمعلومات المستلمة فينبغي أن تطابق المعلومات الأصلية المرسلة.
4. **عدم الإنكار:** بتدخل طرف ثالث موثوق به يكفل التحقق من صحة التوقيعات وسلامة المعاملة[2].

---

[1] أنظر: بلحسيني حمزة ، مرجع سابق، ص 82.

[2] أنظر: بلقاسم حامدي، مرجع سابق، ص 239 وما بعدها.

ومما سبق فإن استخدام التشفير يحقق أكبر درجة من الأمن و الحماية لمستخدمي شبكة الانترنيت نتيجة لاستعمال أفضل طرق التشفير التي يصعب حلها، ومن خلال منع الغير من الدخول إلى البيانات والمعلومات والحفاظ على سريتها وخصوصيتها للأطراف باستخدام وسائل إلكترونية رقمية، أو رموز معينة عوضا عن الكتابة التقليدية[1].

ثانيا- طرق التشفير:

التشفير كوسيلة لتأمين التوقيع الإلكتروني والوثيقة الإلكترونية يمكن أن يتم بطريقتين الأولى تسمى بالتشفير المماثل و الثانية تسمى التشفير اللامماثل.

1- التشفير المماثل:

في هذا النوع من التشفير يكون المفتاح السري معلوما للطرفين بحيث يستخدم كل من المرسل و المرسل إليه نفس المفتاح السري لتشفير الرسالة وفك شفرتها، حيث يتفق الطرفان منذ البداية على عبارة مرور يتم استخدامها وتتكون من حروف كبيرة وصغيرة ورموز أخرى، لتقوم بعد ذلك برمجيات التشفير بتحويل عبارة المرور إلى عدد ثنائي وهو الذي يشكل مفتاح تشفير الرسالة، وبعد أن يتم استقبال الرسالة يستخدم المستقبل نفس عبارة المرور وذلك من أجل فك النص المشفر وتحويله إلى شكله الأصلي المفهوم.

ومن أهم عيوب هده الطريقة أن الرسالة يستطيع فك شفرتها أي شخص غير المرسل إليه، وذلك بمجرد علمه أو حصوله على المفتاح السري مما يؤدي إلى انعدام الثقة في هذا النوع وتراجع العمل به، وفيما يخص المشرع الجزائري فهو لم ينص على هذه الطريقة من التشفير في القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين[2].

---

[1] أنظر: بن غانم العبيدي (أسامة)، مرجع سابق، ص 239 و ما بعدها.

[2] أنظر: بلحسيني حمزة، مرجع سابق، ص 78- إبراهيم أبو الهيجاء (محمد)، **عقود التجارة الإلكترونية**، ط1، دار الثقافة، عمان،د س، ص 74.

2 -التشفير اللامماثل (بالمفتاح العام):

جاء هذا النوع من التشفير لتجنب مشكلة التبادل غير الآمن للمفاتيح في التشفير المماثل، فعوضا عن استخدام مفتاح واحد يستخدم التشفير اللامماثل نوعين من المفاتيح تربطهما علاقة رياضية، أحدهما مفتاح خاص والثاني مفتاح عام[1].

يتكون المفتاح الخاص من مجموعة من الرموز والأرقام تخزن على بطاقة إلكترونية، ويستخدم هذا المفتاح لتشفير الرسالة و فك شفرتها و يكون معروفا لطرف واحد فقط هو المرسل الذي يبقى محتفظا بسريته[2]، وقد عرفه المشرع الجزائري في نص المادة الثامنة من الفقرة الثانية في القانون 15-04 بأنه "عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، و يرتبط هذا المفتاح بمفتاح تشفير عمومي".

أما المفتاح العام فهو على خلاف المفتاح الخاص يكون معروفا لطرفين أو أكثر، إلا أنه هو الآخر يتكون من مجموعة من الرموز والأرقام والتي يتم تبليغها إلى المرسل إليه ليتمكن من فك شفرة الرسالة التي تم تشفيرها بالمفتاح الخاص، وقد عرفه المشرع الجزائري في المادة الثانية الفقرة التاسعة بأنه "سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".

ورغم الاختلاف بين المفتاحين إلا أنهما يكملان بعضهما، وتعتبر هذه الطريقة أكثر أمانا من الطريقة الأولى لأن من يقع بحوزته المفتاح العام لا يقع في علمه المفتاح الخاص، و بالتالي عدم إمكانية فك شفرة الرسالة[3].

---

[1] أنظر: بلقاسم حامدي، مرجع سابق، ص 240.

[2] أنظر: بيومي حجازي (عبد الفتاح)، **التوقيع الإلكتروني في النظم القانونية المقارنة**، مرجع سابق، ص 31 و ما بعدها.

[3] أنظر: بلحسيني حمزة، مرجع سابق، ص 79.

الفرع الثالث: أساليب و طرق فك التشفير.

يتعرض التشفير إلى الانتهاك باستخدام أساليب وتقنيات مختلفة ومتطورة وهذا ما سيتم توضيحه من خلال هذا الفرع.

أولا- كشف مفاتيح الشفرة المتعلقة بالتوقيع الإلكتروني:

بفضل التوقيع الإلكتروني يتمكن مرسل المعلومات والرسائل الإلكترونية من تشفيرها وإضافة التوقيع[1]، إلا أنه قد يتم التلاعب في المعلومات الموجودة داخل النظام عن طريق استخدام الجاني لكلمة السر أو مفتاح الشفرة والتسلل إلى المعلومات المخزنة بالنظام المعلوماتي[2]، ويتم ذلك باستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك يتم تصميمها على غرار البرامج و الأنظمة المشروعة، أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني والقيام بنسخها وإعادة استخدامها بعد ذلك[3].

حيث تحتوي هذه البرامج على مليارات من الشفرات وتقوم باستغلال الحاسب الآلي في تجربة هذه الشفرات في ثوان معدودة، حتى تقوم بفتح وكشف المفاتيح والمواقع المشفرة[4].

ثانيا- فض المعلومة المشفرة:

يتعرض تشفير البيانات بوصفها طريقة من طرق حمايتها للاعتداء مثله مثل التوقيع الإلكتروني عن طريق فض الشفرة أو تسريبها من قبل من له حق الاحتفاظ بها، ولذلك يتعين حمايتها جنائيا ضد هذه الاعتداءات.

---

[1] أنظر: بن جامع (بلال)، مرجع سابق، ص 152.

[2] أنظر: سوير سفيان، مرجع سابق، ص 43.

[3] أنظر: بن سعيد بن سيف الغافري (حسين)، مرجع سابق، ص 18.

[4] أنظر: بن سعود محمد السراني (عبد الله)، مرجع سابق، ص 75.

وفي هذا الإطار عاقب المشرع المصري كل من يقوم بكشف مفاتيح التشفير المودع بمكتب التشفير، أو بفض معلومات مشفرة في غير الأحوال المصرح بها، وبذلك يخرج من نطاق هذه الحماية المعلومات المشفرة التي كشفت مفاتيح تشفيرها، أو فضت شفرتها دون أن تكون مودعة لدى مكتب التشفير.

وكشف مفاتيح الشفرة يكون من خلال تسليم برنامج الشفرة ذاته لمن ليس له حق في ذلك ولديه القدرة على فض الشفرة بنفسه أو بواسطة غيره.

أما فض المعلومات المشفرة يعني إعلانها وإذاعتها في غير الأحوال المصرح بها قانونا، كأن يقوم الجاني بفض شفرة بعض المعلومات وتسليمها لشركة منافسة وكانت هذه المعلومات تتعلق بصفقة جاري إبرامها لهذه الشركة مثلا، ويقوم الجاني ببيعها لصالح شركة أخرى.

ولذلك فإن تجريم كشف مفاتيح الشفرة أو تجريم فض المعلومات المشفرة يخدم في النهاية مصلحة التجارة الإلكترونية، لأن الصورة الأولى تحمي في الغالب سرية التوقيع الإلكتروني، أما الثانية فهي تحمي أموال وبضائع التجارة الإلكترونية ذاتها[1].

[1]أنظر: بيومي حجازي (عبد الفتاح)، **التجارة الإلكترونية و حمايتها القانونية**، مرجع سابق، ص 111 و ما بعدها.

خلاصة الفصل الثاني:

إن التجريم المقرر لحماية الحق في الحياة الخاصة في إطار نظم المعالجة الآلية، هو في الأصل يوفر حماية للبيانات والمعطيات الآلية التي يتم معالجتها وتخزينها داخل النظام المعلوماتي لارتباطها بخصوصية الأفراد، ذلك أن الاعتداء على هذه البيانات والمعطيات يشكل في حد ذاته اعتداء على الحياة الخاصة.

إلا أن هذا لا ينفي القول بأن هناك بعض الحماية العرضية الغير مباشرة للتوقيع الإلكتروني، إذ أنه لا يمكن أن يتحقق الاعتداء على هذه البيانات والمعطيات إلا من خلال اختراق الأرقام السرية وكشف المفاتيح المشفرة وإذاعتها.

الخاتمة:

إن الاستخدام المتزايد للتوقيع الإلكتروني بالنظر إلى الأهمية التي يكتسبها تستلزم ضرورة التدخل القانوني من أجل توفير الحماية الجنائية اللازمة له، خاصة مع عدم إمكانية تطبيق نصوص التزوير العادية على جريمة تزوير التوقيع الإلكتروني، و هذا ما فعله المشرع الفرنسي من خلال تعديل نصوص التزوير لتشمل كل أنواع التزوير بما فيها التزوير الإلكتروني، كما لجأت بعض التشريعات إلى إصدار قوانين خاصة توفر الحماية الكافية للتوقيع الإلكتروني و هذا ما فعله المشرع المصري، من خلال إصداره لقانون التوقيع الإلكتروني.

و من خلال دراستي للحماية الجنائية للتوقيع الإلكتروني في إطار جرائم التزوير في الفصل الأول، و التطرق لهذه الحماية في إطار التجريم المقرر لحماية الحق في الحياة الخاصة في الفصل الثاني تم التوصل إلى مجموعة من النتائج يمكن إجمالها فيما يلي:

1- إن جريمة تزوير التوقيع الإلكتروني تختلف عن جريمة التزوير العادية، حيث تقوم بأفعال مختلفة عن جريمة تزوير التوقيع العادي من خلال الحصول على منظومة إنشاء التوقيع الإلكتروني بطريقة غير مشروعة، أو من خلال فك تشفير الشفرة الخاصة بها و إعادة نسخها من جديد.

2- النصوص العامة لجرائم التزوير لا تنطبق على جرائم التزوير الإلكتروني، التي ترتكب في بيئة رقمية و عالم افتراضي غير العالم المادي الملموس، مما يستتبع معه القول بأن المشرع الجزائري لم يكفل التوقيع الإلكتروني بحماية جنائية خاصة من خلال القواعد العامة لجريمة التزوير و ذلك على عكس كل من المشرع المصري و التونسي.

3- إن حماية النظام الآلي لمعالجة المعطيات يعني حماية المعلومة في حد ذاتها والذي بدوره يعتبر حماية عرضية غير مباشرة للتوقيع الإلكتروني، لأن الاعتداء على هذه المعلومات و البيانات لا يمكن تصور حصوله إلا من خلال الاعتداء على التوقيع الإلكتروني.

4- يعتبر الاعتداء على حرمة الحياة الخاصة من خلال الاعتداء على المعلومات والمعطيات الآلية المخزنة في الحاسب الآلي، اعتداء غير مباشر على التوقيع الإلكتروني المعتمد عليه لحمايتها.

5- حماية النظام الآلي تتضمن بالضرورة حماية التوقيع الإلكتروني حتى و إن كان المشرع الجزائري لا يقصده رأسا، و إنما يقصد سرية و سلامة المعلومات والمعطيات الآلية.

و من خلال هذه النتائج يمكن تقديم بعض التوصيات ندكر منها:

1- ضرورة صياغة نصوص قانونية عامة لتشمل مختلف أنواع الجرائم الواقعة على التوقيع الإلكتروني مثلما فعله المشرع الفرنسي في باب التزوير الإلكتروني.

2- توفير حماية جنائية خاصة للتوقيع الإلكتروني من خلال تعديل النصوص التقليدية القائمة، و تضمينها ما يفيد صراحة حماية التوقيع الإلكتروني تحت طائلة العقاب على كل خرق في هذا المجال.

3- أو ضرورة اعتماد قانون خاص بالتوقيع الإلكتروني يتناول كل صور الاعتداء عليه و يكفل حماية جنائية خاصة به، كما هو معمول به لدى أغلب التشريع المقارن.

4- كما يجب الفصل بين جرائم المساس بالنظام الآلي لمعالجة المعطيات و جريمة التزوير، حيث أن المصلحة القانونية المحمية في إطار جرائم المساس بالنظام

الآلي هي سرية المعلومات و ليس التوقيع الإلكتروني، و إن كانت توفر حماية غير مباشرة له.

و بهذا ننهي هذا البحث بعرض أهم النتائج و الاقتراحات و التي يكون من الملائم أخذها بعين الاعتبار، نظرا للمكانة الهامة التي بات يحتلها التوقيع الإلكتروني في مجال المعلوماتية و في شتى المجالات الأخرى.

هذا و يبقى موضوع التوقيع الإلكتروني يثير الكثير من التساؤلات و الإشكاليات القانونية الهامة، و هذا البحث يعتبر بمثابة اللبنة أو الخطوة الأولى في طريق معالجة جوانب أخرى مختلفة عن هذا الموضوع.

قائمة المراجع:

المراجع باللغة العربية:

أولا . النصوص القانونية:

- القانون رقم 04/15 المؤرخ في 1 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسمية عدد 6، المؤرخة في 10 فبراير 2015.
- قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع، منشورات الأمم المتحدة، نيويورك، 2002.

ثانيا. الكتب:

1- إبراهيم أبو الهيجاء (محمد)، عقود التجارة الإلكترونية، ط1، دار الثقافة، عمان، د س.

2- أمين الرومي (محمد)، النظام القانوني للتوقيع الالكتروني، دار الكتب القانونية، مصر،2008.

3-أحمد عبد الله غرايبية (عبد الله)، حجية التوقيع الإلكتروني في التشريع المعاصر،ج1،ط1، دار الراية للنشر و التوزيع،عمان، 2009.

4-بن سيف الغافري (حسين)، الجرائم الواقعة على التجارة الإلكترونية، سلطنة عمان، 2006، موقع المنشاوي للدراسات والبحوثwww.minshawi.com

5-بيومي حجازي (عبد الفتاح)، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، د س.

6-بيومي حجازي (عبد الفتاح)، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية،مصر، 2007.

7-بيومي حجازي (عبد الفتاح)، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية،مصر، 2007.

8- بيومي حجازي (عبد الفتاح)، التجارة الإلكترونية و حمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الكتب القانونية، مصر 2007.

9- بيومي حجازي (عبد الفتاح)، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، د م، 2009.

10- بيومي حجازي (عبد الفتاح)، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط1، منشأة المعارف،الاسكندرية، 2009.

11- بن سعود محمد السراني (عبد الله)،فعالية الاساليب المستخدمة في جريمة التزوير الالكتروني، ط1،جامعة نايف العربية للعلوم الامنية، الرياض، 2011.

12- بن سعيد (لزهر)، النظام القانوني لعقود التجارة الالكترونية، دار هومة، الجزائر، 2012.

13- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، د س.

14- يوسف حسن(يوسف)، العقود التجارية الالكترونية الدولية، ط1، المركز القومي للاصدارات القانونية، القاهرة، 2012.

15- محمد سلامة (عماد)، الحماية القانونية لبرامج الحاسب الآلي و مشكلة قرصنة البرامج، ط1، دار وائل للنشر، عمان، 2005.

16- محمد عيد نصيرات (علاء)، حجية التوقيع الإلكتروني في الإثبات، ط1، دار الثقافة،عمان، 2005.

17- محمد الجنبيهي (منير)، تزوير التوقيع الإلكتروني،دار الفكر الجامعي،الاسكندرية، 2006.

18- محمد عبيدات (لورنس)، إثبات المحرر الإلكتروني، ط1، دار الثقافة،عمان، 2009.

19- عبد الحميد (ثروت)، التوقيع الإلكتروني، دار الجامعة الجديدة،الاسكندرية، 2007.

20- عبد الحميد نبيه (نسرين)، الجانب الإلكتروني للقانون التجاري، منشأة المعارف،الاسكندرية، 2008.
21- عبد القادر المومني (نهلا)، الجرائم المعلوماتية، ط1، دار الثقافة،عمان، 2008.
22- عبد الفتاح مطر (عصام)، التجارة الإلكترونية، دار الجامعة الجديدة،الاسكندرية، 2015.
23- فواز محمد (المطالقة)، الوجيز في عقود التجارة الإلكترونية،دار الثقافة للنشر،جامعة البلقاء، د س.
24- فرج يوسف (أمير)، بطاقة الائتمان و الحماية الجنائية لها، دار المطبوعات الجامعية،الاسكندرية، 2008.
25- فرج يوسف (أمير)، التوقيع الإلكتروني، دار المطبوعات الجامعية،الاسكندرية، 2008.
26- فوزي السقا (إيهاب)، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2008.
27-سعيد الغريب (فيصل)، التوقيع الإلكتروني و حجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005.
28-سعيد أحمد إسماعيل (محمد)، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، ط1، منشورات الحلبي الحقوقية، لبنان، 2009.
29-خشير مسعود، الحماية الجنائية لبرامج الكمبيوتر،دار الهدى، عين مليلة، الجزائر، 2010.
30-غسان ربضي (عيسى)، القواعد الخاصة بالتوقيع الإلكتروني، ط 2، دار الثقافة،الاردن، 2012.

ثالثا. الرسائل و المذكرات الجامعية:

1- بن جامع (بلال)، المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت، ماجستير، كلية العلوم الإنسانية و العلوم الاجتماعية، جامعة منتوري، 2005.

2- بن عبد الله بن معيض العبيدي (خالد)، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، ماجستير، كلية الدراسات العليا، 2009.

3- بن عقون(حمزة)،السلوك الاجرامي للمجرم المعلوماتي، ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011.

4- بوفروعة سوفيان، نظام المعلومات المحاسبي ودوره في تسيير المؤسسة الاقتصادية، ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، 2011.

5- براهيمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، دكتوراه،كلية الحقوق، جامعة محمد خضير بسكرة، 2014.

6- كميني خميسة، الإثبات بالكتابة في الشكل الإلكتروني، مذكرة التخرج لنيل شهادة المدرسة العليا للقضاء، 2007.

7- صالح شنين، الحماية الجنائية للتجارة الإلكترونية، دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، 2012.

8- سامي حميد الجادر (عدبة)، العلاقة التعاقدية المنبثقة عن استعمال بطاقة الائتمان، ماجستير، كلية العلوم القانونية، جامعة الشرق الأوسط عمان، 2008.

9- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، ماجستير،كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012.

رابعا. المجلات و الدوريات:

1- أبومارية (علي)، التوقيع الإلكتروني ومدى قوته في الإثبات، مجلة جامعة الخليل للبحوث،فلسطين، مجلد 5، عدد 2، 2010.

2- بلحسيني حمزة، الحماية القانونية والفنية للتوقيع الالكتروني في مجال البيئة الرقمية، مجلة العلوم القانونية والادارية، جامعة جيلالي الياس بسيدي بلعباس، عدد11، 2015.

3- بن غانم العبيدي (أسامة)، حجية التوقيع الإلكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، عدد 56، دس.

4-حنان مليكة، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم 4 الصادر بتاريخ 2009/2/25، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلد 26، عدد 2، 2010.

5- Mohammed Alisalem Abbas talibrozoqi, The Legal basis - Forthe protito of crditcardfraud;

مجلة المحقق للعلوم القانونية والسياسية، العدد 2، 2015.

6-عبد القادر (محفوظ)، حورية سويقي، انعكاسات المعلوماتية على الوظيفة القضائية، المجلة المصرية للدراسات القانونية والاقتصادية، العدد 3، يناير 2015.

خامسا. النشرات:

- 1- OUCH، النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي، يوليو (تموز)، 2001، على الموقع http : //WWW.Securingthehuman.org

سادسا. الموسوعات العلمية:

1- أنور بندق (وائل)، موسوعة القانون الإلكتروني و تكنولوجيا الاتصالات، ط1، دار المطبوعات الجامعية، الاسكندرية، 2007.

المراجع باللغة الفرنسية:

- OLIVIER D'AU ZON , le droit commerce électronique, Héricy, France, 2004
- Bernard Bouloc, Droit pénal général, 23° édition,Dalloz, paris, 2013.

الفهرس: