وزارة التعليم العالي والبحث العلمي
جامعة ابن خلدون– تيارت
كلية الحقوق والعلوم السياسية

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر
في الحقوق
التخصص: قانون جنائي
بعنوان:

الحماية الجنائية للتوقيع الإلكتروني

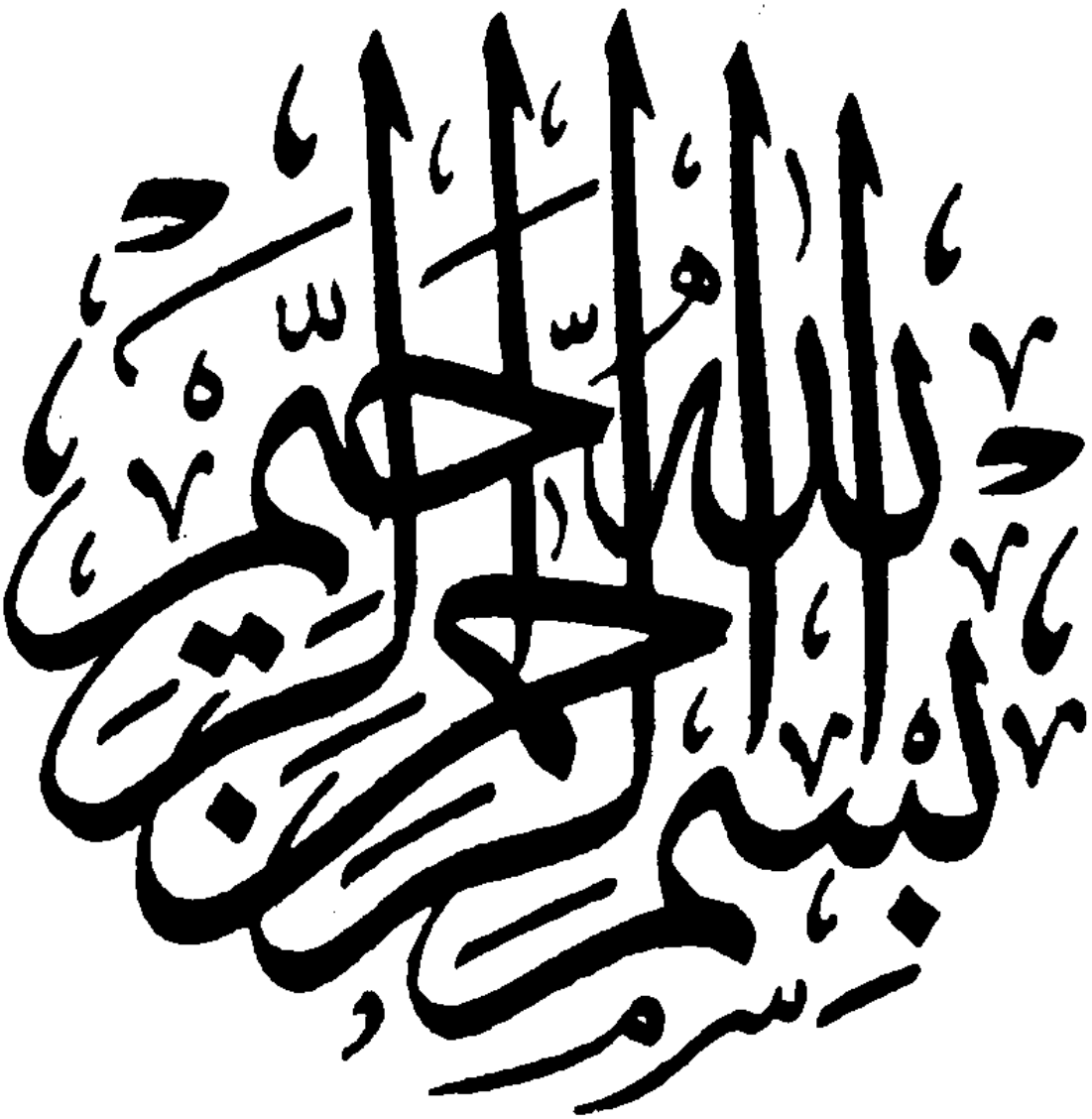
إعداد الطالبة:
* بلخير زهرة

إشراف الأستاذ الدكتور:
* بوشي يوسف

لجـنة المنـاقـشة		
د. عيشوبة فاطمة	أستاذة محاضرة (أ)	رئيسا
أ/د. بوشي يوسف	أستاذ التعليم العالي	مشرفا ومقررا
د. عبد الصدوق خيرة	أستاذة محاضرة (أ)	عضوا مناقشا
د. باهة فاطمة	أستاذة محاضرة (أ)	عضوا مدعوا

السّنة الجامعيّة

1441 ـ 1442هـ /2020- 2021م


بسم الله الرحمن الرحيم

كلمة شكر

﴿وَأَمَّا بِنِعْمَةِ رَبِّكَ فَحَدِّثْ﴾

الحمد لله والصلاة والسلام على رسول الله، أما بعد:

نشكر أولئك الأخيار الذين مدّوا لنا يد المساعدة خلال هذه الفترة وفي مقدمتهم أستاذتنا المشرفة على المذكرة الأستاذ الدكتور *بوشي يوسف* فله من الله الأجر ومنّا كل التقدير والاحترام حفظه الله، ومتعه بالصحة والعافية،

ونتقدم بأسمى آيات الشكر والامتنان إلى أساتذتنا الأجلاء الذين قبلوا مناقشة مذكرتنا

كما نتقدم بجزيل الشكر والعرفان إلى جميع أساتذتنا الأفاضل وكل عمّال وموظفي جامعة ابن خلدون –تيارت–

والشكر كل الشكر إلى كل من مد لنا يد العون في إنجاز هذه المذكرة وإلى كل الأحبة والأصدقاء

إهداء

أهدي عملي هذا و جهدي المتواضع:

إلى من علمني معنى الحياة و الحياء و الحب و التضحية و العطاء، إلى من تكتحل عيناه برؤية ما جنيت "أبي العزيز حفظه الله وأطال في عمره"

إلى من أضاءت لنا درب الحياة بنور الأخلاق التربية الفضيلة فعلمتنا أن العلم تواضع و العبادة إيمان و نجاح إلى أمي الغالية

إلى إخوتي وأخواتي

إلى براعم العائلة

إلى صديقاتي العزيزات

و إلى كل أفراد العائلة من الكبير إلى الصغير

و إلى كل الأحبة الذين لم يذكرهم قلمي هذا.

زهرة

مقدمة

مقدمة:

لقد كان التطور التكنولوجي الذي شهد مختلف وسائل الاتصال الحديثة أثر بالغ في تغيير وتطوير العلاقات بين الأشخاص في المجتمع، خاصة في مجالات تبادل السلع والخدمات، وإبرام العقود التجارية، حيث ظهر خلال القرن الماضي ما يعرف بالتجارة الإلكترونية التي لقيت رواجا كبيرا وحظيت بإقبال واسع وسط المستهلكين، نظرا لما توفره من مميزات عديدة، أهمها إلغاء الحدود الجغرافية بين المورد والمستهلك واختصار الزمان، وقلة التكاليف وتطور أنظمة الدفع، فبعد أن كان العقد يبرم بين الحاضرين ويتم تبادل الإيجاب والقبول في مجلس العقد، أصبح التعاقد يتم عبر شبكة الانترنت بين أشخاص لا يجمعهم مكان واحد، ولا يعرف بعضهم البعض في أغلب الأحيان، كما أن التوقيع على العقود شهد هو الآخر تطورا مذهلا بظهور التوقيع الإلكتروني الذي حل محل التوقيع المادي الملموس على الورق، لأنه نظرا لمتطلبات التجارة والعقود الإلكترونية، كان محتما أن توجد صيغة أخرى للتوقيع، تكون هي الأخرى إلكترونية، فظهرت أنواع شتى للتوقيع الإلكتروني كالتوقيع البيومتري والرقمي وغيرهما.

والتوقيع هو وسيلة يستخدمها الشخص لتحددي هويته والتعبير عن إرادته في الالتزام بمحتوى التصرف القانوني، وقد تطورت هذه الوسيلة مع تقدم الحضارات خاصة التي شهدت التعامل التجاري، ففي بداية الأمر كان استخدام الشمع على شكل ختم في العصور الرومانية القديمة لتوثيق المراسيم التي كانت تصدر باسم الملك، وقد تطورت وسيلة التوقيع مع استعمال ورق الكولان في القرون الوسطى المتقدمة، ومع بداية القرن السادس عشر أصبح التوقيع بخط اليد إلزاميا، وبعد تطور العلم ف سنة 1877م تم اختراع طريقة وضع البصمة على الورق، لأن كل شخص يتميز ببصمات أصابع لا يمكن أن تتشابه مع شخص آخر.

وفي الفترة القريبة الماضية دخلت البشرية مرحلة جديدة مع التطور الفكري، المعرفي والتقني، حيث ظهر التوقيع الإلكتروني الذي غير المفاهيم الكلاسيكية للكتابة والتوقيع التقليدي، فبدأت الدول تهتم به خصوصا مع تزايد استخدامه من يوم لآخر عبر شبكة الانترنت التي اختصرت المسافات بين الدول والأفراد وتشجيعا للتجارة الإلكترونية، فقد تضافرت الجهود على الصعيد الدولي والإقليمي والوطني لإصدار تشريعات وأحكام قانونية تقر بحجية هذه الأشكال المبتكرة، ومن أهم هذه التشريعات: قانون الأونيسترال بشان التجارة الإلكترونية سنة 1996 رقم 85، وقانون الأونيسترال بشان التوقيعات الإلكترونية لسنة 2001 الصادر في 2001/01/10، والتوجيه الأوروبي للتجارة الإلكترونية لسنة 2000 الصادر في 2000/06/08، إرشادات التوقيع الإلكتروني التي وضعتها نقابة المحامين الأمريكيين 1995.

والجزائر كغيرها من دول العالم سعت هي الأخرى من الاستفادة من تكنولوجيات الإعلام والاتصال، والعمل على الانتشار الواسع لاستعمال الحاسوب وشبكة الانترنت في شتى المجالات، فقد أصدر المشرع الجزائري القانون رقم 04/15 المؤرخ في 2015/02/01 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

أهمية الموضوع:

يعتبر موضوع الحماية الجنائية للتوقيع الإلكتروني بالغ الأهمية سواء من الناحية الإجرائية كونه يعالج جرائم الاعتداء على التوقيع الإلكتروني، أو من الناحية الموضوعية من حيث القواعد العامة أو في النصوص الخاصة التي تضع ضوابط قانونية و قضائية لردع مرتكبيها، كما تتجلى أهمية الموضوع أيضا في محاولة الوقوف على توجهات المشرع الجزائري في تنظيمه للتوقيع والتصديق الإلكترونيين، ووسائل الحماية الجنائية التي اعتمدها لمواجهة جرائم الاعتداء على هذه المنظومة الإلكترونية.

أسباب اختيار الموضوع:

كانت أسباب اختيار هذا الموضوع في ضوء بعدين موضوعي وذاتي، أما الأسباب الموضوعية فتمحورت حول الحداثة القانونية للحماية الجنائية للتوقيع والتصديق الإلكترونيين، مما يدفع نحو البحث في مدى انسجام النصوص القانونية للمنظومة من المستجدات الراهنة في مجال المعاملات الإلكترونية، وخاصة في أهمية التوقيع الإلكتروني، وأهمية المصادقة على هذا التوقيع بما يضفي عليه حجية في الإثبات، أما الأسباب الذاتية فترجع إلىّ أهمية وضرورة البحث في هذا الموضوع والطموح العلمي الذي يدفع باتجاه تقصي الجديد في ميدان القانون الجنائي للأعمال، والرغبة في المساهمة في إثراء النقاش القانوني في مثل هذه المواضيع.

الدراسات السابقة:

لقد كان لهذا الموضوع دراسات سابقة تمثلت فيمايلي: الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، لعزيزة لرقط، وهو بحث واجتهاد للدراسات القانونية والاقتصادية بالمركز الجامعي لتمنراست، العدد 2017/01/11، والحماية الجنائية للتجارية الإلكترونية، دراسة مقارنة، لصالح شنين، وهو بحث مقدم لنيل شهادة الدكتوراه في القانون الخاص بكلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2013/2012، الحماية الجنائية للتوقيع الإلكتروني، دراسة مقارنة، وهو بحث مقدم لنيل شهادة الدكتوراه في قانون الأعمال، لـ ترجمان نسيمة، كلية الحقوق والعلوم السياسية، جامعة تيارت، 2020/2019، وكذلك الحماية الجزائية للمعاملات الإلكترونية، دراسة مقارنة، وهي رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق، الدهبي خدوجة، جامعة أحمد دراية، أدرار، 2019/2018.

الإشكالية:

بالنظر لأهمية الحماية الجنائية للتوقيع الإلكتروني في المعاملات المدنية عامة، والتجارية خاصة التي أولاها المشرع لهذا الإجراء القانوني، ومدى حجيته في الإثبات، وعن هذه المشكلة يمكن أن نتساءل:

أ–ما مدى فعالية الحماية التي أقرها المشرع الجزائري للتوقيع الإلكتروني؟

ب–ما مدى انسجام النصوص المنظمة للحماية الجنائية للتوقيع الإلكتروني مع جرائم الاعتداء عليهما في ظل بيئة إلكترونية سريعة التطور؟

خطة البحث:

لدراسة موضوع البحث في ضوء الإجابة على التساؤلات تم الاعتماد على المنهج التحليلي والمقارن من خلال ما جاءت به التشريعات الأجنبية والوطنية، وخاصة التشريع الجزائري فيما يتعلق بالتوقيع والتصديق الإلكترونيين، ووسائل حمايتهما، فانتهجنا الخطة التالية:

الفصل الأول: الحماية الموضوعية للتوقيع الإلكتروني

المبحث الأول: التوقيع الإلكتروني كمحل للحماية الجنائية.

المبحث الثاني: الجرائم الماسة بالتوقيع الإلكتروني.

الفصل الثاني: الحماية الإجرائية للتوقيع الإلكتروني.

المبحث الأول:إجراءات الإثبات الجنائي للتوقيع الإلكتروني.

المبحث الثاني: التعاون الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني.

الفصل الأول

الحماية الموضوعية للتوقيع الإلكتروني

المبحث الأول:التوقيع الإلكتروني كمحل للحماية الجنائية.

المبحث الثاني: الجرائم الماسة بالتوقيع الإلكتروني.

تمهيد:

يعتبر التوقيع الإلكتروني أهم وسيلة مناسبة للمعاملات الإلكترونية والتجارة الإلكترونية خاصة، حيث يساهم في تثبيت المعاملات وخلق الثقة لدى الأطراف في التعاقد الإلكتروني، مما يشجع في زيادة حجم تبادلات التجارة الإلكترونية، ورغم الإيجابيات التي يقدمها التوقيع الإلكتروني، إلا أنه كان هدفا لعدة اعتداءات، إضافة إلى الاعتداءات التي مست شهادة التصديق الإلكتروني المنشأ له، كما لم تسلم البيانات التي يتضمنها.

وأصبح التوقيع الإلكتروني مع ظهور الوثائق الإلكترونية، يلعب دورا محوريا في إثبات حجية هذه الوثائق وإضفاء الحماية القانونية لها، وحتى يؤدي هذا التوقيع وظائف التوقيع التقليدي، سعت التشريعات الوطنية والدولية إلى تبيان مفهومه، خصائصه وصوره، وكذا وسائله.

ومن هذا المنطلق سوف نقسم هذا الفصل إلى مبحثين، حيث نتناول التوقيع الإلكتروني كمحل للحماية الجنائية (**المبحث الأول**)، بينما نتطرق إلى الجرائم الماسة بالتوقيع الإلكتروني (**المبحث الثاني**).

المبحث الأول: التوقيع الإلكتروني كمحل للحماية الجنائية.

يعد التوقيع الإلكتروني العنصر الأساسي في ظهور التجارة الإلكترونية، التي كانت بحاجة إلى توقيع يتلاءم وطبيعتها، قصد تضمين المعاملات الإلكترونية وتوثيقها بصفة عامة، والعقود المبرمة ضمت التجارة الإلكترونية بصفة خاصة، فقد أصبح اعتماد التوقيع الإلكتروني ضرورة عالمية إذ سارعت معظم التشريعات بالاعتراف به، كما هو الحال عليه في التشريع الفرنسي والمصري، أو ضمن قانون التجارة الإلكترونية مثل التشريع التونسي أو الأردني.

ويتعين لوضع إستراتيجية وقائية لحماية التوقيع الإلكتروني الوقوف على مفهوم التوقيع الإلكتروني ووسائله.

وفي ضوء ذلك سوف نقسم هذا المبحث إلى مطلبين، حيث نتناول مفهوم التوثيق الإلكتروني (**المطلب الأول**)، ونتطرق إلى وسائل التصديق الإلكتروني (**المطلب الثاني**).

المطلب الأول: مفهوم التوقيع الإلكتروني.

يهدف التوقيع الإلكتروني في القواعد التقليدية بيان هوية الشخص الموقع والتعبير عن إرادته وهو عنصرا جوهريا لوجود المحرر، فقد أخذ التوقيع صورا مختلفة ابتداء من التوقيع على الحجر أو الجلد أو الخشب، ثم بخط اليد والحبر والبصمة وصولا إلى التوقيع الإلكتروني، وهو علامة أو إشارة تميّز شخصية الموقع تعبر عن إرادته بالالتزام بمضمون السند الموقع وإقراره له.[1]

ويتميز التوقيع بخصائص يختلف فيها عن التوقيع التقليدي إذ يتميز بالسرعة والمرونة في إنجاز العمليات المصرفية، ويتمتع بدرجة المصداقية التي تمكن من الاطمئنان له في هذا المجال، وتتعدد صور التوقيع الإلكتروني بحسب الطريقة التي يتم بها التوقيع، وتتباين هاته الصور من حيث درجة ومستوى ما تقدمه من ضمان.

[1] – محمد المرسي زهرة، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، ط1، 1995، ص114.

الفرع الأول: تعريف التوقيع الإلكتروني.

يقصد بالتوثيق في المعاملات الإلكترونية التحقق من هوية الموقع، وأن الرسالة الموقعة منه تنسب إليه، ذلك أن المعاملات الإلكترونية تتم على دعامة إلكترونية غير ملموسة، يصعب التحقق من شخصية المتعامل مع الطرف الآخر، لذا أوجبت القوانين المقارنة هذا الأسلوب للحفاظ على صحة هذه المعاملات وسلامتها القانونية والحفاظ على سريتها.

أولا: تعريف التوقيع الإلكتروني وفقا للتشريعات والتوجيهات الدولية.

اختلفت التعاريف حول التوقيع الإلكتروني، فقانون الأونسترال النموذجي للتوقيع الإلكتروني لسنة 2001 عرّفه على أنه: "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، ويجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة بيانات ولبيان موافقة الموقع على المعلومات الواردة فيها"[1]

كما تدخل المشرع الفرنسي بتعديل بعض نصوص القانون المدني لتتفق مع التوقيع على العقود والمحررات الإلكترونية، فنص في المادة 4/1316 من القانون المدني الفرنسي المعدل بالقانون رقم 2000/230 الصادر في 13 مارس 2000 على تعريف التوقيع بأنه: «**التوقيع الذي يميز هويّة صاحبه ويضمن علاقته بالواقعة التي أجراها وتؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه**».

وهو ما يعني أنه إذا ما تم التوقيع في شكل إلكتروني وحب استخدام طريقة موثوق بها لتمييز هوية صاحبه. وجديرا بالذكر أن هذه المادة لا تطبق فقط على العقود المدنية الإلكترونية بل يمكن تطبيقها على العقود الإدارية، حيث أن المادة 03 من المرسوم رقم 2002-692 تؤكد

[1] – المادة 02 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

على أن التوقيعات والطلبات التي يتم إرسالها عن طريق وسيط إلكتروني، يجب أن يتم توثيقها وفقا للشروط المنصوص عليها في المادة 4/1316 من القانون المدني الفرنسي.[1]

وفي القانون الأمريكي حظي التوقيع الإلكتروني بنصيب وافر الأهمية في التشريع الأمريكي على مستويي الاتحاد الفدرالي والولايات المتحدة في آن واحد، فقد صدر القانون الموحد للمعاملات الإلكترونية لعام 1999 على مستوى الولايات المتحدة الأمريكية وقد عرف القسم 2.8 من بأنه: «**صوت أو رموز أو عملية إلكترونية ترفق أو تربط منطقيا بسجل يقوم بتنفيذها أو إقرارها شخص يقصد منها التوقيع على السجل**»[2]

أما القانون الفدرالي الأمريكي بشأن التوقيعات الإلكترونية في التجارة العالمية والمحلية الصادر في 30 يونيو 2000 فعرّف التوقيع الإلكتروني بأنه: «**أصوات، إشارات، رموز أو أي إجراء آخر مرتبط به منطقيا بنظام معالجة المعلومات إلكترونيان ويقترن بتعاقد أو مستند أو محرر يستخدمه الشخص قاصد التوقيع على المحرر أو المستند**»[3]

أما القانون الإنجليزي فقد نصت المادة 1/7 من قانون الاتصالات الإنجليزي لعام 2000 على أنه في مسائل الإثبات القانوني يعتبر التوقيع المرتبط بأنه وسيلة اتصالات إلكترونية وأنه شهادة تفيد توقيع صاحبها أنهما مقبولان كدليل إثبات في أية منازعة تتعلق بالتوقيع أو البيانات.[4]

---

[1] – Lecleccq Jean, La signature electronique, lectur critique, technique et juridique, le décret du 30 mars 2001 relatif a la signature, p 56.

[2] – خالد ممدوح إبراهيم، التوقيع الإلكتروني، الدار الجامعية، الإسكندرية، مصر، ط1، 2000، ص 41.

[3] – إزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2016، ص 50.

[4] – أيمن سعد سليم، التوقيع الإلكتروني "دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر،2004، ص 62.

ثانيا: تعريف التوقيع الإلكتروني في التشريعات العربية.

قامت الدول العربية بإصدار تقنيات خاصة بتنظيم التوقيع الإلكتروني، وأخرى عدّلت من قوانينها الخاصة بالإثبات من أجل مواكبة التقدم التكنولوجي، ومنها:

01-القانون التونسي:

تعتبر تونس من الدول العربية ذات السبق في إصدار قانون التوقيع الإلكتروني، حيث صدر قانون التوقيع الإلكتروني عام 2000 وهو القانون رقم 83-2000 الخاص بالتوقيع الإلكتروني والتجارة الإلكترونية، إلا أن المشرع التونسي لم يورد تعريفا خاصا بالتوقيع الإلكتروني وإنما اكتفى بتنظيم أحكامه، وذلك من خلال توضيح الإجراءات المتعلقة بالتشفير الخاصة بالتوقيع الإلكتروني في المادة 2/6-7.

02-القانون المصري:

نصت المادة 14 الرابعة عشر من القانون المصري رقم 15-04 على أن: « **التوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية، إذ روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون**»[1]

ونصت المادة 18 من ذات القانون على أنه: « **يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:**

[1] – المادة 14 من قانون التوقيع الإلكتروني المصري رقم 83 لسنة 2015.

-ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره، وسيطرة الموقع وحده دون غيره على الوسيط الإلكتروني، مع إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني»[1]

وكل هذه الشروط منصوص عليها في نص المادة 06 من قانون الأونيسترال النموذجي، فعرّف المشرع المصري التوقيع في القانون 15-04 أنه ما يوضع على محرر إلكتروني ويتحقق في شكل حروف وأرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد ويسمح بتحديد شخص الموقع وتمييزه عن غيره.

كما عرّفه قانون التجارة الإلكترونية المصري في المادة الأولى منه بأنه: «**حروف وأرقام ورموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميّزه عن غيره**»[2]

وبمناقشة التعريفين المذكورين أعلاه نجد أن التعريف الخاص بالتوقيع الإلكتروني في قانون التجارة الإلكترونية المصري، ويعتبر هو الأفضل والأدق.

03-القانون الجزائري:

اعتد المشرع الجزائري بالتوقيع الإلكتروني لأول مرة بنص المادة 2/327 من القانون المدني.[3] ومن ثمة في القانون المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.[4]

---

[1] - المادة 18 من قانون التوقيع الإلكتروني المصري رقم 15-04.

[2] - راشد بن حمد البلوشي، التوقيع الإلكتروني والحماية الجزائية المقررة له "دراسة في القانون العماني والقانون المقارن"، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2018، ص 25.

[3] - المادة 2/327 من الأمر 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني الجزائري المعدل والمتمم بموجب القانون 07-05 المؤرخ في 13 مايو 2007.

[4] - المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 2001/05/09.

وصولا إلى تعريف المشرع الجزائري للتوقيع الإلكتروني في قانون خاص بالتوقيع والتصديق الإلكترونيين حصرا متمثلا في القانون رقم 15-04 المؤرخ في 2015/02/01 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، فعرّفه في المادة 1/2 من ذات القانون على أنه: «**مجموعة من البيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة للتوثيق**»

فاعترف المشرع الجزائري للتوقيع الإلكتروني في القانون المدني في المواد 323مكرر و 323 مكرر1 و 327، ونصت المادة 323 مكرر المستحدثة بالقانون 05-01 المؤرخ في 2015/07/20 على ما يلي: «**ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها**»

ونصت المادة 323 مكرر 1 من نفس القانون على أنه: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات على الورق شرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**»

وكذلك المرسوم التنفيذي رقم 07-162 لسنة 2007 فقد عرّف المشرع الجزائري التوقيع الإلكتروني من خلاله بنص المادة 03 منه.[1]

بالإضافة إلى الفقرة 02 من المادة 03 من المرسوم السابق الذكر، تضمنت التوقيع المؤمن وعرّفته على أنه: «**توقيع إلكتروني يفي بالمتطلبات الآتية:**

-أن يكون خاصا بالموقع.

[1] - المادة 03 من المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 الصادر في 2001/05/09 ونصها: «**التوقيع الإلكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323مكرر و 232 مكرر1**»

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

– يضمن مع الفعل المرتبط به صلة، بحيث يكون أي تعديل لاحق للفعل قابلا للكشف»

ويتضح من خلال هذه النصوص أن المشرع الجزائري قد عرّف التوقيع الإلكتروني من خلال مجموعة عناصر قانونية وتقنية، إضافة إلى تبنيه التوقيع الإلكتروني العام أو البسيط والتوقيع الإلكتروني المؤمن.[1]

الفرع الثاني: خصائص ووظائف التوقيع الإلكتروني.

سوف نتطرق لأهم الخصائص التي يتميز بها التوقيع الإلكتروني، كما نتناول أهم وظائفه.

أولا: خصائص التوقيع الإلكتروني.

يتميز التوقيع الإلكتروني بخصائص أساسية ومتميزة عن التوقيع الكتابي التقليدي كونه يتم كليا أو جزئيا عبر وسائط إلكترونية من خلال أجهزة الكمبيوتر أو عبر شبكة الأنترنت، ومن بين الخصائص التي يتميز بها ما يلي:

01–الخصوصية:

يؤدي إلى رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين على شبكة الأنترنت خاصة في مجال التجارة الإلكترونية من خلال إمكانية تحديد هوية المرسل والمستقبل إلكترونيا، والتأكد من مصداقية الأشخاص والمعلومات.

كما يساعد التوقيع الإلكتروني المؤسسات على حماية نفسها من عمليات التزييف وتزوير التوقيعات.

[1] – يمينة حوحو، عقد البيع الإلكتروني "دراسة مقارنة"، أطروحة دكتوراه، جامعة بن عكنون، الجزائر،2012، ص 177.

02-التعرّف على المستخدم:

تتم عملية التحقق من هوية الأشخاص والتعرف على مصادر البيانات والبطاقات الذكية، او عن طريق شهادة التصديق الإلكتروني المصدرة من جهة التصديق الإلكتروني، وكلما زادت الحاجة لدقة تحديد الهوية يتم اللجوء إلى عدة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم.[1]

03-وحدة البيانات:

هي عملية حماية البيانات ضد التغيير أو التعريف عنها ببيانات أخرى، وتتم هذه العملية باستخدام تقنية البيانات ومقارنة ببصمة الرسالة المرسلة لبصمة الرسالة المستقبلة أثناء نقلها، وأن مستقبل الرسالة يمكنه معرفة ذلك عبر تلقي، حيث أنه إذا حصل أي تغيير أو تعديل على المستند أثناء إرساله اعتبر تزويرا.

04-السرعة والمرونة:

يعتبر الإمضاء بخط اليد وسيلة خلق لحالة واقعية ظاهرة، ومشاهدة وتعبير مجرد عن حالة نفسية باطنية، تتمثل في نقل القبول إلى صورة محسوسة، وقد برزت العديد من التقنيات والتي يمكنها النهوض بهذه الغاية، والتي تجاوز بعضها مرحلة التجربة لتدخل مرحلة التسويق، ومن ذلك تحديد الشخص من خلال صوته، التي ترتكز على مقارنة بعض الكلمات التي يتفوه بها المتعاقد عند إبرام التصرف القانوني بوسائل إلكترونية مع تسجيل صوتي سابق، وكذلك ما يصطلح عليه Reconnaissance dynamique de la signature.

حيث يسجل الإمضاء بواسطة آلة إلكترونية حساسة، والتي يمكنها مقارنة التوقيع بالإمضاءات السابقة مع الأخذ بعين الاعتبار الحالة النفسية والمالية للشخص، غير أن الإمضاء

[1] – لالوش راضية، أمن التوقيع الإلكتروني، رسالة ماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 37.

الإلكتروني يبقى التقنية الأكثر انتشارا واستقرارا وهو ما من شأنه أن يدخل تحويرات على قانون الإثبات.

ولقد استعملت هذه التقنية بالخصوص في سحب الأموال إلكترونيا بواسطة البطاقة المغناطيسية، فهذه الأخيرة متعددة فهناك بطاقات السحب، والتي تمكن من سحب الأموال من الموزع الآلي للنقود وهناك بطاقات والتي تستعمل لتسديد حسابات أصحاب المزادات الكبرى، وكذلك الخدمات، وهي نفس الوظيفة التي تؤديها بطاقات الائتمان، والتي تتميز عن غيرها بوجود اتفاقية اعتماد بين واضع البطاقة "يكون غالبا مؤسسة مصرفية" والزبون، ومن نتائجها استفادة هذا الأخير من البطاقة في الوفاء بحاجياته على أن يسدد مبالغ الاعتماد خلال مدة زمنية معينة والجانب المهم في كل هذا أنم استعمال البطاقات المغناطيسية يتم بعد قراءتها إلكترونيا، وللتأكد من صحة الرقم السري على المدخل من طرف الزبون، ثم في المرحلة الأخيرة تسجيل العملية المصرفية المنجزة منه، ثم نقل كل هذه المعطيات إلكترونيا إلى الحاسوب المركز على المؤسسة، ليقوم إلكترونيا بتسجيل العملية بحساب الزبون.[1]

05-مصداقية التوقيع الإلكتروني:

إن التصديق على التصرف القانوني يعني إعطاءه شكلا قانونيا ملزما، مثال ذلك التأشيرة على المحرر بصورة تمكن من معرفة مصدره، وهو ما كان يوفره الإمضاء بخط اليد.

غير أن حداثة التقنيات كانت وراء هذا النوع من التوقيع الإلكتروني، الذي تعتمده التجارة الإلكترونية ف إجراءاتها على شبكة اتصال مفتوحة، كما أن غالبية العقود التي تتم بين أطرافها تعد من العقود المبرمة بين غائبين، وذلك بسبب اختلاف مكان وزمان التعاقد، وغياب العلاقة

[1] - لالوشي راضية، المرجع السابق، ص 37.

المباشرة بين أطراف التعاقد إذ أنهم في أغلب الأحيان لم يدخلوا في علاقات مع بعضهم البعض من قبل.

لذلك فإن توافر عنصري الأمان والثقة في هاتين الحالتين ليس مطلوبا فحسب بل ضروري لتطوير التجارة الإلكترونية وتنمية المبادلات الاقتصادية، لذلك ارتأت التشريعات الدولية والإقليمية والوطنية إيجاد وسيط ثالث وظيفة توطيد العلاقات وتوثيقها بين الأشخاص الذين يعتمدون على الوسائط الإلكترونية خاصة شبكة الأنترنت في إبرام تصرفاتهم.[1]

ومن خلال ما سبق في خصائص التصديق نستنتج أنه يسند لمؤدي خدمات التصديق الإلكتروني بأنها عملية إلكترونية تهدف إلى ضمان صحة البيانات الإلكترونية وسلامتها، وتغطي مجالات عدة كالتجارة الإلكترونية والإدارة والخدمات البنكية، فيتم إصدار وتسليم شهادات التصديق الإلكتروني التي تضمن فيها السلامة وصحة تلك البيانات.[2]

ففي فرنسا تختص الإدارة المركزية سلامة نظم المعلومات بالتصديق على التوقيع الإلكتروني، ولها أن تمنح ترخيصا لمزاولة نشاط خدمات التصديق الإلكتروني، وفقا للشروط والإجراءات المنصوص عليها في قانون التوقيع الإلكتروني ولائحته التنفيذية، كما أنها تختص باعتماد الجهات الأجنبية المختصة بإصداراتها ذات التصديق الإلكتروني.[3]

أما في مصر فإن هيئة تنمية صناعة تكنولوجيا المعلومات هي سلطة التصديق الإلكتروني العليا، ولها أن ترخص في مزاولة نشاط خدمات التصديق الإلكتروني، وفقا للشروط والإجراءات

[1] – عرض بعنوان: التوقيع الإلكتروني، 06مارس 2020.

[2] – يمينة حوحو ، المرجع السابق، ص 208.

[3] – المرسوم الصادر عن مجلس الدولة في 2002/04/18.

المنصوص عليها في قانون التوقيع الإلكتروني ولائحته التنفيذية، كما أنها تختص باعتماد الهيئات الأجنبية المختصة بإصداراتها ذات التصديق الإلكتروني.[1]

أما في التشريع الجزائري فدور مؤدي خدمات التصديق إلى جانب تسليمه لشهادات المصادقة الإلكترونية، يقوم بأداء خدمات أخرى مرتبطة بالتوقيع الإلكتروني، منها حفظ الوثائق الإلكترونية، واتخاذ التدابير اللازمة لتوفير الحماية لها وفقا للشروط المنصوص عليها قانونا، وهو ما نصت عليه المادة 03 من المرسوم التنفيذي رقم 07-162 لسنة 2007 بقولها أن مؤدي خدمات التصديق الإلكتروني يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني.[2]

إذ تختص السلطة الاقتصادية بتقديم ترخيص للتصديق الإلكتروني من أجل القيام بنشاط تأدية خدمات التصديق الإلكتروني، وهو ما جاء في نص المادة 33 من الفصل الثالث، القسم الأول، الفرع الأول من القانون رقم 15-04 لسنة 2015، كما أضاف القانون نفسه وأشار بنص المادة 41 وما يليها إلى أن مؤدي خدمات التصديق الإلكتروني يكلف بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني.[3]

ثانيا: وظائف التوقيع الإلكتروني.

لاشك في أن التوقيع أيا كانت صوره وأشكاله لابد أن تتوفر فيه شروط معينة لكي يؤدي وظيفة أي إضفاء القوة الثبوتية على المحرر، وهذه الوظيفة لا تتحقق إلا إذا تم تحديد التوقيع بشكل واضح وصريح من خلال شروطه وكذا وظائفه وخلاف ذلك لا يعتد به قانونا.

[1] – عابد قايد عبد الفتاح قايد، المرجع السابق، ص 76.

[2] – ينظر: المادة 03 من المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30.

[3] – القانون رقم 15-04 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين.

وكما هو الحال بالنسبة للتوقيع التقليدي تجمع بعض التشريعات على أن التوقيع الإلكتروني وحتى يحوز على القوة الثبوتية فلابد من خلال التعاريف السابقة أن يحقق وظائف أساسية تتمثل في:

01-مدى تحديد التوقيع الإلكتروني لهوية الشخص الموقع:

حتى يقوم التوقيع بوظيفته، لابد أن يكون التوقيع علامة مميزة لشخصية الموقع عن غيره، وتضمن تحديد هويته، وقد أكد هذا الشرط قانون الأونسترال النموذجي الخاص بالتوقيعات الإلكترونية، حيث نصت المادة 01 منه على أنه إذا استخدمت طريقة لتعيين هوية ذلك الشخص، وأيضا المادة الثانية من قانون الأونسترال بشأن التوقيعات الإلكترونية لعام 2001 ما يلي: «**يجوز أن تستخدم لتعيين هوية الموقع**».[1]

هذا وقد نصت المادة 02/ فقرة 02 من القانون 15-04 بأن الشخص الموقع هو شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي، أو المعنوي الذي يمثله. [2] وبالتالي فإنه بتوافر هذا الشرط في التوقيع الإلكتروني يؤدي إلى اتجاه نية الموقع على المحرر بمضمونه، ويكون شاهدا على نيته بالالتزام بمضمون العقد الموقع عليه. ومن الضروري أن يكون التوقيع دالا ومحددا لشخص الموقع ليتحقق دوره في الإثبات.

02-التعبير عن إرادة الموقع:

ذكرنا سابقا أن التوقيع بشكل عام يعرف على أنه بمثابة تعبير عن إرادة الموقع بمضمون التصرف القانوني، وهذا ما أكدته محكمة النقض المصرية، حيث قررت بأن ثبوت صحة التوقيع

[1] - خالد ممدوح إبراهيم، التوقيع الإلكتروني، الدار الجامعية، الإسكندرية، مصر، ط1، 2000، ص 110.

[2] - ينظر: المادة 02/ف2 من القانون رقم 15-04 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بجمهورية مصر العربية.

بعدم إنكاره صراحة كافية لإعطاء الورقة حجيتها في أن صاحب التوقيع قد ارتضى بمضمونها والالتزام بها ومؤداه إعطاء الورقة حجيتها.[1]

ولعل هذا الشرط يعتبر من الشروط المشتركة بين التوقيع الكتابي والتوقيع الإلكتروني، حيث يستوي في ضرورة توفر هذا الشرط أن يكون التوقيع كتابيا حرر بخط اليد على الورق وأن يكون إلكترونيا سواء كان هذا التوقيع رموزا، أرقاما، إشارات بحيث توقع على بيانات محرر إلكتروني.[2]

03-إثبات حضور صاحب التوقيع:

بالرغم من أن التوقيع الإلكتروني لا يعني بالضرورة الحضور المادي والجسدي للأفراد في مجلس العقد وقت إبرام العقد او التصرف القانوني، إلا أن هناك من يرى بأن استعمال البطاقة الإلكترونية وإدخالها في المكان المناسب بجهاز الصرف الآلي وإدخال الرقم السري ثم تدوين قيمة المبلغ المراد سحبه على الجهاز يعد دللا على الحضور المادي للشخص ذاته لأن الرقم السري يكتب بحضور الشخص المعني.[3]

الفرع الثالث: صور التوقيع الإلكتروني.

أدى التطور الحاصل في نطاق نظام المعلومات والاتصالات إلى ظهور العديد من الصور التي يتخذها التوقيع الإلكتروني والتي تختلف باختلاف الطريقة التي تتم بها، كما تختلف من حيث قدرتها على توفير الثقة والأمانة ووسائل الحماية التي تعتمد على الوسلة التقنية المستخدمة.[4]

---

[1] – محكمة النقض المصرية، النقض المدنين جلسة 05 يونيو 2001، الطعن رقم 564 المشار إليه في المحاماة، العدد 02، 2002، ص 70.

[2] – راشد بن حمد البلوشي، المرجع السابق، ص 51.

[3] – فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2005، ص 216.

[4] – سماح مقران، التوقيع الإلكتروني ودوره في عصرنة الإدارة الإلكترونية، أطروحة دكتوراه، جامعة قاصدي مرباح، ورقلة، 2013/2012، ص 13.

وصور التوقيع الإلكتروني متعددة ومتنوعة، ولعل أهم الأنواع المعروفة حتى الآن والتي توصلت التكنولوجيا المتطورة إليها تتمثل في التوقيع الرقمي "Signature jigital" والتوقيع بالقلم الإلكتروني pen-op والتوقيع بالنقر على مربع الموافقة ok.box والتوقيع بالخواص الذاتية البيومتري biométriques والتوقيع باستخدام البطاقة الممغنطة الذكية المقترن بالرقم السري على PINم ونتعرض لكل منها على التوالي:

أ-التوقيع الرقمي Digital Signature:

بدأ باستخدام التوقيع الرقمي في المعاملات البنكية، حيث نجد البطاقات الذكية smart card وبطاقات الموندكس mondex-card التي تحتوي على رقم سري يستطيع حامل البطاقة من خلالها القيام بكافة العمليات البنكية من خلال جهاز الصرف الآتي ATM، ثم تطور استخدام هذا التوقيع وبدأ يستخدم كأسلوب موثوق به في الرسائل المتبادلة إلكترونيا.

يقصد بالتوقيع الرقمي بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة على صورة مشفرة.[1]

يتم تحويل المحرر المكتوب باستخدام العمليات الحسابية من أسلوب الكتابة العادية إلى معادلة رياضية وتحويل الترقيم إلى أرقام، وحتى يكتمل المحرر من الناحية القانونية فإنه يجب وضع التوقيع

[1] - **التشفير**: يقصد بالتشفير او الترميز هو "فرع علم الرياضيات التطبيقية الذي يعني تحويل نص الرسائل إلى صيغ غير مفهومة ثم بعد ذلك إعادتها إلى صيغتها الأصلية" وقد طورت شركة IBM الامريكية لأجهزة الكومبيوتر أحد نظم التشفير أو عملية رياضية مبنية على خوارزميات -لوغاريتمات- تنشأ صورة رقمية للرسالة أو شكلا مضغوطا من الرسالة يشار إليها بعبارة ملخص الرسالة Message digest ويطلق عليها ايضا بصمة رسالة Message fin ger printe تتخذ شكل قيمة بعثرة hash values أو نتيجة بعثرة hash result تنفرد به الرسالة إلى حد كبير، أو على تغيير يطرأ على الرسالة الإلكترونية يترتب عليه دائما نتيجة بعثرة مختلفة عندما تستخدم نقص دالة التمويه، وقد تستخدم أحيانا دالة تمويه معززة تعرف باسم دالة تمويه ذات اتجاه واحد، بحيث إذا استعمل غيرها ينتج عنها استحالة حسابية computation ally infeasible بمعنى أن تكون العملية غير مقبولة. ينظر: وثيقة الأونسترال الصادرة باللغة العربية رقم : A/CN9/426-14JUNE , 1996, P34.

عليه وهو ما يحدث بإضافة الأرقام إلى المعادلة الرياضية، حيث يكتمل المحرر ويتم حفظه في جهاز كمبيوتر.

ينشأ التوقيع الرقمي ويتحقق من صحته باستخدام التشفير، وبناء على ذلك إذا أراد الموقع إرسال رسالة بيانات عبر البريد الإلكتروني مثل فإنه يقوم بإعداد ملخص الرسالة باستخدام برنامج تشفير وباستخدام المفتاح الخاص وإرسالها للشخص المستلم، الذي يستخدم المفتاح العام للتحقق من صحة التوقيع الرقمي، ثم ينشئ المرسل إليه ملخص رسالة باستخدام نفس برنامج التشفير ويقارن بين ملخصي الرسالتين، فإذا كانتا متطابقتين، فهذا دليل على أن الرسالة وصلت سليمة كما هي، ولم يحدث بها أي تغيير، أو تحريف، أما إذا تم إحداث تغيير في الرسالة فسيكون ملخص الرسالة التي أنشأها المستلم مختلفة عن ملخص الرسالة التي أنشأها الموقع.[1]

وقد خلا قانون التوقيع الإلكتروني المصري من تعريف لعملية التشفير، ولكن أجاز شروع التجارة الإلكترونية المصري على عملية تشفير البيانات والمعلومات التي يتم التعامل معها وتدوينها أو تسجيلها عبر الوسائط الإلكترونية، كما قرر أحقية أصحاب البيانات المشفرة في الخصوصية بمعنى أن المعلومات المشفرة خاصة بأصحابها ولا يجوز فضها أو الاطلاع عليها أو نسخها بغير موافقة كتابية منه شخصيا أو بناء على أمر قضائي.

ب-التوقيع بالقلم الإلكتروني pen-op :

وهذه الطريقة عبارة عن قلم إلكتروني pen-computer-signature يمكنه الكتابة على شاشة الكمبيوتر عن طريق برنامج هو المسيطر والمحرك لكل هذه العملية، ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من التوقيعات، [2] الأولى وهي خدمة التقاط التوقيع the

[1] - Digital signature Guide lines, American Bar Association, NSA, 1996, p09.

[2] - نجوى أبو هيبة وآخرون، مبادئ القانون، نظرية القانون، دار الفكر العربي، بيروت، د س ن، ص51.

signature capture service، والثانية وهي خدمة التحقق من صحة التوقيع the signature vérification service.[1]

وتتمثل هذه الطريقة في نقل التوقيع المحرر بخط اليد عن طريق التصوير بالماسح الضوئي "scanner"،[2] ثم تنقل هذه الصورة إلى الرسالة الإلكترونية المراد منها إضافة هذا التوقيع إليها لإضفاء الحجية عليها، على الرغم من سهولة هذه الطريقة في الاستعمال إلا انها طريقة محفوفة بالمخاطر، حيث يصعب أحيانا نسبة الرسالة الإلكترونية إلى موقعها، إذ بإمكان المرسل إليه الاحتفاظ بنسخة من صورة التوقيع التي وصلت ثم يعيد وضعها على أية وثيقة محررة عبر وسيط إلكتروني ويدعي أن واضعها هو صاحب التوقيع الفعلي.[3]

لكننا نرى أن هذه المشكلة يمكن حلها عن طريق شيئين، هما تكنولوجيا المفتاح العام القائمة على التشفير، وإيجاد جهة تصديق معتمدة من قبل السلطة التنفيذية يمكن الرجوع إليها للتحقق مقدما من شخصها منشئ التوقيع قبل البدء في التعامل معه، حيث سيكون لدى هذه الجهة نموذج لهذا التوقيع يحدد هوية منشئه، ويؤدي ذلك إلى وجود درجة عالية من الثقة والأمان في استخدام القلم الإلكتروني في التوقيع.

ج-التوقيع بالضغط على مربع الموافقة ok-box:

كثيرا ما يحدث في العقود الإلكترونية أن تتم الموافقة عن طريق النقر على زر الموافقة في المكان المخصص لذلك بلوحة مفاتيح كمبيوتر، او بالضغط على الخانة المخصصة المقبول في

[1] - عايض راشد المرعي، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه جامعة القاهرة 1998 ،ص112.

[2] - E.caprioli, collage de dtrasbaurg , sur le commerce électronique, 1999.

[3] - Alain benssoussan, le commerce électronique, op cit, p34.

نموذج العقد المعروض على شاشة الكمبيوتر، وزيادة في التأكيد قد يتطلب من العميل أن يضغط مرتين لضمان الجدية في التعامل.[1]

ولكن هذه الطريقة لا تعتبر في حد ذاتها توقيعا يكتسب به المحرر الإلكتروني العناصر اللازمة لاعتباره دليلا كاملا، ولذلك تلجأ المنشآت التجارية في الغالب الأعم إلى إضافة خانة في نموذج التعاقد الموجود على صفحة الويب، يضع فيها المتعاقد الرقم السري بالإضافة إلى إمكانية استخدام المفتاح الخاص الذي تقوم على منح الشهادة الخاصة به، جهات معتمدة من قبل الدولة.[2]

د–التوقيع باستخدام الخواص الذاتية "Biométric signature":

إن التوقيع البيومتري باستخدام الخواص الذاتية أو الطبيعية كإجراء للتوثيق يقوم بصفة أساسية على الخواص الفيزيائية والطبيعية والسلوكية للإنسان، مثال ذلك بصمة الأصبع " finger printing". ومسح شبكية العين " rétinal scans"، ونبرة الصوت " voice recognition"، وعند استخدام أي من هذه الخواص يتم أولا الحصول على صورة للشكل وتخزينها داخل الكمبيوتر حتى يمكن الرجوع إليها عند الحاجة، وهذه البيانات الذاتية يتم تشفيرها حتى لا يستطيع أي شخص الوصول لها ومحاولة العبث بها أو تغييرها، وذلك أن طرق التوثيق البيومتري "Biométric authentication methods " التي تستخدم عبر شبكة الأنترنت بدون تشفير، يمكن مهاجمتها وتغييرها، حيث يمكن أن ينتحل شخص شخصية المستخدم.[3]

وارتباط هذه الخواص الذاتية بالإنسان تسمح بتمييزه عن غيره بشكل موثوق به إل أقصى الحدود وهو ما يتيح استخدامها في التوقيع على العقود الإلكترونية، وهذا النوع من التوقيع كشأن

[1] - Alain benssoussan, le commerce électronique, op cit, p34.

[2] – حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الأنترنت، دار النهضة العربية، القاهرة، ط1، 1998، ص39.

[3] - Benjamin Wright. Op cit, p 03-15.

كل أنواع التوقيع الإلكتروني يرتبط استخدامه والوثوق فيه بمدى درجة تقدم التكنولوجيا التي تؤمن انتقاله بدون القدرة على التلاعب فيه.[1]

هـ-التوقيع باستخدام بطاقات الائتمان المقترنة بالرقم السري pin:

نتيجة تطور تكنولوجيا الاتصالات والمعلومات وازدياد التعامل بأسلوب التجارة الإلكترونية ظهرت البطاقات الممغنطة البنكية التي تستخدم عن طريق ماكينة الصراف الآلي ATM، تحتوي هذه البطاقات على شريط التسجيل المغناطيسي للمعلومات مثل اسم المستخدم، ورقم الهوية، وتاريخ صلاحية البطاقة ورقم تعريف الشخصية، أما ذاكرة البطاقة فتحتوي على نظام دفاعي للحماية Brute Force Attacks ، لأنه بعد إجراء عدة محاولات غير ناجحة لكي يضمن المستخدم الرقم السري pin فإن العملية لا تتم، كما أن البطاقة يمكن سحبها بواسطة ماكينة الصرف.[2]

وتتم عملية سحب النقود آليا من خلال ماكينة الصرف عن طريق إدخال البطاقة ثم إدخال الرقم السري الخاص بالمستخدم، فإذا كان الرقم صحيحا واتبعت الإجراءات تتم عملية السحب، وهكذا حل التوقيع السري محل التوقيع اليدوي.[3]

والجدير بالذكر أن اللائحة التنفيذية للقانون لم تحدد صور التوقيع الإلكتروني، وذلك تحسبا لما قد يظهر من أشكال جديدة ومتعددة للتوقيع الإلكتروني نتيجة التطورات التكنولوجية، ولكن وضحت أن التوقيع الإلكتروني بكافة صوره يتمتع بحجية في الإثبات إذا توافر فيه ثلاثة شروط: أولها: ارتباط التوقيع الإلكتروني بالموقع، وحدد دون غيره، وذلك إذا استند هذا التوقيع إلى منظومة

[1] - حسين جميعي، المرجع السابق، ص 41.

[2] - Elinor Harris solomons, électronic money flows, op cit, p229.

[3] - Michael Rowe, électronic trade payments, op cit, p83.

تكوين بيانات إنشاء توقيع إلكتروني مؤمن، [1] وأن يكون هذا التوقيع مرتبطا بشهادة تصديق الكتروني معتمدة (م9). وثانيها: سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني، وذلك عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص،[2] متضمنة البطاقة الذكية المؤمنة[3] الكود السري المقترن بها(م10).

وثالثها: إمكانية كشف أي تعديل أو تبديل بيانات التوقيع الإلكتروني وذلك باستخدام تقنية شيفرة المفتاحين الخاص والعام.(م11)

وتقوم حجية التوقيع الإلكتروني في شكل كتابي يمكن أن يؤدي مجموعة متنوعة من الوظائف حب طبيعة المستند الذي يحمل التوقيع، فمثلا التوقيع يمكن أن يكون دليلا على نية الموقع الإقرار بتحريره نص المستند، وأيضا كدليل للإثبات.[4] وفي حالة قيام نزاع مستقبلي بين الأطراف، وكذلك فهو أداة للتعبير عن إرادة الشخص في قبوله الالتزام بمضمون العقد ووسيلة لتوثيق العقد وتأمينه من التعديل، كما أنه يميز شخصية صاحبه ويحدد هويته.

---

[1] – عرّفت المادة الأولى من اللائحة التنفيذية المخصصة للتعريفات، منظومة تكوين بيانات إنشاء التوقيع الإلكتروني بأنها: «**مجموعة عناصر مترابطة ومتكاملة، تحتوي على وسائط إلكترونية وبرامج حاسب آلي يتم بواسطتها تكوين بيانات إنشاء التوقيع الإلكتروني باستخدام المفتاح الشفري الجذري**»

[2] – عرفت المادة الأولى من اللائحة التنفيذية للقانون المفتاح الشفري الخاص بأنه: «**أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ بها على بطاقة ذاتية مؤمنة**»

[3] – عرّفت المادة الأولى من اللائحة التنفيذية للقانون البطاقة الذكية بأنها:«**وسيط إلكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني ويحتوي على شريحة إلكترونية بها معالج إلكتروني وعناصر تخزين**»

[4] – قضت محكمة النقض –بموجب التفرقة بين التصرف والدليل المعد لإثباته–، ثبوت صحة التوقيع على الورقة العرفية لا يعني صحة التصرف المثبت بها، جواز الطعن في التصرف القانوني بالغلط أو التدليس أو الإكراه أو عدم مشروعية السبب أو بأي دفع موضوعي أو شكلي آخر، امتناع ذلك بالنسبة للورقة. الطعن رقم 7155 سنة 64 قن جلسة 2004/09/18، المستحدث من المبادئ التي قررتها محكمة النقض من أول أكتوبر 2003 حتى آخر سبتمبر 2004، ص 03.

أما التوقيع الإلكتروني فخلاف قيامه بالوظائف السابقة فهو يتفوق عن التوقيع التقليدي بالنظر إلى أن الاستيثاق من شخصية صاحب التوقيع يتم بشكل روتيني في كل مرة يتم فيها استخدام الرقم السري أو المفتاح الخاص، وبالتالي فإنه لا مجال للانتظار حتى ينشب النزاع للبحث في مدى صحة التوقيع، كما هو الشأن في معظم الأحوال بصدد المحررات الموقعة بخط اليد.[1]

ضف إلى ذلك ما توفره التقنية الحديثة المستخدمة في تأمين التوقيع الإلكتروني عن طريق ما يسمى نظام المعاملات الإلكترونية الآمنة "transaction secure électronic"، ويوفر هذا النظام التحقق من شخصية صاحب التوقيع.[2]

المطلب الثاني: وسائل التصديق الإلكتروني.

إن التصديق هو مجموعة من الأشياء أو العناصر التي تعتمد على الغرض الذي يراد استخدام التوثيق لتحقيقه.[3] أي هو مجموعة من الإجراءات والعمليات الرامية إلى التأكد من هوية صاحب التوقيع الإلكتروني والتأكيد على سلامة المحرر الذي يحمل هذا التوقيع بهدف ضمان الأمان والموثوقية حول هذا المحرر الإلكتروني والتوقيع الإلكتروني ويقوم بهذه الإجراءات طرف محايد بين أطراف المعاملات الإلكترونية يطلق عليه اسم مقدم خدمات التصديق الإلكتروني، كما أن هناك جهات مختصة بإصدار شهادة التصديق وشروط يجب أن تتوفر في هذه الجهة، وكيفية التصديق الإلكتروني.

[1] – حسين عبد الباسط جميعي، المرجع السابق، ص 46.

[2] – Mustapha Hashen sherif, protocols for secure électronic commerce, p27.

[3] – حسام محمد نبيل الشنراقي، الجرائم المعلوماتية "دراسة مقارنة على جرائم الاعتداء على التوقيع الإلكتروني"، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2013، ص 79.

الفرع الأول: جهة التصديق الإلكتروني.

لقد تنوعت واختلفت التسميات في شأن الجهة المختصة بتصديق التوقيع الإلكتروني بين تسمية جهة التصديق في قانون المعاملات الإلكترونية الأردني وتسمية مقدم أو مزود خدمات التصديق وفق التشريع التونسي ومؤدي الخدمة في التشريع الجزائري.

أولا: تعريف جهة التصديق الإلكتروني.

تعددت التعريفات الفقهية والقانونية دوليا وإقليميا لجهة التصديق على التوقيع الإلكتروني ومن بين أهم هذه التعريفات نورد ما يلي:

عرّف جانب من الفقه القانوني مزود خدمات التصديق بأنه: "هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق به، يقدم خدمات أمنية في التجارة الإلكترونية، من خلال إصدار شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، لتوثيق هوية الأشخاص مستخدمي التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه"[1]

وعرّف قانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 جهة التصديق أو مقدم خدمات التصديق بنص المادة 02 بأنه: "الشخص الذي يصدر الشهادات الإلكترونية، ويمكن أن يقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية"[2]

أما التوجيه الأوروبي للتوقيعات الإلكترونية فقد عرّف مقدم خدمة التصديق بنص المادة الثانية الفقرة 11 منه بأنه: "كل كيان أو شخص طبيعي أو معنوي يقدم شهادات التصديق أو خدمات أخرى لها علاقة بالتوقيعات الإلكترونية"[3]

[1] – نادية ياس البياتي، التوقيع الإلكتروني عبر الأنترنت ومدى حجيته في الإثبات، دار البداية ناشرون وموزعون، الأردن، ط1، 2014، ص 263.

[2] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 89.

[3] – التوجيه الأوروبي الصادر في 13-12-1999 بشأن التوقيعات الإلكترونية.

كما عرّفه القانون الفرنسي بالمرسوم رقم 272 لسنة 2001 بأنه: "شخص يقدم شهادات التصديق أو خدمات أخرى في مجال التوقيع الإلكتروني"

ومن التعريفات العربية التي عرفت مزود خدمات التصديق ما أورده القانون الإتحادي رقم 01 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة بنص المادة الأولى منه بقوله أنه: "أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات التصديق الإلكتروني أو خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بأحكام هذا القانون"[1]

أما القانون المصري الخاص بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات نجده خاليا من أي تعريف لجهة التصديق على التوقيع الإلكتروني، إلا أن اللائحة التنفيذية لهذا القانون عرّفت جهات التصديق على التوقيع الإلكتروني بأنها: "الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع"[2]

كما عرّفت المادة الأولى من مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني مزود خدمات المصادقة الإلكترونية بأنه: "كل شخص طبيعي أو اعتباري ينشئ ويسلم ويتصرف في شهادات المصادقة الإلكترونية، ويقدم خدمات أخرى ذات علاقة بالتوقيع الإلكتروني"[3]

أما المشرع الجزائري فقد تناولها بصفة عرضية في المادة 03 من المرسوم رقم 07-162 لسنة 2007 والتي نصها: «**مؤدي خدمات التصديق هو كل شخص في مفهوم المادة 08/ف08**

[1] – عابد فايد عبد الفتاح فايد، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني "دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني"، دار الجامعة الجديدة، الإسكندرية، 2004، ص 65.

[2] – أمير فرج يوسف، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008، ص 14.

[3] – أمير فرج، المرجع السابق، ص 52.

من القانون رقم 03-2000 المؤرخ في 05-08-2000 يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني»[1]

وبالرجوع إلى نص المادة 08/ف08 من القانون أعلاه فقد جاء فيها أن: «**موفد الخدمة هو كل شخص معنوي أو طبيعي يقدم خدمة مستعملا وسائل المواصلات السلكية واللاسلكية**»[2]

كما تناول المشرع الجزائري تعريف جهات التصديق الإلكتروني أو مؤدي خدمات التصديق في القانون رقم 15-04 في الفقرة 12 من المادة 02 والتي نصت على أن: «**مؤدي خدمات التصديق هو كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يقدم شهادات أخرى في مجال التصديق الإلكتروني**»[3]

ثانيا: الشروط الواجب توافرها في الجهة المختصة بإصدار شهادات التصديق الإلكترونية.

لابد من توافر بعض الشروط في كل شخص سواء كان طبيعيا أو اعتباريا يتقدم بطلب إلى الجهة المختصة للحصول على ترخيص لممارسة مهنة إصدار شهادات التصديق الإلكترونية، وذلك لتحقيق مدى معين من الأمان والثقة في التوقيع الإلكتروني، إن المشرع الجزائري بالرجوع إلى المادة 34 من القانون 15-04 التي تحدد الشروط التي تجب على كل طالب بترخيص لتأدية خدمة التصديق الإلكتروني أن يستوفيها وهي كالآتي:

-أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي.

- أن يتمتع بقدرة مالية كافية.

[1] - المرسوم التنفيذي رقم 07-162.

[2] - يمينة حوحو، المرجع السابق، ص 202.

[3] - القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ج ر رقم 06 المؤرخة في 2015/02/10.

– أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيا الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي.

– أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني.

وهناك شروط أخرى يجب توافرها بالجهة المختصة بإصدار شهادات التصديق الإلكترونية وهي شروط فنية كأن يكون الشخص الطبيعي أو الممثل المعنوي ذا كفاءة مهنية في ممارسة نشاط إصدار شهادات التصديق، كأن يكون مهندس تقنيات حديثة أو من مبرمجي الحاسبات الإلكترونية أو أن تكون لديه خبرة مهنية بمجال عمله وهذا الشرط هو أحد المتطلبات الأساسية التي حددها التوجيه الأوروبي بشأن التوقيعات الإلكترونية للجهة المختصة بإصدار شهادات التصديق في المادة 02 من الملحق الثاني التي تنص على أنه يجب على المكلفين بخدمات التوثيق «**الاستعانة بموظفين متمتعين بالمعارف النوعية والخبرة والتوصيفات الضرورية لتوريد الخدمات وعلى الأخص الاختصاصات على مستوى الإدارة والمعارف المتخصصة تكنولوجيا في التوقيعات الإلكترونية**»

ولقد أشار المشرع الجزائري في المادة 03/ف1 من المرسوم رقم 07-162 بقوله: «**الوثيقة التي تثبت من خلالها بأن مؤديا لخدمات التصديق الإلكتروني يقدم خدمات مطابقة لمتطلبات نوعية خاصة**»[1] ويقصد بالنوعية الخاصة مجموعة المؤهلات.

ولم يعرّف المشرع الجزائري تلك الوثيقة عكس المشرع الفرنسي الذي جاء مجمل تعريفه لها في المادة 01/ف12 من المرسوم 2001-272 بأنها قرار صادر من الغير وهو هيئة التأهيل تصرح أو

[1] – المادة 03/ف10 من المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى خدمة المواصلات السلكية واللاسلكية.

تشهد بأن مؤدي خدمة المصادقة الإلكترونية يزود الخدمات الإلكترونية بالشروط المطلوبة الخاصة بالتأهيل.

ثالثا: دور واختصاصات جهة التصديق.

أ–دور جهة التصديق الإلكتروني: لجهات التصديق أو التوثيق الإلكتروني أدوارا يمكن عرضها في النقاط التالية:

–التحقق من هوية الشخص الموقع:

تقوم جهات التوثيق بإصدار شهادة توثيقية إلكترونية تفيد التصديق على التوقيع الإلكتروني في تعاقد معين تشهد بموجبها بصحته ونسبته إلى مصدر صدر عنه، ويستتبع التحقق من هوية الموقع من خلال جهة التوثيق تحديد الأهلية القانونية للمتعاقد وكذلك التحقق من سلطات هذا الشخص واختصاصاته الوظيفية.[1]

–إثبات مضمون التبادل الإلكتروني:

يقصد بالتبادل الإلكتروني مجموعة معايير يتم استخدامها في تبادل معلومات العمل وتناقلها بين الشركاء التجاريين من خلال أجهزة الكمبيوتر وفي تنفيذ صفقات الأعمال بطريقة إلكترونية،[2] حيث تتولى جهة التوثيق كذلك التحقق من مضمون التبادل الإلكتروني بين الأطراف وسلامته وجديته وبعده عن الاحتيال والغش، فضلا عن إثبات وجوده ومضمونه.[3]

[1] – محمد مأمون سليمان، التحكيم الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2011، ص

[2] – إيمان العاني، البنوك التجارية وتحديات التجارة الإلكترونية، رسالة ماجستير، جامعة منتوري، قسنطينة، 2007، ص 71.

[3] – محمد مأمون سليمان، المرجع السابق، ص 251.

-تحديد لحظة إبرام العقد:

إن تحديد لحظة إبرام التصرف القانوني ليس شرطا لصحة هذا التصرف ومع ذلك فإن تحديد تلك اللحظة يكون ضروريا، إذ أن وقت إبرام العقد يعد هو لحظة بداية لبدء الآثار القانونية.

-إصدار المفاتيح الإلكترونية:

تتولى هاته الجهة إصدار مفاتيح إلكترونية سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الإلكترونية أو المفتاح العام الذي بواسطته فك التشفير بالإضافة إلى ذلك تقوم هاته الجهة بإصدار التوقيع الرقمي.

-إلزامية لجوء الأطراف لجهات التصديق الإلكتروني:

لقد أجيز للأطراف أن يحددوا وجوبا استخدام مزودي خدمات تصديق معينين أو فئة معينة من الشهادات فيما يتصل بالرسائل أو التوقيعات الإلكترونية المقدمة لهم.[1]

مع الإشارة إلى أن المشرع المصري لم يرخص للأشخاص الطبيعيين القيام بأعمال شهادات التصديق الإلكتروني وإنما فقط الأشخاص الاعتبارية.[2]

ب-اختصاصات مؤدي خدمات التصديق الإلكتروني:

إن لجهة التصديق الإلكتروني عدة خصائص نذكر منها:

-التأكد من صحة البيانات المدونة في شهادة التصديق:

إن أهم اختصاص يسند لمؤدي خدمات التصديق الإلكتروني هي عملية التصديق الإلكتروني التي تهدف إلى ضمان صحة البيانات الإلكترونية وسلامتها والتأكد من هوية الموقع

[1] - محمد مأمون سليمان، المرجع السابق، ص 251.

[2] - إياد محمد عارف عطا سده، مدى حجية المحررات الإلكترونية في الإثبات، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2009، ص 117.

وصحة توقيعه وسلطاته في التوقيع، [1] حيث جاء نص المادة 03/ف1 من المرسوم التنفيذي الجزائري رقم 07-162 ما يلي: «**يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني، معنى هذا أن مؤدي خدمات التصديق إلى جانب تسليمه لشهادات المصادقة الإلكترونية فهو يقوم بأداء خدمات أخرى مرتبطة بالتوقيع الإلكتروني وهي متنوعة مثل حفظ الوثائق الإلكترونية واتخاذ التدابير اللازمة لتوفير الحماية لها وفقا للشروط والضوابط المنصوص عليها قانونا أي أن يقوم بالتحقق من التوقيع الإلكتروني قد تم تنفيذه من شخص معين ومحدد، فبفضل التصديق الإلكتروني يمكن تحديد هوية المتعامل وربط معطيات تعامله مع ضمان سلامة هذه المعطيات وصحتها بواسطة شهادة التصديق الإلكتروني**»[2]

-الالتزام بالسرية:

ويقصد بالسرية هي الحفاظ على البيانات ذات الطابع الشخصي المقدمة من العميل إلى الجهة المختصة بإصدار شهادات التصديق الإلكتروني فنجد التوجيه الأوروبي بشأن التوقيعات الإلكترونية أوصت في المادة 18/ف1 بأن تلتزم الجهات التي تصدر شهادات التصديق الإلكترونية بالحفاظ على شكل البيانات ذات الطابع الشخصي، [3] وقد تبنت التشريعات الوطنية ما نص عليه التوجيه الأوروبي فقد نص الفصل 15 من قانون المبادلات الإلكترونية الفرنسي على: «**يتعين على مزودي خدمات المصادقة الإلكترونية وأعوانهم المحافظة على سرية المعلومات الواردة فيه ويمنع عليه استعمالها خارج المصادقة الإلكترونية**»[4]

[1] – عيسى غسان ريضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ط1، 2005، ص49.

[2] – يمينة حوحو، المرجع السابق، ص 196.

[3] – ثروت عبد الحميد، التوقيع الإلكتروني "ماهيته–مخاطره–كيفية مواجهته– ومدى حجيته في الإثبات"، دار النهضة العربية، القاهرة، مصر، 2002، ص 165.

[4] – عيسى غسان ريضي، المرجع السابق، ص 134.

-إلغاء وإيقاف العمل بشهادة التصديق:

تلتزم الجهة المختصة بإصدار شهادات التصديق الإلكترونية بإلغاء أو إيقاف شهادة التصديق في حالة وجود سبب يقيني بموجب ذلك، فقد يتضح لهذه الجهة وجود تغيير جوهري في بيانات شهادة التصديق الإلكترونية، كما لو علمت بتزوير الوثائق المقدمة لها من ذوي الشأن لإصدار شهادة التصديق، أو تبين لها من جراء تحرياتها أن الشخص الذي صدرت الشهادة باسمه فقد أهليته أو أفلس أو فقد وظيفته.

الفرع الثاني: خصوصية شهادة التصديق الإلكتروني.

بعد أن تطرقنا لجهات التصديق الإلكتروني خرجنا بمجموعة من الأدوار والالتزامات الملقاة على عاتق هذه الجهات، وبعد إصدار شهادات المصادقة من أبرزها وتحتاج شهادة التصديق إلى الوقوف على تعريفها، أنواعها وأهم بياناتها.

أولا: تعريف شهادة التصديق الإلكتروني.

عرّف قانون الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 هادة التصديق الإلكتروني بأنها: «**رسالة بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبيانا إنشاء التوقيع**»

كما عرّف التوجيه الأوروبي في المادة 03 شهادة التصديق الإلكتروني بأنها: «**تلك التي تربط بين أداة التوقيع وبين شخص معين وتؤكد شخصية الموقع**»

وعرّفها جانب من الفقه بأنها: «**الشهادات التي تصدرها جهات التوثيق المرخص لها من قبل الجهات المسؤولة في الدولة لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح**

ينسب إلى من أصدره، ويستوفي كافة الشروط والضوابط المطلوبة فيه كونه دليل إثبات يعول عليه»[1]

وقد نص القانون الفرنسي على مفهوم شهادة التصديق الإلكتروني في المادة الأولى من المرسوم الصادر في 2001/03/30 عن مجلس الدولة، واعتبرها شهادة تفيد صحة التوقيع الإلكتروني وتصدر عن جهة مختصة بذلك، تقر فيها بأن التوقيع الإلكتروني تم حفظه بطريقة سليمة من لحظة إرساله حتى لحظة التصديق عليه.[2]

أما قانون التوقيع الإلكتروني المصري في مادته الأولى الفقرة (و) أن شهادة التصديق الإلكتروني هي: «**الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع** » وأحال القانون في شأن البيانات التي يجب أن تشتمل عليها شهادة التصديق الإلكتروني إلى اللائحة التنفيذية للقانون في المادة 20.[3]

وجاءت المادة 02 من قانون المعاملات والتجارة الإلكترونية لإمارة دبي أن شهادة المصادقة الإلكترونية هي شهادة يصدرها مزود خدمات التصديق يفيد فيها هوية الشخص أو الجهة الحائزة على أداة توقيع معينة.

ويعرّف البعض شهادة التوثيق الإلكتروني بأنها تلك الشهادات التي تصدر من جهة معتمدة ومرخّصة من قبل الدولة لإثبات نسبة التوقيع الإلكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة وهذه الشهادات يقصد من الحصول عليها تأكيد نسبة رسالة البيانات أو العقد الإلكتروني إلى مصدره، وأن التوقيع الإلكتروني هو توقيع صحيح وصادر ممن نسبت إليه.[4]

---

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 104.

[2] – يوسف زروق، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه، جامعة تلمسان، 2013، ص 277.

[3] – خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، مصر، ط1، 2006، ص 197.

[4] – المرجع نفسه، ص 197.

وتعرّف بأنها: "وثيقة إلكترونية على شكل شهادة رقمية تصدر عن جهة التصديق تثبت نسبة المعطيات للموقع"[1]

أما في التشريع الجزائري فقد نصت المادة 03 مكرر 7 من المرسوم التنفيذي رقم 07-162 لسنة 2007 على تعريف شهادة المصادقة الإلكترونية بأنها: « **وثيقة تصدرها جهة التصديق الإلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع**»

كما عرّفها القانون 15-04 لسنة 2015 والمتعلق بالتوقيع والتصديق الإلكترونيين في المادة 02/ف7 بأنها: «**وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع**»

ثانيا: أنواع شهادات التصديق الإلكتروني.

إن أغلب التشريعات وضعت نوعين من شهادات التصديق الإلكتروني: شهادات التصديق الإلكتروني الوطنية (العادية أو البسيطة)، وشهادات التصديق الإلكتروني المعتمدة (الموصوفة).

أ-شهادات التصديق الإلكتروني العادية:

عرّفها القانون الفرنسي في المرسوم الصادر في 2001/03/30 عن مجلس الدولة والخاص بالتوقيع الإلكتروني بأنها: « **وثيقة تصدرها الجهة المختصة بالتصديق الإلكتروني وتقر فيها بصحة بيانات التوقيع الإلكتروني ومدى صلته بالموقع، ولا تضمن بيانات محددة**»[2]

أما القانون الجزائري فقد أشار في المادة 3مكرر8 من المرسوم 07-162 لسنة 2007 إلى شهادة التصديق الإلكتروني العادية حيث سماها الشهادة الإلكترونية، وجاء في نص هذه المادة

[1] - يمينة حوحو، المرجع السابق، ص 210.

[2] - يوسف زروق، المرجع السابق، ص 279.

أن: «**الشهادة الإلكترونية هي وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع**»[1]

وهو نفس ما جاء به القانون رقم 15-04 المتعلق بالتوقيع والتصدق الإلكترونيين حيث عرّفها على أنها: «**شهادة تصدر عن جهات التصديق الإلكتروني المتنوعة تثبت الصلة بين معطيات التوقيع الإلكتروني والموقع، إذ تحدد هوية الشخص الموقع وتثبت ارتباط معطيات التوقيع الإلكتروني به**»

وفي حقيقة الأمر فإن شهادة التصديق الإلكتروني العادية هي شهادة لا تفي بالمتطلبات المستوجبة في شهادة المصادقة الموصوفة، إذ أنها تصدر من أي جهة مختصة في إثبات هوية الموقع لا غير، في حين شهادة التصديق الموصوفة تصدر عن جهة التصديق الإلكتروني المختصة في هذا المجال والموثوق بها.[2]

ب-شهادات التصديق الإلكتروني المعتمدة:

هي شهادة تصدرها الجهة المختصة بإصدار شهادة التصديق الإلكتروني، وتهدف إلى تأكيد صحة بيانات التوقيع الإلكتروني ونسبته إلى صاحبه، وتتضمن الشهادة المعتمدة عدة بيانات تجعلها أكثر أمانا للمتعاملين، إذ نصت المادة 20 من قانون التوقيعات الإلكترونية المصري على أن تحدد اللائحة التنفيذية لهذا القانون البيانات التي يجب أن تشتمل عليها شهادة التصديق الإلكتروني.[3]

أما المشرع الجزائري فقد تناولها في المادة 03مكرر09 من المرسوم 07-162 بأنها: «**شهادة إلكترونية تستجيب لمتطلبات محددة** » وهو نفس ما جاء به القانون 15-04، إلا

[1] - يمينة حوحو، المرجع السابق، ص 215.

[2] - المرجع نفسه، ص 215.

[3] - عابد فايد محمد فايد، المرجع السابق، ص 78.

أن هذا الأخير أضاف مجموعة من البيانات التي يجب أن تحتويها هذه الشهادة ، وإلى جانب النوعين الأولين لشهادة التصديق الإلكتروني نجد أنواعا أخرى من الشهادات التي تقوم هيئات التصديق الإلكتروني بإصدارها، غذ تتنوع بحسب الغرض منها، ونذكر على سبيل المثال:

*شهادة توثيق التوقيع الرقمي، وتعد من أكثر أنواع الشهادات انتشارا وأكثرها أهمية.

* شهادة توثيق تاريخ إصدار التوقيع الإلكتروني وهي التي توثق وقت وتاريخ صدور التوقيع الرقمي، حيث يقوم صاحب الشهادة بعد التوقيع عليها بإرسالها إلى جهة التوثق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها.[1]

* شهادة الإذن، حيث تتولى تقديم بيانات عن صاحب التوقيع الإلكتروني كمؤهلاته محل إقامته، التراخيص التي يملكها وعمله.[2]

* شهادة البيان التي تتحقق من صحة واقعة أو حدث ما وقت وقوعه، ومن هنا تظهر أهمية هذه الشهادة ومدى خطورة المعلومات التي تتضمنها والتي يعتمد عليها الغير وعلى أساسها يحدد تعاملاته.[3]

* شهادة المصادقة الإلكترونية الصادرة عن جهات أجنبية وهذه الأخيرة تكون مختصة بإصدارها، إذ نصت المادة 22 من قانون التوقيع الإلكتروني المصري على أنه: «**تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني**»، وقد بينت المادة 21 من اللائحة التنفيذية لقانون التوقيع الإلكتروني حالات وإجراءات وضمانات اعتماد الهيئة للجهات

[1] – خالد ممدوح إبراهيم، المرجع السابق، ص 197.

[2] – محمد حسن رفاعي العطار، المرجع السابق، ص 208.

[3] – خالد ممدوح إبراهيم، المرجع نفسه، ص 197.

الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني في مصر، وهو ما سار عليه أيضا كل من قانوني إمارة دبي وتونس.[1]

ثالثا: بيانات شهادة التصديق الإلكتروني.

إن أغلب التشريعات أعطت أهمية جد بالغة لشهادة التصديق الإلكتروني خاصة في مجال الإثبات، وذلك من حيث تحديد بياناتها بدقة، إذ اشترطت مختلف التشريعات المنظمة للتوقيع والتصديق الإلكتروني بيانات أساسية وأخرى ثانوية، فنجد مثلا المرسوم التنفيذي الفرنسي رقم 272/01 المؤرخ في 2001/03/30 في المادة 06/ف01 منه تنص على مجموعة من البيانات الإلزامية التي يجب أن تحتويها شهادة المصادقة الإلكترونية الموصوفة، [2] كما أشار التوجيه الأوروبي لسنة 1999 المتعلق بالتوقيع الإلكتروني إلى ضرورة اشتمال شهادة التصديق على جملة من البيانات تضمنتها المادة 08 وتمثلت في:[3]

- تحديد هوية مقدم خدمات التصديق والدولة المرخصة له بمزاولة نشاطه.
- هوية الموقع عبر تحديد اسمه الحقيقي أو المستعار، بشرط أن يفيد التحقق من هويته.
- المفتاح العام والذي يمكن عبره الوصول للمفتاح الخاص للموقع والخاضع لسيطرته ورقابته.
- تحديد مدة صلاحية الشهادة والتي غالبا ما تتراوح ما بين سنة إلى سنتين.
- الرقم التسلسلي للشهادة.
- التوقيع الإلكتروني لمقدم خدمات التصديق.
- تحديد قيمة الصفقات التي يمكن أن تستخدم الشهادة فيها والغرض من استخدام الشهادة.

[1] – عابد فايد محمد فايد، المرجع السابق، ص 79.

[2] – يمينة حوحو، المرجع السابق، ص 211.

[3] – يوسف زروق، المرجع السابق، ص 285.

بينما المشرع المصري ميّز بين نوعين من البيانات التي تتضمنها شهادة التصديق الإلكتروني بيانات تضمنتها نص المادة 20 من اللائحة التنفيذية لقانون التوقيع الإلكتروني، وبيانات اختيارية عند الحاجة نصت عليها ذات المادة.[1]

أما المشرع الجزائري نجده قد عرّف شهادة التصديق في المادة 02/ف7 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، وفي نص المادة 15 من نفس القانون أردف المشرع مصطلح "الموصوفة" إلى شهادة التصديق، حيث جمع بين المصطلح وبين مجموعة متطلبات شهادة التصديق الإلكتروني الموصوفة وهي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:[2]

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

2- أن تمنح للموقع دون سواه.

3-يجب أن تتضمن على الخصوص البيانات الآتية:

أ-إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق موصوفة.

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

ج-اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته.

د- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني.

---

[1] - المادة 20 من اللائحة التنفيذية لقانون التوقيع المصري 15-04 الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات الصادر بموجب القرار رقم 109-05 وقد نشرت هذه اللائحة في جريدة الوقائع المصرية، العدد115 الصادر في 2005/05/25.

[2] - المادة 15 من القانون رقم 15-04 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين المؤرخ في 01-02-2015، الجريدة الرسمية للجمهورية الجزائرية، العدد06.

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

و- الإشارة إلى بداية أو نهاية مدة صلاحية شهادة التصديق الإلكتروني.

ز- رمز تعريف شهادة التصديق الإلكتروني.

ح-التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني.

خ-حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني عند الاقتضاء.

ج- حدود استعمال شهادة التصديق الإلكتروني عند الاقتضاء.

ي-الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر عند الاقتضاء.

المبحث الثاني: الجرائم الماسة بالتوقيع الإلكتروني.

مع انتشار التبادل والتعاقد عبر الأنترنت ووسائل الاتصال الحديثة، نشأ تغيير جذري على مستوى شكل الجرائم التي تمس هذا النوع من المعاملات، وهو الذي يؤثر خاصة على الثقة في الصفقات التجارية التي تتم عبر الأنترنت والتي أضحت تؤثر على مسألة التوقيع الإلكتروني باعتباره أهم الآليات المستحدثة في مجال المعاملات الإلكترونية، والتي تمثل عاملا عاما في إتمام التعاملات الإلكترونية في المجال التجاري والمصرفي وكافة أنواع العقود الإلكترونية، ولقد حرصت العديد من الدول على وضع أسس للحماية الجنائية وفق تشريعاتها الداخلية تنسيقا مع التشريعات الدولية في مجال مكافحة الجرائم الماسة بهذه الآلية، ولذا نجد أغلب التشريعات عملت على تناول مسألة الحماية بدءا من ضبط القواعد القانونية التي تنظم آلية التوقيع الإلكتروني.

وفي ضوء ما تقدم سوف نقسم هذا المبحث إلى مطلبين، حيث نتناول الجرائم التقليدية للتوقيع الإلكتروني (**المطلب الأول**)، بينما نتطرق إلى الجرائم المستحدثة الماسة بالتوقيع الإلكتروني (**المطلب الثاني**).

المطلب الأول: الجرائم التقليدية للتوقيع الإلكتروني.

إن بيئة المعاملات الإلكترونية وعلى الرغم من الإيجابيات التي حملتها وساهمت في تطور هذه المعاملات، لا تخلو من بعض السلبيات التي قد تقوض جهود الأطراف المعنية وتحول دون خلق بيئة آمنة ومتوقة لكافة المتعاملين خاصة مع تنامي الظواهر مثل القرصنة والتزوير الإلكتروني، وهو ما استدعى تدخل مشرعين لسن القوانين الكفيلة بوضع آليات ووسائل الحماية الجنائية للتوقع والتصديق الإلكترونيين، من أي فعل من الأفعال الإجرامية الماسة بأمنه وثقته بين المتعاملين به وكذا حجيته في المعاملات التجارية كما هو الحال بالنسبة لجريمة تزوير التوقيع الإلكتروني، جريمة إتلاف التوقيع الإلكتروني، وغيرها من الجرائم.

ومن ثمة سوف نتناول الجرائم الماسة بالمحل الإلكتروني (**الفرع الأول**)، بينما نتطرق إلى . جرائم الاعتداء على حجية التوقيع الالكتروني (**الفرع الثاني**).

الفرع الأول: الجرائم الماسة بالمحل الإلكتروني.

نتناول في هذا الفرع الحماية الموضوعية للمحل الإلكتروني والاهتمام بجرائم الأموال، وهي البيانات التي تتناول الذمة المالية، وإذا ما تم تناول تلك الحماية فلابد من التعرض لها في بعض الجرائم التي تمس الذمة المالية، وسنحدد في هذا الفرع الجرائم المرتكبة بشكل متكرر وسنخصص في دراستنا السرقة والاحتيال المعلوماتي، وكذا توضيح أركان الجريمة المادية والمعنوية والشرعية وبناء على ما تقدم سوف نتناولها من خلال مجموعة من النقاط الضرورية.

أولا: جريمة السرقة الإلكترونية.

جريمة السرقة الإلكترونية بصورة عامة تعتبر من الجرائم التقليدية وتعد من أخطر الجرائم التي ينصب محلها على المال العام، وتؤدي إلى حرمان صاحب الحق بصورة كلية.

أما في المجال المعلوماتي فالوضع يختلف، حيث أن محل الجريمة هنا يختلف عنه في الجريمة بصورتها التقليدية، فمحلها هنا المعلومات والبيانات الموجودة داخل النظام المعلوماتي أو داخل الحاسب الآلي، والمحفوظة داخل الدعامات المادية، على اعتبار أن المال إما أن يكون ذا طبيعة مادية بحتة، وإما أن يكون ذا طبيعة مادية تحتوي في مضمونها على قيمة حقيقية معنوية.[1]

[1] – يوسف بن سعيد الكلياني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري، دار النهضة العربية، مصر، ط1، 2017، ص 86.

تعد جريمة السرقة من جرائم الاعتداء على الملكية والحيازة، فهي تؤدي إلى إخراج المال من حيازة صاحبه أو حائزه وإدخاله في حيازة شخص آخر بدون وجه حق وهي أكثر الجرائم وقوعا وخطورة وصلة بالحياة العملية مقارنة مع غيرها من الجرائم.[1]

تعرّف بأنها أخذ الشيء في الخفاء وتطلق مجازا على الشيء المسروق سرق منه مالا، كما يطلق مجازا على السمع متخفيان إذ يقال استرق السمع، ومنه قوله تعالى: ﴿**إِلَّا مَنِ اسْتَرَقَ السَّمْعَ فَأَتْبَعَهُ شِهَابٌ مُبِينٌ**﴾[2]

وتعرّف السرقة في مفهومها الواسع بأنها: اختلاس مال منقول مملوك للغير بغية تملكه، وعرّفها الفقه بأنها اعتداء على ملكية المنقول وحيازته بنية تملكه، أما تعريفها في المجال المعلوماتي فهي سرقة البيانات أو المعلومات، او برامج وإدخالها في حيازته دون علم وإرادة صاحبها الشرعي سواء كانت مخزنة على أشرطة ممغنطة أو أسطوانات مدمجة.[3]

وعليه يمكن تعريف سرقة البيانات الإلكترونية على أنه عبارة عن الاستيلاء على البيانات أو المعلومات بواسطة اختراق أنظمة الحاسب الآلي أو المواقع الإلكترونية وحيازتها بطريقة تمكن الغير من حرمان صاحب الحق منها والبعض من مكوناتها. ومن ثمة سوف نتناول أركان جريمة السرقة في مجال المعلومات الإلكترونية.

أ-أركان جريمة السرقة المعلوماتية:

إن بلورة مفهوم أركان جريمة السرقة في إطار المعاملات الإلكترونية يستلزم بيان ركن الاختلاس الممثل للنشاط المادي للجريمة، بالإضافة إلى بيان خصوصية الركن المعنوي من خلال عنصري القصد الجنائي العام والخاص.

---

[1] - دلخار صلاح الدين بوكاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط 1، 2016، ص 76.

[2] - سورة الحجر، الآية: 18.

[3] - يوسف بن سعيد الكلياني، المرجع السابق، ص 77.

-الاختلاس:

يعرف الاختلاس في جريمة السرقة بأنه انتقال حيازة المال محل السرقة من المالك إلى يد المجني عليه، ويقتضي ذلك حرمان المالك من حيازة وملكية المال. [1] وبالتالي قد يأخذ فعل الاختلاس صفة الأخذ عنوة أو خلسة أو حتى الحصول على المال عن طريق اليد العارضة بتغير نية الجاني في الاستيلاء وتملكه، وهنا يظهر الجاني في مظهر صاحب السيطرة الفعلية على المال محل السرقة.

إن المفهوم الوارد أعلاه يتعارض مع فكرة سرقة المعلومات الإلكترونية وذلك نظرا لصعوبة الاعتراف بانتقال حيازة المعلومات من يد إلى أخرى، ففعل الاختلاس في مجال المعاملات الإلكترونية يأخذ أساليب خاصة تتحقق بفعل الالتقاط الذهني للبيانات، وهو ما ينشأ عن حفظ وتخزين المعلومات بمجرد البصر أو السمع، أو الالتقاط الهوائي للبيانات المعالجة أو المنقولة، وهو ما يتماشى وطبيعة عمل ونظام أجهزة الحاسوب، وما يتصل بها من توابع تصدر أثناء تشغيلها بإشعاعات كهرومغناطيسية يمكن التقاطها: ترجمتها إلى بيانات مرئية، وكذا عملية نسخ ونقل المعلومات من النظام المعلوماتي، وهو ما يترجم فعل الأخذ من خلال اتخاذ فكرة النسخ للمعلومات المخزنة على الدعامات المادية.[2]

إن القول بسرية المعلومات بفعل النسخ يوسع مفهوم فكرة الاختلاس التي لا تقتصر على الحرمان وإنما شكل الاعتداء على حق صاحب المعلومة في الاستئثار بما يتضمنه من سرية وخصوصية لتلك المعلومات.

[1] – مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001، ص 146.

[2] – عبد الله حسين علي محمود، المرجع السابق، ص 261.

فنجد أنه من أولى المواقف التي استقرت عليها أحكام القضاء الاعتراف بفعل الاختلاس الوارد على المعلومات نظرا لصعوبة إثبات فعل انتقال الحيازة ورفض اعتبار النسخ أو الاطلاع على المعلومات المسجلة بالحاسب الآلي مشكلا لجريمة من جرائم الأموال.

أما الموقف الفقهي لم تكن فكرة اختلاس المعلومات محل اتفاق، فقد أيده البعض وعارضه البعض الآخر، فالاتجاه الرافض لقابلية المعلومات للاختلاس يستند إلى الفكرة المادية للاختلاس والتي تقوم عليها جرائم السرقة في وجهها التقليدي بحيث يرون ضرورة تحقق الفعل المادي المتمثل في نقل الشيء أو أخذه أو نزعه من مالكه متضمنا تغييرا في الحيازة القانونية ويستند أنصار قابلية المعلومات الإلكترونية إلى قبول فكرة صلاحية وقوع الاختلاس على المعلومات أموالا معنوية قابلة للتملك والحيازة، وبالتالي فهي قابلة أيضا للأخذ الاختلاس والاعتداء عليها بأشكال أخرى.

ونجد أن المشرع الجزائري قد جاء بنص المادة 350 ق ع ، الذي أقرّ فيه مصطلح "شيء" الذي يعتبر مفهوما مرنا يتماشى مع الأموال المعلوماتية، وكذا استحداث نص المادة 394 مكرر من قانون العقوبات الذي جاء بحكم تجريم الاعتداء على البيانات والمعلومات المعالجة آليا، والتي تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، غلا أنها تحقق كذلك وبصورة غير مباشرة حماية للمعلومات في حد ذاتها.

-الركن المعنوي:

من بين ما تنص عليه القواعد العامة لجريمة السرقة هو ضرورة توافر الركن المعنوي والمتمثل في القصد الجنائي، حيث يتحقق القصد العام في جريمة السرقة في إطار المعاملات الإلكترونية بتوافر عنصري العلم والإرادة، فيجب أن يعلم الجاني بأن المال ليس ملكا له، وأن تتجه إرادته إلى ارتكاب فعل الحيازة وتحقيق النتيجة لإجرامية، ذلك أن عدم توافر عنصر الإرادة ينفي القصد الجنائي، ولا تقع جريمة السرقة إلا بتوافر نية حرمان المالك من سلطاته الفعلية كمالك.

بالإضافة إلى جملة الصعوبات المتعلقة بالنشاط الإجرامي الواقع في مجالات المعاملات الإلكترونية تثار صعوبة أخرى تخص الركن المعنوي في جريمة السرقة، ويتعلق الأمر بمدى توافر القصد الخاص المتمثل في نية التملك للمعلومات أو الأموال الإلكترونية، وفي الواقع فإن النية المقصودة هنا هي اتجاه إرادة الجاني إلى الاستيلاء على المعلومات الخاصة بالمعاملات الإلكترونية بغية الاحتفاظ بها من أجل استخدامها لأغراض غير مشروعة تضر بمصلحة المجني عليه.[1]

وبهذا فإن الرجوع إلى القصد الخاص في إطار جرائم السرقة التقليدية لا يثير أي صعوبة على اعتبار أن محل السرقة هو أشياء مادية قابلة للتملك والحيازة، وفعل الاختلاس الذي يصدر من الجاني يصب في اتجاه نيته السيئة بالاستيلاء على الأشياء محل السرقة وحرمان صاحب الحق من أوجه السيطرة عليها، بالإضافة إلى عنصري العلم والإرادة.

لكن وبإسقاط ذلك على بيئة المعاملات الإلكترونية، وتعمقنا في تصور قيام الجريمة على المستوى الافتراضي بغياب التواجد المادي بين أطراف المعاملات فإننا نصطدم بفكرة مدى قيام نية الشخص في الاعتداء على المعلومات والبيانات المتعلقة بالمعاملة الإلكترونية بغرض التملك وحرمان المجني عليه منها.

مع العلم أن مجرى العقل الإجرامي في الإطار الإلكتروني لا يظهر بمظهره الحقيقي ولا يكشف مسار الفعل الإجرامي لمرتكب الفعل فغالب الاعتداءات تتمحور في فعل اختلاس المعلومات مع بقاء المعلومة لدى المجني عليه.

إن النظر إلى توافر القصد الخاص في الجرائم المتعلقة بالمعاملات الإلكترونية يبرز لنا مدى سهولة إتيانه، على اعتبار أن نية التملك هي ظاهرة بشكل واضح في المجال الإلكتروني، بحيث تبدأ الجريمة بالبقاء داخل الأنظمة المعلوماتية ومن ثم الاعتداء على البيانات والمعلومات الخاصة

[1] – هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر،1992، ص 235.

بالمعاملات الإلكترونية، وهو ما يفسر سلوك الشخص بالاستحواذ على تلك المعلومات فيما بعد.[1]

ثانيا:جريمة الحصول على التوقيع الالكتروني بالطرق الاحتيالية.

بعد الوقوف على جريمة الدخول غير المشروع لقاعدة البيانات التي تتعلق بالتوقيع الالكتروني، هناك جريمة أخرى لا تقل خطورة عن هذه الأخيرة متمثلة في الحصول على التوقيع الالكتروني بطرق الاحتيال.

حيث يعد الاحتيال في مجال نظم معلومات التوقيع الالكتروني من أهم الجرائم التي يمكن أن تقع على التوقيع الالكتروني وتسبب خسائر اقتصادية فادحة، نظرا للتطور المذهل في مجال التعامل واختراق التوقيعات الالكترونية في حسابات آلية موصولة بشبكة الإنترنت[2].

1- الاحتيال التقليدي: "الاستيلاء على مال مملوك للغير بخداعه وحمله على تسليم ذلك المال"[3].

ويرى البعض أن مصطلح الاحتيال يمكن تعريفه على أنه: " الاستيلاء بطريق الاحتيال على شيء مملوك للغير بنية تملكه، ولذلك يستعمل الجاني أساليب احتيالية قصد الاستيلاء على مال الغير[4].

[1] - أحمد خليفة الملط، المرجع السابق، ص 274.

[2] - حسام محمد نبيل الشنراقي، المرجع السابق، ص 179.

[3] - محمد هشام صالح عبد الفتاح، جريمة الاحتيال دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، نابلس، فلسطين،2008، ص 08.

[4] - حنان براهيمي، جريمة التزوير تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة ، 2015، ص 57.

وعرفه الفقه على أنه:" كل سلوك ينطوي على خداع المجني عليه بغرض الاستيلاء على أمواله، وهو ما يفترض إتيان الجاني أسلوبا من أساليب الاحتيال، ويعد وفقا لهذا التعريف إحدى عناصر الركن المادي لجريمة النصب[1].

ويعرف الاحتيال أيضا بأنه:" توصل الشخص إلى تسليم أو نقل مال منقول مملوك للغير إلى حيازته أو حيازة شخص آخر، وذلك باستعمال طرق احتيالية أو اتخاذ اسم كاذب أو حمل اسم آخر على تسليم أو نقل أو حيازة سند موجب لدين أو إيراد"[2].

2- الاحتيال الالكتروني (المعلوماتي)

نصت المذكرة التفسيرية للاتفاقية الأوربية لمكافحة جرائم المعلومات الموقعة في بودابست عام 2001 في المادة 08/ب على أن: « **التلاعب في المكونات المادية للحاسب والتلاعبات المعلوماتية الاحتيالية كون مجرمة إذا سببت ضررا اقتصاديا أو ماديا للغير، أو أن يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو لغيره، ومصطلح الضرر يشمل النقود والأشياء غير المادية**»[3].

كما عرف الاحتيال المعلوماتي بأنه:" التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة ، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناء على هذه الأوامر أو التعليمات ، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير[4].

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص 186.

[2]- حنان براهيمي،المرجع السابق، ص 57

[3] حسام محمد نبيل الشنراقي، المرجع نفسه، ص 08.

[4]- حنان براهيمي، المرجع نفسه، ص ص 57-58.

ثانيا: الركن المادي:

يتمثل الركن المادي لجريمة الاحتيال الالكتروني في التلاعب في معلومات وبيانات لها قيمة مالية بطرق احتيالية قد لا تكون محصورة تماشيا مع طبيعة الاحتيال الالكتروني ، فالجريمة المعلوماتية بصفة عامة جريمة متطورة ومتجددة لارتباطها بتكنولوجيات المعلومات [1].ولدراسة أعمق للركن المادي في جرائم الاحتيال على نظم معلومات التوقيع الالكتروني ، لابد من توضيح مسألة الأفعال التي يجرمها القانون، وهي استخدام الوسائل +الاحتيالية لخداع المجني عليه، وهنا إما يكون المسؤول عن نظام معلومات التوقيع الالكتروني أو الحاسب الآلي.

أ- الوسائل الاحتيالية:

هناك خلاف فقهي بشأن تطبيق النص التقليدي للاحتيال على الاحتيال في مجال المعلومات ومدى إمكانية تصور الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط وعلى أساس هذا الخلاف الفقهي تنوعت الوسائل الاحتيالية المستخدمة من قبل مرتكبي الجرائم المعلوماتية بتطور استخدامات الحواسيب، فجريمة النصب التقليدية اشترط فيها المشرع عدة أساليب ووسائل لكي يبلغ الجرم المرتكب مبلغ الاحتيال، وهي الطرق الاحتيالية والتصرف في مال ثابت ليس ملكا للجاني واتخاذ اسم كاذب أو صفة غير صحيحة.

أما فيما يتعلق بالاحتيال الالكتروني، فأنه اقتصار الفعل المادي على تلك الوسائل في شكلها التقليدي المادي البحت، حيث لا يحقق المعالجة القانونية لهذه المسألة[2].

[1]- حسام محمد نبيل الشنراقي، المرجع السابق، ص 184.

[2]- المرجع نفسه، ص 190.

ب- تسليم معلومات التوقيع الالكتروني (النتيجة الإجرامية)

في مجال المعلومات الالكترونية يقوم الحاسب الآلي بفعل التسليم بالمفهوم المادي للكلمة، كما أن التسليم يجب ألا ينظر إليه في الشكل المادي فقط، وإنما هو عمل قانوني عنصره الجوهري إرادة المجني عليه المعيبة بالخداع وليست المناولة المادية سوى مظهره المادي أو أثره[1].

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

ج- علاقة السببية بين طرق الاحتيال وتسليم المعلومات:

لا يكفي لقيام جريمة الاحتيال التامة أن يصدر من الجاني فعل الاحتيال، وأن يسلم المجني عليه الشيء المملوك له إلى هذا الجاني، بل يلزم أن تتوفر صلة ما بين فعل الاحتيال وتسليم الشيء المملوك وأن يكون الثاني ثمرة أو نتيجة للأول [2]. بمعنى لابد من توافر علاقة سببية ما بين فعل الاحتيال وفعل التسليم، وهذا فيما يتعلق بجريمة الاحتيال بصفة عامة، أما فيما يتعلق بجريمة الحصول على التوقيع الالكتروني بالوسائل الاحتيالية فأن توافر العلاقة السببية يجب تحقيق الركن المادي في هذه الجريمة، فالوسائل الاحتيالية لما حدث تسليم المعلومات ن ولما وقع المجني عليه سواء كان شخصا طبيعيا أو نظام معلوماتي[3].

الركن المعنوي:

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

---

[1]- محمد هشام صالح عبد الفتاح، المرجع السابق، ص 58.

[2]- المرجع نفسه، ص 58.

[3]- المرجع نفسه، ص 214.

أ–القصد الجنائي العام:

يقوم القصد الجنائي العام على عنصري العلم والإرادة، إذ ينبغي أن يعلم الجاني أن التوقيعات الإلكترونية التي يستولي عليها مملوكة للمجني عليه أو لغيره، كما ورد بالمذكرة التفسيرية للإتفاقية الأوروبية لمكافحة جرائم المعلوماتية في المادة 08/مقطع (ب) أن الجريمة يجب أن ترتكب عمدا أو يتمثل العنصر العام للقصد في التلاعب أو التدخل المعلوماتي الذي يسبب ضرا مادي للغير.[1]

ب–القصد الجنائي الخاص:

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

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

أما في إطار معلومات التوقيع الإلكتروني فإنه يجب أن تتجه إرادة الجاني إلى تحقيق ربح غير مشروع له أو لغيره وهو ما فسرته المذكرة التفسيرية لاتفاقية بودابست الموقعة في 2001/04/23

[1] – محمد هشام صالح عبد الفتاح، المرجع السابق ، ص 214.

[2] – المرجع نفسه ، ص 68.

[3] – أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني، المجلة العربية للدراسات الأمنية والتدريب، مجلد 28، العدد 56، جامعة نايف للعلوم الأمنية، 2012، ص 365.

بأن جريمة الاحتيال في مجال المعلومات تتطلب بالإضافة للقصد العام قصدا خاصا يتمثل في نية الغش بغرض الحصول على منفعة اقتصادية لشخص الجاني أو لغيره.[1]

رابعا: عقوبة الجريمة.

لم يتطرق المشرع الجزائري في التعديل الذي أجراه على قانون العقوبات الجزائري إلى جريمة الاحتيال، إذ تنص المادة 372 على: «**كل من توصل إلى استيلام أو تلقي أموالا أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة احتيالية أو عتاد مالي أو بإحداث الأمل في الفوز أو بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500إلى 20.000دج**»[2]

الفرع الثاني: جرائم الاعتداء على حجية التوقيع الالكتروني.

يرتبط السلوك المادي لجرائم الاعتداء على التوقيع الإلكتروني بتداول بيانات المحرر الإلكتروني كجريمة التعامل غير المشروع في نشاط التصديق وانتهاك سرية وخصوصية البيانات أنه من المتصور أن يكون محل الجريمة هو المساس بحجية التوقيع الإلكتروني في الإثبات كما هو الحال في جريمة الإتلاف و التزوير التوقيع الإلكتروني وهو ما سنتطرق إليه في هذا الفرع.

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 214.

[2] – ينظر: المادة 372 من الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات الجزائري، المعدل بالقانون رقم 16-02، المؤرخ في 19 يونيو 1916.

أولا: إتلاف التوقيع الإلكتروني.

01-تعريف إتلاف التوقيع الإلكتروني

أ-الإتلاف التقليدي:

إن الفقه قام بتعريفه على أنه: "التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له"[1]

ويعني أيضا: "تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، ويقصد به إفناء مادة الشيء أو هلاكه كليا أو جزئيا"[2]

ب-الإتلاف الإلكتروني:

يمكن تعريفه بأنه: "إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواء استيلاء على أموال أو اطلاع على معلومات، ولكن إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته"[3]

وعرّف جانب من الفقه الإتلاف الإلكتروني على أنه: "محو المعلومات أو البرامج كلية أو تدميرها إلكترونيا أو أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال"

02-أركان جريمة إتلاف التوقيع الإلكتروني.

أ-الركن المادي لجريمة إتلاف التوقيع الإلكتروني:

يتمثل السلوك الإجرامي المكون للركن المادي لجريمة الإتلاف المعلوماتي في إتلاف أو تعييب التوقيع الإلكتروني، ويتحقق فعل الإتلاف بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني ويتحقق

[1] - حسام محمد نبيل الشنراقي، المرجع السابق، ص 226.

[2] - حنان براهيمي، المرجع السابق، ص 54.

[3] - عبد الفتاح بيومي حجازي، المرجع السابق، ص 547.

فعل الإتلاف بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني قدرته على العمل عن طريق نشر فيروس معلوماتي أو سكب سائل على الوسيط الإلكتروني المحفوظ عليه، ويحدث تعييب التوقيع الإلكتروني كذلك بذات الوسيلة على نحو يفقده القدرة على العمل أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوها أو غير واضح.[1]

ب–الركن المعنوي:

يتطلب القصد الجنائي لجريمة إتلاف البيانات المعالجة إلكترونيا، أن تتجه إرادة الجاني إلى إتيان كل سلوك من شأنه تخريب أو محو أو تعديل نظم المعالجة الآلية للمعطيات، مع توقعه للنتيجة المتوصل إليها من نشاطه الإجرامي والتي تمثل الأساس النفسي النابع من إرادته الكاملة.[2]

واختلف في مسألة مدى توافر القصد الجنائي في الاعتداء على مشتملات نظام المعالجة داخليا كما هو موضح سابقا، والمتمثل في أفعال الإدخال والمحو والتعديل أو تلك الخارجة عن النظام، وبالرغم من أن موقف المشرع الجزائري كان واضحا من خلال المادة 394 مكرر من قانون العقوبات، بحيث جاء المفهوم مرنا وواسعا ليشمل كل السلوكات الماسة بتسيير نظام المعالجة وسلامته داخليا وخارجيا من أفعال التصميم وتجميع وتوفير أو نشر أو الإتجار في البيانات الإلكترونية واستغلالها لأي غرض خارج عن القانون وهو ما يوضح نية الغش المتمثلة في سوء الاستخدام والاعتداء على النظام في كل مراحله، مما يثبت الركن المعنوي للجريمة.

03–العقوبة المقررة لجريمة إتلاف التوقيع الإلكتروني:

اهتمام المشرع العربي بجريمة الإتلاف الإلكتروني لم يكن بذات المستوى الموجود لدى المشرع الغربي، فأغلب الدول العربية لم تحرك ساكنا لمواجهة هذا النوع المستحدث من الجرائم، وإنما اعتمدت على النصوص القائمة المنصوص عليها في مدونتها العقابية، ومع ذلك قامت بعض

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 542.

[2] – طعباش أمينة، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية،2012، ص 69.

الدول العربية باستحداث نصوص خاصة بهذه الجرائم، فنجد المشرع المصري جرّم الإتلاف وفقا لنص المادة 361 من أنوع العقوبات،[1] والمشرع العماني في القانون رقم 143 لسنة 1994 بشأن الأحوال المدنية.

أما المشرع الجزائري وفقا للتعديل الذي أجراه المشرع على قانون العقوبات أصبحت المادة 394 مكرر 01 تنص على: «**يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من 500.000دج إلى 2000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عطل بطريق الغش المعطيات التي يتضمنها**»

ومن الواضح تأثر المشرع الجزائري بالمشرع الفرنسي، فهذه المادة تعد ترديدا لما أورده المشرع الفرنسي في مادته 3/323 ممن قانون العقوبات الفرنسي.[2]

ثانيا: جريمة التزوير الإلكتروني.

عرّفه الفقه بأنه تغيير للحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها، كما تم تعريفه بأنه: "تغيير الحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، او لها شأن في إحداث نتيجة معينة"[3]

وعرّف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلي لعام 1994 في مقرراته وتوصياته بشأن جرائم الكمبيوتر والتزوير الإلكتروني بأنه المجرى الطبيعي لمعالجة البيانات التي

[1] – تنص المادة 361 من قانون العقوبات المصري على: كل من خرّب أو أتلف عمدا أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد عن 06 أشهر وبغرامة لا تتجاوز 300جنيه أو بإحدى هاتين العقوبتين»

[2] – Article 323/3 du code pénal : « le fait d'intreduire frauduleusement des donnés un susteme detraitement automatisé, d'extraire de détenir, de reproduire, de transmettre, de suprimer ou de modifier frauduleusement les donnés qui l contient est puni de cinq ans d'empruonnement et de 150000€ d'amende»

[3] – حنان براهيمي، المرجع السابق، ص 189.

ترتكب باستخدام الكمبيوتر، وتعد فيينا لو ارتكب بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.[1]

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

01-الركن المادي لجريمة تزوير التوقيع الإلكتروني:

يتمثل الركن المادي لجريمة تزوير التوقيعات الإلكترونية في سلوك الجاني والمتمثل في تغيير الحقيقة والتي تكون مثل التوقيع الإلكتروني، ويحصل التزوير بأي وسيلة كانت كاستخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك.

التزوير التقليدي نصت عليه المادة 214 من قانون العقوبات الجزائري الي غاية المادة 218 فتزوير المحررات هو تغيير حقيقة المضمون وإظهاره بمعنى جديد وعلى ذلك بصفه الفقهاء بأنه تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق المبينة في القانون تغييرا من شانه ان يسبب ضررا للغير إن التزوير الالكتروني أو ألمعلوماتي يتضمن إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو بالإضافة ويتضمن أيضا نسخ الأقراص المدمجة إلى أقراص أخرى.

أ-تغيير الحقيقة (سلوك الجاني):

تغيير الحقيقة هو استبدالها بما يخالفها، أي هو إدخال تغيير على المحرر المراد تزويره على نحو يغير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته.[2]

[1] - عباس حفصي، جرائم التزوير الإلكتروني "دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، جامعة أحمد بن بلة، وهران، 2015، ص 18.

[2] - حسام محمد نبيل الشنراقي، المرجع السابق، ص 249.

وتغيير الحقيقة سواء كان في محرر رسمي أو عرفي يمكن تصور حصوله في المحررات في نطاق المعلوماتية، وفي هذه الحالة تسمى جريمة التزوير بأنها تزوير معلوماتي كتزوير التوقيع الإلكتروني، وهو ينصب على مخرجات الحاسب الآلي أي البيانات والمعلومات الخارجة منه.[1]

ويقصد بتغيير الحقيقة أيضا ليس تغيير الحقيقة الواقعية المطلقة وإنما الحقيقة النسبية، كأن يثبت في المحرر المزور ما يخالف إرادة صاحب الشأن ويقوم بتزوير توقيع صاحب الشأن عليها حتى ولو صادف ذلك الواقع فعلا.[2]

ويكون التزوير في نطاق المعلومات بتغيير الحقيقة في الشرائط أو المحررات التي تمثل مخرجات الحاسب الآلي طالما حدث تغيير في بيانات الحاسب الآلي نفسه.

ب–محل التزوير:

لقد ثبت علميا ضيق النصوص التقليدية بشأن مواجهة جريمة التزوير الذي يقع في مجال المعاملات الإلكترونية وحماية الثقة الواجب توافرها في المحررات الإلكترونية، خاصة مع تعاظم الاعتماد على تلك المحررات في تسيير أمور وشؤون المجتمع الحديث.

فقد اتخذ الموقف الجزائري نفس الموقف التشريعي للدول السابقة من خلال الاعتراف بحجية الكتابة الإلكترونية، وبالتالي الاعتراف بالمحررات الإلكترونية في الإثبات، وهذا من خلال النص المستحدث 323مكرر1 بموجب القانون 05-01 المتضمن تعديل القانون المدني، والتي جاءت صياغتها كالتالي: «**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق يشترط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**»

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 254.

[2] – المرجع نفسه، ص 250.

ج-وسائل وطرق التزوير:

من أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني استخدام برامج حاسوبية أو أنظمة معلوماتية خاصة بذلك يتم تصميمها على غرار البرامج والنظم المشروعة أو محاولة بعض الأشخاص كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها وإعادة استخدامها بعد ذلك.[1]

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

للإشارة فإن التزوير في المعلومات والتوقيعات الإلكترونية يمر بثلاثة مراحل أساسية وهي:[3]

1-مرحلة التلاعب بالبيانات والتوقيعات عند الإدخال في النظام المعلوماتي إذ يقوم الجاني بالتلاعب في التوقيعات الإلكترونية التي يتم إدخالها للنظام دون المساس بالبرنامج.

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

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

---

[1] - صالح شنين، المرجع السابق، ص 360.

[2] - حنان براهيمي، المرجع السابق، ص 248.

[3] - حسام محمد نبيل الشنراقي، المرجع السابق، ص ص 269-270.

02-الركن المعنوي:

لا تكتمل جريمة تزوير التوقيعات الإلكترونية أو الوثيقة المعلوماتية إلا بتوافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، فهذه الجريمة هي جريمة عمدية.[1]

وصورة الركن المعنوي فيها هي القصد الجنائي بنوعيه، القصد الجنائي العام والمتمثل في علم الجاني أنه يغير الحقيقة، وأن هذا التغيير ينصب على محرر بإحدى الطرق المنصوص عليها قانونا، وأن من شأن فعله إحداث الضرر، وعليه فإن هذا الفعل هو فعل محظور ومعاقب عليه ومع ذلك يقبل القيام به، وتتجه إرادته إلى الفعل ويقبل النتائج المترتبة عليه بمعنى أنه يجب أن تتجه إرادته إلى فعل تغيير الحقيقة والأثر المترتب عليه، وهو أن يشتمل المحرر على البيانات المخالفة للحقيقة.[2]

03-عقوبة الجريمة:

عاقب المشرع الجزائري على التزوير في مجال معلومات التوقيع الإلكتروني في المادة 214 المعدلة بالقانون رقم 82-04 المؤرخ في 13 فبراير 1982 بالسجن المؤبد كل قاضي أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته.

المطلب الثاني: الجرائم المستحدثة الماسة بالتوقيع الإلكتروني.

انطلاقا من أن التوقيع الإلكتروني هو مجموعة من البيانات في شكل إلكتروني، فإنه توجد خطورة الاعتداء عليه بجرائم تأخذ أشكالا وصورا متعددة، ومن ثمة سنقسم هذا المطلب إلى فرعين: حيث نتطرق في الفرع الأول إلى جرائم الاعتداء على النظام المعلوماتي، بينما نتناول في الفرع الثاني جرائم الاعتداء على بيانات التوقيع الإلكتروني.

[1] – حسام محمد نبيل الشنراقي، المرجع السابق ، ص 224.

[2] – خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، رسالة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 190.

الفرع الأول: جرائم الاعتداء على النظام المعلوماتي.

إن ربط أجهزة الحاسبات الآلية مع بعضها البعض عن طريق الشبكات المعلوماتية أدى إلى سرعة انتقال المعلومات فيما بينها من جهة، وإلى سهولة التطفل عليها عن طريق الدخول إلى الحاسبات من جهة أخرى،[1] فالنظام المعلوماتي قد يتعرض إلى اختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو البقاء فيه،[2] وقد يتعرض إلى تعطيله وإعاقته بشكل تام أو تباطؤ أو اضطراب في عمله مما يؤدي إلى نتائج غير صحيحة ومخالفة للحالة المعهودة لعمل النظام، وهذا ما يعرف بإفساد أو تعطيل النظام المعلوماتي، ومن هنا سوف نتطرق في هذا الفرع إلى جريمتين، أولهما: جريمة الدخول غير المصرح به على قاعدة بيانات خاصة بالتوقيع الإلكتروني، وجريمة إفساد أو تعطيل النظام المعلوماتي.

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

عند تناول هذه الجريمة لابد من التفرقة بين الدخول والبقاء غير المصرح به، فالأول يتحقق باختراق نظم معلومات التوقيع الإلكتروني، أما البقاء فقد يترتب على الدخول غير المصرح به أو أن يكون الدخول قد تم بشكل قانوني مصرح به إلا أن القائم بالدخول استمر داخل النظام متجاوز الحد المسموح به للبقاء داخله فأصبح بذلك مرتكبا للجريمة رغم أن الدخول في بداية الأمر كان مشروعا.[3]

إن فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يعني الدخول بمعناه المادي كالدخول إلى مكان أو منزل أو حديقة، وفي نفس الاتجاه الدخول إلى الحاسب الآلي، أو مكان وجوده، إنما يقصد بالدخول هنا كظاهرة معنوية تشبه تلك التي يغير عنها بقولها الدخول إلى فكر أو مملكة

[1] – دلخاز صلاح بوناني، الحماية الجنائية الموضوعية لمعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط 1، 2016، ص 188.

[2] – نهلا عبد القادر الموسني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط1، 2008، ص 158.

[3] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 137.

التفكير لدى إنسان أي: "الدخول إلى العمليات الذهنية التي يقوم بها النظام المعلوماتي"، فالدخول إلى النظام المعلوماتي يتشابه مع الدخول إلى ذاكرة إنسان.[1]

ويتحقق الدخول غير المصرح به جهاز الكمبيوتر بالوصول إلى المعلومات أو البيانات المخزنة داخل نظام الكمبيوتر والقوائم والمعدات والمكونات دون رضاء المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها، أو بمعنى آخر إساءة استخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات الموجودة بداخله لاستخدامها في عرض ما.[2]

01-الركن المادي للجريمة:

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح به، [3] ودائما ما يثار التساؤل بشأن هذا الفعل وكيف يمكن تحديد ما إذا كان الفعل المرتكب هو ذاته الفعل المؤثم قانونا.[4]

أ-فعل الدخول:

لم تحدد التشريعات المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، ويمكن تعريفه بأنه الدخول إلى المعطيات المخزنة داخل نظام الحاسوب دون رضا المسؤول عن هذا النظام.[5]

---

[1] – دلخار صلاح بوتاني، المرجع السابق، ص 191.

[2] – أحمد عصام عجيلة، الحماية الجنائية للمحررات الإلكترونية، دار النهضة العربية، القاهرة،2014، ص 251.

[3] – صالح شنين، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة"، رسالة دكتوراه، جامعة تلمسان،2013، ص 74.

[4] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 141.

[5] – صالح شنين، المرجع نفسه، ص 69.

لقد رصد الفقه الإنجليزي مشكلة بشأن تحديد معنى الدخول في القانون، حيث تطلب هذا التحديد التمييز بين المشروعية وعدم المشروعية في فعل الدخول، حيث انتهى القانون الإنجليزي لتقرير ضرورة أن يكون الدخول غير مصرح به تطبيقا للمادة 05 من القسم 17، وكذا بين الدخول المباشر من الحاسب الذي يحوي البيانات ومنها بيانات التوقيع الإلكتروني والدخول عن بعد.[1]

وفكرة الدخول وفقا للتشريع الأمريكي تتمثل في: "مجرد فعل الدخول دون تطلب تحقق الضرر وعلى ذلك فإن الدخول غير المصرح به يتضمن عنصرين هامين هما: عنصر المكان، ويتمثل في الدخول إلى النظام أو المرور بداخله، والثاني عنصر الزمان وهو الوقت الذي يستغرقه التواجد داخل نظام المعلومات"[2]

وهذا معناه أن الفقه القانوني يشهد اختلافات حول تحديد طبيعة الفعل المجرم قانونا نتيجة فعل الدخول إلى نظام معلومات التوقيع الإلكتروني بين مشروعية الفعل في حد ذاته ثم تجاوز هذه المشروعية إلى الفعل المجرم قانونا يتمثل إما في دخول مشروع لنظام المعلومات في بداية الأمر، لكن الاستمرار فيه وتجاوز المدة المحددة يجعل منه فعلا مجرما.

أما المشرع التونسي فقد استعمل عبارة النفاذ عوضا عن عبارة الدخول، ليؤكد الخاصية اللامادية لهذه الجريمة، فعبارة الدخول قد يكون لها مدلول مادي في حين أن النفاذ له مدلول الحماية، أو عن طريق إدخال برنامج فيروس أو باستخدام الرقم الكودي لشخص آخر، أو تجاوز نظام الحماية إذا كان ضعيفا، ويستوي أن يتم الدخول مباشرة أو بطريقة غير مباشرة كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلفزيونية.[3]

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 143.

[2] – المرجع نفسه، ص 145.

[3] – صالح شنين، المرجع السابق، ص 74.

ب–عدم التصريح بالدخول:

نصت المادة 23 من القانون المصري 15 لسنة 2004 على أنه: «**مع عدم الإخلال بأي عقوبة أشد منصوصا عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن 10آلاف جنيه، ولا تتجاوز 100ألف جنيه أو بإحدى هاتين العقوبتين كل من توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته**»[1]

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

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

* إذا كان دخول الفاعل لأماكن من النظام لم يصرح له بدخولها.[2]

2–الركن المعنوي:

إن جريمة الدخول غير المصرح به في نظم المعلومات التوقيع الإلكتروني من الجرائم العمدية التي يتمثل الركن المعنوي فيها في القصد الجنائي العام بركنيه العلم والإرادة، ولا تتطلب قصدا جنائيا خاصا، وذلك لكونها من جرائم الخطر التي يعاقب المشرع فيها على مجرد إتيان الفعل المجرم، وعلى ذلك يعاقب المشرع بعقوبة الجريمة التامة على إتيان الفعل المادي مع توافر القصد الجنائي دون اشتراط تحقق النتيجة المتوخاة من الجريمة.[3]

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 151.

[2] – المرجع نفسه ، ص 151.

[3] – المرجع نفسه، ص 167.

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

أ-القصد الجنائي العام:

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

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

في حين لم يتطلب المشرع المصري في القانون رقم 04-15 قصدا في جريمة الدخول غير المشروع داخل النظام المعلوماتي للتوقيع الإلكتروني، ومن ثم فإن القواعد العامة بشأن القصد الجنائي تسرب على هذه الجريمة.[4]

ومن هنا نستخلص أن القصد العام في جريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني يتطلب أن يكون مرتكب هذا الدخول على علم بما يرتكبه، أو أن أفعاله هذه مخالفة للقانون جراء دخوله غير المشروع.

ب-القصد الجنائي الخاص:

هذا القصد لم تتطلبه التشريعات بوجه عام، ولكن تطلبته بجوار القصد العام، فمثلا نجد أنه في القانون النرويجي تشدد العقوبة إذا ارتكب فعل الدخول غير المصرح به بنية الحصول للفاعل

[1] - حسام محمد نبيل الشنراقي، المرجع السابق، ص 169.

[2] - المرجع نفسه، ص 169.

[3] - المرجع نفسه، ص 170.

[4] - عبد الفتاح بيومي حجازي، المرجع السابق، ص569.

أو لغيره على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الاطلاع على المعلومات التي يحوزها النظام.[1]

وكذلك في الدنمارك تشدد العقوبة متى ارتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات.

أما في التشريع الجزائري فلا يبدو من نص المادة 394مكرر من قانون العقوبات أن المشرع يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول أو البقاء غير المصرح بهما وأنه يكفي لقيامهما توافر القصد العام القائم على العلم والإرادة، وكذلك الشأن مع نص المادة 1/223 من قانون العقوبات الفرنسي المطابقة للمادة السابقة، فهي لا تشترط قصدا خاصا.[2]

3-عقوبة جريمة الدخول غير المصرح به على قاعدة بيانات خاصة بالتوقيع الإلكتروني:

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

إن المشرع الجزائري ضمن سياق التعديل الذي أجراه المشرع على قانون العقوبات الجزائري فقد تناول جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي، وذلك في المادة 394 مكرر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي، فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء. والعقوبة بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000دج.

[1] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 173.

[2] – محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 167.

ثانيا: جريمة تعطيل أو إفساد النظام المعلوماتي.

تتحقق هذه الجريمة بتعطيل وإعاقة النظام المعلوماتي عن القيام بوظائفه المعتادة حيث يترتب على ذلك توقف النظام عن العمل بشكل تام أو تباطؤ واضطراب في عمله مما يؤدي إلى إصدارات نتائج غير صحيحة ومخالف للحالة المعهودة لعمل النظام وللوقوف على هذه الجريمة لابد أن نبين مفهومها وأركانها ثم العقوبة المقررة لها.

01-تعريف جريمة تعطيل وإفساد النظام المعلوماتي:

تعرف جريمة تعطيل وإفساد النظام المعلوماتي بأنها: "الاعتداء على نظم المعالجة الآلية للمعلومات بمنعها من أداء وظائفها بصورة تامة أو إجراء تعديل في تلك الوظائف"[1]

وتعرف بأنها: "كل فعل يتسبب في توقف أو تباطؤ أو ارتباك عمل نظام المعالجة ومن ثمة ينتج عن ذلك تغير في حالة النظام"[2]

02-أركانها:

أ-الركن المادي:

يمثل النشاط الإجرامي المكون للركن المادي لهذه الجريمة، إما في فعل تعطيل النظام المعلوماتي وإما في إفساد نشاط أو وظائف هذا النظام.[3]

وفعل التعطيل أو الإفساد قد يقع بوسيلة مادية، كما في حالة وقوع النشاط الإجرامي على أجهزة الحاسب الآلي بكسرها أو سكب سائل عليها أو إحراقها مثلا أو قد يقع بوسائل معنوية

[1] - دلخار صلاح بوتاني، المرجع السابق، ص 227.

[2] - نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية "دراسة نظرية وتطبيقية"، دار النهضة العربية، القاهرة، 2003، ص 225.

[3] - علي عبد القادر القهوجي، الحماية الجنائية للحاسب الآلي، دار الجامع للطباعة والنشر، الإسكندرية، 2004، ص 128.

عندما يقع النشاط الإجرامي على الكيانات المنطقية المعنوية الحاسب الآلي كإدخال الفيروسات مثلا.[1]

***فعل التعطيل أو إفساد النظام المعلوماتي:**

يتمثل مضمون الركن المادي لجريمة تعطيل أو إفساد النظام المعلوماتي في فعلي التعطيل والإفساد اللذين ينصرفان إلى أي عمل يأتيه الجاني ويكون من شأنه إعاقة النظام المعلوماتي أو إدخال سير عمله.

-فعل التعطيل:

العطل لغة: الخلو من الشيء ويقال تعطيل الرجل أي بق بلا عمل.

أما اصطلاحا: هو منع النظام المعلوماتي بصفة كلية أو جزئية من العمل وهو ما يرد على النظام بأكمله أو على أحد البرامج الموجودة بداخله.[2]

إن التعطيل الذي من شأنه منع سير وظائف النظام المعلوماتي عن العمل يقتضي أن يكون موجها إلى برامج تشغيل النظام التي تقوم بأداء وظائف عمل النظام وليس المعلومات بالمعنى الضيق كالبرامج التشغيلية أو التطبيقية التي يرجع إليها النظام في القيام بعمله.

إن التعطيل يتم بوسائل مادية أو معنوية، فتكون مادية سواء اقترنت بهدف أم لا إذا ما انصب نشاط إجرامي بطريقة مادية وعلى الأجهزة المادية عن طريق تخريبها، إما بكسرها أو سكب سائل عليها، ويكون التعطيل بوسيلة معنوية مثل إدخال فيروس تدميري يؤدي إلى توقف دائم لنظام أو طريق إدخال قنبلة معلوماتية زمنية مبرمجة.[3]

---

[1] – دلخار صلاح بوتاني، المرجع السابق، ص 229.

[2] – أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2010، ص 160.

[3] – علي عبد القادر القهوجي، المرجع السابق، ص 129.

-فعل الفساد:

الإفساد أصله فسد، ومعناه **لغة:** الخلل والاضطراب أو التلف أو العطب، أما **اصطلاحا** يقصد به ممارسته "أي فعل على النظام المعلوماتي من شأنه أن يعدل في وظيفته دون أن يعوقه عن أداء هذه الوظيفة"

أي بمعنى جعل النظام غير قابل للاستعمال، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

تتعدد وسائل إفساد النظام المعلوماتي كما سبق وأن أشرنا باستخدام وسائل معنوية تنشب على الكيانات المنطقية للنظام كالقيام بإدخال برنامج فيروسي قد وضع من قبل أشخاص على علم ودراية وخبرة بالبرمجة المعلوماتية استخدموا تقنيات متقدمة في وضعها لها القدرة على التكاثر بنسخ نفسها والانتقال والانتشار في الأنظمة المعلوماتية وقد تؤدي في النهاية إلى تعطل النظام بالكامل.[1]

وهناك برنامج الدورة المعلوماتية التي تقوم بالانتقال من حاسب آلي إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها، فتغطي شبكة بأكملها، ولديها إمكانية تعطيل نظام الحاسب إلا بصورة كاملة عن طريق استغلال أي خلل أو فجوة في نظام تشغيل الحاسب.[2]

وهناك برنامج يثير حدثا في لحظة زمنية معينة محددة بالساعة واليوم والسنة ويتم إدخالها في برنامج، وتنفذ في جزء من الثانية وعدة ثوان أو دقائق بحسب التحديد اللازم وسمي هذا البرنامج بالقنبلة الزمنية كونها تنشط وتعمل على تعطل النظام في وقت محدد بالساعة واليوم والسنة.[3]

---

[1] – دلخار صلاح بوتاني، المرجع السابق، ص 236.

[2] – سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، مصر، 2008، ص 106.

[3] – حسام محمد نبيل الشنراقي، المرجع السابق، ص 197.

ب–الركن المعنوي لجريمة تعطيل أو إفساد النظام المعلوماتي:

جريمة التعطيل هي جريمة عمدية لا يكفي لقيامها تحقيق الركن المادي فقط، بل لابد من توافر الركن المعنوي أيضا، والذي يتخذ صورة القصد الجنائي العام بتوافر عنصريه العلم والإرادة، وأن يتجه كلاهما إلى العناصر المشكلة للركن المادي للجريمة كافة، إذ يجب أن يعلم الجاني أن النشاط الإجرامي الذي يأتيه من شأنه تعطيل وإفساد النظام المعلوماتي، وإن ذلك يتم دون رضا صاحب الحق في السيطرة على ذلك النظام أو ضد إرادته، ومع ذلك تتجه إرادته إلى فعل التعطيل أو الإفساد، فإذا تحقق الركن المادي والركن المعنوي بعنصريه قامت الجريمة.[1]

03–عقوبة جريمة التعطيل وإفساد النظام المعلوماتي:

لم يتعرض المشرع الجزائري إلى جريمة تعطيل أو إفساد النظام المعلوماتي حتى بعد إضافة القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، وذلك بالتعديل الذي أجراه المشرع على قانون العقوبات واكتفى بالنص على جريمة الاعتداء على معطيات المعلومات، والمادة 394مكرر1.[2]

وبرز البعض موقف المشرع الجزائري بعدم النص على جريمة تعطيل النظام المعلوماتي للتشابه الكبير بينها وبين جريمة الاعتداء على المعطيات، كما اعتبر المشرع الجزائري إفساد النظام نتيجة ظرف مشدد لجريمة الدخول بطريق الغش، وذلك في الفقرة الأخيرة من نص المادة 394 مكرر من قانون العقوبات.[3]

[1] – علي عبد القادر القهوجي، المرجع السابق، ص 131.

[2] – القانون رقم 09–04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج، العدد07، المؤرخة في 2009/08/16.

[3] – ينظر: المادة 394 مكرر1 من الأمر 66–156 المتضمن قانون العقوبات المعدل والمتمم.

الفرع الثاني: جرائم الاعتداء على بيانات التوقيع الإلكتروني.

نظرا لخطورة جرائم الاعتداء على بيانات التوقيع الإلكتروني في العصر الحديث استجابت التشريعات الأجنبية والعربية لمتطلبات عصرنة هذه التقنية، واتخذت التدابير التشريعية اللازمة التي يمكنها صد الآثار السلبية الإجرامية الناجمة عن إساءة استعمالها، ومن خلال هذا سنتناول أهم الجرائم الواقعة على التوقيع والتصديق الإلكترونيين في ظل القانون رقم 15-04 المؤرخ في 2015/02/01.

فبالرجوع إلى النصوص القانونية التي أقرها القانون رقم 15-04 نجد أنها تتفق في كون أن الجرائم المنصوص عليها هي جرائم عمدية يتطلب لقيامها توافر الركن المعنوي الذي يقوم على القصد الجنائي العام بعنصريه العلم والإرادة، ولا تحتاج إلى القصد الجنائي الخاص، فنجد المشرع الجزائري بموجب القانون 15-04 قرر أن الجرائم هي جرائم خطر، وليست جرائم ضرر وبالتالي يكفي لقيامها توفر السلوك الإجرامي دون الحاجة إلى تحقق أو عدم تحقق نتيجة معينة، [1] وترتيبا على ما تقدم سوف يتم دراسة هذه الجرائم على الركن المادي مع تبيان النص القانوني لها وهي على النحو التالي:

أولا: صور الاعتداء على بيانات التوقيع والتصديق الإلكترونيين.

أفرد المشرع الجزائري في قانون التوقيع والتصديق الإلكترونيين الفصل الثاني من الباب الرابع لمجموعة الجرائم، منها ما يتعلق بطالب شهادة التصديق الإلكتروني، ومنها ما يتعلق بتأدية خدمات التصديق الإلكتروني، وأخرى خاصة بالتوقيع الإلكتروني.[2]

[1] – عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي، تمنراست، العدد01، جانفي 2017، ص 118.

[2] – حسين جفالي، الحماية الجنائية لتوقيع المستهلك الإلكتروني في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 03، المجلد01، كلية الحقوق والعلوم السياسية، جامعة عمار خليجي، ص 271.

أ-جنحة إفشاء بيانات شهادة التصديق الإلكتروني:

نصت على هذه الجريمة المادة 70 من القانون 15-04 والتي جاء فيها: «**يعاقب بالحبس من 03 أشهر إلى سنتين وبغرامة من 200.000دج إلى مليوني دج أو بإحدى هاتين العقوبتين كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون**»

حيث نصت المادة 42 من القانون 15-04 على أنه يجب على مؤديي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.[1]

ويظهر أن المشرع الجزائري اشترط لقيام هذه الجريمة توفر مجموعة من الأركان:

1-صفة الجاني:

لكي تقوم هذه الجريمة يجب أن تتوافر لدى القائم بها صفة العمل لدى الجهة المختصة بإصدار شهادة التصديق الإلكتروني، فعلة التجريم تكمن في أن الجاني قد اؤتمن على هذه المعلومات أو البيانات بسبب وظيفته.

2-الركن المادي:

وهو إتيان الجاني بفعل إيجابي وهو إفشاء أو إعلام الغير بالمعلومات المتعلقة بالتوقيع الإلكتروني، وتنقسم المعلومات من حيث إمكانية الوصول إليها على معلومات متاحة ومعلومات سرية أو غير متاحة، فالمتاحة هي المنشورة على المواقع الإلكترونية المفتوحة للجمهور، وأما غير

[1] - ينظر: المادة 70 و 42 من القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق لـ 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

المتاحة فهي التي يقتصر العلم بها على أشخاص محددين كمالكها أو من يملك السلطة القانونية عليها.[1]

3-الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام أي العلم والمعرفة أي الجاني يعلم بوقائع الجريمة كونها من المحظورات ومع ذلك تتجه إرادته إلى الفعل المجرم وتقبل النتيجة المترتبة عليها وهي إفشاء بيانات شهادة التصديق الإلكترونية.

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

نصت على هذه الجريمة المادة 68 من القانون 15-04 على أنه: «**يعاقب بالحبس من 03 أشهر إلى 03 سنوات وبغرامة من مليون دج إلى خمسة ملايين دج أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير**»

1-صفة الجاني:

أن يكون ممن قدمت إليه بيانات التوقيع الإلكتروني الموصوف من الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني أو من اتصل بها بحكم عمله.

2-الركن المادي:

من خلال نص المادة 68 على ثلاثة أفعال وهي: **الحيازة** وهي حيازة الجاني بيانات توقيع إلكتروني خاصة بالغير، و **الإفشاء** وهو البوح أو إحاطة علم الغير ببيانات التوقيع الإلكتروني أو الوسائط الإلكترونية أو معلومات من الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني،

[1] - محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، مصر، 2010، ص 53.

و**الاستعمال** أي استعمال من قدمت إليه بيانات التوقيع الإلكتروني الخاص بالغير كل شخص طبيعي أو معنوي صاحب التوقيع الإلكتروني.

وبالتالي يعد أحد هذه الأفعال كاف لقيام هذه الجريمة وتتحقق في الحالة التي يقوم بها الجاني بإفشاء بيانات إنشاء التوقيع الإلكتروني.[1]

3-الركن المعنوي:

تعد هذه الجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي وهو إفشاء من قدمت إليه بيانات التوقيع الإلكتروني واستخدامها وحيازتها واتجاه إرادة الجاني إلى ارتكاب الفعل المعاقب عليه قانونا.

ج-جنحة جمع البيانات الشخصية للموقع واستخدامها في غير غرضها:

نصت على هذه الجريمة المادة 71 من القانون 15-04 على أنه: «**يعاقب بالحبس من 06أشهر إلى 03 سنوات وبغرامة من 200.000دج إلى مليون دج أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون**[2]»

1-صفة الجاني:

يجب أن تقع هذه الجنحة من مؤدي خدمات التصديق الإلكتروني أو أحد العاملين به وأن يستخدم هذه البيانات التي قام بجمعها دون رضا الموقع في غير الغرض المخصص لها.[3]

---

[1] - عزيزة لرقط، المرجع السابق، ص 124.

[2] - المادة 43 من القانون 15-04 تنص على أنه: «لا يمكن لمؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة، ولا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني ولا يمكن استعمال هذه البيانات لأغراض أخرى»

[3] - عزيزة لرقط، المرجع السابق، ص 122.

2-الركن المادي:

يتحقق الركن المادي بإتيان الجاني فعل إيجابي وهو استخدام بيانات التوقيع الإلكتروني في غير الغرض المخصص لها أو جمع بيانات دون الحصول على الموافقة الصريحة.

3-الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني أن نشاطه الإجرامي معاقب عليه قانونا وهو جمع البيانات الشخصية للموقع واستخدامها في غير غرضها الأصلي.

ثانيا: جرائم الاعتداء على شهادة التصديق الإلكتروني.

لقد عدد القانون رقم 15-04 صور تجريمية متعددة ماسة بشهادة التصديق الإلكترونية ومن أهم هذه الجرائم ما يلي:

أ-إصدار شهادة تصديق إلكتروني بدون ترخيص أو سحبه:

نصت المادة 72 من القانون 15-04 على أنه: «**يعاقب بالحبس من سنة إلى 03 سنوات وبغرامة من 200.000دج إلى مليوني دج أو بإحدى هاتين العقوبتين فقط كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات تصديق إلكتروني يستأنف ويواصل نشاطه بالرغم من سحبه ترخيصه تصادر التجهيزات التي استعملت في ارتكاب الجريمة طبقا للتشريع المعمول به**»[1]

[1] - المادة 72من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

1-الركن المادي:

يتضح من نص المادة أن المشرع جرم قيام أية جهة غير مرخص لها من السلطات المختصة السلطة الاقتصادية حسب أحكام المادة 33من ذات القانون، إصدار شهادات التصديق الإلكتروني المعروفة بموجب الفقرة 07 من المادة 02 من القانون 15-04.

ويترتب على ذلك أن جريمة إصدار شهادة التصديق الإلكتروني من جهة لا تملك رخصة بذلك أو تم سحب الرخصة منها م الجرائم الشكلية التي يتطلب قيامها توافر السلوك الإجرامي فقط، والذي يتمثل في قيام جهة قبل الحصول على الترخيص وفقا للشروط والإجراءات التي حددها القانون 15-04 خاصة المواد 33 وما يليها منه في إصدار شهادات التصديق الإلكتروني أو الاستمرار في منح شهادات التصديق الإلكتروني أو الاستمرار في منح شهادات التصديق بالرغم من سحب الرخصة المخولة لمؤدي خدمات التصديق.

2-الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية الذي يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي المتمثل في إصدار شهادة تصديق إلكتروني قبل الحصول على ترخيص لمزاولة النشاط من الهيئة المختصة، ويتطلب القصد اتجاه إرادة الجاني إلى إصدار شهادة تصديق إلكتروني قبل الحصول على ترخيص أو سحبه.

ب-جنحة الإدلاء بإقرارات كاذبة للحصول على شهادات التصديق:

نص عليها المشرع الجزائري في المادة 66 على أنه: «**يعاقب بالحبس من 03 أشهر إلى 03 سنوات وبغرامة من 20.000دج إلى 200.000دج أو بإحدى هاتن العقوبتين فقط كل من ادلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة**»[1]

[1] - ينظر: المادة 66 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

1-الركن المادي:

وهو قيام الجاني بتقديم إقرارات كاذبة سواء لمؤدي الخدمات أو للطرف الثالث الموثوق باعتباره المسؤول عن منح شهادة التصديق.

فلا يشترط لقيام الركن المادي حلول ضرر معين أو تحقق نتيجة معينة وإنما يكفي لقيامها تحققا للنشاط الإجرامي وهو تقديم معلومات خاطئة وكاذبة.[1]

3-الركن المعنوي:

تعد جريمة عمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي وهو الإدلال بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني واتجاه إرادة الجاني إلى تقديم تصريحات كاذبة للحصول على الشهادة.

ج-جنحة الإخلال بأخبار السلطة الاقتصادية عن التوقف:

نصت عليها المادة 67 من القانون 15-04 على: «**يعاقب بالحبس من شهرين إلى سنة واحدة وبغرامة من 200.000دج إلى مليون دج أو بإحدى هاتين العقوبتين فقط كل من يؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58و59 من هذا القانون**»[2]

1-الركن المادي:

تعد هذه الجريمة من جرائم السلوك الخطر يقوم ركنها المادي بمجرد اتخذا مؤدي الخدمات موقف سلبي يتمثل في عدم إعلام السلطة الاقتصادية بالتوقف عن نشاطه المحدد حسب أحكام المادة 41 من ذات القانون، وبالتالي فإن السلوك الإجرامي المكون للركن المادي يتحقق بامتناع

[1] - عزيزة لرقط، المرجع السابق، ص 124.

[2] - ينظر: المادة 67 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

الجهة المختصة المرخص لها إصدار شهادات التصديق الإلكتروني عن الإستمرار في إصدار الشهادات دون إعلام السلطة الوصية بذلك سواء في الحالات العادية أو الاستثنائية المنصوص عليها في المادتين 58-59 من نفس القانون.

2-الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي والذي يتمثل في عدم إعلام السلطة الاقتصادية بالتوقف عن النشاط واتجاه إرادة الجاني لإتيان كل من السلوك الإجرامي والنتيجة معا.[1]

[1] - عزيزة لرقط، المرجع السابق، ص 120.

الفصل الثاني

الحماية الإجرائية للحماية الجنائية للتوقيع الإلكتروني

المبحث الأول: التعاون الدولي لمكافحة جرائم التوقيع الإلكتروني.

المبحث الثاني: إجراءات الإثبات الجنائي في جرائم التوقيع الإلكتروني.

يعد الوقوف على أهم فصول الحماية الجنائية الموضوعية للمعاملات الإلكترونية، نجد أن الدراسة تقف عند منحى آخر وهو الجانب الإجرائي الذي يمثل استكمالا لمفهوم تلك الحماية وشموليتها، ويعزز القواعد الموضوعية، فالجوانب الإجرائية للحماية الجنائية من جرائم المعاملات الإلكترونية هي التي تنقل نص التجريم من الركود إلى جانب الحركة، وعند الانتقال إلى دائرة التطبيق العملي للحماية الجنائية للمعاملات الإلكترونية، تظهر التحديات التي تبدأ من أولى مراحل التحقيق وجمع الأدلة التي ولدت مشكلات وعقبات عملية، وقعت كحجر عائق أمام السلطات والهيئات المختصة قانونا في مواجهة هذه الطائفة من الجرائم من جهة، ومن جهة أخرى فإن الطبيعة الخاصة للمعاملات الإلكترونية ولدت مشكلة السيطرة على الدليل غير المادي، وغموض مسرح الجريمة الافتراضي الذي أثر على وسائل وآليات التحقيق والإثبات.

وبناء على ما سبق سيتم تقسيم هذا الفصل إلى مبحثين مستقلين، يخصص الأول منهما لبيان إجراءات الإثبات الجنائي في جرائم التوقيع الإلكتروني (**المبحث الأول**)، ثم دراسة التعاون الدولي لمكافحة جرائم التوقيع الإلكتروني (**المبحث الثاني**).

المبحث الأول: إجراءات الإثبات الجنائي في جريمة التوقيع الإلكتروني.

لقد ساهم التطور الكبير في علوم الحاسب الآلي في تجاوز الحدود مما أصبح من الممكن أن ترتكب أفعال النسخ والبحث غير لمشروع في دولة، بينما يكون الجاني موجودا في دولة أخرى، هذا وما ترتب على أن الاختصاص بالنظر في تلك الجرائم، كما يعتبر تحديد القضاء المختص بالنظر في جرائم الاعتداء على التوقيع الإلكتروني من أهم الصعوبات التي أسفر عنها التعامل التقني للحاسب الإلكتروني عن بعد.

هناك جرائم مستحدثة تطلبت نوعا جديدا من الأدلة يسمى بالأدلة الرقمية أو الأدلة الإلكترونية، تتفق وطبيعة الوسط الافتراضي الذي ارتكبت فيه الجريمة، فكان التحدي أمام المشرع الجزائري ليس فقط تحديد هذه الأفعال بدقة، ولكن إيجاد حلول للمشكلات المتعلقة بالدليل الإلكتروني من حيث الوسائل المستعملة في ذلك، وإجراءات الحصول عليه، سواء كان دليل تقليدي أو دليل حديث، ومن هنا سوف نتطرق في هذا المبحث إلى الاختصاص في جرائم التوقيع الإلكتروني في (**المطلب الأول**) ونتناول الإثبات الجنائي في جرائم التوقيع الإلكتروني في (**المطلب الثاني**)

المطلب الأول: الاختصاص في جرائم التوقيع الإلكتروني.

بما أنه لا يوجد اختصاص تشريعي في الجزائر، سوف نتناول الاختصاص القضائي بالنظر في جرائم الاعتداء على التوقيع الالكتروني، فتحديد القضاء المختص بالنظر في جرائم الاعتداء على التوقيع الإلكتروني من أهم الصعوبات الحديثة التي أسفر عنها التعامل التقني للحاسب الالكتروني عن بعد، مما يؤدي إلى صعوبة تحديد المحكمة المختصة، وأن دراسة لسلطة القاضي في قبول الدليل الإلكتروني، وهذا ما سنتناوله في الفرعين التالين:

الفرع الأول: الاختصاص القضائي بالنظر في جرائم الاعتداء على التوقيع الإلكتروني.

ثار خلاف فقهي وقضائي كبير حول تحديد المحكمة الجنائية المختصة في الجرائم بمنظومة التوقيعات الإلكترونية، ولكننا سنتطرق للنصوص القانونية الجزائرية التي استحدثها المشرع الجزائري خاصة بالقواعد الإجرائية قصد مكافحة الجرائم المعلوماتية سواء في قانون الإجراءات الجزائية أم ضمن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.[1]

فنجد المشرع الجزائري نص على ثلاث معايير تحكم الاختصاص المحلي وهي المحكمة التي ارتكبت الجريمة في نطاق إقليمها، أو المحكمة التي يقبض على المتهم في نطاقها أو المحكمة التي يقيم المتهم في دائرتها، فالمشرع الجزائري قام بتوسيع الاختصاص لكل من الضبطية القضائية ثم وكيل الجمهورية وقاضي التحقيق.[2]

أولا: الاختصاص المحلي للضبطية القضائية.

غالبا ما تبدأ الإجراءات الجزائية في الدعوى العمومية بمرحلة البحث والتحري أي مرحلة جمع الاستدلالات التي تتولاها أصلا الضبطية أو الشرطة القضائية، ولقد حدد قانون الإجراءات الجزائية الجزائرية لأحكام الضبط القضائي في المواد 12، 28، 42، 55، 63، 65 وتشمل الضبطية القضائية ضباط الشرطة القضائية وأعوانه وبعض الموظفين المنوطة بهم بعض مهام الشرطة القضائية، وتنفيذ السياسة الإجرائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية خاصة في مجال البحث والتحري[3]، أجازت المادة 7/16 تمديد اختصاصات ضباط الشرطة القضائية في

[1]-القانون رقم 09-04 المؤرخ في 05 أغسطس 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، العدد47.

[2]-د. نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، 2013/2012، ص 231.

[3]-يزيد بوحليط، مرجع سابق، ص 394.

حالة المبحث والمعاينة إلى كافة الإقليم الوطني، ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا، وبعلم وكيل الجمهورية المختص إقليميا بذلك،[1] كما يلتصق بمهام الضبط القضائي إعمال المعاونة والمساعدة حسب نص المادة 20 من قانون الإجراءات الجزائية الجزائري المنوطة بأعوان الضبط القضائي الذين تبينهم المادة 19 من قانون الإجراءات الجزائية الجزائري.[2] ومن ناحية أخرى يمكن لضباط الشرطة القضائية وأعوان الشرطة القضائية في حالة عدم اعتراض وكيل الجمهورية تمديد عمليات المراقبة للأشخاص الذين يوجد ضدهم مبرر يحمل على الانتباه وهذا حسب المادة 16 مكرر من ق.إ.ج.ج والتي نصت على : "يمكن لضباط الشرطة القضائية وتحت سلطة أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمدد وعبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على النتباه فيهم بارتكاب الجرائم المبينة في المادة 16 من نفس القانون[3] . "

ثانيا: الاختصاص المحلي لوكيل الجمهورية.

لقد حددت المادة 37 من ق.إ.ج.ج الاختصاص المحلي لوكيل الجمهورية بصفة واضحة وموضوعية ويعرف الاختصاص المحلي بأنه: "تلك الدائرة القضائية التي يستطيع فيها وكيل الجمهورية مباشرة وظيفته بصفة مباشرة طبقا لقانون الإجراءات الجزائية".[4]

---

[1]–المادة 7/16 من قانون الإجراءات الجزائية الجزائري.

[2]–المادة 19 من ق.إ.ج.ج المعدلة : "يعد من أعوان الضبط القضائي موظفو مصالح الشرطة وذو الرتب في الدرك الوطني ورجال الدرك، ومستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية"، عدلت بالأمر رقم 10/95 المؤرخ في 1995/02/25، الجريدة الرسمية، العدد11،

[3]–هذه الجرائم هي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

[4]–مولاي ملياني بغدادي، الإجراءات الجزائية في التشريع الجزائري، الجزائر، ص139.

فيتحدد الاختصاص المحلي لوكيل الجمهورية حسب المادة 37 من ق.إ.ج.ج بمكان وقوع الجريمة، ومحل إقامة أحد الأشخاص من المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم القبض على هؤلاء الأشخاص [1]، ولكن نظرا لخصوصية جرائم التوقيع الإلكتروني واحتمال ارتكابها في مجموعة من الأماكن واختراقها الحدود الجغرافية أورد المشرع الجزائري استثناءا من هذا المبدأ تماشيا والتطورات الحاصلة في مجال التكنولوجيا وتقنية المعلومات، فبموجب المادة 2/37 من ق.إ.ج.ج أجاز المشرع تمديد الاختصاص المحلي لوكيل الجمهورية ليشمل كافة الإقليم الوطني[2]، وعليه اصدر المشرع الجزائري المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق أين وزعت المواد من 2 إلى 5 منه الاختصاص المحلي لبعض المحاكم، [3] وتجدر الإشارة إلى أن المحاكم التي تم تمديد اختصاصها اصطلح على تسميتها بالأقطاب الجزائية أو محكمة القطب المتخصص.

ومن ناحية أخرى نجد أن المشرع وتحسبا لهذا النوع من الجرائم نص على مجموعة من الإجراءات لتسهيل عملية البحث والتحري عن هذه الجرائم فنصت المادة 144 مكرر2 على توسيعه للاختصاص المحلي للنيابة العامة في مجال الجرائم الإلكترونية وأجبرها أن تباشر إجراءات المتابعة تلقائيا.[4]

[1]-راجع المادة 1/37 من ق.إ.ج.ج.

[2]-تنص المادة 2/37 من ق.إ.ج.ج عرى أنه: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات...الصرف".

[3]-المواد من (2،5) المرسوم التنفيذي المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق رقم 63 المؤرخة في 2006/10/08، ص 30.

[4]-المادتان 144 مكرر و144 مكرر2 من قانون العقوبات الجزائري.

ثالثا: الاختصاص المحلي والنوعي لقاضي التحقيق.

أ-الاختصاص المحلي:

ويقصد بالاختصاص المحلي لقاضي التحقيق هو المجال الذي يباشر فيه قاضي التحقيق عمله وطبقا لنص المادة 40 من ق.إ.ج.ج فإن الاختصاص المحلي يتحدد لقاضي التحقيق وفقا لـ:

- ✓ مكان وقوع الجريمة.
- ✓ أو محل إقامة احد الأشخاص المشتبه في مساهمتهم في اقترافها.
- ✓ أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.[1]

وبموجب الفقرة 2 المادة 40 وسع المشرع الاختصاص المحلي لقاضي التحقيق كلما تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبالتالي يصبح لقاضي التحقيق التابع لهذه المحكمة اختصاص إقليمي يتجاوز اختصاصه العادي ويمكنه التنقل أو انتداب أي ضابط شرطة قضائية للقيام بمهام تتعلق بالتحقيق القضائي في الجرائم الخطيرة الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

بما سبق يتبين أن المشرع الجزائري بموجب التعديل الوارد بالأمر 04-14 وسع الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق إلى محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه ترك تحديد كيفية تطبيق تلك الإجراءات

[1]-المادة 40 من ق.إ.ج.ج.

[2]-المادة 2/40 الجرائم المذكورة سالفا.

للتنظيم، كما يتبين من خلال استقراء نص المادتين 37 و40 من ق.إ.ج.ج أن الاختصاص المحلي لوكي الجمهورية وقاضي التحقيق يعتبر واحدا.[1]

ب–الاختصاص النوعي:

كمل تنص المادة 15 من القانون 09-04 على انه: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".[2]

الاختصاص النوعي للمحاكم بالنظر في جرائم الاعتداء على التوقيع الإلكتروني:

يعتمد هذا المعيار على تقسيم المشرع للجرائم نوعيتا بالنظر إلى جسامتها إلى جنايات، جنح، ومخالفات، ووفقا للمشرع المصري تختص محكمة الجنح الجزائية بالنظر في المخالفات والجنح، ماعدا الجنح التي تقع بواسطة الصحف أو غيرها من طرق النشر على غير الأفراد، وغنه بالرجوع إلى نص المادتين 23 و24 من قانون التوقيع الإلكتروني المصري، قد نص على أن عقوبة جميع جرائم الاعتداء على التوقيع الإلكتروني هي الحبس، أو الغرامة أو إحدى هاتين العقوبتين، ومن ثم تعد هذه الجرائم من قبل الجنح كأصل عام وينعقد الاختصاص ل حكمة الجنح بالنظر لنوعية الجرائم، إلا أنه ولما كان المشرع قد استهل هاتين المادتين بعبارة مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات، أو أي قانون آخر، فإن مؤدى ذلك أنه وكلما كان الاعتداء على التوقيع الإلكتروني يشكل جناية، فإن الاختصاص في هذه الحالة ينعقد لمحكمة الجنايات كما هو الحال لو كان التوقيع الإلكتروني قد توافرت فيه شروط المحرر الرسمي، وتم تزوير، ففي هذه الحالة

[1]– نجاة بن مكي، مرجع سابق، ص 215.

[2]– القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، العدد47، المؤرخة في 16 أوت 2009.

تشكل الواقعة جناية تزوير محرر رسمي أو استعماله فيما زور من اجله، وينعقد الاختصاص بنظرها لمحكمة الجنايات.[1]

الفرع الثاني: سلطة القاضي الجنائي في قبول الدليل الإلكتروني.

يعد قبول الدليل الجنائي الخطوة الإجرائية الأولى التي يمارسها القاضي اتجاه الدليل الجنائي بصفة عامة، والدليل الالكتروني بصفة خاصة، وذلك قبل البدء في تقديره للدليل للتأكد من صلاحيته وملاءمته لتحقيق ما قدم من أجله ويهدف القاضي الجنائي في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الإلكتروني لقاعدة المشروعية، والتي لا يمكن بدونها أن يترتب على الدليل أي آثار قانونية، بل يثير إهمالها أو مخالفة ما يستلزمه من شروط وآثار قانونية إلى بطلانه أمام القضاء.

أولا: أساس قبول الدليل الإلكتروني في الإثبات الجنائي.

إن موقف القوانين فيما يتعلق بسلطة القاضي الجنائي في قبول الدليل الإلكتروني بالنسبة لجرائم التوقيع الإلكتروني يخضع لنظام الإثبات السائد في الدولة، وتنقسم هذه الدولة إلى ثلاث فئات:

1-وهي القوانين اللاتينية والتي تبنت مبدأ حرية الإثبات ومنها سلطة القاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستعيد المشرع بعضها صراحة.[2]

2-وهي القوانين الأنجلوساكسونية حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، وغما في مرحلة تحديد العقوبة، فيسود مبدأ حرية الإثبات.[3]

---

[1]-أيمن رمضان محمد أحمد، مرجع سابق، ص 386.

[2]-أحمد عصام عجيلة، مرجع سابق، ص 480.

[3]-أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، ط2، 2006، ص 14.

3-تأخذ بنظام الأدلة القانونية، بحيث تحدد الأدلة التي يجوز للقاضي الجنائي قبوله كقانون الهولندي 339ق.إ الجنائية والقانون الألماني الذي يحدد على سبيل الحصر وسائل الإثبات الذي يتعين على القاضي قبولها.[1]

1-مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني:

تتبنى الدول التي تتأثر قوانينها بالصياغة اللاتينية في مجال الإثبات الجنائي مبدأ حرية الإثبات ومنها سلطة القاضي في قبول جميع الأدلة، حيث يمثل هذا المبدأ لنظام الإثبات الحر، [2] ويطلق عليه أيضا مبدأ اقتناع القاضي أي حرية جميع الأطراف في اللجوء إلى كافة وسائل الإثبات للدليل على صحة ما يدعونه، فلسفة الاتهام أن تلجأ إلى أية وسيلة لإثبات وقوع الجريمة على المتهم أو يدفع المتهم كذلك بكل الوسائل، ويستظهر القاضي الحقيقة بكل ذلك أو بغيره من طرق الإثبات.[3]

فقد أقر قانون الإجراءات الفرنسي مبدأ حرية الإثبات الجنائي صراحة بمقتضى المادة 427 بحيث يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخص.

-كما أقر المشرع المصري هذا المبدأ بموجب المادة 1/302 من قانون الإجراءات الجنائية.[4]

ونجد المشرع الجزائري كذلك أقر بمبدأ الإثبات الجنائي في المادة 212 من ق.إ.ج.ج التي تنص على: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي نص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا للاقتناع الشخصي".

[1]-سعيد السيد قنديل، مرجع سابق، ص 194.

[2]-المرجع نفسه، ص 194.

[3]-أحمد عصام عجيلة، مرجع سابق، ص 486.

[4]-المادة 1/302 ق.إ.ج المصري: "يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته".

وتكمن الأسباب الداعية لضرورة إعمال مبدأ حرية الإثبات في نطاق نظرية الإثبات الجنائي فيما يلي:

-حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه والتي تتيح في نفس الوقت السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها لتمكين القاضي من أداء رسالته في إرساء العدالة بين المتقاضين.

-إن الإثبات في الدعوى الجنائية يرد على وقائع قانونية، مادية أو نفسية يصعب بل يستحيل الحصول على دليل مسبق لها.

-الإثبات في الدعوى الجنائية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك للمحكمة أن تستدعي بكل الوسائل الممكنة كي يعتد لها رواية ما حدث.

-من المسلم به أن قرينة الإثبات تلقي عبء الإثبات كلية على عاتق سلطة الاتهام، مما جعلت مهمة هذه الأخيرة جد صعبة.[1]

-إن طبيعة المصلحة التي تحميها الدعوى الجنائية تختلف عن تلك التي تحميها الدعوى المدنية.

-مبدأ حرية الإثبات يعد إثبات إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي لو تم استخدامها كأدلة إثبات على مواجهة الجرائم المستحدثة ومنها الجريمة الإلكترونية.

2-النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي:

يؤدي القاضي الجنائي دورا إيجابيا هاما وبصفة خاصة في الإثبات يكمن في عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة بل واجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة العقلية فيها.[2]

[1]-سعيد السيد قنديل، مرجع سابق، ص 198.

[2]-محمد محمود مصطفى، مرجع سابق، ص 419.

ويختلف دور القاضي الجنائي بالنسبة للدليل الإلكتروني بحسب النظام الإجرائي السائد في الدولة، ففي النظام الاتهامي يكون لدور القاضي سلبيات، لان هذا النظام ينظر إلى الدعوى الجنائية من قبل طرفيها نظرة متساوية، أما في النظام التقني فيكون دور القاضي إيجابيا في تحقيق الدعوى الجنائية [1]، والقاضي هنا ليس قاضي حكم فحسب وإنما يشمل أيضا قضاء للتحقيق باعتبار أن مشكلة الإثبات قد تثور في أي مرحلة كانت عليها الدعوى الجنائية، بل يمكن أن تثور قبل ذلك، أي في مرحلة جمع الاستدلالات أيضا.

ثانيا: ضوابط الدليل الإلكتروني وأثره على اقتناع القاضي.

إن القاضي الجنائي وغن تمتع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الإلكتروني حيث ترك له المشرع سلطة واسعة فله أن يتحرى الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة لدليل ما حتى ولو كان دليلا علميا كالدليل الإلكتروني.[2]

أ-الضوابط المتعلقة بمصدر الاقتناع:

ففي هذا الشأن يحكم اقتناع القاضي بالأدلة الإلكترونية شروط قبو الدليل الإلكتروني، فالقاضي ليس حر في تقدير أي دليل كان، بل هو حر في تقدير الدليل الإلكتروني المقبول في الدعوى، أي تم الحصول عليه بطريقة مشروعة إعمالا بمبدأ الشرعية الإجرائية، وبالتالي يستبعد في مقابل ذلك سائر الأدلة الإلكترونية غير المقبولة لأنها لا تدخل ضمن عناصر تقديره، [3] وعليه لا يجوز للقاضي الاستناد إلى دليل استمد من إجراءات باطلة، لان ما بني على باطل فهو باطل.

---

[1]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص 191.

[2]- يزيد بوحليط، مرجع سابق، ص 414.

[3]-محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع، مجلة القانون والاقتصاد، العدد 51، 1991، ص 139.

فالقواعد الأساسية في الإجراءات الجنائية انه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أورق الدعوى، وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته، ويقوم هذا الشرط على مبدأ الشفوية والمواجهة في المحاكمة الجنائية،[1] وهو من المبادئ الأساسية في الإجراءات الجنائية نص عليه المشرع الجزائري بموجب نص المادة 212/ف2 من ق.إ.ج.ج،[2] إذ ينبغي على القاضي أن يطرح كل دليل مقدم في دعوى المناقشة أمام الخصوم في الجلسة حتى يكونوا على بينة مما يقدم ضدهم من أدلة.

ويتطلب مبدأ المواجهة نوعين من الضمانات منها مبدأ مواجهة المتهم بالتهمة المنسوبة إليه وان يمنح له الوقت الكافي لتحضير دفاعه وكذا الاستفادة عند الاقتضاء بمترجم، أما النوع الآخر من الضمانات يتمثل في السماح لكل طرف بتقديم ما لديه من مستندات وسؤال الشهود إثارة أي دفوع، إيداع مذكرات.

كما يشمل على عنصر آخر أكثر أهمية يتمثل في ضرورة أن يكون للدليل الإلكتروني أصل في أوراق الدعوى، ومن أجل ذلك اوجب المشرع تحضير محضر الجلية لإثبات وقائع الدعوى الجنائية وأدلتها لكي يتمكن قاضي الموضوع أو أي من الخصوم من الرجوع إلى هذا المحضر، وذلك منعا للتحكم وتحقيق العدالة، إضافة إلى ذلك فإن هذا التدوين يمكن للمحكمة المطعون أمامها من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب.[3]

[1]-يزيد بوحليط، مرجع سابق، ص 415.

[2]-نص المادة 212/ف2 من قانون الإجراءات الجزائية الجزائري: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا".

[3]-محمود نجيب حسني، مرجع سابق، ص 210.

ب–الضوابط المتعلقة بالاقتناع ذاته:

إن مبدأ الإثبات الجنائي يتيح للقاضي حرية كبيرة في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية وعليه فغن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية إلى مرتكبها أمر متروك ل حكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة محكمة النقض التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة الحكم،[1] فمن هنا سوف نتعرض للقيود التي تحكم الاقتناع ذاته إلى:

***بلوغ الاقتناع القضائي درجة اليقين:**

وهذا يستوجب أن يقترب اقتناع القاضي بدرجة اليقين قدر المستطاع، وأن يتجلى القانون والتخمينات ويمكن أن يصل إلى اليقين عن طريق المعرفة الحسية التي تدركها الحواس من خلال المعاينة، وهي الأدلة والاستقراءات والاستنتاجات التي توصل إلى الحقيقة التي يهدف إليها، وتجنب أن يصدر حكمه استنادا إلى معايير غير منطقية.[2]

***توافق الاقتناع القضائي مع مقتضيات العقل والمنطق:**

أن يكون استخلاص محكمة الموضوع لوقائع الاستخلاص معقولا صائغا لمعيار معقولية الاقتناع بما في ذلك الأدلة الرقمية، أي أن تكون هذه الأدلة مؤدية إلى ما رتبه الحكم عليها من غير تعسف في الاستنتاج ولا تتعارض مع مقتضيات العقل والمنطق.[3]

***مناقشة الأدلة الإلكترونية:**

إذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم ويترتب على ذلك بأن هذه المخرجات سواء

[1]–عائشة بن قارة مصطفى، مرجع سابق، ص 276.

[2]–يوسف بن سعيد الكلباني، مرجع سابق، ص 426.

[3]–يزيد بوحليط، مرجع سابق، ص 416.

كانت مطبوعة انم بيانات معروضة كانت، أم بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية تكون محلا للمناقشة عند الاعتماد عليها كأداة أمام المحكمة،[1] وتأسيسا على ذلك لا يمكن للقاضي أن يؤسس اقتناعه الأدنى على عناصر الإثبات التي صرحت في جلسات المحاكمة، وخضعت لحرية مناقشة أطراف الدعوى [2]

ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استنادا إلى علم شخصي له، أو استنادا إلى رأي الغير، إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه، فقرر الاستناد إليه ضمن باقي القائمة في أوراق الدعوى المعروضة عليه.بحيث ان الاقتناع الذي يكون قد اصدر حكمه بناءا عليه متولد من عقيدته وهو ليس من تقرير الخبير.[3]

المطلب الثاني: الإثبات الجنائي في جرائم التوقيع الإلكتروني.

ظهرت جرائم مستحدثة سببها سواء استخدام شبكة الانترنت تطلبت نوعا جديدا من الأدلة يسمى بالأدلة الرقمية أو الأدلة الإلكترونية تتفق وطبيعة الوسط الافتراضي الذي ارتكبت فيه الجريمة، فكان التحدي أمام المشرع الجزائري والمشرع المقارن ليس فقط تحديد هذه الأفعال بدقة، ولكن إيجاد حلول للمشكلات المتعلقة بالدليل الإلكتروني من حيث الوسائل المستعملة على ذلك وإجراءات الحصول عليه سواء أكانت دليل تقليدي أو دليل حديث، وهذا ما سنتناوله.

الفرع الأول: الإجراءات التقليدية لجمع الدليل على جرائم الاعتداء على التوقيعات الإلكترونية.

يتطلب الكشف عن جرائم الاعتداء على التوقيع الإلكتروني اتباع استراتيجيات خاصة تتعلق باكتساب القائمين بجمع الدليل مهارات تقنية على نحو يساعدهم على مواجهة تطورات

[1]-هلالي عبد الله أحمد، المرجع السابق، ص 104.

[2]-محمد فهمي طلبه، المرجع السابق، ص 21.

[3]-يوسف بن سعيد الكلباني، المرجع السابق، ص 426

تقنية الحاسب الآلي وشبكاته، بحيث تتعقد وتتنوع التقنيات المرتبطة بارتكاب تلك الجرائم، حيث تتعدد أدلة الإثبات الجنائي التقليدي على جرائم الاعتداء على التوقيع الإلكتروني كتلقي التبليغات والشكاوى.

أولا: تلقي التبليغات.

1-تلقي التبليغات والشكاوى على جرائم الاعتداء على التوقيع الإلكتروني:

أدى التطور التقني الهائل في مجال تكنولوجيا الإعلام ولاتصال إلى إساءة استخدام هذا الفضاء الافتراضي، مما تنتج عنه أنماط جديدة للإجرام سواء من حيث الأساليب المستعملة أو نوعية الحياة أو أصناف المجني عليهم وهو ما دفع بالمجلس الأوروبي إلى اتخاذ جملة من التدابير الإجرائية،[1] على مجال مكافحة جرائم الاعتداء على التوقيع الإلكتروني مثل استقبال الشكاوى والتبليغات عبر الانترنت، ويقصد بها مجموعة الإجراءات والمراحل التي تتم في دائرة البلاغات والشكاوى وتمر خلالها البلاغات والشكاوى بداية من استقبالها مرورا بدراستها والتحري حولها والتصرف فيها وفقا للتشريعات النافذة للتأكد من صحتها وتباشر الهيئات متلقية البلاغات والشكاوى من تلقاء نفسها التحري والتحقيق في جرائم الاعتداء على منظومة التوقيع الإلكتروني وتحليل مرافقاتها وإعطاء التوظيف القانوني لما تتلقاه من بلاغات وشكاوى وإعداد السجلات والاستمارات المنظمة لعملية تلقي البلاغات والشكاوى، متضمنة البيانات لكل منها شاملا مرفقاتها.[2]

إضافة إلى ذلك إعداد نظام توثيق إلكتروني لكافة البلاغات والشكاوى الواردة إلى البيئة، وإعداد تقارير دورية عن البلاغات والشكاوى التي تلقتها الإدارة متبوعة بنتائج دراستها ومقترحات

[1]-Christiane féralschuhl , cyber droit, le droit à l'épreuve de l'internet, édition dalloz, 2009, P358.

[2]-فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر،2016، ص 160.

التعامل معها وانتهاء الإجراءات التي تمت بشأنها، وفي هذا الإطار.[1]

2-الجهة المختصة بتلقي الشكاوى والتبليغات:

يكون من اختصاصات الضبط القضائي طبقا لقانون الإجراءات الجنائية تلقي البلاغات والشكاوى،[2] التي تبلغ إليهم أو التي يعينون بها بأية كيفية، فقد يتم كتابيا أو شفويا ويصطلح على البلاغ في هاتين الحالتين 'بالبلاغ المادي' وقد يقدم بواسطة البريد أو البرقية أو التليفون أو الصحف، وهذا ما يصطلح عليه 'بالبلاغ المعنوي' أو قد يقدم عن طريق الانترنت وهذا ما يسمى 'بالبلاغ الرقمي' وعلى ضباط الشرطة القضائية أن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.

أما المشرع الجزائري وفي هذا الشأن نصت المادة 17 من قانون الإجراءات الجزائية الجزائري على أنه: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و 13 ويتلقون الشكاوى والتبليغات ويقومون بجميع الاستدلالات وإجراء التحقيقات الابتدائية، وعليه نجد أن المشرع الجزائري لم يحدد طريقة تقديم الشكاوى من طرف الأشخاص المتضررين من الجريمة فقد تكون شفاهة، كما قد تكون مكتوبة وسواء كانت هذه الشكوى مقدمة على المضرور نفسه أو من محاميه"[3].

[1]-حسام محمد نبيل الشراقي، جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013، ص 337.

[2]-راجع في ذلك نص المادة 24 من قانون الإجراءات الجنائية المصري، والمادة 29 من ذات القانون، فنصت المادة 24 على مايلي: "يجب على مأمور على الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشان الجرائم وثم يبعثوا بها فورا إلى النيابة العامة، ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلنون بها بأية كيفية وعليهم أن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة ."

[3]-يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص 58.

أما البلاغات فتعني ما يرد إلى ضباط الشرطة القضائية من إخبار عن الجريمة سواء كانت شفاهة أو كتابة، بمعنى نقل العلم بوقوع حادث أو جريمة إلى السلطة المختصة بناء على أسباب معقولة.[1]

كما نصت المادة 18 من ق.إ.ج.ج على أنه: "يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم".[2]

ولقد رأينا سلفا أن المشرؤع الجزائري لم يشترط وسيلة محددة من تلقي الشكاوى والتبليغات، فقد تكون كتابة أو شفاهة بدليل تضمن، نصت المادة 17 من قانون الإجراءات الجزائية لفظ ويتلقون الشكاوى والبلاغات وهو لفظ عام لم يحدد وسيلة بحد ذاتها مما يفتح المجال أمام القيام بهذا الإجراء بأعلى وسيلة كانت ومنها استعمال تقنية الاتصال متمثلة في شبكة الانترنت والهاتف الخلوي.

وفي مجال مكافحة الجريمة عموما والجرائم الإلكترونية خصوصا، قامت قيادة الدرك الوطني باستثناء إطلاق خدمة عمومية جديدة عبر 48 ولاية باستعمال تكنولوجيا الإعلام والاتصال تحت اسم 'الشكوى المسبقة والاستعلام عن بعد'.

حيث تدخل هذه الخدمة في إطار وسائل تنفيذ مهام وإحداث الدرك الوطني والتكفل الجيد بشكاوى المواطنين، حيث يمكن هذا التنظيف المنجز من طرف مهندسي الإعلام الآلي للدرك الوطني المواطنين من إيداع البلاغات والشكاوى المسبقة عن طريق الانترنت وتأكيد لذلك تقوم وحدة الدرك الوطني في غضون 30 يوما مما يمكن أجهزة الضبطية القضائية من ربح الوقت والسرعة في البدء في إجراءات البحث والتحري عن الجرائم الإلكترونية.

[1]– يزيد بوحليط، المرجع السابق، ص 59.

[2]–المادة 18 من قانون الإجراءات الجزائية الجزائري، المحدد بالأمر 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم.

3-آلية تلقي التبليغات والشكاوى:

ويتضح من المهام السابقة أن آلية تلقي البلاغات والشكاوى تتكون من المراحل التالية:

-مرحلة الاستقبال والتوثيق بمحضر التحري.

-مرحلة جمع المعلومات والأدلة.

-إحالة البلاغات والشكاوى إلى ولالات تطبيق القانون أو فرق العمل الخاصة المحلية أو الدولية.

وينبغي التنويه أن لا تشمل الإجراءات تجاه البلاغات والشكاوى، فهذه الإجراءات متنوعة بحسب نوع الشكوى أو البلاغ، كما أنها متعددة منها جمع المعلومات وإجراء التحريات ومنها التحقيق ومتابعة الإجراءات والجهات القضائية بعد انتهائها من التحقيق فيها، كما أن جرائم الاعتداء على التوقيع الإلكتروني ليست بمقدور أي شخص الإبلاغ عنها ما لم تتوافر لديه القدرة على التعامل مع الجهاز الآلي أو نظم تقنية المعلومات.[1]

فالبلاغ عن جرائم الانترنت قد يكون جواز على أي شخص علم بوقوع الجريمة أن يبلغ أولا مأموري الضبط القضائي سواء كان له مصلحة في ذلك أو لا، بعكس الشكوى التي يجب أن تصدر من المتضرر أو من وكيله، خاصة وان هناك جهات تحجم من الإعلان والبلاغ عن هذه الجرائم خاصة البنوك والمؤسسات المالية خوفا من تزعزع ثقة العملاء بها أو قد يكون واجبا، وهذا ما أقرته لجنة خبراء مجلس أوروبا الإلزام بإبلاغ جهة خاصة، والإلزام بإبلاغ سلطات إشرافية، وتشكيل جهاز خاص لتبادل المعلومات وكذا إصدار شهادة امن خاصة.[2]

4-العناصر الأساسية للتحقيق في جرائم الاعتداء على التوقيع الإلكتروني:

يجب أن تتوافر في البلاغ والشكوى العناصر الأساسية اللازمة للتحقيق في الجريمة، كما يجب على المحقق أن يستظهر هو مايلي:

[1]- فهد عبد الله العبيد الحازمي، المرجع السابق، ص 162.

[2]- المرجع نفسه، ص 127.

-أظهار الركن المادي: النشاط أو السلوك المادي في جرائم منظومة التوقيعات الإلكترونية ومعرفة هذا النشاط والشروع فيه ونتيجته.

-إظهار الركن المعنوي: إظهار الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.

-تحديد وقت ومكان ارتكاب الجريمة: تتميز مسألة النتيجة الإجرامية في الجرائم الإلكترونية مشاكل متعددة بخصوص مكان وزمان تحقق النتيجة الإجرامية وتثير أيضا إشكاليات القانون الواجب التطبيق لوجود عدة دول في هذا المجال، ذلك أن جرائم التوقيع الإلكتروني من الجرائم العابرة للحدود.[1]

يجب على المحقق الجنائي أثناء القيام بالتحقيق مراعاة مايلي:

*/توفير معلومات مسبقة عن مكان وقوع الجريمة، ومن المالك لهذا المكان، ونوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها وتحديد إمكانية التعامل معها فنيا.

*/الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.[2]

ب-البيئة التي يتم من خلالها إجراء التبليغات والشكاوى في جرائم الاعتداء على التوقيع الإلكتروني:

نظرا للطبيعة الخاصة لجرائم الاعتداء على التوقيع الإلكتروني يمكن القول بأنه: "لتلقي الشكاوى والبلاغات عبر شبكة الانترنت أهمية بالغة في مجال مكافحة الجرائم على المستوى الإجرائي، إذ يوفر ضباط الشرطة القضائية السرعة اللازمة على مباشرة إجراءات البحث والتحري

[1]-خالد ممدوح إبراهيم، المرجع السابق، ص 218.

[2]-فهد عبد الله العبيد الحازمي، المرجع سابق، ص 166.

بما يمكنهم من الكشف المبكر عن الجريمة ومرتكبيها، وخاصة أن هناك إحجاما من طرف المتضررين في التبليغ عن هذه الجرائم لأسباب عديدة قد تكون شخصية أو اقتصادية...إلخ".[1]

ونظرا لما للبلاغ من أهمية في البحث الجنائي، سارعت الدول إلى تطوير هذه الآلية تماشيا ومقتضيات العصر المتطورة وذلك من خلال استحداث أجهزة وهي كالآتي:

1-أجهزة تلقي التبليغات والشكاوى:

تتلقى الشكاوى والبلاغات بواسطة شبكة الانترنت واتخاذ الإجراءات اللازمة للكشف عن الجريمة وملاحقة مرتكبيها، ومن هذه المواقع نجد وزارة العدل الأمريكية usdoj-go وموقع المباحث الفيدرالي Fbi gov وموقع منظمة الانتربول interpol.int والمجلس الأوروبي col.gov وأيضا موقع البلاغات للمخابرات المركزية الأمريكية cia وكذلك منظمة الانترنت الأمنية IFCC.[2]

وفي فرنسا يتم الإبلاغ عن الجرائم الإلكترونية عبر الموقع الإلكتروني لجهاز الشرطة الفرنسي judiciaire gendarmerie défense باعتباره الجهة المختصة بالتحقيق والتحري عن تلك الجرائم وموقع جمعية مزود الدخول وخدمات الانترنت http//www.pointide .contact.net AFA

وفي مصر يتم الإبلاغ عن الجرائم الإلكترونية عبر المواقع الإلكترونية عبر شبكة الانترنت www.moiegypt.gov-eg وموقع http://www.ccd.gov-eg.

[1]- يزيد بوحليط، المرجع السابق، ص 316.

[2]-IFCC :والذي أسسه مكتب التحقيقات الفيدرالي (FBI) والمركز الوطني لجرائم الياقات البيضاء (NW3c) في فرجينيا الغربية بالولايات المتحدة الأمريكية من اجل مكافحة ظاهرة الاحتيال عبر الانترنت.

ثانيا: التفتيش وضوابطه في جرائم الاعتداء على التوقيع الإلكتروني.

إن التفتيش غرضه ضبط الأدلة المادية للكشف عن الجريمة ومرتكبها، فكل ما يضبط بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فيعرف التفتيش بأنه: "ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، الغرض منه البحث عن الأدلة المتعلقة بالجريمة للوصول إلى الحقيقة في متابعة أي شخص يشتبه في انه ارتكب الجريمة ويكون على المكونات المادية بأشكالها أي شيء يتصل بجريمة معلوماتية يمكن الكشف عنها وعن مرتكبيها".

يدخل في نطاق التفتيش التقليدي وفقا لقانون الإجراءات الجزائية الجزائري والمعمول بها إلا أن هناك حالات خاصة للتفتيش في هذه المكونات والمتمثلة في:

- ✓ إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته تأخذ نفس الأحكام المقررة لتفتيش السكن بنفس الضمانات المقررة قانونا.
- ✓ إذا كانت مكونات الكمبيوتر منعزلة عن غيرها من أجهزته كمسكن غير مسكن المتهم [1]، بحيث إذا كانت هناك بيانات مخزنة في نظام آخر، فإن عملية الكشف تصبح صعبة وربما مستحيلة، لذلك تتم عملية التفتيش مراعاة للقيود والضمانات التي أوجبها المشرع الجزائري على التفتيش داخل النظم المعلوماتية والتي تضمنها قانون الإجراءات الجزائية.

1-القواعد الإجرائية للتفتيش:

بما أن التفتيش هو إجراء من إجراءات التحقيق يهدف إلى ضبط أدلة الجريمة موضع التحقيق وكل ما يفيد في الكشف عن الحقيقة، وذلك وفقا لقواعد إجرائية تتلخص فيمايلي:

[1]-عبد القادر عدو، الجريمة الإلكترونية إجرائيا، دار هومة، الجزائر، ط2، 2016، ص 80.

أ-إجراء الإذن:

لم يشترط المشرع الجزائري كقاعدة عامة الإذن في تفتيش المنظومة المعلوماتية، لكن طبق عليها القواعد التقليدية في حالة ما إذا تعلق بالانتقال إلى منزل المشتبه فيه من أجل تفتيش منظومة معلوماتية، فتطبق في هذه الحالة القواعد الخاصة بتفتيش المنازل والأماكن الخاصة، إذ ألزم المشرع إذن مكتوب صادر عن وكيل الجمهورية المختص من أجل القيام بإجراء التفتيش وإلا اعتبر التفتيش تعسفا،[1] ويمكن التفرقة بين حالتين:

1-الانتقال لتفتيش منظومة معلوماتية في الأماكن الخاصة ويطبق على إجراء تفتيش الأماكن الخاصة كالمنازل بإذن مكتوب.

2-الانتقال إلى التفتيش في مكان عام كمقهى أو ساحة عامة تطبق عليه نفس القواعد التي تطبق على تفتيش الأماكن العامة لا وجود للإذن.

ولقد نص المشرع الجزائري على الإذن في الدخول إلى الأماكن الخاصة في نص المادة 44 من ق.إ.ج.ج، إذ يتطلب إذن مكتوب من طرف وكيل الجمهورية أو قاضي التحقيق يستظهر عند دخوله المنزل، كما يتضمن الإذن وصف للجريمة موضوع البحث عن الدليل وحضور الشخص المعني، وعليه يجب الانتقال إلى مكان تواجد جهاز الحاسوب ومكوناته وملحقاته وحجزها.[2]

ب-إجراء التفتيش بحضور أشخاص معينين قانونا:

ومن بين هؤلاء الأشخاص المشتبه فيه، المتهم، القائم بالتفتيش وشاهدين، فالأصل في التفتيش وكما عرفته القواعد الخاصة يتم بحضور المتهم أو من يجوز أن يمثله، وضابط الشرطة القضائية القائم بالتفتيش، وإذا تعذر حضور المتهم أو من يجوز أن يمثله، يتم التفتيش بحضور

[1]-عبد القادر عدو، الجريمة الإلكترونية إجرائيا، المرجع السابق، ص 86.

[2]-المادة 44 من ق.إ.ج.ج.

شاهدين من غير الموظفين الخاضعين للسلطة، إلا أن المشرع الجزائري استثنى هذه القواعد في نص المادة 45 من ق.إ.ج.ج على أنه لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إذ يمكن تفتيش المنظومة المعلوماتية بدون حضور المتهم أو الشاهدين.[1]

ج–مواعيد التفتيش:

كقاعدة عامة بخصوص الجرائم التقليدية، فإن تفتيش الأماكن الخاصة، لا يكون قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، والعبرة بساعة دخول إلى المنزل إلا إذا طلب صاحب المنزل ذلك، غير أن تفتيش المنظومة المعلوماتية لا يخضع لهذه القواعد، إذ نص المشرع على أنه لا يجوز إجراء التفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في كل ساعة من ساعات النهار والليل، بناء على إذن مسبق من وكيل الجمهورية المختص، وهذا ما نصت عليه المادة 47/ف3 من ق.إ.ج.ج. كونها حالة من الحالات الاستثنائية التي أقرها القانون.[2]

كما أن المكونات المعنوية للحاسوب الآلي وشبكة الاتصال قد تكون عرضة للإخفاء أو التغيير أو التدمير أو التلاعب بالبيانات المخزنة، والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عم التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كاستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة.[3]

---

[1]–ناصر جوادي، إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، دار العلوم، الجزائر، ط3، 2011، ص 47.

[2]–ناصر جوادي،إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 48، أنظر المادة 47/ف3 من ق.إ.ج.ج..

[3]–معمش زهية، غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق، جامعة عبد الرحمن ميرة، بجاية، 2012/2011، ص 25.

د–رضا المشتبه فيه بالتفتيش:

لا يجوز تفتيش المساكن أو حجز الأشياء المثبتة للمتهم إلا برضا صريح من الشخص الذي ينفذ هذه الإجراءات، ويجب أن يكون الرضا مكتوب بخط يده أو استعان به أو اختاره في حالة عدم قدرته على الكتابة شريطة اختياره بنفسه لهذا الشخص ويذكر ذلك في المحضر، وعندما يتعلق الأمر بالتحقيق في جريمة ماسة بالأنظمة المعلوماتية فتطبق الأحكام المنصوص عليها في نص المادة 47 مكرر من ق.إ.ج.ج.

وحسب المادة 45 من ق.إ.ج.ج. فتتم عملية التفتيش التي تجري طبقا للمادة 44 أعلاه على الوجه الآتي:

*/إذا وقع التفتيش في مسكن شخص يشتبه في انه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.[1]

*/إذا وقع التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا وأشياء لها علاقة بالأفعال الإجرامية، فغنه يتعين حضوره وقت إجراء التفتيش وإن تعذر ذلك اتبع الإجراء المنصوص في الفقرة السابقة.

ولضابط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى أعله الحق في الإطلاع على الأوراق أو المستندات قبل حجزها.

[1]–راجع المادة 47 مكرر والمادتان 44، 45 من ق.إ.ج.ج.

و–تحرير محاضر التفتيش:

المحاضر هي عبارة عن ملخص وافي وبسيط عن الواقعة يتضمن إثبات جميع ما قام به المحقق من إجراءات قانونية وفنية من أجل كشف الغموض عن الواقعة وضبط الأدلة.[1]

ويكون بتكليف القائم بالتفتيش باصطحاب كاتب من أعوان الضبط القضائي يحرر محضر خاص بالتفتيش سواء كان ايجابيا أو سلبيا، ويتم تسجيل جميع وقائع التحقيق والتفاصيل وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل دقة وأمانة.[2]

وأوجب القانون على المحقق أن يوقع على المحاضر وكذلك بالنسبة للكاتب، ويجب أن يتم التوقيع على كل صفحة من صفحات المحاضر في النهاية، وذلك لإبعاد أية شبهة كالتزوير، أما بالنسبة للكاتب يكفي توقيعه مع المحقق في نهاية محضر التحقيق، لأن الثقافة القائمة بالمحضر مستمدة من توقيع النيابة العامة.[3]

2–اتصال حاسب المتهم بحاسب موجود على مكان آخر خارج الدولة:

من الشبكات التي تواجه سلطات التحقيق على جميع الأدلة قيام بعض مرتكبي الجرائم بتخزين بياناتهم على نظم المعلومات خارج الدولة عن طريق شبكة الاتصالات البعدية وذلك لعرقلة التحقيقات.[4]

وعلى هذا الإطار صدر عن المجلس الأوروبي توصيات تجيز أن يمتد تفتيش الحاسوب إلى شبكة المتصل بها، ولو كانت تلك الشبكات تقع خارج إقليم الدولة، فتنص التوصية رقم 13

[1]–ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في القانون الجنائي الأعمال، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، 2015/2014، ص 16.

[2]–غرداين حسام، الجريمة الإلكترونية وإجراءات التصدي لها، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، جامعة الجزائر، 2015/2014، ص 87.

[3]–ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، المرجع السابق، ص 47.

[4]–هلالي عبد الله احمد، مرجع سابق، ص 78.

لسنة 1990 المتعلقة بالمشكلات القانونية لـ ق.إ.ج المتصلة بتقنية المعلومات على انه "لسلطة التفتيش عند التنفيذ تفتيش المعلومات وفقا لضوابط معينة تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دمت انه من الضروري على التدخل الفوري على القيام بذلك".[1]

وعلى المسار نفسه وبعد ما نص المشرع الجزائري على تمديد التفتيش داخل الإقليم الوطني اتجه إلى تمديد تفتيش المنظومة المعلوماتية خارج الإقليم الوطني من خلال نص المادة 5/05 من القانون رقم 09-04 التي تنص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار ق.إ.ج وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو بعد...إلى...إذ تبين مسبقا بأن المعطيات المبحوث عنها ولا يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل".[2]

د-ضوابط تفتيش الحاسب الآلي على جرائم التوقيع الإلكتروني:

تضمنت التشريعات الإجرائية ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية كالتفتيش وتنقسم الشروط العامة للتفتيش إلى نوعين من الشروط:

أ-الشروط الموضوعية للتفتيش:

يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة وهي كالآتي:

[1]-سعيد السيد قنديل، المرجع السابق، ص 147.

[2]-يزيد بوحيط، المرجع السابق، ص 484.

1-سبب التفتيش في البيئة الإلكترونية:

يتمثل هذا الشرط في وجود جريمة على التوقيعات الإلكترونية والتي تتمثل في كل فعل مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة تمس التوقيعات الإلكترونية وكذا تورط شخص أو عدة أشخاص في ارتكاب جرائم التوقيع الإلكتروني أو الاشتراك، وكذا توفر دلائل قوية أو قرائن تفيد في الكشف عن المجرم المعلوماتي.[1]

وفي مجال وقوع جريمة من جرائم التوقيع الإلكتروني سواء كانت جناية أو جنحة، نجد أن المشرع الجزائري أدرج فصلا خاصا الفصل السابع والخاص بالجرائم والسادس بأنظمة المعالجة الآلية للمعطيات كما مد حماية جنائية للتوقيع الإلكتروني من خلال قانون التنظيم الإلكتروني رقم 15 سنة 2004 من خلال المادة 23 من ذات القانون، أما باقي صور الإجرام الإلكتروني لم يتعرضلها مما يتطلب تدخلا تشريعيا لسد هذا الفراغ ومواجهة هذه الصور المستحدثة للإجرام الإلكتروني.

أما في مجال اتهام شخص أو أشخاص معنيين بارتكاب الجريمة والمشاركة فيها فينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو للاعتقاد بأنه ق ساهم في ارتكاب الجريمة سواء بوصفه فاعلا أو شريكا فيها. [2]

3-محل التفتيش:

محل التفتيش في الجريمة الإلكترونية هو الحاسب الآلي ونظم معلوماته ومكوناته سواء المادية أو المعنوية، بالإضافة للأشخاص الذين يستخدمونه وقد سبق وأن أشرنا إلى مكونات الحاسب الآلي المادية والمعنوية.

[1]-حسام نبيل الشنراقي، المرجع السابق، ص 465.

[2]-فهد عبد الله العبيد العازمي، المرجع السابق، ص 262.

4-السلطة المختصة بالتفتيش:

بما أن التفتيش إجراء من إجراءات التحقيق الابتدائي ومن أخطر الإجراءات التي تمس بحقوق وحريات الأشخاص، عمدت معظم التشريعات بالاستناد إلى جهة خاصة لكي يتم وفق إجراءات محددة قانونا.

أما بخصوص المشرع الجزائري فنجده حدد بوضوح الجهة المختصة سواء في مجال الإذن بوضع ترتيبات المراقبة الإلكترونية أو في مجال الدخول بغرض تفتيش منظومة المعلوماتية أو جزء منها، فنجد نص المادة 1/4 من القانون 09-04 السالف الذكر: "إذ يختص النائب العام لدى مجلس قضاء الجزائر يمنح ضباط الشرطة القضائية المتبنى للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته المنصوص عليها بموجب المادة 13 من نفس القانون إذن بتفتيش لمدة 6 أشهر قابلة للتجديد التي تسمح باللجوء إلى المراقبة الإلكترونية".[1]

فيما عدا هذه الحالة الخاصة وبموجب نص المادة 05 من القانون 09-04: "يجوز للسلطات القضائية المختصة وكذا الشرطة القضائية...الدخول بغرض التفتيش"، إذ يتعين الرجوع إلى المادة 37 من ق.إ.ج.ج سواء بالنسبة لوكيل الجمهورية أو قاضي التحقيق بموجب المادة 40 اللتان تنصان على تحديد الاختصاص لكل من وكيل الجمهورية أو قاضي التحقيق في جرائم محددة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

[1]-المادة 04 من القانون 09-04.

[2]-المادتان 37 و40 من من ق.إ.ج.ج من الأمر 66-155 المؤرخ في 23 يونيو 1966 المتضمن من ق.إ.ج.ج. المعدل والمتمم بالقانون 07/17 المؤرخ في 27 مارس 2017.

5-ضبط الأدلة في مجال الاعتداء على التوقيع الإلكتروني:

عقب التوصل للأدلة الإلكترونية في مسرح الجريمة الإلكترونية، يجب أن يتم جمع تلك الأدلة بشكل كافي وفق نظم معينة حتى تكون لها حجية أمام القضاء وتتم عملية الضبط وفق مجموعة من المراحل:

مرحلة جمع الدليل:

تعتبر هذه المرحلة من أهم المراحل التي تلجأ إلى جهات التحقيق للكشف عن الحقيقة حيث يتم إتباع الإجراءات التالية من خلالها:

- ✓ تسجيل كل ما يتم من إجراءات في الملاحظات.
- ✓ مراقبة الشاشة وتحديد ما إذا كانت معلقة أو مطفأة.
- ✓ تسجيل الموديل والرقم المتسلسل للجهاز.
- ✓ إزالة أعلى أقراص مدمجة موجودة لتجنب تلف الأدلة.
- ✓ تسجيل كل الأفعال المرتبطة بالتلاعب بالجهاز لحفظ الموثوقية في المعلومات ومثال هذه الأجهزة تسجيل الصوت، أجهزة الرد الآلي.

مرحلة نقل وتخزين الأدلة:

نص المشرع الجزائري في هذا الإطار في المادة 6 من القانون رقم 09-04 السالف الذكر على: "عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية على معطيات مخزنة يتم نسخ كل المعطيات اللازمة لفهمها على دعامة التخزين الإلكترونية تكون قابلة للحجز والوضع في أقراص وفقا للقواعد المقررة في ق.إ.ج.ج" وفي جميع الأحوال على السلطة أن تقوم بالتفتيش والحجز والسهر على سلامة المعطيات في المنظومة المعلوماتية وهو ما ذهبت إليه المادة 27 من ق.إ.ج.ج تحت عنوان 'ضبط المعلومات المخزنة' والتي تنص: "تلتزم كل دولة طرف يتبنى

الإجراءات الضرورية لتمكين السلطات المختصة من ضبط المعلومات التقنية وعمل نسخة من المعلومات التقنية وكذا الحفاظ على سلامة تقنية للمعلومات، وأيضا إعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص المادة 3/6 من ق.إ.ج.ج وهذا تحت طائلة العقوبات وفقا للمادة 85 من ق.إ.ج.ج، بالإضافة إلى وضع تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواد التي تكون محلا للجريمة.[1]

ثالثا: الانتقال والمعاينة في جرائم التوقيع الإلكتروني.

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة، وهي من أهم إجراءات التحقيق على الإطلاق، فتعرف المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في الكشف عن الحقيقة.

1-معاينة مسرح الجريمة الإلكترونية:

تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، ولمعاينة مسرح هذه الجرائم يجب التفرقة بين حالتين:

*/معاينة الجرائم الواقعة على المكونات المادية للجهاز: تتم المعاينة في جهاز الإعلام الآلي كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي لا تثير أي مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.[2]

[1]-يزيد بوحليط، المرجع السابق، ص 488-489.

[2]-أحمد حزيط، الوجيز في الإجراءات الجزائية، دار هومة، الجزائر، ط2 ، 2015، ص8 3

*/معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها وهي برامج الجهاز وبياناتهن وهاته المكونات تثير صعوبات أهمها: نقص وقلة الآثار المادية التي تقع على المكونات غير المادية للجهاز.

*/تردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة والتي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها.[1]

2-القواعد الإجرائية لمعاينة مسرح الجريمة الإلكترونية:

هي جملة من الإجراءات المطبقة في كافة الجرائم، إلا أن التشريع الجزائري ينص على جملة من القواعد التي تعد وجوبية للقيام بالمعاينة، فأجاز المعاينة في الجنح وجعلها وجوبية في الجنايات، وهي قد تتم في مكان عام أو خاص، فإذا كانت في مكان عام فضابط الشرطة القضائية لا يحتاج أي إذن ندب سلطة تحقيق بإجراءاتها، أما إذا كان خاص فلابد من شروط خاصة.

أ-إخطار وكيل الجمهورية:

لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضابط الشرطة القضائية، وهذا ما نصت عليه المادة 42 من ق.إ.ج.ج.[2]

وعملا بنص المواد 18، 32، 42، 63 من ق.إ.ج.ج بالإضافة إلى نص المادتان 42 و49 من قانون القضاء العسكري من واجبات ضباط الشرطة القضائية إذا ما علموا بأية جريمة بأن يقوموا بإخطار وكيل الجمهورية سواء كان مدنيا [3] أو عسكريا باعتباره المسؤول المباشر عن الشرطة القضائية، على أن يكون الإخطار مسبوقا بتأكيد ضباط الشرطة القضائية من ووقع الجريمة

[1]- أحمد حزيط المرجع السابق، ص 39.

[2]- ينظر: المادة 42 ق ا ج ج

[3]-حمزة بحاة، المرجع السابق، ص 19.

فعلا، كما أن الإخطار يكون باستعمال كافة الوسائل المتداولة عليها، فقد يكون بالكتابة أو باستعمال الهاتف النقال أو عن طريق أجهزة أخرى كالفاكس.

ب–أوقات المعاينات:

ألزم المشرع الجزائري ضباط الشرطة أخذ الإذن من وكيل الجمهورية المختص من أجل الدخول إلى منازل الأشخاص للقيام بالتفتيش والمعاينات، فتطبق هذه القواعد عند الانتقال لمعاينة الجرائم الإلكترونية، حيث يجوز إجراء المعاينات في النظم المعلوماتية في كل ساعات النهار والليل وفي محل سكاني أو غير سكاني بناء على إذن مسبق من وكيل الجمهورية المختص.[1]

وبالرجوع إلى نص المادة 47 من ق.إ.ج.ج أجاز المشرع إجراء المعاينة والتفتيش والحجز، في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار أو الليل دون تأخير هذه الإجراءات، عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما يجوز لضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك.[2]

ج–رضا صاحب السكن:

لا يجوز تفتيش المساكن ومعاينتها وضبطك الأشياء المشتبه فيها إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، أو يجب أن يكون هذا الرضا صريحا وكذلك الشأن بخصوص الجرائم الواقعة على النظم المعلوماتية وهذا ما نص عليه المشرع الجزائري في نص المادة 64 من ق.إ.ج.ج.[3]

ولنجاح المعاينة في الجرائم المعلوماتية يجب إتباع ومراعاة القواعد الفنية والمتمثلة في:

---

[1]–أحمد حزيط، الوجيز في الإجراءات الجزائية، المرجع السابق، ص 39.

[2]–راجع المادتان 47 و49 من ق.إ.ج.ج.

[3]–المادة 64 من ق.إ.ج.ج تنص على مايلي: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه".

*/القيام بتصوير الجهاز وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة، مع التركيز على تصوير أجزاءه الخلفية وملحقاته ومراعاة التاريخ والزمان الذي التقطت فيه كل صورة.

*/يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للجهاز) اللازمة، للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة.

*/وضع مخطط تفصيلي للمنشاة الواقعة بها الجريمة مع كشف تفصيلي على المسؤولين بها ودور كل واحد منهم.

*/ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

*/إبعاد الموظفين والفضوليين على أجهزة الإعلام الآلي وكذلك عن الأماكن التي توجد بها أجهزة أخرى.[1]

*/عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجلات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة.

*/التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصه بالإضافة إلى رفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.

[1]–أمحمدي بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لقانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، 2016، ص 66.

*/يجب أن تقتصر مباشرة عملية المعاينة على مأمور الضبط والباحثين ممن تتوفر فيهم الكفاءات العلمية والخبرة الفنية في مجال جهاز الإعلام الآلي واسترجاع المعلومات وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة.[1]

رابعا: الخبرة التقنية في جرائم الاعتداء على التوقيع الإلكتروني.

يتخذ المحقق الجنائي العديد من الإجراءات والوسائل التي تساعده على التوصل للجناة في جرائم الاعتداء على التوقيع الإلكتروني، لعدم قيامه بتلك الإجراءات لوحده، فقد أجاز له القانون الاستعانة بأهل الخبرة من قبل جهاز التحقيق عند التعامل مع هذه الجرائم تعد ضرورة ملحة لما لهذه الجرائم من طابع فني خاص.

تعرف الخبرة بأنها: "إبداء رأي فني من شخص مختص في شان واقعة ذات أهمية في الدعوى الجنائية".[2]

وبمعنى آخر هي: "تنقيب وبحث يرتبط بمادة لتطلب معارف علمية أو فنية خاصة لا تتوافر لدى المحقق أو القاضي".[3]

1-أهمية الخبرة التقنية في مجال جرائم الاعتداء على التوقيع الإلكتروني:

يعتبر دور الخبير في جرائم الاعتداء على التوقيع الإلكتروني تمديد الأهمية وذلك نظرا لتطور وتقدم وسائل شبكات الاتصال والحاسبات المرتبطة بالجهاز بصورة يعتذر على المتخصص ملاحقتها واستتباعها لدرجة يمكن القول أنه لا يوجد خبير قادر على التعامل مع كافة أنواع الجرائم التي ترتكب بواسطتها وذلك لقلة معرفته الدقيقة في سائر أنواع الحسابات والبرامج

[1]- أمحمدي بوزينة آمنة، المرجع السابق، ص 67.

[2]-داود سليمان علي الحماد علي ، المرجع السابق، ص 174.

[3]-يزيد بوحليط، المرجع السابق، ص 329.

والشبكات.[1] لذلك يجب أن يتوافر لدى خبراء الحاسب الآلي المنتدبين للتحقيق المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة، ومن مهام الخبير:إمكانية نقل أدلة الإثبات لأوعية أخرى دون تلف وكيفية النظام المعلوماتي عند الحاجة.

2-موقف المشرع الجزائري بالنسبة للخبرة التقنية:

لقد نظم المشرع الجزائري إلى حد ما إنجاز الخبرة الرقمية بما يتوافق وخصوصية الجريمة الإلكترونية وصعوبة التحقيق فيها، لذا حاول وضع نصوص قانونية تسهل وضع ترتيبات لإجراء الخبرة الرقمية وذلك في عدة مستويات:

*/فعلى مستوى تعيين الخبرة فنجد نص المادة 144 من ق.إ.ج.ج والتي تبين لنا كيفية اختيار الخبراء كما أسلفنا سابقا، نجد نص المادة 05 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي مفادها تسخير السلطات المكلفة بتفتيش كل شخص له دراية بعمل المنظومة المعلوماتية.

*/أما على مستوى الهيئات نجد أن المشرع الجزائري نص على إسناد هيئات بكوادر مؤهلة تقوم بإجراء الرقمنة كإسناد المعهد الوطني للبحث في عالم التحقيق الجنائي.[2] وإسناد قيادة الدرك الوطني للمركز الوطني لمكافحة الجريمة المعلوماتية الموجودة ببئر مراد رايس بالجزائر العاصمة، وإسناد المعهد

[1]-عمر بن يونس، الجرائم في استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، القاهرة، مصر،2004، ص 121.

[2]- المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/29 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي.

الوطني للأدلة الجنائية وعلم الإجرام، [1] تأهيلا عن توفير الوسائل الحديثة على مجال تكنولوجيا الإعلام والاتصال.[2]

الفرع الثاني: الإجراءات المستحدثة لجمع الدليل في جرائم الاعتداء على التوقيع الإلكتروني.

إن الإجراءات التقليدية المحددة من أجل الحصول على الدليل الإلكتروني نجد فيها الصعوبات التي تحيط بها نظرا لعدم كفايتها مما يسهل للكثير من المجرمين الإفلات من العقاب، لذا أصبح من الضروري على أن تواكب التشريعات المختلفة الطبيعة الخاصة لهذه الجرائم من خلال الاعتماد على وسائل متطورة وحديثة للكشف عن الجريمة والقبض على مرتكبيها، وعدم إفلات المجرم من العقاب من هذا النوع المستحدث من الجرائم.

موقف المشرع الجزائري من اعتراض المستند الإلكتروني:

لقد أغفل المشرع الجزائري تعريف اعتراض المراسلات، ولكنه بالمقابل اكتفى بتنظيم هذه العملية بموجب المادة 65 مكرر 05 من ق.إ.ج.ج"إذ اقتضت ضروريات التحري على الجريمة المتلبس بها أو التحقيق الابتدائي...في الجرائم الآلية للمعطيات...يجوز لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات

[1]–المرسوم الرئاسي رقم 183–04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانون الأساسي رقم 41 المؤرخ في 2004/06/27، ص 18.

[2]– في إطار المجودات المبذولة من طرف السلطة القضائية بالجزائر بخصوص تدريب وتكوين ضباط الشرطة القضائية والقضاة في مجال البحث والتحري عن الجرائم الإلكترونية أشرف خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفدرالي على تكوين ورشات حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة تهدف إلى إطلاعهم على آخر التكنولوجيا لمحاربة الجريمة.

مقال منشور على الموقع الرسمي : http// :www.djazzairess.com/alkhabar اطلع عليه على الساعة 9:24 بتاريخ 16 أوت 2020.

التقنية دون الموافقة العينية من أجل التقاط وتكتب وتبث وتسجيل الكلام أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص".[1]

أما بالرجوع إلى نص المادة 46 من التعديل الدستوري المؤرخ في 2016/03/06 والتي تنص على: "لا يجوز انتهاك حرمة حياة مواطن الخاصة وحرمة شرفه يحميها القانون سرية المراسلات والاتصالات الخاصة...وعليه يضمن الدستور سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة والنشر أو الإطلاع أو الاعتراض تحت طائلة العقوبات".

كما نص المشرع أيضا على سرية المراسلات بموجب المادة 105 الفقرة الأخيرة من القانون رقم 2000-03 المؤرخ في 2000/08/05 تحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

كما نص أيضا على سرية البيانات المتعلقة بالتصديق الإلكتروني بنص المادتين 42 و43 من القانون رقم 15-04[2] المؤرخ في 2015/02/01 يحدد القواعد العامة لتوقيع والتصديق الإلكتروني على مؤدى خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.

1-التدابير التقنية لاعتراض بيانات السجل الإلكتروني:

يلزم لاتخاذ اعتراض محتوى المستند أو السجل الإلكتروني، اتخاذ بعض التدابير التقنية بغرض تيسير عملية جمع المعلومات أو تسجيلها أو تأكيد ذلك بنص المادة 21 من اتفاقية بودابست على التدابير التي يجوز لسلطة التحقيق اللجوء إليها عند اعتراض محتوى بيانات السجل الإلكتروني.

[1]-المادة 65 مكرر05 من ق.إ.ج.ج.

[2]-المادتين 42، 43 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

*/تجميع أو تسجيل البيانات من خلال تطبيق واستخدام الوسائل الفنية على أراضي تلك الدولة التي تكون طرف في الاتفاقية.

ألزم جهاز تقديم الخدمة المعلوماتية في حدود قدرته الفنية بمايلي:

-تجميعها أو تسجيلها خلال تطبيق واستخدام الوسائل الفنية والتعاون ومساعدة السلطات المختصة في تجميع أو تسجيل مضمون البيانات، يجب على تلك السلطة أن تتوخى السرية التامة عن اعتراض من مضمون البيان الإلكتروني وذلك حفاظا على سرية البيانات التي تم اعتراضها ومؤدى كل ذلك أن الإفصاح عن تلك البيانات لا يكون إلا عندما تكون الجريمة الاعتداء على التوقيع الإلكتروني.[1]

2-السلطة المختصة في إصدار إذن الاعتراض:

3-مدة الاعتراض:

حرصت معظم التشريعات المعاصرة على تحديد مدة معينة للاعتراض منها من التعسف وإساءة استعمال السلطة، غير أن هذه التشريعات لم تنشر على وتيرة واحدة من شأن هذه المراقبة فمنها مما حدد المدة بأمد قصير كالتشريع المصري، حيث حددها بثلاثين يوما قابلة للتجديد لمدة أو مدة أخرى مماثلة طبقا للتحديد الوارد في نص المادتين 90، 206 من قانون الإجراءات المصري.

أما المشرع الجزائري فنص على مدة الإذن لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق، وهذا ما نصت عليه المادة 65 مكرر5 من ق.إ.ج.ج.[2]

[1]-هلالي عبد الله احمد، المرجع السابق، ص 182.

[2]-أيمن رمضان محمد أحمد، المرجع السابق، ص 190.

أ-في تسجيل الأصوات وإجراءات القيام به:

تسجيل الأصوات هو النقل المباشر للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق، شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه، [1] وهي تلك المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام، ويتم ذلك عن طريق حفظ الحديث على جهاز معد لذلك للاستماع إليه مرة أخرى.[2]

وفي هذا الإطار نجد أن المشرع الجزائري نص من خلال نص المادة 65 مكرر 05 من ق.إ.ج.ج السابقة الذكر على تسجيل أحاديث المتهم[3].

حيث أجاز المشرع وضع ترتيبات تقنية دون علم وموافقة المعنيين من أجل تسجيل الأحاديث في الأماكن العامة أو الخاصة، حيث أن أخذ المشرع الجزائري بالمذاهب الموضوعية ، حيث طبيعة الحديث أساس الحماية الجنائية بغض النظر على المكان الذي أجري فيه وهو المعيار الذي أخذ به المشرع الفرنسي أيضا، [4] بما أن المشرع المصري تأثر بالقانون الفرنسي وأصدر القانون رقم 37 لسنة 1982 بمقتضاه أضيفت المواد 309 مكرر التي اعتنق من خلالها معيار المكان الخاص لتحديد طبيعة الحديث وإضفاء حماية عن المحادثات الخاصة، ذلك أنه يسيغ حماية على المحادثات التي تدور في أماكن خاصة، ويتطلب شروط وإجراءات خاصة للاعتداد بالدليل المستمد من التسجيل، لذلك من الأفضل تعديل هاتين المادتين على نحو يكفل الأخذ بطبيعة الحديث وبمكان صدور وسبب وطبيعة الحديث فقط، كالنهج الذي أخذ به المشرعين الفرنسي والأمريكي.

[1]-ياسر محمد الكومي، المرجع السابق، ص 250.

[2]-حازم محمد حنفي، المرجع السابق، ص 74.

[3]-المادة 65 من ق.إ.ج.ج.

[4]-يزيد بوحليط، المرجع السابق، ص 370-371.

ب–يتم تسجيل الأصوات عن طريق أجهزة التسجيل السلكية واللاسلكية:

تعمل عن طريق إخفاء الميكروفون داخل المكان المراد سماع المحادثات التي تدور فيه، وتوصيل هذا الميكروفون بواسطة أسلاك دقيقة كغيرها من الأنظمة المستخدمة، [1] ويتم تسجيل الأصوات طبقا للتشريع الجزائري بتسخير أعوان ومصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب المادة 65 مكرر 8، إذن التسجيلات الصوتية الحديثة لها حجية كبيرة في الإثبات الجنائي، لان التقنيات الإلكترونية المتطورة للتسجيل لا تحتمل الخطأ، وبإمكان الخبراء كشف أعلى تعديل أو تلاعب بواسطة تقنية عالية الكفاءة.

ج–التقاط الصور:

لقد عرف جانب من الفقه الجنائي الصورة بأنها: "امتداد ضوئي لحجم الإنسان وهي لسبب لها فكرة أو دلالة الإشارة إلى شخصية صاحبها [2] حيث أن التصوير المرئي يعتمد على توثيق مشاهد متحركة، ويقوم هذا الأجراء أساسا على استخدام الكاميرات أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بما تتخلله من صور لحادثة معينة".

د–أجهزة التصوير المرئي التي تستخدم في تسجيل الأحداث والجرائم:

- ✓ التصوير المرئي بكاميرات السينما والتلفاز.
- ✓ التصوير المرئي بكاميرات الفيديو.
- ✓ التصوير المرئي بالكاميرات الرقمية وهو ما يسمى بكاميرات الديجتال.
- ✓ التصوير المرئي بكاميرات الهاتف الخلوي.

[1]–طارق سرور، المرجع السابق، ص 310.

[2]–حازم محمد حنفي، المرجع السابق، ص 128–129.

- ✓ التصوير المرئي عن طريق أجهزة مراقبة وكاميرات خاصة.
- ✓ التصوير المرئي بالكاميرات السرية.
- ✓ التصوير عن طريق القرصنة الإلكترونية.

موقف التشريعات المقارنة من الدليل الإلكتروني المتحصل من التصوير المرئي:

جرم المشرع المصري بموجب المادة 309 مكرر من قانون العقوبات تسجيل الأحاديث والنقاط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص، حيث أجازت المادة 95 من ق.إ.ج.ج لقاضي التحقيق أو القاضي الجزائي أن يقوم بتسجيلات لأحاديث تجري في مكان خاص.

مما يعني حجية التصوير المرئي في الإثبات الجنائي تخضع لما تخضع له سائر الأدلة الجنائية الأخرى من ضرورة توافرها على مشروعية الدليل الجنائي، أما بخصوص إجراء التصوير المرئي في الأماكن العامة نجد نص المادة 21 من قانون الإجراءات الجنائية أجازت لجهات التحقيق القيام بتصوير المتهم حال وجوده في مكان عام.[1]

أما المشرع الجزائري فقد اعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة لمكافحة الجرائم المستحدثة، ومنها الجرائم الإلكترونية، غير أنه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذا الإجراء، وإنما نص على مجال تطبيقه وتوضيح إجراءات القيام به، فبالرجوع إلى نص المادة 65 مكرر05 والاتجاه في فحواها: "إذا اقتضت بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط...في أماكن خاصة أو عمومية".[2]

[1]-حازم محمد حنفي، المرجع السابق، ص 133.

[2]-راجع في ذلك المادة 65 مكرر05 من ق.إ.ج.ج.

وعلى خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة، واستثنى المشرع الجزائري التقاط الصور في الأماكن العمومية، غير أنه سمح بهذا في بعض القوانين الخاصة كالترصد الإلكتروني والاختراق بموجب المادة 56 من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته.[1]

المبحث الثاني: التعاون الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني.

يعتبر موضع التعاون الدولي في مجال مكافحة جرائم التوقيع الإلكتروني من أهم الآليات المعتمدة لمكافحة هذه الجرائم وتمنع المجرمين من الإفلات من العقاب، نظرا ما تتميز به هذه الجرائم من خاصية، أنها عابرة للحدود الوطنية وتتم عبر عدة دول، فبالرغم من أهمية التعاون الدولي على الصعيد الأمني أو المساعدة القضائية، غلا أنه تعترضه عدة إشكالات تقف أمام فعاليته ويتخذ صورا عديدة منها للتعاون الدولي على الصعيد الشرطي في مرحلة جمع الاستدلالات، وكذا المساعدة القضائية على مستوى مرحلة المحاكمة وتسليم المجرمين ووضع الضوابط والإجراءات الدولية.

ومن ثم نقوم بتقسيم هذا المبحث إلى مطلبين ، حيث نتطرق إلى التدابير الدولية لمكافحة جرائم الاعتداء على التوقيع الإلكتروني في (**المطلب الأول**) بينما نتناول التعاون القضائي الدولي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني في (**المطلب الثاني**)

[1] -تنص المادة 56 من القانون رقم 06-01 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته: "من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو إتباع أساليب تحر خاصة كالترصد الإلكتروني والاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة، تكون للأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول بهما"، ج.ر رقم14، المؤرخة في 200.6/03/08.

المطلب الأول: التدابير الدولية لمكافحة جرائم الاعتداء على التوقيع الإلكتروني.

تتسم جرائم التوقيع الإلكتروني بالنظر إلى طبيعتها بطابع دولي، لذا لا تستطيع الدول بجهودها المنفردة القضاء علة هذه الجريمة، لذا من الضروري أن تساعد الدول بعضها البعض في تقديم الأدلة على أن يكون المحققون والنواب العامون على دراية بآليات متبعة للحصول على هذه المعلومات ويتحقق هذا التعاون بعقد اتفاقيات دولية، وتدعيم التعاون مع البوليس الدولي، أما على المستوى الوطني لابد من خلق أجهزة اتصال متطورة تتماشى وطبيعة الجرائم والقبض على المجرمين، بالإضافة إلى تنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وتقديم المعونة ف مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء، وتتمثل الإجراءات الجنائية في إجراءات ضبط مرتكبيها من قبض وتفتيش وتسليم لتصبح منطقة قضائية واحدة، ومن ثم نقسم هذا المطلب إلى فرعين، نتعرض في الفرع الأول إلى التدابير الدولية الإجرائية مباشرة على جهات المكافحة، ونتعرض في الفرع الثاني إلى التدابير الدولية الإجرائية المعتمدة في مجال تسليم المجرمين.

الفرع الأول: التدابير الدولية الإجرائية الواجب مباشرتها على مستوى جهات المكافحة.

في ضوء التزايد المستمر لجرائم المعلومات بوجه عام والتوقيع الإلكتروني خاصة، قامت العديد من الدول بإنشاء جهات مختصة، ودعمت هذه الدول هذه الجهات بالتقنيين المتخصصين ورجال البحث الجنائي المدربين تدريبا خاصا لمكافحة هذا النوع من الجرائم نظرا للطبيعة الدولية لهذه الجرائم وكونها متعدية الحدود، فأبرمت العديد من الاتفاقيات وانعقدت مؤتمرات دولية وإقليمية وحتى وطنية.

أولا: جهات مكافحة جرائم التوقيع الإلكتروني على المستوى الدولي.

أ-التدابير الإجرائية الصادرة من المجلس الأوروبي.

أصدر المجلس الأوروبي التوجيه رقم 95 في سنة 1990، وضع فيد بعض التدابير الإجرائية لتعزيز التعاون الدولي في المجال الإجرائي لمكافحة جرائم الاعتداء على التوقيع الإلكتروني، حيث حث الدول الأعضاء في المجلس لتحديد قوانين الإجراءات الجنائية الوطنية بما يلائم هذا التطور،[1] وأهم ما ورد في هذه التوصيات:

*إن تحول النصوص الإجرائية للسلطة القائمة بالتفتيش ضبط برامج الكمبيوتر وقواعد البيانات الموجودة بالأجهزة وفقا لذات إجراءات التفتيش التقليدية.

*النص على مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة، ويقتضي الأمر التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي، وجب وضع قاعدة قانونية صريحة تسمح بسهولة تطبيق هذا الإجراء.[2]

*تعديل القوانين الإجرائية بما يمكن سلطات التحقيق أمر للغير بأن يقدم المستندات الإلكترونية المخزنة في الجلسة متى كانت تفيد في كشف الحقيقة في جريمة ضرورية من أجل تحويل سلطاته المختصة إلى سلطة التفتيش أو الولوج بطريقة مشابهة للنظام المعلوماتي أو جزء منه.

ب-التدابير الإجرائية الصادرة من المنظمة الدولية للشرطة الجنائية 'إنتربول' لمكافحة جرائم التوقيع الإلكتروني.

تعد المنظمة الدولية للشرطة الجنائية إنتربول oipc من أهم الأجهزة الدولية في مجال مكافحة جرائم الاعتداء على التوقيع الإلكتروني، وتتخذ من باريس مقرا لها، وتحمل هذه المنظمة على تشجيع التعاون المتبادل بين أجهزة الشرطة في الدول بما يحقق مكافحة فعالة للجريمة، كما

[1]-مدحت عبد الحليم رمضان، المرجع السابق، ص 76.

[2]-Alain Bensoussan, Internet aspect juridique, Herses Paris, France, 2eme édition, 1998, P 20.

أنها ستهتم في إقامة النظم التي تساعد على منع ومكافحة جرائم القانون العام، وتقوم منظمة الإنتربول بذلك من خلال وظيفتين:

1-جمع البيانات والمعلومات المتعلقة بالجريمة والمجرم بواسطة المكاتب المركزية الوطنية لها، والمتواجدة في الأقاليم دون أعضاء.

2-التعاون فيضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدول طالبة التسليم.

وتختص أيضا هذه المنظمة بالجرائم ذات الطابع الدولي، وخاصة المتعلقة بالعنف ضد الأطفال وجرائم الأموال.[1]

وتقوم منظمة الإنتربول الآن بدور رئيسي في مجال تبادل المعلومات وتعميم التحذيرات والتنبيهات المتضمنة المعلومات الإستخبارية، والإحاطات التحليلية والفنية عن الأخطار الإجرامية المحتملة، والتقصي في قواعد البيانات، وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم التوقيع الإلكتروني، كما أنشأت منظمة الإنتربول وحدات لمكافحة جرائم التكنولوجيا، كما قامت بوضع استراتيجيات محكمة لمواجهة هذا النوع من الجرائم بالتعاون مع مجموعة الثماني من خلال الآليات الآتية:[2]

*إنشاء مركز اتصالات أمني عبر شبكة الانترنت يعمل على مدى اليوم الكامل طوال الأسبوع في كل إدارات الشرطة في الدول الأعضاء في المنظمة.

*استخدام وسائل حديثة في الجرائم، كما تقوم المنظمة بتزويد أجهزة الشرطة في الدول الأطراف بكتيبات إرشادية حول جرائم المعلومات والتوقيع الإلكتروني.

[1]-حسام محمد نبيل الشنراقي، المرجع السابق، ص 738.

[2]-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسية مقارنة، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص 155.

*يتولى الانتربول إقامة العلاقات بين الدول المنظمة وتبادل المعلومات بين سلطات التحقيق بشأن الجرائم الحديثة في نطاق عدة دول كجرائم التوقيع الإلكتروني.

ج–التدابير الإجرائية الصادرة من الاتحاد الدولي للاتصالات:

لقد استحدث الاتحاد الدولي للاتصالات دليلا إلكترونيا لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة عبر الانترنت، وذلك بالتعاون المشترك مع الوكالة الأوروبية المختصة بأمن الشبكات والمعلومات وأطراف دولية أخرى الاهتمام بشؤون الأمن المعلوماتي على شبكة الانترنت، [1] بحيث يستطيع أن يلاحق المعلومات بأحدث المعايير الأمنية المتجددة باستمرار ثم يصبها في قاعدة بيانات تفتح أمام المعنيين بما يسهل مهمة البحث عن المعلومات المطلوبة، وإلى جانب الاتحاد الدولي للاتصالات يوجد مؤسسات دولية أخرى كمؤسسة الانترنت للأسماء والأرقام المخصصة ICANW، ومنتدى إدارة الانترنت IFG، ومنظمة التعاون الاقتصادي والتنمية OECD، ومجموعة الثماني الاقتصادية G_8...إلخ، هذه المؤسسات الدولية تسعى لمواجهة الجريمة المعلوماتية الرقمية عبر الانترنت.[2]

د–التدابير الإجرائية الصادرة عن الجمعية الدولية لقانون العقوبات:

وقد تبنى المؤتمر الدولي الخامس عشر للجمعية العامة قانون العقوبات للعديد من التوصيات التي تتعلق بالتدابير الإجرائية والتي تنطبق على جرائم الاعتداء على التوقيع الإلكتروني ومنها:[3]

–أن تمكن سلطات التحقيق والتحري سلطات قصرية كافية تتعادل مع الحماية الكامنة لحقوق الإنسان وحرمة الحياة الخاصة.

[1]–وهذا ما أقره المجلس الأوروبي على مستوى الدول الأوروبية عندا اعتبر اتفاقية المجلس الأوروبي بمثابة النظام العام الأوروبي في مجال حماية شيكات الاتصالات عبر الانترنت ومكافحة الجريمة المعلوماتية الرقمية

[2]–فهد عبد الله العبيد الحازمي، المرجع السابق، ص 665.

[3]–أيمن رمضان محمد أحمد، المرجع السابق، ص 398.

-أن يتم تحديد السلطات التي تقوم بإجراء التفتيش والضبط عند تفتيش شبكات الحاسب.

-أن يتم تحديد السلطات المختصة باعتراض الاتصالات داخل نظام الحاسب ذاته أو بينه وبين نظم الحاسب الأخرى مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

-السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات وخاصة ضبط الأشياء غير المحسوسة، تفتيش شبكات الحاسب.

-السماح للسلطات العامة باعتراض الاتصالات داخل الحاسب ذاته مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.[1]

و-التدابير الإجرائية الصادرة بمؤتمر هافانا 1990:

أصدر مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة سجناء هافانا 1990 قرار بشان الجرائم ذات الصلة بالكمبيوتر، ومنها جرائم الاعتداء على التوقيع الإلكتروني، الذي حث الدول الأعضاء في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح عمليات إساءة استعمال الكمبيوتر التي تستدعي تطبيق جزاءات جنائية على الصعيد الدولي بالتدابير التالية:[2]

-تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان أن تطبق الجزاءات والقوانين الراهنة بشأن سلطات التحقيق، وقبول الأدلة في الإجراءات القضائية على نحو ملائم، وإدخال التغيرات المناسبة إذا دعت الضرورة إلى ذلك.

-تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

-التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد للآداب المتبعة في استخدام أجهزة الحاسوب، وتدريس هذه الآداب ضمن المناهج الأساسية.

[1]-حنان محمد حسن، المرجع السابق، ص 222.

[2]-أيمن رمضان محمد أحمد، المرجع السابق، ص 402.

-اعتماد سياسات بشأن خبايا الجرائم المتعقلة بالكمبيوتر تنسجم مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة، وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة وتدابير لتشجيع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم.

ثانيا: جهات مكافحة جرائم التوقيع الإلكتروني على المستوى الإقليمي.

لمكافحة جرائم لتوقيع الإلكتروني على الصعيد الإقليمي، لابد من تضافر جهود الدول، ووجود آليات لضبط المتهمين وتقديمهم للمحاكمة، وهذا ما سنتطرق له على النحو التالي:

أ-على المستوى الأوروبي:

اتفاق شنقن 'chengen' وتم التوقيع عليها في 1985/06/14، ويهدف هذا الاتفاق بإلغاء الحدود بتوحيد مجالات التعاون بين أجهزة الشرطة للدول الأعضاء باستثناء فضاء جماعي من غير حدود سمي بـ système information schengen، واستحدثت هذه الاتفاقية وسلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات الأمنية التي فرضتها الظروف الجديدة، ومنه جرائم الانترنت والتوقيع الإلكتروني وهاتان الوسيلتان هما:[1]

1-حق المراقبة غير المحدود:

وفقا للمادة 40 من الاتفاقية، يجب على رجل الشرطة في إحدى دول الاتفاقية أن يستمر في مراقبة شخص مشتبه فيه موجود في إقليم دولة أخرى طرف في الاتفاقية في إطار أعمال جمع الاستدلالات التي بدأها لكشف غموض الجريمة، ويخضع هذا الحق لعدة شروط تختلف إذا كانت المراقبة في الأحوال العادية يجب الحصول على إذن مسبق من الدولة بالاستمرار في المراقبة، أما في

[1]-حسام محمد نبيل الشنراقي، المرجع السابق، ص 741.

حالة الضرورة فيجوز لرجل الشرطة أن يتجاوز الحدود الإقليمية لدولة إلى إقليم دولة أخرى دون إذنها، وذلك في جرائم حددتها المادة 07 من المعاهدة.[1]

2-الحق في ملاحقة المجرمين خارج الحدود:

نصت المادة 41 من الاتفاقية على رجل الشرطة التابع للدولة في ملاحقة أحد المجرمين على إقليم دولة طرف في الحالتين، إذا كان المجرم قد ضبط في حالة تلبس بارتكاب إحدى الجرائم الجسيمة المحددة في المادة، وفي حالة هروب المحبوس لرجل الشرطة أن يتجاوز حدود دولية لملاحقة المجرم على إقليم دولة أخرى طرف في الاتفاقية وبدون إذن منها، ونصت الاتفاقية على نظام تسجيل المعلومات يسمى نظام معلومات شنجن، ويمثل قاعدة معلومات متعلقة بالأشخاص المطلوبين والأموال والأسلحة التي يتم البحث عنها، ويساعد على ملاحقة مرتكبي الجرائم عبر الانترنت، ومنها جرائم التوقيع الإلكتروني، وقد تم إبرام اتفاقية تعالون بين الشرطة القضائية والجمارك في فرنسا وسويسرا في مارس 1998 لتسهيل مهام هذا النظام.

ب-على مستوى الأوروجيست:

يوجد على مستوى الأوروجيست جهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة الجرائم الإلكترونية، والتي تم إنشاؤها 2002/02/28 من قبل مجلس أوروبا، وينعقد له الاختصاص عندما تمس الجريمة دولتين على الأقل من أعضاء الاتحاد الأوروبي، أو دولة عضو مع أخرى في العالم الثالث، أو دولة عضو مع الرابطة الأوروبية وتشمل في غير تلك الحالات المؤسسات، وتعد الأوروجيست دعامة فعالة في التحقيقات ومطاردة المتهمين لاستكمال

[1]-المادة 07 من اتفاقية شنغن.

التحقيقات في الجرائم ويتكون من نواب عموم ومستشارين قائمين بالضبط القضائي للدول الأعضاء في الاتحاد الأوروبي ذوي الاختصاص والمنتدبين.[1]

ج-على المستوى العربي:

1-القانون الجزائي العربي الموحد الإسترشادي:

اعتبر مجلس وزراء العدل العربي بتاريخ 19 نوفمبر 1996 القانون الجزائي العربي الموحد كقانون نموذجي، وذلك بالقرار 229/12 [2] وقد حرم هذا القانون الاعتداء على حقوق الأشخاص الناتجة عن المعالجات المعلوماتية، حيث جرمت المواد من 461 إلى 463 جمع المعلومات الاسمية، ومعالجتها آليا أو استعمالها بالمخالفة لأحكام القانون أو المساس بسرية معلومات الأشخاص وبمطابقة المادتين 462 و 463 نلاحظ أنهما تناولتا صورتين من الجرائم الماسة بسرية المعلومات الإلكترونية، حيث تناولت المادة 462 جريمة الاعتراض غير القانوني للبيانات، وفي المادة 463 جريمة الدخول غير الصريح أو البقاء داخل نظام المعالجة.

2-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010:

والتي أبرمت في 2010/12/21، ووقعت عليها 17 دولة عربية، [3] ووافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدولي العربية بالقاهرة، ومن بين الدول الموقعة عليها الجمهورية الجزائرية الديمقراطية الشعبية، وتهدف هذه الاتفاقية إلى تعزيز التعاون الدولي فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها.

---

[1]-نبيلة هبة هروال، المرجع السابق، ص 159-160.

[2]-هذا القانون منشور على الموقع الإلكتروني لجامعة الدول العربية، نقلا عن الموقع الإلكتروني:
http://www.arab league online.org، اطلع عليه بتاريخ 06جوان 2020، الساعة: 14:35.

[3]-نص هذه الاتفاقية منشور على الموقع الإلكتروني لجامعة الدول العربية. نقلا عن الموقع الإلكتروني:
http://www.arab league online.org، اطلع عليه بتاريخ: 05 جويلية 2020، الساعة: 10:00.

واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، أخذا بالمبادئ الدينية والأخلاقية السامية، ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها.[1]

الفرع الثاني: التدابير الدولية الإجرائية المعتمدة في مجال تسليم المجرمين.

إن تسليم المجرمين حسب المحكمة العليا الأمريكية هو الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني، حيث تتسلم دولة ما من دولة أخرى شخص متهم او مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة أو المخالفة للقانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة.[2]

وتتعدد مصادر تسليم المجرمين إلى مصادر أصلية تتمثل في المعاهدات والاتفاقيات، التي تكون اتفاقيات التسليم فيها ثنائية، وهي التي تتم بين دولتين وفقا للشروط والضوابط الموضوعية من قبلها، [3] واتفاقية التسليم المتعدد الأطراف، وتكون أطرافها عدة دول، ومن أمثلة هذه الاتفاقيات اتفاقية جامعة الدول العربية لتسليم المجرمين عام 1953، والاتفاقية الدولية الأوروبية لتسليم المجرمين 1957، والقانون الداخلي الدولي والعرف، كما يوجد مصادر احتياطية تتمثل في قواعد المجالات والأخلاق والمعاملة بالمثل.

[1] –ينظر: ديباجة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في 2010/12/21.

[2] –رقية عواشرية، نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، مجلة المفكر، جامعة محمد خيضر، بسكرة، العدد04، 2008، ص 19.

[3] –ومن هذه الاتفاقيات الخاصة بتسليم المجرمين، نجد اتفاقية بين مصر واليونان 1986، اتفاقية بين الجزائر وبلجيكا 1970، اتفاقية التعاون القضائي وتسليم المجرمين مع بولندا في 1993، اتفاقية بين المغرب واسبانيا 1999.

أولا: شروط تسليم المجرمين في جرائم الاعتداء على التوقيع الإلكتروني.

لقد وضعت الاتفاقيات الدولية عدة شروط لتسليم المجرمين وهي:

1-عدم جواز تسليم الرعايا:

من المبادئ السائدة والمستقر عليها في المجتمع الدولي، والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات الدولية مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم، وأغلبية المعاهدات تأخذ بهذا النظام كفرنسا ومصر، بينما الدول الأجلو ساكسونية كالولايات المتحدة الأمريكية وبريطانيا تأخذ بمبدأ تسليم الرعايا، نص المادة 51 من الدستور المصري 1971: "لا يجوز إبعاد مواطن عن البلاد أو منعه من العودة إليها"، [1] وكذا هذه القاعدة نجدها في القانون السويسري 1829، وفي مشروع جمعه القانون الدولي 1938 والقانون الفرنسي 1937 والقانون الألماني، وفي المعاهدات مثل معاهدة تسليم المجرمين بين العراق والمملكة العربية السعودية 1931، وكذا معاهدة بين سويسرا وأمريكا 1900 تقضي بان أية حكومة من الحكومتين غير ملزمة بتسليم رعاياها.

في حين أن بعض التشريعات تفرض قيود في تسليم رعاياهم، ففي القانون الفرنسي نص يبيح تسليم الشخص المطلوب الذي اكتسب الجنسية الفرنسية بعد ارتكاب الجريمة المادة 05، وفضلا عن ذلك فإن القانون الفرنسي لا يمنع من مرور شخص فرنسي يقتضي بتسليمه عبر الأراضي الفرنسية المادة 28.[2]

[1]-جميل عبد الباقي الصغير، المرجع السابق، ص 89.

[2]-فهد عبد الله العبيد الحازمي، المرجع السابق، ص 535.

2-عدم التسليم في الجرائم السياسية:

فلا يجوز التسليم في الجرائم السياسية، [1] حيث يكون الغرض منه اتخاذ إجراءات انتقامية ضد الشخص المطلوب تسليمه، وهو عمل لا يليق في الدولة المطلوب منها التسليم أن تساهم في تنفيذه. ولقد أكد البند العاشر من المادة 16 من اتفاقية باليرمو بشأن جرائم الكمبيوتر على أنه في حالة رفض دولة طلب التسليم وقع عليها الالتزام بمعاقبة المتهم، كما نصت الاتفاقية العربية لمكافحة الجريمة في مادتها 6/ف1 على أنه لا يجوز التسليم إذا كانت الجريمة المطلوب من أجلها التسليم معبرة بمقتضى القواعد القانونية النافذة لدى الدولة المتعاقدة المطلوب إليها التسليم جريمة لها صيغة سياسية. وكذلك المادة 03 من معاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين لسنة 1950، وأيضا المادة 04 من اتفاقية جامعة الدول العربية لتسليم المجرمين لسنة 1952، وأيضا المادة 20 من الاتفاقية الأمنية لدول مجلس التعاون الخليجي.

3-عدم جواز التسليم في الجرائم العسكرية:

هذا ما نصت عليه المادة 06 من الاتفاقية العربية لمكافحة الجرائم على انه لا يجوز التسليم إذا كانت الجريمة المطلوب من أجلها التسليم تنحصر في الإخلال في الوجبات العسكرية.

4-عدم جواز التسليم من تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها:

إذا كان الشخص المطلوب تسليمه قد سبقت محاكمته عن الجريمة المطلوب تسليمه لأجلها غير أو عوقب عنها فإنه لا يجوز تسليمه، ليس هذا فحسب، بل انه لا يجوز التسليم متى كان قيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله.[2]

---

[1]-المادة 53 من الدستور المصري، تسليم اللاجئين السياسيين، وكذا المادة 03 البند الرابع من القانون العماني حيث نص على إذا كان المطلوب تسليمه قد منح حق اللجوء السياسي في السلطنة قبل طلب التنازل واستمر متمتعا بهذا الحق بعد ورود الطلب.

[2]-محمد كمال محمود الدوسيقي، المرجع السابق، ص 185.

5-أن يكون قانون الدولة طالبة التسليم مختص بمحاكمة الشخص المطلوب تسليمه:

يجب أن ينعقد الاختصاص بنظر جرائم الاعتداء على التوقيع الإلكتروني لقانون الدولة طالبة التسليم، وبالمقابل يتعين ألا يكون قانون الدولة المطلوب إليها التسليم مختصا بمحاكمة الشخص المطلوب تسليمه عن ذات العقل المنسوب إليه، ومن هنا التطبيقات العملية للتسليم في جرائم الاعتداء على التوقيع الإلكتروني في هذا المجال عملية odysseusفي فيفري 2004 بمبادرة من يوروبول، حيث قامت الشرطة من خلالها بعمليات شملت 15 دولة: استراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج...وقد تم تسليم المتهمين إلى سلطات التحقيق في بريطانيا حيث قضي بإدانتهم.[1]

6-أن يكون الاعتداء على التوقيع الإلكتروني المنسوب إلى المتهم يشكل جريمة في قانون الدولة طالبة التسليم:

يشترط لقيام الدولة بتسليم شخص ما إلى دولة أجنبية أن يكون الاعتداء على التوقيع الإلكتروني المنسوب إلى المتهم مجرما في قانون الدولة طالبة التسليم، وفي قانون الدولة المطلوب إليها معا، وقد أكدت المادة 24 من اتفاقية بودابيست بشان جرائم الحاسب الآلي أنه يجب تسليم المتهمين بين الأطراف فيما يتعلق بالجرائم المبينة في المواد 2، 11 من الاتفاقية، بشرط أن تكون تلك الجرائم معاقب عليها بموجب القوانين في بلد كل من الطرفين المعنيين بحرمان من الحرية لفترة أقصاها سنة على الأقل أو بعقوبة اشد، ما لم يوجد اتفاق أو معاهدة بخلاف ذلك.[2]

وكذلك ما تضمنته المادة 166 من القانون رقم 302-2004 حول التعاون القضائي الدولي في المسائل الجنائية أحكاما مماثلة.

[1]-إيهاب محمد يوسف، المرجع السابق، ص 23.

[2]-هيلالي عبد الله أحمد، المرجع السابق، ص 410.

7-عدم انقضاء الدعوى العمومية أو العقوبة:

يشترط بجواز التسليم ألا تكون الدعوى العمومية أو حكم القاضي بفرض العقوبة قد انقضى بأحد أساليب الانقضاء المحددة في التشريعات الوطنية للدولة طالبة التسليم والمطلوب إليها التسليم أو الدولة التي ارتكبت الجريمة على أراضيها.[1]

ثانيا: إجراءات تسليم المجرمين في جرائم التوقيع الإلكتروني.

وهي تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته، وبين تامين الصالح العام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة، بحيث بلا يفلت أي مجرم من العقاب.

1-مراحل طلب التسليم: يمر طلب التسليم بثلاث مراحل:

أ-المرحلة الأولى: تتمثل في تلقي الطلب واتخاذ إجراءات التحري وجمع الاستدلالات والقبض على الشخص المطلوب وهي من اختصاص الشرطة.

ب-المرحلة الثانية: استجواب المقبوض عليه وحبسه احتياطيا، أو إطلاق سراحه بكفالة أو بدونها، أو كمنعه من مغادرة الأراضي الإقليمية إلا أن يتم الفصل في الطلب الوارد بشأنه، وهي من اختصاص الادعاء العام.

ج-المرحلة الثالثة: وهي فحص الطلب من قبل المحكمة المختصة والبت فيه بالقبول أو بالرفض مع توافر الشروط الشكلية.[2]

[1]-ياسر محمد الكومي محمود أبو حطب، المرجع السابق، ص 360.

[2]-سليمان أحمد فضل، المرجع السابق، ص 421.

2-الأوراق والمستندات المرفقة بالطلب:

- زمان ومكان ارتكاب الجريمة وتكييفها القانوني مع الإشارة إلى المواد القانونية المطبقة عليها.
- وصف الشخص المطلوب تسليمه بأكبر قدر ممكن من الدقة وأية بيانات أخرى.
- أن تطلب من الدولة المطلوب منها التسليم بأية طريقة من طرق الاتصال الكتابية حسب توقيف الشخص احتياطيا إلى حين وصول طلب التسليم.[1]

3-نقل الأشخاص المحكوم عليهم:

تنص اتفاقية الأمم المتحدة لمكافحة الفساد un التعاون الدولي المادة 45 بشأن نقل الأشخاص المحكوم عليهم، يجوز للدول الأطراف أن تنظر في إبرام اتفاقيات أو ترتيبات ثنائية أو متعددة الأطراف بشأن نقل الأشخاص الذين يحكم عليهم بعقوبة الحبس أو بأشكال أخرى من الحرمان من الحرية، لارتكابهم أفعالا مجرمة لإقليمها لكي يكمل أولئك الأشخاص مدة عقوبتهم هناك، إضافة إلى ذلك يجب أن تسلم مع الشخص كل ما كان في حوزته أثناء القبض عليه، وكل ما يمكن أن يكون دليلا عن الجريمة، ويجوز الاحتفاظ بها إذا رأت الدولة المطلوب إليها التسليم لزوما لذلك، أو أن تحتفظ بحق استرجاءها مستقبلا.[2]

أما نفقات التسليم يتم تحديدها وفقا لما جاء بنصوص المعاهدة المبرمة بين الدولتين المتعاقدتين أو بين الدول المتعاقدة في حالة المعاهدة الدولية متعددة الأطراف، أما الأموال التي تدفع لنقل الشخص المطلوب تسليمه فعلى عاتق الدولة طالبة التسليم ما لم يتم الاتفاق على غير ذلك.[3]

---

[1]-ياسر محمد الكومي محمود أبو حطب، المرجع السابق، ص 421.

[2]-المادة 37 من الاتفاقية الأمنية الخليجية 1994 والمادة 12 من اتفاقية جامعة الدول العربية لتسليم المجرمين 1953.

[3]-فهد عبد الله العبيد الحازمي، المرجع السابق، ص 552.

ثالثا: مظاهر التعاون الدولي في مجال تسليم المجرمين.

لضبط المجرمين وتحقيق قواعد العدالة، وضمان عدم الإفلات من العقاب سارعت العديد من الدول إلى إبرام اتفاقيات ومعاهدات لفتح المجال أمام التعاون الدولي في مجال تسليم المجرمين وتحقيق مبدأ عالمية العقاب.

1-عالمية حق العقاب في جرائم التوقيع الإلكتروني:

ويطلق عليه مبدأ عالمية النص الجنائي أو نظام العقاب العالمي يهدف إلى التصدي لتنامي الظواهر الإجرامية ذات الأبعاد الدولية من خلال تجاوز القيود التي يفرضها مبدأ الإقليمية، فينعقد اختصاص القاضي الجنائي لأي دولة من دول العالم بغض النظر عن المكان الذي ارتكبت فيه الجريمة الإلكترونية أو جنسية من ارتكبها أو نوع الجريمة، [1] ويؤسس هذا المبدأ على فكرة التضامن بين الدول في مكافحة الجرائم، فالتدخل الدولي وفقا لهذا المبدأ يهدف إلى تجنب إفلات المجرمين من العقاب وضمان محاكمة الجناة بغض النظر عن جنسياتهم أو جنسية المجني عليهم، أو مكان أو نوع الجريمة وقد نظر الفقه الجنائي إلى مبدأ العالمية بوصفه مكملا لغيره من المبادئ التي تحكم نطاق تطبيق العقوبات لسد ما يتسرب عليها من نقص.[2]

2-تطبيقات عملية التعاون الدولي لتسليم المجرمين في جرائم التوقيع الإلكتروني:

ومن التطبيقات العملية لتسليم المجرمين في جرائم الاعتداء على التوقيع في هذا المجال عملية محطم الجليد التي قام بها يوروبول europl في 12 يونيو 2005، تم خلالها مداهمة وتفتيش الأماكن في 13 دولة أوروبية وهي: النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، ايطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا، السويد وبريطانيا وتم توقيف أفراد في كل من فرنسا،

[1]-سليمان أحمد فضل، المرجع السابق، ص 411.

[2]-يعترف القضاء الفرنسي بمبدأ العالمية، إذا ارتكبت الجريمة محل طلب التسليم على إقليم الدولة الطالبة من قبل أحد رعاياها أو أجنبي وذلك وفقا لقانون التسليم الفرنسي الصادر في 10 مارس 1927 في مادته الثالثة البند 3/3.

بلجيكا، المجر، ثم تم تسليمهم إلى بريطانيا التي قامت بتقديمهم للمحاكمة الجنائية وحكم القضاء بإدانتهم.[1]

ومن الوقائع العملية التي طرحت على القضاء المغربي نجد قضية zotob، وكذا المواقع المعتدى عليها خاصة بالكونجرس الأمريكي، وكذا مواقع مؤسسات إعلامية ضخمة بالو.م.أ، بالإضافة إلى موقع مطار سان فرانسيسكو الأمريكي، ومواقع عديدة لمستعملي windows2000 وقد اتهم في هذه القضية الشاب المغربي 18 سنة كمتهم رئيس ومنهم آخر ووجهت لهما تهمة تكوين عصابة إجرامية، وتهمة السرقة واستعمال بطاقات ائتمان مزورة وتهمة الولوج غير المشروع لنظم المعالجة الآلية للمعطيات وتزوير الوثائق الإلكترونية.[2]

المطلب الثاني: التعاون القضائي الدولي لمكافحة جرائم التوقيع الإلكتروني.

تبقى إشكالية الاختصاص القضائي في الجرائم الإلكترونية وعبر الانترنت تتشعب على عدة أوجه مما يخلق ضرورة لحلها، بما يحقق العدالة الجنائية، وتوقيع العقاب على الجناة والحد من إفلاتهم من قبضة القضاة من خلال التعاون الشرطي الدولي على الصعيد الإجرائي الجنائي، وعلى نحو يتيح الاتصال مباشرة بين أجهزة الشرطة في مختلف الدول، وإنشاء مكاتب متخصصة عن مرتكبي تلك الجرائم،[3] فيتعذر على الدولة بمفردها مكافحة هذه الجرائم كونها ترتكب في الغالب عبر إقليم أكثر من دولة، حيث لا يتحقق التعاون الدولي في مجال مكافحة جرائم التوقيع الإلكتروني إلا من خلال عدة محاور أهمها تفعيل دور المنظمة الدولية للشرطة الجنائية وتعجيل اتفاقات الشرطة الدولية.[4]

---

[1]-إيهاب محمد يونس، المرجع السابق، ص 220.

[2]-فهد عبد الله العبيد الحازمي، المرجع السابق، ص 572.

[3]-أيمن رمضان محمد أحمد، مرجع سابق، ص 416.

[4]-يوسف بن سعيد الكلباني، المرجع السابق، ص 292.

الفرع الأول: التعاون الدولي الشرطي لمكافحة جرائم الاعتداء في مرحلة جمع الاستدلالات.

تمثل المساعدة البوليسية بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم المعلوماتية بصفة عامة، وجرائم التوقيع الإلكتروني بصفة خاصة، أحد أهم هذه الجرائم، حيث يستحيل علة الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، فتوقيع العقاب يستلزم تعاون دولي شرطي لذلك أنشأت العديد من منظمات الشرطة على الصعيد الدولي وأنشأت مكاتب شرطة الانترنت لمكافحة جرائم الاعتداء على التوقيع الإلكتروني.

أولا: المنظمات الدولية للشرطة الجنائية.

1-منظمة الشرطة الجنائية 'إنتربول':

يأخذ التعاون الدولي [1] لمكافحة الجريمة المعلوماتية عدة صور، كتوقيع الاتفاقيات الدولية وتنظيم المؤتمرات الدولية، بالإضافة إلى تبادل المساعدة الشرطية والأمنية، حيث قطع التعاون الشرطي الدولي شوطا طويلا سواء على مستوى التعاون الثنائي أو متعدد الأطراف إقليميا وعالميا، وكان من ابرز العلامات على طريق هذا التعاون إنشاء منظمة للشرطة الجنائية الدولية إنتربول، [2] التي تم إنشاؤها في 1923/09/07وتعد من أهم المنظمات الناشطة في مجال مكافحة الجريمة نظرا إلى ما تقدمه من إمكانية تعقب وضبط مرتكبي الجرائم على اختلاف أنواعها أينما وجدوا وتسليمهم إلى الهيئات المختصة بغية محاكمتهم وتوقيع العقوبة المناسبة عليهم، وتضم حاليا 190 بلد عضوا فيها، ويعمل لديها 541 موظف من 79 جنسية مختلفة، وتباشر مهامها بأربع لغات

[1]-علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، دراسة الإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إشراك للنشر والتوزيع، مصر، ط1، 2000، ص 18.

[2]-اشتق اسم إنتربول من اسم المنظمة وقد كان يمثل العنوان البرقي للمنظمة في باريس، ثم أصبح الاستخدام هو الاسم الرسمي للمنظمة، إنتربول باللغة الإنجليزية Police International Organisation Criminalو بالفرنسية Organisation International De Police Criminelle.

رسمية (الإنجليزية، الفرنسية، الاسبانية، العربية)، أما مقرها الحالي بليون فرنسا،[1] كما ظهرت العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة، وأبرزها بعض النماذج الهامة نذكر منها:

- التعليم والتدريب الشرطي المتخصص والمعونات الفنية وتبادل المراجع والخبرات والبحوث.
- ربط شبكات الاتصال والمعلومات: يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة.

وقد حاولت منظمة الإنتربول تيسير الاتصال بين هذه الأجهزة الشرطية عن طريق إنشاء شبكة اتصال خاصة.[2]

بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدّها بالمعلومات المتوفرة لديها على إقليمها، وخاصة بالجرائم المتشعبة في عدة دول، ومنها جرائم الإنترنت، ومن الأمثلة على دور الإنتربول فيما يتعلق بالجرائم المعلوماتية ما حصل في الجمهورية اللبنانية عندما تم توقيف احد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصر دون 10 أعوام من موقعه على شبكة الانترنت وذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص.

2-أجهزة المنظمة الدولية للشرطة الجنائية:

لقد مرت جهود المنظمة في هذا المجال بعد مراحل إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من: طوكيو، نيوزلندا، نيروبي، أذربيجان، بيونس إيرس لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك، ونظرا إلى تنوع أنظمة الدول المختلفة، فقد

[1]- ينظر: الموقع الإلكتروني: www.algérie police.dz تاريخ الإطلاع: 2016/05/05.

[2]-التعاون الشرطي في إطار هذه المنظمة يحكمه مبدأ احترام السيادة الوطنية للدول الأعضاء.

كان هناك خياران لأنظمة الاتصال،[1] داخل هذه الشبكة أولهما هو نموذج يخصص للدول المركزية وتجرى الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، والثاني للدول اللامركزية وتجري الاتصالات فيه مباشرة بين أجهزة الشرطة في الدول المختلفة، وعلى غرار هذه المنظمة، أنشأ المجلس الأوروبي لكسمبورغ عام 1991 شرطة أوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود، ومنها الجرائم المعلوماتية، أما على المستوى العربي فنجد أن مجلس وزراء الداخلية العرب انشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[2]

أ-تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث جسيمة مفاجئة بشكل لا يمكن توقعه أو يستحيل التنبؤ بتوقيت حدوثه، أو يصعب مواجهته بالإمكانات القومية للدولة المنكوبة بمفردها، ومع وقوع مثل هذه الكوارث غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتضافر الجهود الدولية، لا سيمل أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول متقدمة تقنيا وتكنولوجيا ولها صيت كبير في مواجهة الجرائم المعلوماتية والبعض الأخر يفتقد لذلك.[3]

---

[1]-Malcon Anderson, policing the word, interpol the politics of international police, Co, operation press, oxford, 1989, P168, 185.

[2]-نجاة بن مكي، المرجع السابق، ص 150.

[3]-حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، يُنظر الموقع الإلكتروني: .www.arb/aws.com

ب–القيام ببعض العمليات الشرطية والأمنية المشتركة:

تعقي مجرمي المعلوماتية عامة وشبكة الانترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شانها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم وبالتالي وضع حد لها.[1]

ولقد انضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية (إنتربول) أثناء انعقاد الجمعية العامة للإنتربول بهلسنكي/فنلندا خلال شهر أوت 1963 بمشاركة 53 بلد ممثلة بالمكتب المركزي الوطني، حيث يعمل هذا الأخير تحت الوصاية المباشرة لمديرية الشرطة القضائية/المديرية العامة للأمن الوطني ويباشر مهامه وفقا لنصوص التشريعات الوطنية، ملتزما بالأطر القانونية المسيرة للمنظمة الدولية للشرطة الجنائية، كما يجب على المكتب المركزي الوطني تسيير نشاطاته ضمن إستراتيجية واضحة ومحددة المعالم وفقا لما تقتضيه الاحتياجات الأمنية المسجلة على الصعيد الوطني، وضروري أن تكون في سياق الوظائف الأساسية المقررة من طرف المنظمة الدولية للشرطة الجنائية خدمات اتصالات شرطية عالمية مأمونة، خدمات بيانات ميدانية، وقواعد بيانات شرطية، خدمات إسناد شرطي، التدريب وإنماء القدرات الذهنية والنفسية لتلقي التدريب وتأهيل القائمين على جمع الاستدلالات والتحقيق الابتدائي، وتدريب القضاة على معالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية، وقد اتجهت بعض الدول مثل كندا سنة 1980 وفرنسا 1983 وإنجلترا 1987 وفنلندا 1990 إلى إعطاء دورات تدريبية لجهات الضبط القضائي عن كيفية التحقيق في الجرائم الإلكترونية، وكذا ينظم البوليس الدولي دورات تدريبية في مجال جرائم التوقيع

[1]–علاء الدين شحاتة، المرجع السابق، ص 116.

الإلكتروني من أجل تحسين أداء الأعضاء من رجال الشرطة في مجال الكشف عن الجريمة وجمع المعلومات ومتابعة الجناة وإقامة الدليل، إلا أن التدريب لا يقتصر على رجال الشرطة بل يمتد للخبراء القضائيين.[1]

ثانيا: مهام المكتب المركزي الوطني في المجال الشرطي.

ومن بين مهام المكتب المركزي الوطني في المجال الشرطي نذكر مايلي:

- مباشرة التحقيقات الدولية من وإلى خارج الوطن بالتنسيق مع المصالح الوطنية ونظيرتها الأجنبية.
- تقديم الدعم الفني والتقني إلى كافة الأجهزة والمصالح الوطنية المكلفة بإنقاذ القانون.
- التبادل السريع والآني للمعلومات الشرطية والجنائية ما بين المكاتب المركزية الوطنية بالتنسيق مع الأمانة العامة لمنظمة الإنتربول.
- إصدار نشرات البحث حول التحف الفنية محل السرقة بغية إجراء أعمال التحري والتحقيق قصد استرجاعها.
- تجميع المعلومات العملياتية، وتحليلها وتبليغها للتحري والاستغلال إلى المصالح الوطنية المختصة.
- البحث والتحري حول المركبات محل السرقة بغض وضع اليد عليها.
- ملاحقة المجرمين المبحوث عنهم دوليا، بغرض الإيقاف والتسليم.
- التقصي والتحري في جوازات السفر المزورة محل بحث دولي أو وطني.[2]

كما تم تدشين مقر آلية التعاون بين أجهزة الشرطة الإفريقية (أفريبول) يوم 2015/12/13 ببن عكنون (الجزائر العاصمة) ويرمي إنشاء هذه الآلية إلى التوصل إلى اعتماد رؤية شاملة تسمح

[1]-علاء الدين شحاتة، المرجع السابق، ص 117.

[2]-ينظر الموقع: www.arb/aws.com.

بتحسين فعالية ونجاعة مصالح الشرطة الإفريقية من خلال تدعيم القدرات التنظيمية والتقنية والعملياتية.[1]

الفرع الثاني: التعاون القضائي الدولي لمكافحة جرائم الاعتداء على الموقع الإلكتروني في مرحلتي التحقيق والمحاكمة.

تبقى إشكالية الاختصاص القضائي في الجرائم الإلكترونية تتشعب على عدة أووجه مما يخلق ضرورة حلها بما يحقق العدالة الجنائية، وتوقيع العقاب على الجناة والحد من إفلاتهم، وتحتوي العديد من الاتفاقيات الدولية والقوانين الجنائية الداخلية نصوص تشجع على المساعدة القضائية بين الدول، وتتخذ المساعدة القضائية في جرائم الاعتداء على التوقيع الإلكتروني صور متعددة تتعلق بحفظ البيانات والقدرة على النفاذ إلى البيانات المخزنة.

أولا: المساعدة القضائية الدولية في الكشف عن جرائم الاعتداء على التوقيع الإلكتروني.

إن المساعدة القضائية الدولية هي كل إجراء قضائي تقوم به دولة من شانها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم.[2]

ونصت العديد من الاتفاقيات على المساعدة القضائية، حيث ركزت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية المعتمدة من طرف الجمعية العامة للأمم المتحدة 2000/11/15 في المادة 18 على المساعدة القانونية المتبادلة، وفي المادة 19 على التحقيقات المشتركة بين الدول، وفي المادة 20 على أساليب التحري الخاصة لهذا النوع من الجرائم.[3]

[1]- ينظر الموقع: www.arb/aws.com.

[2]-محمد مدحت المراسى، أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة، مجلة مركز بحوث الشرطة، أكاديمية الشرطة، العدد22، سنة 2002، ص 127.

[3]-خالد ممدوح إبراهيم، المرجع السابق، ص 407.

كما نصت المادة 27 من اتفاقيات بودابيست بشأن جرائم الحاسب الآلي على أهمية المساعدة القضائية في بعض الإجراءات دون حاجة أن تكو الدولة طرفا في تلك المعاهدة،و كذا المادة 18 من اتفاقية باليرمو للجريمة المنظمة الوطنية 2000 على دول الأطراف أن تقدم كل منها للأخرى المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية.

1-بيانات طلب المساعدة القضائية:

يتضمن طلب المساعدة القضائية السلطة المقدمة الطلب وكذا موضوع وطبيعة التحقيق أو الملاحقة أو الإجراء القضائي الذي يتعلق به الطلب، واسم وظائف السلطة التي تتولى التحقيق أو الملاحقة أو الإجراء القضائي وملخصها للوقائع ذات الصلة بالموضع، باستثناء ما يتعلق بالطلبات المقدمة لغرض تبليغ مستندات قضائية وصف المساعدة الملتمسة وتفاصيل أي إجراءات معينة تود الدولة الطرف الطالبة إتباعها، وهوية أي شخص معني ومكانه وجنسيته حيثما أمكن ذلك، والغرض الذي تلتمس من أجله الأدلة أو المعلومات أو التدابير، وتقدم الطلبات كتابة أو حيث ما أمكن بلغة مقبولة لدى الدولة، ويتعين إبلا غ الأمين العام للأمم المتحدة باللغة المقبولة لدى الدولة الطرف وقت قيام كل دولة طرف بإيداع صك تصديقها على هذه الاتفاقية أو الانضمام إليها.[1]

فنجد المشرع الجزائري وفق كثرا في تسهيل قبول طلبات المساعدة القضائية باعتماد الطلب حتى وإن جاء عبر وسائل تكنولوجيا الإعلام والاتصال الحديثة، شرط التأكد من صحته، وهذا بسبب السرعة المتطلبة للبحث والتحري الإلكتروني ذات الطبيعة الخاصة وملاحقة المجرم الإلكتروني لضمان عدم إفلاته من العقاب.[2]

[1]-هيلالي عبد الله أحمد، المرجع السابق، ص 489.

[2]-المادة 36 من الأمر 05-06 المؤرخ في 2005/08/23 التعاون المعلوماتي على مراعاة مبدأ المعاملة بالمثل، توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا أو بالطريقة الإلكترونية إلى الجهات المختصة، وتكون مصحوبة بكل المعلومات الضرورية، إذا كان وجه الطلب إلكترونيا يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا.

وهذا ما يمكن لسلطات البحث والتحري الجزائرية بالتعاون مع السلطات الألمانية والولايات المتحدة الأمريكية بالجزائر ومكتب الإنتربول فرع بالجزائر، القبض على رأس الشبكة الإجرامية المختصة في القرصنة الإلكترونية، حيث قام ابن مدينة عنابة باختراق قاعدة بيانات متواجدة بمدينة ميونخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة بـ 1500بطاقة ائتمان باستعمال عنوان إلكتروني Adressip مما مكنه من تحويل ما قيمته 100.000دولار منذ2005 من حسابات زبائن البنك الكندي، حيث أدانت محكمة عنابة قسم الجنح الجاني بجنحة التصميم والإدخال عن طريق الغش لمعطيات المنظومة المعلوماتية، وكذا جنحة التقليد ومعاقبته عام حبسا نافذا وغرامة قدرها 500.000دج طبقا لنصوص المواد 394 مكرر 1 و394 مكرر2 من ق.ع.ج والمواد 151 و152 و153 من القانون رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة.[1]

2-القيود الواردة على طلبات المساعدة القضائية الدولية:

إن اللجوء إلى المساعدة القضائية الدولية ليست مطلقة وفق المشرع الجزائري، حيث نصت المادة 18 من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على رفض تنفيذ طلبات المساعدة إذا كان من شانها المساس بالسيادة الوطنية أو النظام العام، ويمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو شرط عدم استعمالها في غير م هو موضح في الطلب.[2]

كما ألزمت الاتفاقية الدولية الموضوعية لتوقيع الأمم المتحدة في نيويورك في 2005/09/14 والخاصة بقمع أعمال الإرهاب النووي للأطراف وفق نص المادة 7/ف2 باتخاذ

[1]-أنظر الحكم رقم 10/077357 الصادر عن محكمة عنابة قسم الجنح بتاريخ 2010/06/28.

[2]-المادة 18 من القانون 19-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

التدابير لحمية سرية المعلومات التي يحصل عليها سرا بموجب هذه الاتفاقية من دولة أخرى، [1] ونجد أيضا اتفاقية الأمم المتحدة لمكافحة التعاون الدولي UN في المادة 46/ف21 نصت على الحالات التي يجوز فيها رفض تقديم المساعدة القضائية المتبادلة وهي كالآتي:

- إذا رأت الدولة الطرف متلقية الطلب أن تنفيذ الطلب قد يمس بسيادتها وأمنها ونظامها العام ازو معالجتها الأساسية الأخرى.
- إذا كان القانون الداخلي للدولة الطرف متلقية الطلب يحظر على سلطاتها تنفيذ الإجراء المطلوب بشأن أي جرم مماثل.
- إذا كانت تلبية الطلب تتعارض مع النظام القانوني للدولة الطرف متلقية الطلب فيما يتعلق بالمساعدة القانونية المتبادلة.
- كما لا يجوز للدول الأطراف أن ترفض طلب مساعدة القانونية المتبادلة لجمر دان الجرم يعتبر أيضا متصلا بأمور مالية ويتعين إبداء باب الرفض، [2] وكما يجوز لدولة الطرف متلقية الطلب أن ترجئ المساعدة القانونية المتبادلة بسبب تعارضها مع التحقيقات والملاحقات أو الإجراءات القضائية الجارية.[3]

كما نصت المادة 26 من ذات الاتفاقية على أن قبل الرفض لأي طلب، أن تتشاور الدولة الطرف متلقية الطلب مع الدولة الطرف الطالبة النظر في إمكانية تقديم المساعدة رهنا بما تراه

[1]-المرسوم الرئاسي رقم 270/10 المؤرخ في 2010/11/10 يتضمن التصديق ويتحفظ على الاتفاقية الدولية لقمع أعمال الإرهاب المقترحة للتوقيع في مقر الأمم المتحدة بنيويورك في 2005/09/14، ج.ر، العدد 68 ، المؤرخة في 2010/11/10، ص06.

[2]-راجع في ذلك نص اتفاقية الأمم المتحدة لمكافحة الفساد UN التعاون الدولي المادة 23/46.

[3]-راجع في ذلك نص اتفاقية الأمم المتحدة لمكافحة الفساد UN التعاون الدولي المادة 26/46.

ضروريا من شروط وأحكام، فإذا قبلت الدولة الطرف الطالبة بتلك المساعدة مرهونة بتلك الشروط وجب عليها الامتثال لتلك الشروط.[1]

ثانيا: صور المساعدة القضائية الدولية.

يأخذ أسلوب المساعدة القضائية صورا متعددة تتعلق بتبادل المعلومات، وكذا نقل الإجراءات وإنابته القضائية، وهناك صور أخرى تتعلق بالمساعدة القضائية في مجال حفظ البيانات والقدرة على النفاذ إلى البيانات المخزنة، والمساعدة في مجال اعتراض البيانات الخاصة بمحتوى التوقيع الإلكتروني.

1-تبادل المعلومات في جرائم التوقيع الإلكتروني:

ويشمل تقديم المعلومات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، بصدد جريمة ماعدا الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم،[2] وهناك مظهر آخر للتبادل هو السوابق القضائية للجناة والتي تتعرف من خلالها على الماضي الجنائي، والتي تساعد في تشديد العقوبة في حالة العود، فنجد فرنسا مثلا لا تسمح بإعطاء صور ضوئية من صحف الحالة الجنائية إلا عن رعايا الدول التي تربط بها اتفاقيات تبادل المعلومات، كل ذلك يتم من خلال تعزيز الاتصال بين سلطات الدول وأجهزتها ودوائرها المختصة بمكافحة الجرائد الإلكترونية.[3]

ومن أجل تسيير تبادل المعلومات بصورة مأمونة وسريعة بشأن كل ما يتعلق بتلك الجرائم:

*هوية الأشخاص المشتبه فيهم في تلك الجرائم وأماكن وجودهم وأنشطتهم وأماكن الأشخاص الآخرين المعنيين.

[1]-راجع في ذلك نص اتفاقية الأمم المتحدة لمكافحة الفساد UN التعاون الدولي المادة 26/46.

[2]-المادة 05 من اتفاقية الرياض العربية للتعاون القضائي 1983.

[3]-المادة 05 من اتفاقية الرياض العربية للتعاون القضائي 1983.

*حركة عائدات الجرائم أو الممتلكات المتأتية من ارتكاب الجرائم.

*تبادل المعلومات عبر الوسائل والأساليب المحددة.

كما يمكن أن تقوم الجهة المختصة في دولة ما بإرسال إلى الجهة المختصة لدى دولة أخرى وهي بصدد النظر إلى جريمة ما بيانات عن الأحكام القضائية النهائية الصادرة ضد مواطنيها أو الأشخاص المولودين أو المقيمين في إقليمها.[1]

كما حرصت المادة 26 من اتفاقية بودابست على التأكيد على واجب الدولة التي تمتلك معلومات هامة مساعدة دولة أخرى في عرض التحقيقات، وتداول الدعاوى الجنائية أو الملاحقة في وجود هذه المعلومات، في هذه الحالة لا يقدم أي طلب بالمساعدة المتبادلة.[2]

كما تنص المادة 66 من قانون رومانيا 2004/203 على حق السلطات الرومانية المختصة في أن ترسل تلقائيا إلى السلطات الأجنبية المختصة المعلومات والبيانات الضرورية التي تسمح لهذه الأخيرة باكتشاف الجرائم المرتكبة بواسطة جهاز الحاسوب، أو يحل القضايا المتعلقة بتلك الجرائم.[3]

ونظرا لما تثيره مسألة المساعدة القضائية بين الدول من حساسية متعلقة بسيادة الدولة من جهة وبطبيعة جرائم الحاسوب م جهة أخرى، فنجد المشرع الجزائري وضع شروط المساعدة القضائية في نص المادة 17 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي تنص على أن تتم الاستجابة إلى طلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات للدولة ذات الصلة والاتفاقيات الدولية الثنائية، ومبدأ المعاملة بالمثل وهذا ما جاءت به أيضا المادة 04 من نفس القانون على أن تلتزم كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية تنفيذ

[1]-محمد كمال محمود الدوسقي، المرجع السابق، ص 148.

[2]-إيهاب محمد يوسف، المرجع السابق، ص 23.

[3]-Art 66 of Romaina law, N°161, 2003.

التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأ المساواة والسيادة الإقليمية للدول، وعدم التدخل في الشؤون الداخلية للدول الأخرى، فقد وضع المشرع الجزائري هذه الشروط طبقا لمبدأ المعاملة بالمثل واحتراما للسيادة الوطنية، وأيضا حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، نظرا لما تمثله هذه المعلومات من خطورة على سلامة الشخص أولا، ثم على الدولة ثانيا.[1]

2-نقل الإجراءات في جرائم التوقيع الإلكتروني:

ويقصد بها قيام دولة ما بناء على اتفاقية أو معاهدة اتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة حتى توافر ت شروط معينة، [2] من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخصية في الدولة الطالبة والدولة المطلوبة إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

إلا أن الاعتماد على الآليات التقليدية للتعاون عند تقديم الطلب بالطريق الدبلوماسي تجعلها تتسم بالبطء، وهو ما يتعارض مع طبيعة جرائم التوقيع الإلكتروني، وتطبيقا لذلك أبرمت اتفاقيات جديدة لتقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق مثل: الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال.

[1]-يزيد بوحليط، المرجع السابق، ص 516-517.

[2]-سالم محمد سليمان الأوحلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، مصر، 1998، ص 428.

3-الإنابة القضائية في جرائم التوقيع الإلكتروني:

يقصد بالإنابة القضائية هي طلب اتخاذ إجراء قضائي م إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة للدولة المطلوبة للقيام من إقليمها نيابة عنها بإجراء قضائي يتعلق بدعوى ناشئة عن جريمة دولية معلوماتية للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويقدر عليها القيام به بنفسها.[1]

فالإنابة القضائية تسهل إذن الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارستها بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود أو إجراء التفتيش والمعاينات، وتنفيذ التفتيش والحجز وغيرها.[2]

ومن بين الاتفاقيات التي أبرمت في مجال الإنابة القضائية، تلك التي أبرمت بين فرنسا والجزائر سنة 1962، ومع ألمانيا 1984، ومع مصر 1982، والاتفاقية الأوروبية للتعاون القضائي في المواد الجنائية 1962، وجمهورية مصر العربية مع الكويت 1988، وبين دول الجامعة العربية 1953 ووافقت عليها مصر بالقانون رقم 1954/30، والاتفاقية الخاصة بالتعاون القضائي في المواد الجنائية مع المملكة المغربية 1989 واتفاقية التعاون القضائي مع البحرين.

4-حفظ البيانات المخزنة:

تتخذ المساعدة القضائية صورا متعددة تتعلق بحفظ البيانات المخزنة في أجهزة الحاسب الآلي، وهذا ما تناولته المادة 29 من اتفاقية بودابست التي تنص على أنه: "يجوز لأي طرف أن

[1]-حازم الحارون، الإنابة القضائية الدولية، المجلة الجنائية القومية ، القاهرة، دورة ثالثة، ص 20، عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2000، ص 12.

[2]-فهد عبد الله العبيد الحازمي، المرجع السابق، ص 494.

يطالب الطرف الآخر أن يأمر ليحافظ على البيانات المخزنة بواسطة نظام كمبيوتر يقع داخل إقليم ذلك الطرف الآخر...".[1]

كما حددت هذه الاتفاقية الفترة اللازمة للتحفظ على البيانات وهي مدة 60 يوما على الأقل، وإذا تبين للسلطات الدولية المطلوب إليها حفظ البيانات قد يتخذ إجراءات من شانها تهديد السرية أو عرقلة التحقيق الذي تجريه الدولة الطالبة، فعليها أن تبلغها بذلك على وجه، ومن مميزات هذا الإجراء أنه سريع ويكفل حماية سرية البيانات التي تهم الشخص المعني.[2]

[1]-ينظر المادة 29 من اتفاقية بودابست.

[2]-أيمن رمضان محمد أحمد، المرجع السابق، ص 437.

خاتمة

خاتمة:

من خلال تناولنا لموضوع الحماية القانونية للتوقيع الإلكتروني سواء من جانبه الموضوعي أو الشكلي، وبينا موقف المشرع الجزائري، ثم تناولنا مدى ملاءمة القواعد الإجرائية التقليدية لضبط الجاني في تلك الجرائم ومحاكمته، وكذلك التعاون الدولي سواء في مرحلة البحث والحقيق الأولي أو في مرحلة المحاكمة، ففي ضوء هذه الدراسة نلخص النتائج التالية:

*/بخصوص تعريف التوقيع الإلكتروني فإن معظم التشريعات الدولية والعربية متفقة إلى حد ما، إلى أن التوقيع الإلكتروني يتخذ شكل معلومات إلكترونية يتم إجراؤه من خلال التقنية الإلكترونية، ويتخذ أشكالا وصورا وقد تكون على شكل حروف أو أرقام أو رموز.

*/كما أن للتوقيع وظيفتين أساسيتين الأولى تكمن في تحديد الموقع، والثانية في صحة المعلومات الصادرة عنه، لكن المشرع الجزائري أحاط شروط قانونية أخرى، وهي ضرورة الاعتراف به حتى يرتب الآثار القانونية التي يرتبها التوقيع اليدوي، أولهما استعمال منظومة موثوق بها، وثانيها أن تتضمن تلك المنظومة الصلة بين التوقيع الإلكتروني والموقع.

*/ومن شروط صحة التوقيع الإلكتروني هو الرجوع إليه عند الحاجة، ولكن المشرع الجزائري لم ينص على ذلك، كما يجب أن يكون هذا الإطلاع مضمونا طوال مدة صلاحية محتوى التوقيع الإلكتروني، ولضمان توفر كل هذه الشروط يجب اعتماد آليات تحقق هذا الحفاظ الذي يكون في الغالب محفوظا على الحامل الإلكتروني، وهذه العبارة الأخيرة لم يعرفها المشرع الجزائري ويستحسن أن يقوم بذلك.

*/قام المشرع الجزائري على صعيد التجريم والعقاب على تجريم الاعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة باستعمال تكنولوجيا الإعلام والاتصال، مثل جرائم الإهانة أو السب أو القذف باستعمال الوسائل الإلكترونية، وعموما بأي وسيلة إلكترونية توفرها التقنية

الحديثة بموجب المواد 144 مكرر و 144 مكرر2 والمادة 146 من قانون العقوبات والمواد 303 مكرر و 303 مكرر3 من نفس القانون.

*/وفي نفس الشأن قام المشرع بتعديل قانون العقوبات مرة أخرى بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004، بالإضافة إلى القسم السابع مكرر عنوانه جرائم المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر و 394 مكرر7 مثل جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وجريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات وغريها، كما اتجه المشرع إلى تجريم بعض أشكال الجرائم الإلكترونية بموجب بعض القوانين الخاصة، كقانون البريد والمواصلات السلكية واللاسلكية، وإصدار القانون رقم 15-04 المؤرخ في 2015/02/01 المتعلق بالتوقيع والتصديق الإلكترونيين الذي جرم كافة الاعتداءات التي تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول والبقاء غير المصرح بهما مما يلزم الرجوع غلى القواعد العامة المدرجة في قانون العقوبات والتي يعاب عليها لأنها لم تتناول التزوير المعلوماتي وفقا للقانون 23/06 بالرغم من أهميته في التوقيع الإلكتروني.

*/كما اقتصر المشرع الجزائري على الحماية المقررة في مواجهة مؤدي خدمات التصديق في حالة الإخلال بالتزاماتهم، وكذا طالبي الخدمة، في حين أن التحايل الإلكتروني قد يقع من عدة أطراف كالقراصنة مثلا، مما يتعين على المشرع الجنائي مواجهة جميع صور التحايل لأجل حماية كافة المصالح المعتدى عليها.

*/انتهج المشرع الجزائري قانون خاص ومستقل بعدما كان تنظيمه ضمن القواعد العامة لقانون العقوبات بسنه للقانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، إلا أن المشرع الجزائري لم يتمكن من خلال هذا القانون من وضع وسائل الحماية الجنائية لجميع صور الاعتداء، على غرار الجرائم المتعلقة بالاحتيال، التزوير، الدخول والبقاء غير المصرح به، مما يستدعي مرة أخرى للرجوع للقواعد العامة.

*/بالنسبة للضبط القضائي بشان جرائم التوقيع الإلكتروني، فإنه يتبع نفس الإجراءات التي يتبعها بشان الجرائم التقليدية سواء في الظروف العادية أو الاستثنائية، وهذا ما يتلاءم وطبيعة وخصوصية هذه الجرائم.

*/إن تخطي جرائم التوقيع الإلكتروني حدود الدول أفرز مجموعة من التحديات، تجسدت في صعوبات إثبات هذه الجرائم وقبول الدليل باعتبارها لا تترك أثر مادي ملموس كما هو الحال في الجرائم التقليدية، فضلا عما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة الإجراءات عبر الحدود كالمعاينة والتفتيش في نطاق البيئة الافتراضية.

*/لا يجوز امتداد التفتيش في الوسط الافتراضي خارج حدود الدولة احتراما لمبدأ السيادة، ومع ذلك يجوز الحصول على أدلة خارج حدود الدولة تطبيقا لاتفاقيات الإنابة القضائية وفقا لنظام تبادل المساعدات، وبالتالي لابد من التعاون الدولي في هذا المجال باتفاقية ثنائية أو متعددة الأطراف، أو الحصول على إذن الدولة التي يتم التفتيش في مجالها الإقليمي.

*/ينطوي الضبط القضائي في جرائم التوقيع الإلكتروني على تحديات ومشاكل كثيرة أهمها الحاجة إلى سرعة الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش والضبط لملاءمة هذه الجرائم ومشكلا الاختصاص القضائي والقانون الواجب التطبيق، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والماحقة خارج الحدود.

في ضوء هذه النتائج التي توصلت إليها هذه الدراسة يمكن أن تقدم الاقتراحات الآتية:

*/إن قانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني لم يتناول كافة الاعتداءات التي قد تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول والبقاء غير المصرح بهما.

*/يتعين على المشرع الجنائي مواجهة جميع صور التحايل لأجل حماية كافة المصالح المعتدى عليها.

*/ضرورة النص عنى تجريم أو الحصول على برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني كما هو الحال في التشريعات الأخرى.

*/تجريم محاولة الحصول على توقيع أو محرر إلكتروني بنص خاص.

*/بخصوص التحايل الإلكتروني من الأفضل إضافة المشرع الجزائري عبارة أي طرف آخر، كون أن التحايل قد يقع أيضا من طرف القراصنة.

*/وجوب تنظيم المشرع الجزائري للتصديق الإلكتروني سواء كان م جهة وطنية أو من جهة أجنبية، وتحديد هيكل قانوني يحدد القواعد الملائمة فيما يخص المعايير التي ينبغي أن يستوفيها، أو القواعد التي تحكمه لضمان أمن وسلامة المعاملات الإلكترونية.

*/ضرورة أن تعمل الجزائر على استحداث أقسام متطورة داخل أجهزة العدالة تعنى بمكافحة جرائم التوقيع الإلكتروني، والتي من أهم سماتها صعوبة اكتشافها وكذا ضبطها.

*/على المشرع الجزائري إدراج نصوص إجرائية في القانون 15-04 من حيث إجراءات البحث والتحري إلى غاية المحاكمة.

*/ضرورة التعاون الإقليمي والدولي في مجال مكافحة جرائم الاعتداء على التوقيع الإلكتروني عبر شبكة الانترنت، والسعي نحو إيجاد إطار قانوني للتعاون بين أجهزة الشرطة والنيابات العامة العربية والأجنبية والأجهزة المساعدة لها للعمل على ضبط مرتكبي هذه الجرائم وملاحقتهم بالتسليم والمساعدة والإنابة القضائية.

قائمة المصادر والمراجع

قائمة المراجع

أولا: النصوص التشريعية والتنظيمية.

أ-الإتفاقيات والمعاهدات الدولية:

1-الاتفاقيات الخاصة بتسليم المجرمين، نجد اتفاقية بين مصر واليونان 1986، اتفاقية بين الجزائر وبلجيكا 1970، اتفاقية التعاون القضائي وتسليم المجرمين مع بولندا في 1993، اتفاقية بين المغرب واسبانيا 1999.

2-اتفاقية الأمم المتحدة لمكافحة الفساد UN التعاون الدولي المادة 23/46.

3-الاتفاقية الأمنية الخليجية 1994 والمادة 12 من اتفاقية جامعة الدول العربية لتسليم المجرمين 1953.

4-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في 2010/12/21.

5-التعاون الشرطي في إطار هذه المنظمة يحكمه مبدأ احترام السيادة الوطنية للدول الأعضاء.

6-التوجيه الأوروبي الصادر في 13-12-1999 بشأن التوقيعات الإلكترونية.

ب-النصوص التشريعية:

1-الأمر 66-155 المؤرخ في 23 يونيو 1966 المتضمن من ق.إ.ج.ج. المعدل والمتمم بالقانون 07/17 المؤرخ في 27 مارس 2017.

2-الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات الجزائري، المعدل بالقانون رقم 16-02، المؤرخ في 19 يونيو 1916.

3-الأمر 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني الجزائري المعدل والمتمم بموجب القانون 07-05 المؤرخ في 13 مايو 2007.

4-الأمر رقم 10/95 المؤرخ في 1995/02/25، الجريدة الرسمية، العدد11.

5-القانون 19-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

6-القانون رقم 09-04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج، العدد07، المؤرخة في 2009/08/16.

القانون رقم 15-04 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بجمهورية مصر العربية.

7-القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ج ر .رقم 06 المؤرخة في 2015/02/10.

8-القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق لـ 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

9-القانون رقم 15-04 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين المؤرخ في 01-02-2015، الجريدة الرسمية للجمهورية الجزائرية، العدد06.

10-قانون الإجراءات الجزائية الجزائري، المحدد بالأمر 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم.

11-قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

12-قانون التوقيع الإلكتروني المصري رقم 83 لسنة 2015.

ج-النصوص التنظيمية:

1-المرسوم الرئاسي رقم 04-432 المؤرخ في 2004/12/29 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي.

2-المرسوم الرئاسي رقم 270/10 المؤرخ في 2010/11/10 يتضمن التصديق ويتحفظ على الاتفاقية الدولية لقمع أعمال الإرهاب المقترحة للتوقيع في مقر الأمم المتحدة بنيويورك في 2005/09/14، ج.ر، العدد68 ، المؤرخة في 2010/11/10.

3-المرسوم الرئاسي رقم 183-04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانون الأساسي رقم 41 المؤرخ في 2004/06/27.

4-المرسوم التنفيذي المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق رقم 63 المؤرخة في 2006/10/08.

5-المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى خدمة المواصلات السلكية واللاسلكية.

6-المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 الصادر في 2001/05/09 يمينة حوحو، عقد البيع الإلكتروني "دراسة مقارنة"، أطروحة دكتوراه، جامعة بن عكنون، الجزائر، 2012.

7-المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09/05/ 2001.

8-المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30.

9-اللائحة التنفيذية المخصصة للتعريفات، منظومة تكوين بيانات إنشاء التوقيع الإلكتروني حسام محمد نبيل الشنراقي، الجرائم المعلوماتية "دراسة مقارنة على جرائم الاعتداء على التوقيع الإلكتروني"، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2013.

10-اللائحة التنفيذية لقانون التوقيع المصري 15-04 الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات الصادر بموجب القرار رقم 109-05 وقد نشرت هذه اللائحة في جريدة الوقائع المصرية، العدد115 الصادر في 2005/05/25.

ثانيا: الكتب.

1-أحمد حزيط، الوجيز في الإجراءات الجزائية، دار هومة، الجزائر، ط2 منقحة، 2015.

2-أحمد عصام عجيلة، الحماية الجنائية للمحررات الإلكترونية، دار النهضة العربية، القاهرة، 2014.

3-أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، ط2، 2006.

4-إزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2016.

5-أمحمدي بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لقانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، 2016.

6-أمير فرج يوسف، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008.

7-أيمن سعد سليم، التوقيع الإلكتروني "دراسة مقارنة"، دار النهضة العربية، القاهرة، مصر، 2004.

8-ثروت عبد الحميد، التوقيع الإلكتروني "ماهيته-مخاطره-كيفية مواجهته- ومدى حجيته في الإثبات"، دار النهضة العربية، القاهرة، مصر، 2002.

9-حسام محمد نبيل الشراقي، جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013.

10-حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الأنترنت، دار النهضة العربية، القاهرة، ط1، 1998.

11-خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، مصر، ط1، 2006.

12-خالد ممدوح إبراهيم، التوقيع الإلكتروني، الدار الجامعية، الإسكندرية، مصر، ط1، 2000.

13-دلخار صلاح الدين بوكاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2016.

14-راشد بن حمد البلوشي، التوقيع الإلكتروني والحماية الجزائية المقررة له "دراسة في القانون العماني والقانون المقارن"، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2018.

15-سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، مصر، 2008.

16-طعباش أمينة، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2012.

17-عابد فايد عبد الفتاح فايد، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني "دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني"، دار الجامعة الجديدة، الإسكندرية، 2004.

18-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010.

19-عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2000.

20-عبد القادر عدو، الجريمة الإلكترونية إجرائيا، دار هومة، الجزائر، ط2، 2016.

21-علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، دراسة الإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إشراك للنشر والتوزيع، مصر، ط1، 2000.

22-علي عبد القادر القهوجي، الحماية الجنائية للحاسب الآلي، دار الجامع للطباعة والنشر، الإسكندرية، 2004.

23-عمر بن يونس، الجرائم في استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، القاهرة، مصر، 2004.

24-عيسى غسان ريضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ط1، 2005.

25-فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2016.

26-فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2005.

27-محمد المرسي زهرة، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، ط1، 1995.

28-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

29-محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، مصر، 2010.

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

31-مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001.

32-نادية ياس البياتي، التوقيع الإلكتروني عبر الأنترنت ومدى حجيته في الإثبات، دار البداية ناشرون وموزعون، الأردن، ط1، 2014.

33-ناصر جوادي، إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، دار العلوم، الجزائر، ط3، 2011.

34-نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية "دراسة نظرية وتطبيقية"، دار النهضة العربية، القاهرة، 2003.

35-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسية مقارنة، دار الفكر الجامعي، الإسكندرية، ط1، 2006.

36-نجوى أبو هيبة وآخرون، مبادئ القانون، نظرية القانون، دار الفكر العربي، بيروت، د س ن.

37-نهلا عبد القادر الموسني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط1، 2008.

38-هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992.

39-يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

40-يوسف بن سعيد الكلياني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري، دار النهضة العربية، مصر، ط1، 2017.

ثالثا: الأطروحات والرسائل الجامعية.

1-أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2010.

2-حنان براهيمي، جريمة التزوير تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة ، 2015.

3-سالم محمد سليمان الأوحلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، مصر، 1998.

4-سماح مقران، التوقيع الإلكتروني ودوره في عصرنة الإدارة الإلكترونية، أطروحة دكتوراه، جامعة قاصدي مرباح، ورقلة، 2013/2012.

5-صالح شنين، الحماية الجنائية للتجارة الإلكترونية "دراسة مقارنة"، رسالة دكتوراه، جامعة تلمسان، 2013.

6-عباس حفصي، جرائم التزوير الإلكتروني "دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، جامعة أحمد بن بلة، وهران، 2015.

7-يوسف زروق، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه، جامعة تلمسان، 2013.

8-عايض راشد المرعي، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه جامعة القاهرة، 1998.

9-إياد محمد عارف عطا سده، مدى حجية المحررات الإلكترونية في الإثبات، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2009.

10-إيمان العاني، البنوك التجارية وتحديات التجارة الإلكترونية، رسالة ماجستير، جامعة منتوري، قسنطينة، 2007.

11-خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، رسالة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

12-محمد هشام صالح عبد الفتاح، جريمة الاحتيال دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، نابلس، فلسطين،2008.

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

14-ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في القانون الجنائي الأعمال، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، 2015/2014.

15-غرداين حسام، الجريمة الإلكترونية وإجراءات التصدي لها، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، جامعة الجزائر، 2015/2014.

16-معمش زهية، غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق، جامعة عبد الرحمن ميرة، بجاية، 2012/2011.

17-نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور، خنشلة، 2013/2012.

رابعا: المقالات والمجلات العلمية.

1-أسامة بن غانم العبيدي، حجية التوقيع الإلكتروني، المجلة العربية للدراسات الأمنية والتدريب، مجلد28، العدد 56، جامعة نايف للعلوم الأمنية، 2012.

2-حازم الحارون، الإنابة القضائية الدولية، المجلة الجنائية القومية ، القاهرة، دورة ثالثة ،حسين جفالي، الحماية الجنائية لتوقيع المستهلك الإلكتروني في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 03، المجلد01، كلية الحقوق والعلوم السياسية، جامعة عمار خليجي.

3-رقية عواشرية، نظام تسليم المجرمين ودوره في تحقيق التعاون الدولي لمكافحة الجريمة المنظمة، مجلة المفكر، جامعة محمد خيضر، بسكرة، العدد04، 2008.

4-عزيزة لرقط، الجماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي، تمنراست، العدد01، جانفي 2017.

5-محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع، مجلة القانون والاقتصاد، العدد 51، 1991.

6-محمد مدحت المراسى، أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة، مجلة مركز بحوث الشرطة، أكاديمية الشرطة، العدد22، سنة 2002.

سادسا: الأحكام والقرارات القضائية.

1-الحكم رقم 10/077357 الصادر عن محكمة عنابة قسم الجنح بتاريخ 2010/06/28.

2-محكمة النقض المصرية، النقض المدنين جلسة 05 يونيو 2001، الطعن رقم 564 المشار إليه في المحاماة، العدد02، 2002.

سابعا: المراجع باللغة الأجنبية

1- A/CN9/426-14JUNE , 1996.

2-Art 66 of Romaina law, N°161.

3-Christiane féralschuhl , cyber droit, le droit à l'épreuve de l'internet, édition dalloz, 2009Alain 96-Bensoussan, Internet aspect juridique, Herses Paris, France, 2eme édition, 1998

4-Digital signature Guide lines, American Bar Association, NSA, 1996.

5-E.caprioli, collage de dtrasbaurg , sur le commerce électronique, 1999.

6-Lecleccq Jean, La signature electronique, lectur critique, technique et juridique, le décret du 30 mars 2001 relatif a la signature.

7-Malcon Anderson, policing the word, interpol the politics of international police, Co, operation press, oxford, 1989.

8-Mustapha Hashen sherif, protocols for secure électronic commerce.

المواقع الإلكترونية:

1-http://www.arab league online.org .

2-www.arb/aws.com.

3-www.algérie police.dz .

4-http://www.arab league online.org .

5-http// :www.djazzairess.com/alkhabar

فهرس الموضوعات

فهرس الموضوعات