جامـــــــــعة وهـــران 2

كلية الحقوق والعلوم السيـــاسية

أطروحـــــــة

للحصول على شهـــــادة دكتوراه "ل.م.د"

في العلوم الجنائية

الحماية الجزائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري

مقدمة ومناقشة علنا من طرف

السيد(ة): صحراوي مصطفى

أمام لجنـــــــة المناقشـــــــة

اللقب والاسم	الرتبـــــة	المؤسسة الأصلـــية	الصـــــفة
مروان مُحَمَّد	أستاذ	جامعة وهـــران 2	رئيـــــسا
برابح مُحَمَّد	أستاذ محاضر –أ–	جامعة وهـــران 2	مشرفا مقـــــررا
حريز أسماء	أستاذ محاضر –أ–	جامعة وهـــران 2	منـــاقشا
بن سهلة بن علي	أستاذ	جامعة تلمسان	منـــاقشا
مزيان مُحَمَّد أمين	أستاذ	جامعة مستغانم	منـــاقشا

السـنة: 2020-2021

« Protection pénale de la signature et de certification électroniques dans la législation algérienne »

Résumé :

La recherche étudie et analyse la protection pénale que le législateur algérien à accorder au dispositif de signature et de certification électroniques à commencer par l'aspect objectif qui traite de la définition des mécanismes de signature et de certification électroniques et leur nature juridique ainsi que l'intérêt protégé juridiquement à travers les différentes applications de ces deux mécanismes. Nous citons à titre d'exemple : l'administration électronique, le commerce électronique, la protection du consommateur et la protection des données à caractère personnel.

Les exemples de crimes commis à l'égard des mécanismes de signature et de certification électroniques ont été également la loi15-04 délimitant les règles générales concernant la signature et la certification électroniques en cadrant ce moyen important d'opération électroniques de pénalités judiciaires, financières et administratives. En outre, la recherche a traité les aspects procéduraux concernant la détection de ce genre, tout neuf, de crimes et la collaboration juridique international dans ce sens, en arrivant finalement à la déduction des résultats et des observations autour du degré d'efficacité de la politique pénale poursuivie localement et mondialement pour la lutte contre les agressions criminelles à l'égard et la signature et de la certification électroniques.

L'étude s'est basée sur la démarche analytique à savoir l'analyse du contenu des textes juridiques comportant les crimes à l'égard de la signature électroniques et l'attestation de la certification électronique faisant objet de notre étude, et l'inférence des jugements qui s'y rapportent.

La démarche comparative a été utilisée également dans quelques sujets a fin de connaitre la position du législateur algérien en comparaison avec les autres législation et la découverte des expérience des autres pays ainsi que la compréhension des textes juridiques et la conception de quelques propositions à propos de la réforme et l'ajustement des législations en cours.

Mots clés : la signature électronique, la certification électronique, dispositif de création de la signature électronique, cryptographie, confidentialité des informations.

« penal protection for electronic signature and certification in Algerian legislation»

Abstract :

The research dealt by both studying and analysing the disciplinary protection that the Algerian legalization have already added to the electronic electronic signature and certification system , starting with the objective aspect that dealt with the definition of the electronic signature and certification mechanism and its legal essence. The legally protected service in different applications of both mechanisms such as: electronic administration, electronic trade, consumer protection, and protecting personalized data.

It was able to recognize the different types of crimes committed on both mechanisms, signature and certification within penal codes and some other electronic codes particularly the code 15-04 that determines general rule concerned with electronic signature and certification. This effective way has already caught up legal, financial and administrative penalties. The research also dealt with procedural aspect concerned with showing developed type of crimes and the international judicial cooperation in this context. By the end, it leads to conduct the results as well as observation about how useful is the followed criminal policy locally and globally to fight criminal attacks committed on the electronic signature and certification.

This study used an analytical method in analysing the content of legal texts that include crimes committed on electronic signature and certification that are objects of study and their related judgments.

It also used the comparing method in some cases to know the attitude of the Algerian lawmaker compared with other lawmaking and recognize the different experience of other countries understanding legal texts and thinking about suggestions for reforming and modifying the existed legislation.

Key words: Electronic signature, Electronic certification, Establishing electronic signature dispositive ,cryptography, Data confidentiality.

" **الحماية الجزائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري** "

الملخص**:**

تناول البحث بالدراسة والتحليل الحماية الجزائية التي أضفاها المشرع الجزائري على منظومة التوقيع والتصديق الالكترونيين، بداية بالجانب الموضوعي الذي عالج التعريف بآليتي التوقيع والتصديق الالكترونيين وطبيعتهما القانونية، والمصلحة المحمية جزائيا في مختلف تطبيقات هاتين الآليتين، نذكر على سبيل المثال: الإدارة الالكترونية، والتجارة الالكترونية، وحماية المستهلك، وحماية المعطيات ذات الطابع الشخصي.

كما تم التعرف على صور الجرائم الواقعة على آليتي التوقيع والتصديق الالكترونيين ضمن قانون العقوبات وبعض القوانين الخاصة لاسيما القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين حيث أحاط هذه الوسيلة الهامة في التعاملات الالكترونية بعقوبات جزائية ومالية وإدارية ، كما عالج البحث الجوانب الإجرائية المتعلقة بالكشف عن هذا النوع المستحدث من الجرائم، وكذا التعاون القضائي الدولي في هذا الشأن، وصولا في الاخير إلى استخلاص النتائج والملاحظات حول مدى نجاعة السياسة الجنائية المنتهجة محليا وعالميا لمكافحة الاعتداءات الإجرامية الواقعة على التوقيع والتصديق الالكترونيين.

إعتمدت الدراسة على المنهج التحليلي المتمثل في تحليل مضمون النصوص القانونية المتضمنة الجرائم الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني محل الدراسة واستنباط الأحكام المتعلقة بها.

كما تم إستخدام المنهج المقارن في بعض المسائل، لمعرفة موقف المشرع الجزائري مقارنة مع باقي التشريعات، والاطلاع على تجارب الدول المختلفة، وفهم النصوص القانونية وتصور الاقتراحات حول إصلاح وتعديل التشريعات القائمة.

كلمات مفتاحية: التوقيع الإلكتروني، التصديق الإلكتروني، آلية انشاء التوقيع الإلكتروني، التشفير، سرية المعلومات.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

"...رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ"

صدق الله العظيم

(سورة الأحقاف- الآية 15)

شكر وتقدير

في هذا المقام لا يسعني إلا أن أتقدم بجزيل الشكر والعرفان إلى الأستاذ الفاضل "برابح محمد" لما كان له من سعة صدر وحرص تام في سبيل إنجاز هذه الأطروحة،

كما أتقدم بالشكر الجزيل إلى كل أعضاء لجنة المناقشة على قبولهم مناقشة هذه الأطروحة وعلى ما بذلوه من وقت وجهد وملاحظات قيمة،

إلى كل من قدم لي يد العون المساعدة، ولو بالدعاء

لإنجاز هذا العمل المتواضع،

فجزآهم الله عني خيراً.

إهداء

إلى روح أبي وروح أخي اللذان أدعو الله أن يسكنهما فسيح جناته.

إلى أمي أطال الله في عمرها، رمز العطاء والتضحية،

إلى زوجتي، وفلذات كبدي... يسرى أسماء محمد رفيق وعبد الحميد.

إلى أخواتي وكل أفراد عائلتي

أهديكم جميعا ثمرة هذا العمل

قائمة المختصرات:

ق.ع = قانون العقوبات

ق.إ.ج = قانون الإجراءات الجزائية

ق.ع.ف = قانون العقوبات الفرنسي

ق.إ.ج.ف = قانون الإجراءات الجزائية الفرنسي

ق.ع.م = قانون العقوبات المصري

ص = صفحة

ف = فقرة

(إ.ع.م.ج.ت.م) = الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

إ.أ.م.إ.م = الإتفاقية الأوروبية لمكافحة الإجرام المعلوماتي

ج.ر = الجريدة الرسمية

C.P.F = Code Pénal Français

C.P.P.F = Code Pénal de Procédure Pénale Français

U.S.C = United State Code

D = Dalloz

Cass = Cour de Cassation

R.S.C = Revue de Science Criminelles

مقدمة

يمر العالم بمرحلة تحول هائلة نحو التعامل الإلكتروني كبديل عن التعامل الورقي، ظهرت ملامحها من خلال الإقحام المتزايد للتكنولوجيات الحديثة للإعلام والإتصال في جميع المجالات الحيوية داخل الدولة كان من أهمها قطاعي الإدارة والإقتصاد.

وقد أفرز الواقع العلمي أنماطا وأشكالا غير تقليدية في مجال الإتصالات وتبادل المعلومات وإجراء المعاملات بين الأفراد أيا كان موقعهم، وأصبح إنتقال المعلومات يتم عبر وسائط إلكترونية تستخدم فيها إلى جانب الحواسيب شبكة معلومات آلية دولية تربط بين الشبكة المحلية والموسعة، أو ما يعرف بشبكة الأنترنت.

ورغم ما توفره خدمة الأنترنت من إمكانات كبيرة في مجال المعاملات الإلكترونية وإتمام التعاقدات، إلا أنها أفرزت العديد من المشكلات القانونية، لعل من أهمها التوقيع عن بعد أي عبر الأنترنت، وتتطلب جميعها توفير حماية للبيانات المتداولة أي حماية القانون للمعاملات التي تتم على شبكة الإتصالات الحديثة، مما إستدعى إستبدال الأوراق التقليدية بدعامات غير ورقية أتاحت الفرصة للإنفتاح أكثر على التبادل التجاري والعلاقات الإقتصادية بين الدول ليصبح عرض المنتجات والسلع والخدمات وإتمام الصفقات وإبرام العقود لا يحتاج إلى إنتقال المتعاقدين وإلتقائهما في مكان معين .

وكان من الطبيعي أن يصاحب هذه التطورات السريعة ظهور وسائل جديدة ومبتكرة تتناسب مع طبيعة التعاملات التي تجري عبر وسائط إلكترونية فظهر التوقيع الإلكتروني كبديل للتوقيع الكتابي التقليدي، وإنتشرت المحررات الإلكترونية كبديل للمحررات التقليدية المادية، لتشمل معظم القطاعات كالإتصالات والبنوك والإدارات والتجارة الداخلية والخارجية.

ولا شك أن إبرام هذه التعاقدات في فضاء إلكتروني يحتاج إلى إثبات إلكتروني يضفي عليه صفة التصرف القانوني الذي يخلو من الدعامة المادية ليتحول إلى مجرد بيانات رقمية مشفرة تسمى بالتوقيع الإلكتروني، الأمر الذي دفع من جهة أولى إلى إيجاد مفهوم جديد للكتابة في الفضاء الإلكتروني وظهرت بذلك الكتابة الإلكترونية مصحوبة بالتوقيع الإلكتروني، ومن جهة ثانية مواجهة المخاطر التي قد تواجه هذه الآلية أي آلية التوقيع الإلكتروني.

ومع دخوله حيز الخدمة وتعدد إستعمالاته تعددت كذلك تسمياته، إلا أن غالبية الفقه أجمعت على تسميته بالتوقيع الإلكتروني من منطلق إعتماده على الوسائل التكنولوجية التي تترجم الرسائل الإلكترونية إلى لغة يفهمها القارئ ويتعامل معها رجال القانون في مختلف المجالات، في حين أطلق عليه جانب آخر تسمية التوقيع الإجرائي[1]، بالنظر إلى الإجراءات المتبعة في إنشاءه وآليات حمايته وكونه العنصر المكمل للكتابة الإلكترونية.

وتعتبر الثقة والأمان من أهم الركائز في مجال التعاملات الإلكترونية، خاصة وأن المتعاقدين لا يجمعهما مجلس عقد واحد، وقد يتم التعاقد بين متعاملين لا يعرفون بعضهم البعض، وعلى أساس ذلك كان من الضروري إحاطة هذه التعاملات بنوع من الحماية لضمان توثيق هوية المتعاقدين والغرض من التعامل، والحفاظ على صحة البيانات وسلامتها، وضمان سرية تداولها بإعتبارها معطيات ذات طابع شخصي .

أمام هذا الوضع، سعت التشريعات جاهدة إلى إقرار قواعد تنظيمية خاصة يتم من خلالها وضع معايير تقنية توضح كيفية إثبات صحة وحجية التوقيع الإلكتروني، خصوصا ما تعلق بالدليل الإلكتروني، وتأمين المعلومات والمصادقة الإلكترونية، وينظم التدابير الوقائية المعتمدة على التشفير لإسباغ الحماية التقنية عليه.

لذلك بادر المشرع الجزائري بإصدار القانون رقم 04/15 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[2]، قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي تسمح بإحداث جو من الثقة، وصولا إلى تعميم وتطوير المبادلات الإلكترونية وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في الجزائر، كما يسمح هذا الإطار القانوني لعدة قطاعات، من بينها الإدارة الإلكترونية والتجارة الإلكترونية، بمواكبة التحول الرقمي، ضمانا لتسيير أفضل للهيئات والمؤسسات.

---

[1]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، طبعة2004، ص15.

[2]– القانون 04/15 مؤرخ في01 فبراير2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (ج.ر) العدد: 06 المؤرخة في: 10فبراير2015.

ومن بين ما تضمنه القانون 04/15 السالف ذكره، تنظيمه لتدابير وقائية تعتمد أساسا على آلية التشفير كوسيلة لتأمين التوقيع الإلكتروني إلى جانب آلية التصديق الإلكتروني التي تضمن الجوانب الأمنية لتبادل المعلومات على شبكة الأنترنت وهي: السرية والتوثيق والنزاهة وعدم الإنكار، وكلها جوانب تسمح بإرساء مناخ من الثقة لمختلف المعاملات الإلكترونية.[1]

وبالرغم من أهمية التدابير الوقائية لصد أي إعتداء إجرامي على التوقيع الإلكتروني، إلا أن إتباع تلك التدابير مهما بلغ من دقة لن يؤدي إلى منع إرتكابها، لذلك كان ضروريا أن تتناول التشريعات– إضافة إلى التدابير الوقائية– تنظيما لحماية جزائية عن الجرائم الناشئة عن التوقيع والتصديق الإلكترونيين[2]، هذه الحماية التي يكفلها القانون عن طريق قواعد موضوعية وقواعد اجرائية، تعنى القواعد الموضوعية بما توفره النصوص التقليدية في قانون العقوبات من تجريم السرقة والنصب وخيانة الامانة والتزوير، بالإضافة إلى النصوص الخاصة كتلك التي أوردتها نصوص القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، ومختلف القوانين ذات الصلة بآليتي التوقيع والتصديق الإلكترونيين نذكر من بينها:

- القانون رقم: 04/18 المؤرخ في 2018/05/10، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية. [3]
- القانون 03/15 المؤرخ في 01 فيفري 2015، يتعلق بعصرنة العدالة.[4]
- القانون رقم: 05/18 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية. [5]

---

[1]– للاطلاع على تفاصيل الية التصديق الإلكتروني، راجع الموقع الرسمي لسلطة ضبط البريد والاتصالات الإلكترونية الاتي:

https: //www.arpce.dz/ar/gd/ce/، تاريخ الاطلاع: 2019/09/07 على الساعة: 15: 05.

[2]– ايمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2011، ص2.

[3]– القانون رقم: 04/18 المؤرخ في 2018/05/10، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، (ج.ر) العدد: 27 المؤرخة في 2018/05/16.

[4]– القانون 03/15 المؤرخ في 01 فيفري 2015، يتعلق بعصرنة العدالة، (ج.ر) العدد: 06 المؤرخة في: 10فبراير 2015.

[5]– القانون رقم: 05/18 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية، (ج. ر) العدد: 28 المؤرخة في 2018/05/16.

- القانون رقم: 07/18 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. [1]

والمقصود بالقواعد الإجرائية تلك النصوص القانونية التي تنظم جمع الاستدلالات والتحقيق والمحاكمة في مجال الجرائم الواقعة على التوقيع الإلكتروني، سواءا في قانون الإجراءات الجزائية من خلال التعديلات الهامة التي طرأت عليه بداية من سنة 2006 بموجب القانون رقم: 22/06 المؤرخ في 2006/12/20 المعدل لقانون الإجراءات الجزائية، أو من خلال القانون رقم: 04/09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

أهمية الموضوع:

ترجع أهمية كفالة الحماية الجزائية للتوقيع والتصديق الإلكترونيين إلى الدور الذي تلعبه عملية توثيق التعاملات الإلكترونية عن طريق التوقيع الإلكتروني الموصوف مرورا باصدار شهادات التصديق الإلكتروني الموصوفة، وهي أهمية نظرية وعملية، فهو موضوع يتصل بالواقع والمستقبل، عالجته الكثير من التشريعات المقارنة واعترفت له بالقوة القانونية المماثلة للتوقيع التقليدي، غير أن التوقيع الإلكتروني يتمتع بكثير من المزايا جعلت إستخداماته في تزايد مستمر. فمن الناحية النظرية، يعالج الموضوع التعريف بآليتي التوقيع الإلكتروني والتصديق الإلكتروني وطبيعتهما القانونية والمصلحة المحمية في مختلف تطبيقات التوقيع الإلكتروني بداية بالإدارة الإلكترونية، والتجارة الإلكترونية، وحماية المستهلك وحماية المعطيات ذات الطابع الشخصي، كما يعالج الموضوع أيضا صور الاعتداءات الاجرامية الواقعة على التوقيع الإلكتروني، كتزوير التوقيع الإلكتروني وإتلافه، والدخول غير المصرح به إلى آلية إنشاء التوقيع الإلكتروني وانتهاك سريته، مع الاستشهاد بالتشريعات المقارنة لتلك الموضوعات بالنظر إلى الخسائر الفادحة التي تكبدتها الاقتصادات العالمية نتيجة هذه الإعتداءات.

[1]– القانون رقم: 18–07 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج. ر) العدد: 34 المؤرخة في 2018/06/16.

من الناحية العملية تظهر أهمية حماية التوقيع الإلكتروني جزائيا من خلال إزاحة التوقيع الإلكتروني للتوقيع التقليدي من مهد المعاملات المختلفة المدنية والإدارية والاقتصادية، فالتوقيع الإلكتروني هو وسيلة التجارة الإلكترونية الدولية بما تقتضيه من إبرام للتصرفات والصفقات ومن شأن إضفاء الحماية الجزائية للتوقيع الإلكتروني أن يحقق السرعة والسهولة المطلوبة لانجاز مثل هذه التعاملات وتوفير النفقات.

ويتصل التوقيع الإلكتروني بطائفة مهمة من الإجراءات الإدارية والنظم المالية والتجارية فالتوقيع الإلكتروني هو عصب الحكومة الإلكترونية، وله صلة وثيقة بالاعمال المصرفية من خلال تطبيقات التوقيع الإلكتروني في مجال البنوك مثل: الشيك الإلكتروني والاعتماد المستندي الإلكتروني وفي أعمال البورصة وتبادل الأوراق المالية.

وفي مجال حماية الحق في الخصوصية، وباعتبار أن التوقيع الإلكتروني يحتوي على معطيات ذات طابع شخصي في شكل بيانات ومعلومات لا يحق للآخرين الاطلاع عليها، فمن شأن كفالتها بحماية جزائية تحقيق حق من حقوق الانسان وهو الحق في الخصوصية.

يتضح مما سبق ان الحماية الجزائية للتوقيع والتصديق الإلكترونيين عن طريق تحديد الجرائم والأفعال الماسة سواء بالتوقيع الإلكتروني أو بشهادة التصديق الإلكتروني هي حماية للثقة والاستقرار المطلوبين في جميع المعاملات الإلكترونية.

دوافع اختيار الموضوع:

تواجه الجزائر تحديات كبيرة في مجال التحول الرقمي وتجسيد متطلبات الحكومة الإلكترونية وإقامة اقتصاد رقمي أساسه التجارة الإلكترونية وحماية المستهلك الرقمي، ولا يأتي ذلك إلا بتوفير الإطار القانوني اللازم والإقحام المستمر للوسائل التكنولوجية المتطورة، أبرزها آلية التوقيع والتصديق الإلكترونيين. ولان الظاهرة الإجرامية حتمية في حياة المجتمع احتمالية في حياة الفرد، وبفعل الإستخدام السيئ للتوقيع والتصديق الإلكترونيين، ظهرت طائفة من الجرائم المستحدثة، كجرائم التلاعب في بيانات التوقيع الإلكتروني وجرائم مؤدي خدمات التصديق الإلكتروني وغيرها، وما يتركه ذلك من أثار سلبية على الاقتصاد الوطني وعلى الأفراد والمجتمع ككل ومن باب اهتمامنا وشغفنا بهذه التقنية، أردنا البحث في هذا الموضوع من جهة، للتعرف على الجرائم الواقعة على التوقيع الإلكتروني

باعتبارها من الجرائم المعلوماتية المستحدثة وتأثيرها السلبي على الإقبال المتزايد للمستهلك الرقمي على خدمات التوقيع الإلكتروني، ومن جهة أخرى معرفة السياسة الجنائية للمشرع الجزائري في شقيها الموضوعي والإجرائي بخصوص مكافحة هذا النوع المستحدث من الجرائم.

أهداف البحث:

تتلخص أهداف البحث في النقاط الآتية:

- التعرف على الجوانب الموضوعية المتعلقة بالتجريم والعقاب في التشريع الجزائري الخاصة بمكافحة الجرائم الواقعة على التوقيع الإلكتروني بمفهومها الواسع ضمن إطار قانون العقوبات وبعض القوانين الخاصة.
- التعرف على الجوانب الإجرائية المتعلقة بهذا النوع المستحدث من الجرائم، مرورا بكافة مراحل الدعوى، وانتهاءا بالتعاون القضائي والمساعدة القضائية الدولية في هذا الشأن.
- مدى كفاية وفعالية النصوص القانونية في مواجهة الجرائم الواقعة على التوقيع والتصديق الإلكترونيين، في ظل التطور المستمر لتكنولوجيات الإعلام والإتصال.

الدراسات السابقة:

يعتبر موضوع الحماية الجزائية للتوقيع والتصديق الإلكترونيين من الموضوعات الحديثة، نظرا لحداثة آلية التوقيع والتصديق الإلكترونيين ودخولهما حيز الخدمة في شتى المجالات، لا سيما مجالي الحكومة الإلكترونية والتجارة الإلكترونية، نتج عن ذلك وجود دراسات قليلة تناولت بعض جوانب الموضوع نذكر منها:

- ياسر محمد الكومي، الحماية الجنائية والأمنية للتوقيع الإلكتروني، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، 2014.

تطرق فيها الباحث إلى الحماية الجنائية للتوقيع الإلكتروني، سواء من جانبيه الموضوعي أو الاجرائي في التشريع المصري المقارن، وكذا الحماية الامنية للتوقيع الإلكتروني، وتعرض في سياق ذلك إلى المعوقات التي تواجه مكافحة جرائم الإعتداء على التوقيع الإلكتروني، وطرق القضاء على هذه المعوقات، وصلة ذلك بالتعاون الدولي في مرحلتي التحقيق والمحاكمة.

- أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، أطروحة دكتوراه، دار النهضة العربية، القاهرة، 2011.

تناولت الدراسة موضوع الحماية الجنائية للتوقيع الإلكتروني، في جانبيه الموضوعي والإجرائي، مبينا موقف التشريع المصري والمقارن، ثم تناول سياسة المشرع المصري في تجريم الإعتداء على التوقيع الإلكتروني، ومدى ملائمة القواعد الإجرائية التقليدية لضبط الجاني في تلك الجرائم ومحاكمته، وصلة ذلك بالتعاون الدولي سواء على الصعيد الشرطي، أو في مرحلتي التحقيق والمحاكمة.

يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقيات العربية لمكافحة جرائم تقنية المعلومات– قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

تناول فيها: الجوانب الموضوعية والإجرائية، التي اقرها المشرع الجزائري في إطار مكافحة الجرائم الإلكترونية بمفهومها الواسع، سواء التي تتم بواسطة الحاسوب عندما يكون وسيلة لها، أو تلك التي تقع على الحاسوب عندما يكون هدفا لها، أو تلك التي تتم بواسطة أية وسيلة إلكترونية، وعموما من خلال تكنولوجيات الإعلام والإتصال، وقد تناولت الدراسة على الخصوص الجرائم الماسة بالتوقيع والتصديق الإلكترونيين المنصوص عليها بموجب القانون رقم: 04/15 المؤرخ في: 2015/02/01 يتعلق بالتوقيع والتصديق الإلكترونيين.

- أحمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2014.

تناول فيها الحماية الجنائية الموضوعية والإجرائية للمحرر الإلكتروني، باعتبارها من أهم موضوعات السياسة الجنائية المعاصرة.

صعوبات البحث

طبيعة الموضوع وحداثته: إن الطبيعة التقنية للتوقيع الإلكتروني وارتباطه بإستخدامات تكنولوجية حديثة في الإدارة والاقتصاد (المعاملات المصرفية والتجارة الإلكترونية)، جعلت من موضوع حمايته الجزائية من الصعوبة بما كان، بالنظر إلى ندرة المراجع الجزائرية المتخصصة في هذا المجال، كما تستلزم دراسة الحماية الجزائية للتوقيع والتصديق الإلكترونيين الوقوف على الحماية التقنية التي سنها المشرع الجزائري للحد من مخاطر الإعتداء عليه، وهو ما أضفى على هذا الجانب التقني من الدراسة دقة وصعوبة تتطلب قدرا من التخصص.

إضافة إلى كل ذلك، واجه البحث صعوبة في الوقوف على الحماية الإجرائية للتوقيع الإلكتروني، ومدى انطباق نصوص قانون الإجراءات الجزائية الجزائري، والقانون 04/09 السالف ذكره على الجرائم الواقعة على التوقيع الإلكتروني، في ظل خلو التشريع الجزائري من تنظيم إجرائي يتناول الحماية الجزائية للتوقيع الإلكتروني، وكذا نقص التطبيقات الفضائية المتعلقة بموضوع البحث.

المنهج المتبع:

إعتمدت الدراسة على المنهج التحليلي المتمثل في تحليل مضمون النصوص القانونية المتضمنة الجرائم الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني محل الدراسة واستنباط الأحكام المتعلقة بها.

كما تم إستخدام المنهج المقارن في بعض المسائل، لمعرفة موقف المشرع الجزائري مقارنة مع باقي التشريعات، والاطلاع على تجارب الدول المختلفة، وفهم النصوص القانونية وتصور الاقتراحات حول إصلاح وتعديل التشريعات القائمة.

الإشكالية:

يرتبط التوقيع الإلكتروني بتطبيقات متنوعة، كمجال الادارة الإلكترونية، ومختلف المعاملات المصرفية على مستوى البنوك وتعاملات التجارة الإلكترونية، لذا قد تترك الإعتداءات الاجرامية على هذه التقنية من ناحية أولى آثارا مدمرة على المستوى الاجتماعي أو الاقتصادي للدولة، خاصة في ظل التقدم المذهل لتكنولوجيات الإعلام والإتصال، والإقحام المتزايد للتوقيع الإلكتروني في شتى التعاملات الإلكترونية، ومن ناحية أخرى قد تظهر إلى الوجود صورا جديدة من الجرائم الماسة بالتوقيع

الإلكتروني غير تلك المنصوص عليها في قانون العقوبات أو في القوانين الخاصة، وهذا ما أثار كثيرا من التحديات القانونية والعملية أمام الأجهزة القضائية المكلفة بالبحث والتحري عن هذه الجرائم، سيما ما تعلق بكشفها وإثباتها وإجراءات البحث والتحري واستخلاص الدليل الرقمي، عبر بيئة افتراضية، وصولا إلى ضبط المجرم المعلوماتي وتقديمه للعدالة.

وكان لزاما على المشرع الجزائري أمام هذه التحديات التدخل لصد هذه الإعتداءات عن طريق تعديل النصوص القانونية، واستحداث أخرى في قانون العقوبات أو قانون الإجراءات الجزائية أو القوانين الخاصة أو عن طريق التصديق على الإتفاقيات الدولية وتفعيل التعاون الدولي في مجال مكافحة الجرائم الواقعة على التوقيع الإلكتروني.

وعليه يمكن طرح الإشكالية الآتية:

- ما مدى كفاية الوسائل القانونية التي إعتمدها المشرع الجزائري في مواجهة الجرائم الماسة بالتوقيع والتصديق الإلكترونيين؟

وفي سبيل الإجابة على هذه الإشكالية تثور مجموعة من الإشكاليات الفرعية على النحو التالي:

- ما مدلول التوقيع والتصديق الإلكترونيين ؟
- وما هي أهم صور الإعتداءات التي تقع على التوقيع الإلكتروني وشهادة التصديق الإلكتروني؟
- وما هي الإجراءات الواجب إتباعها لفرض حماية على التوقيع الإلكتروني وشهادة التصديق الإلكتروني؟

خطة البحث:

قصد معالجة الإشكاليات السابق طرحها، تم تقسيم الدراسة إلى بابين، تناول الباب الأول القواعد الموضوعية للحماية الجزائية للتوقيع والتصديق الإلكترونيين، وذلك في فصلين، خصص الفصل الأول منه للأحكام العامة لجرائم التوقيع والتصديق الإلكترونيين، وتم التطرق في الفصل الثاني إلى صور الجرائم الواقعة على التوقيع الإلكتروني.

أما الباب الثاني فيبحث الجوانب الإجرائية للحماية الجزائية للتوقيع والتصديق الإلكترونيين، وقد قسم هو الآخر إلى فصلين: خصص الفصل الأول منه للبحث في إجراءات التحقيق في الجرائم الواقعة على التوقيع الإلكتروني، اما الثاني فقد تناول بالدراسة إجراءات المحاكمة في الجرائم الواقعة على التوقيع الإلكتروني، وتم إنهاء البحث بخاتمة تضمنت أهم النتائج والتوصيات.

الباب الأول

القواعد الموضوعية للحماية الجزائية للتوقيع الالكتروني

لا شك أن ظهور التوقيع الإلكتروني وانتشار التعامل به عن طريق شبكة المعلومات الدولية الأنترنت، سواء فيما خص التجارة الإلكترونية أو الحكومة الإلكترونية أو باقي التطبيقات التي تتدخل فيها آليتي التوقيع والتصديق الإلكترونيين، أدى إلى إثارة العديد من الإشكاليات غير المسبوقة في مختلف النصوص القانونية ذات الصلة بالجوانب الموضوعية محور الدراسة في الباب الأول، إن من حيث النظام القانوني الذي يحكم هاتين الآليتين، أو من حيث الصور المستحدثة للإعتداءات الإجرامية التي تطالها، وعلى ذلك سيتم تقسيم هذا الباب إلى الفصلين التاليين:

- **الفصل الأول:** الأحكام العامة لجرائم الإعتداء على التوقيع الإلكتروني
- **الفصل الثاني:** صور الجرائم الواقعة على التوقيع الإلكتروني

الفصل الأول:

الأحكام العامة لجرائم الاعتداء على التوقيع الالكتروني

تمهيد:

تقتضي دراسة الحماية الجزائية للتوقيع والتصديق الإلكترونيين الوقوف من جهة أولى على ماهيتهما وآلية عملهما، وكذا التدابير التقنية التي يمكن الاعتماد عليها لتوفير حماية وقائية من مخاطر الإعتداء على التوقيع الإلكتروني، إذ أن تلك الحماية وإن بدت في ظاهرها بعيدة عن الإطار الجنائي، إلا أن التعمق في الأمر يؤدي بنا إلى القول بغير ذلك، إذ تبدو الأهمية القصوى في منع وقوع الجريمة أكثر من إدانة الجاني بعد إقترافه للجرم.[1]

ومن جهة ثانية الوقوف على الآثار القانونية للتوقيع والتصديق الإلكترونيين، مقارنة بالتوقيع التقليدي في مجال قواعد الإثبات العامة، في ظل تقدم نظم المعالجة الإلكترونية للبيانات والمعلومات، وكذا مسؤولية المتدخلين في منظومة التوقيع والتصديق الإلكترونيين.

ثم الوقوف اخيرا على الطابع الخاص والذاتي لجرائم التوقيع الإلكتروني وشهادة التصديق الإلكتروني، والتي تمثل نموذجا قانونيا جديدا مقارنة بباقي الجرائم المعلوماتية.

في حدود ذلك سوف يتم تناول هذا الفصل في مبحثين على النحو التالي:

- **المبحث الأول:** ماهية التوقيع والتصديق الإلكترونيين.
- **المبحث الثاني:** النموذج القانوني لجرائم التوقيع الإلكتروني.

[1]– أيمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، مصر 2011، ص27.

المبحث الأول:

ماهية التوقيع والتصديق الإلكترونيين

يهدف التوقيع في القواعد التقليدية عموما إلى قدرة تحديد هوية الشخص الموقع والتعبير عن إرادته، وقد اخذ عبر التاريخ صورا مختلفة وصولا إلى التوقيع الإلكتروني الذي يتضمن مختلف التعاقدات عبر شبكة الأنترنت، فكان من الضروري تنظيمه وتحديد إشكاله وضوابطه وشروط الاعتراف به ضمانا لحجيته القانونية في الإثبات، الذي بدونه لا يمكن أن يكون التوقيع الإلكتروني محلا لأي حماية جزائية.

وعلى ذلك سيتم تفصيل هذا المبحث على النحو التالي:

- **المطلب الأول:** تعريف التوقيع والتصديق الإلكترونيين
- **المطلب الثاني:** أحكام التوقيع والتصديق الإلكترونيين في التشريع الجزائري

المطلب الأول:

تعريف التوقيع والتصديق الإلكترونيين

التوقيع الإلكتروني من التطبيقات التي ظهرت وتوسع في إستخدامها ترتيبا على التوسع في إستخدام الحاسب الآلي[1]، ولما كانت المستندات الإلكترونية بما فيها العقود تتم عن بعد بين أطراف قد يجهل بعضهم البعض، كان من الضروري توفير الضمانات والوسائل التي تكفل تحديد هوية المتعاقدين، وتضمن التعبير عن هويتهم على نحو صحيح وبطريقة تمكن نسبة التصرف إلى صاحبه.[2]

[1]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، مصر، 2005، ص11

[2]– بلحسين حمزة، الحماية القانونية والفنية للتوقيع الإلكتروني، مجلة العلوم القانونية والإدارية، العدد 11، جامعة جيلالي اليابس، سيدي بلعباس، ص83

وظهرت الحاجة كذلك إلى وجود طرف ثالث محايد موثوق به، يتأكد بطرق خاصة من صحة صدور التوقيعات الإلكترونية يطلق عليه اسم سلطة التوثيق، أو مقدمي خدمات التصديق. [1]

وهو ما سيتم تناوله من خلال الفرعين الآتيين:

- **الفرع الأول:** تعريف التوقيع الإلكتروني
- **الفرع الثاني:** تعريف التصديق الإلكتروني

الفرع الأول: تعريف التوقيع الإلكتروني

التوقيع بصفة عامة علامة خطية تسمح بتحديد شخصية صاحبه وتميزه عن غيره من الأشخاص ويعبر عن إرادته في إقرار مضمون أي تصرف قانوني.

والتوقيع الإلكتروني مصطلح لغوي حديث نسبيا نعني به إجراء يتم القيام به بالوسائط الإلكترونية بغرض التوثيق وإثبات الهوية وفي نفس الوقت التعبير عن الإرادة. [2]

أولا: التعريف الفقهي

تعددت وتنوعت تعريفات التوقيع الإلكتروني لدى شراح القانون، فمنهم من نظر إليه من الناحية الآلية، بمعنى كيف يتم؟ وقام بتعريفه بناء على ذلك، بينما نظر آخرون من الناحية الوظيفية، بمعنى ماهية وظيفته؟ ثم عرفه بناء على ذلك. [3]

ومن بين هذه التعريفات أنه: "كل إشارات أو رموز أو أحرف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطا وثيقا بالتصرف القانوني تسمح بتمييز شخص صاحبها وتحديد هويته، وتعبر دون غموض عن رضاه بهذا التصرف القانوني. [4]

---

[1]– بلحسين حمزة، المرجع السابق ص83.

[2]– ابراهيم ابن سطم بن خلف العنزي، التوقيع الإلكتروني وصوره وتطبيقاته، اطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية الرياض 2009، ص 37 .

[3]– ابراهيم ابن سطم بن خلف العنزي، التوقيع الإلكتروني، صوره وتطبيقاته، المرجع السابق، ص 38.

[4]– ثروت عبد الحميد، التوقيع الإلكتروني ماهيته، مخاطره، مدى حجيته في الإثبات، الإسكندرية، دار الجامعة الجديدة، ط1، 2007، ص50.

ويرى آخرون أن التوقيع الإلكتروني هو "إجراء معين يقوم به الشخص المراد توقيعه على المحرر سواء كان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو شفرة خاصة، بحيث يضغط بالرقم أو الشفرة في مكان آمن وسري يمنع استعماله من قبل الغير، ويعطي الثقة بأنه صدر من صاحبه حامل الرقم أو الشفرة".[1]

كما يفرق البعض بين التوقيع الإلكتروني وبين التوقيع الرقمي، فيرى أن التوقيع الإلكتروني يتشكل من سلسلة من الأرقام الحسابية الأصفار والآحاد، من مجموعها يتكون التوقيع الإلكتروني الرقمي.

أما التوقيع الرقمي فهو عبارة عن أرقام مطبوعة تسمى (HASH) لمحتوى المعاملة التي يتم التوقيع عليها. [2]

إزاء ذلك، استقر الفقه والقضاء الفرنسي على أن التوقيع الإلكتروني يؤدي وظيفتين أولهما تحديد هوية الموقع، وثانيهما التعبير عن إرادة الموقع بإقراره بمضمون التصرف. [3]

ثانيا: التعريف القانوني:

عرف المشرع الجزائري التوقيع الإلكتروني في المادة 02 فقره (01) من القانون 04/15 الصادر سنة 2015 المتعلق بالتوقيع والتصديق الإلكترونيين انه " بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".[4]

وكان قد اعترف به بمقتضى المادة 2/327 من القانون رقم 10/05 المؤرخ في 20 جوان 2005[5]، والتي نصت على أنه يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة1/323

---

[1]– نجوى ابو هيبة، التوقيع الإلكتروني تعريفه ومدى حجيته في الإثبات، دار النهضة العربية، القاهرة 2004 ص41.

[2]– محمد امين الرومي، مرجع سابق ص15

[3]– أيمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق، ص30.

[4]– قانون 04/15 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06 لسنة 2015.

[5]– القانون 10/05 المؤرخ في 20 جوان 2005، المعدل والمتمم للأمر 58/75، المتضمن القانون المدني الجريدة الرسمية رقم 44 بتاريخ 26 جوان 2005.

المتمثلة في إمكانية التأكد من هوية الشخص التي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها. [1]

وجاء تعريف المشرع الجزائري للتوقيع الإلكتروني مطابقا إلى حد ما لتعريف قانون الأونستترال النموذجي الموحد لـ سنة2001 بأنه:" بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على ما ورد بها من معلومات"[2]، كما عرفت المادة 4/1416 من التقنين المدني الفرنسي المعدل، والمضافة بقانون التوقيع الإلكتروني الفرنسي 2000/24 الصادر في 2000/04/14 التوقيع بصفة عامة بأنه:" التوقيع الضروري لإتمام التصرف القانوني الذي يميز هوية من وقعه، ويعبر عن رضائه بالالتزامات التي تنشأ عن هذا التصرف عندما يكون إلكترونيا، فيجب أن يتم باستخدام وسيلة آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه". [3]

وقد عرف القانون الاتحادي الأمريكي التوقيع الإلكتروني بأنه:" صوت أو رمز أو معالجة إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو إقرارها من شخص تتوافر لديه نية التوقيع على السجل".[4][5]

وقد اصدر المشرع في ولاية نيويورك تعديلا جديدا على قانون التوقيع والسجلات الإلكترونية الصادر في 06 أوت 2002حيث وضع تعريفا للتوقيع الإلكتروني انه " صوت أو رمز أو معالجة

---

[1]– صالح شنين، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، جامعة ابو بكر بلقايد، كلية الحقوق، تلمسان، 2013، ص52.

[2] –Unictral model law on electronic signature 2001 article 2/BF(electronic signature) the term “electronic signature” means an electronic sound, symbol, or process, attached to or logically associated with a contract or other d or adopted by a person with the intentto sign the record

[3]–la loi no2000-2230du 13 mars 2000.J.O 14 mars 2000.P.3986.J.C.P.2000.III20259.

[4] –“an electronic sound,symbol,orprocess,thatbis attached to or logically associated with”acontract or other record,and that is “executed or adopted by a person with the intent to sign the record. ”E-Sign law 106(5).report to the Governor and Legislature on New York State’s Electronic Signatures and Records Act,p.11.

[5]– التوقيع الإلكتروني لولاية كانسس يعني صوتا أو رمزا أو معالجة إلكترونية مرفقة بسجل أو متحدة به ويتم إجرائها أو إقرارها من شخص مصحوبة بنية التوقيع على السجل.

إلكترونية ملحقة بسجل إلكتروني أو متحدة منطقيا به ويجربها أو يقرها شخص تتوافر لديه شبه التوقيع في هذا السجل[1]، وهو ما يكاد يتطابق مع التعريف الذي نص عليه الشارع الألماني في المادة الثانية من قانون التوقيع الإلكتروني[2]، الذي ميز بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم، ويشترك كل منهما في انه على بيان في صورة إلكترونية ملحق ببيان آخر أو مرتبط به منطقيا ويستخدم هذا البيان لتوثيق نسبته لشخص آخر معين. [3]

غير أن التوقيع الإلكتروني المتقدم في نظر المشرع الألماني ينطوي على ضوابط اشد صرامة من العادي، فهو توقيع يتضمن شفرة مقصورة إستخدامها على شخص معين لا يشاركه غيره فيه، ويكون قادرا على تحديد هوية مستخدمه، أو انه يمكنه ان يحتفظ بشفرة هذا التوقيع تحت إشرافه وحده، أو يكون بالإمكان اكتشاف أي تغيير في بيانات هذا التوقيع لاحقا. [4].

وفي نفس السياق عرف المشرع المصري في القانون 2004/15 بشأن التوقيع الإلكتروني الصادر في 2004/04/22 التوقيع الإلكتروني بأنه: " ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره. [5].

---

[1] –"Electronic signature "shallmean an electronic identifier, including without limitation a digital signatur, whichis unique to the personusingit, capable of verification, under the solecontro of the personusingit,attached to orassociatedwith data in such a mannerthatauthenticates the attachmentof the signature toparticulardata and the integrity of the data transmitted, and intended by the party usingit to have the same force and effect as the use of a signature affixed by hand".ESRA 102 (3).Report to the govenor and legislature,p.7 note3

[2] –Draft of a law on the framwork conditions,2(2),p.4

[3] – حسين بن سعيد بن يوسف الغافري، الجرائم الواقعة على التجارة الإلكترونية، خاص لموقع المنشاوي للدراسات والبحوث: www.minichaoui.com

[4] –Draft of a law on the framwork conditions,2(2),p.4.

[5] – قانون التوقيع الإلكتروني المصري رقم 15 لعام 2004، الجريدة الرسمية العدد 17 تابع(3) الصادر في 2004/04/22.

ثالثا: أنواع التوقيع الإلكتروني:

ترتبط دراسة أنواع التوقيع الإلكتروني بطرق توثيق التعاملات الإلكترونية المختلفة، وتتعدد صور التوقيع الإلكتروني ومن أبرزها التوقيع الكودي أو السري، والتوقيع البيومتري الذي يعتمد على الصفات والخصائص الجسدية والسلوكية للشخص، والتوقيع الرقمي الذي يعتمد على التشفير وربطه بمفاتيح خاصة لفك التشفير.

1. التوقيع الكودي:

تعتمد طريقة التوقيع الكودي أو السري أثناء عملية توثيق المراسلات والتعاملات الإلكترونية على إستخدام مجموعة من الأرقام والحروف يختارها صاحب التوقيع لتحديد شخصيته ولا تكون معلومة إلا منه أو من يبلغه بها. [1]

وينتشر استعمال هذه الطريقة من التوقيع الإلكتروني في عمليات المصارف والدفع الإلكتروني بصفة عامة. [2]

2. التوقيع البيومتري:

تعتمد هذه الصورة على حقيقة علمية هي أن لكل شخص صفات ذاتية خاصة به تختلف من شخص إلى آخر تتميز بالثبات النسبي، مما يعزز الثقة في أن التوقيع بأحد تلك الخواص قد تم عن طريق الموقع ذاته عن طريق تحديد الهوية، وبالتالي منحه الحجية القانونية في الإثبات. [3]

وتتعدد الصفات الجسدية أو البيومترية التي يعتمد عليها التوقيع البيومتري أهمها:

البصمة الشخصية "Figner priting"، مسح العين البشرية "iris et retina scanning"، تعرف الوجه البشري "Facial recognition"، خواص اليد البشرية "hand géométrie"، التحقق من نبرات

---

[1]– ماجد راغب الحلو، مرجع سابق ص 84.

[2]– حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2003، ص179.

[3]– لزهر بن سعيد، مرجع سابق، ص157.

الصوت "Voicrecognation"، التوقيع الشخصي "hand written signature"، البطاقة الذكية " Smart card"، وغير ذلك من طرق أخرى تعتمد على تعاقب نظم الحماية وتعددها في أي نظام واحد. [1]

ففي كل حالة يتم تخزين البيانات الخاصة في الحاسب الآلي واسترجاعها متى دعت الحاجة إليها للتأكد من شخصية صاحبها والسماح له بإتمام العملية المطلوبة، أو الدخول إلى نظام الحاسب الآلي.

3. التوقيع الرقمي:

يعتبر التوقيع الرقمي الأكثر أمنا وسرية وآخر ما توصلت إليه التكنولوجيا في مجال التوقيعات الإلكترونية.

ويقوم على أساس تحويل المحرر المكتوب من نمط الكتابة العادية إلى معادلة رياضية لايمكن لأحد أن يعيدها إلى الصيغة المقررة ماعدا الشخص الذي يملك المعادلة الخاصة بذلك والتي يطلق عليها المفتاح، فهو يعتمد على إستخدام تقنية المفتاحين العام والخاص أو مايعرف بنظام التشفير اللامتناظر أو نظام " شفرة المفتاح العام".[2]

إزاء ذلك تبنى المشرع الجزائري نظام التشفير في المادة الثانية الفقرتين 08، 09 من القانون 04/15 المذكور أعلاه عند تعريفه للمفتاح الخاص والعام على التوالي والذي سيأتي تفصيله لاحقا .

وعليه يلاحظ أن أهمية هذا النوع من التوقيع الإلكتروني هي التي دفعت المشرع الجزائري إلى تثبيته في القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

الفرع الثاني: تعريف التصديق الإلكتروني

تتم التبادلات على شبكة الأنترنت من خلال شبكة مفتوحة لا تحتوي على أي وجود مادي، مما صعب عملية التعرف على هوية الأشخاص الذين يتم التواصل معهم في هذا العالم الافتراضي،

[1]– سليم سعداوي، مرجع سابق، ص81.

[2]– زهدور كوثر، مرجع سابق، ص94.

وسهل في الوقت ذاته افعال سرقة الهوية، واعتراض الآخرين على رسائل الغير واستنكار عملية بيع أو دفع أو تبادل، وعليه فان وضع أجهزة أمنية مثل التصديق الإلكتروني بات من احد الضروريات. [1]

وقد عرفت سلطة الضبط للبريد والمواصلات السلكية واللاسلكية الجزائرية التصديق الإلكتروني انه:" عملية تضمن أربعة جوانب أمنية لتبادل المعلومات على شبكة الأنترنت وهي السرية والتوثيق والنزاهة وعدم الاستنكار كون هذه الجوانب تسمح في إرساء مناخ ثقة عن طريق إقامة بنية ذات مفتاح عمومي"PIXI ".[2]

أولا: التصديق الإلكتروني في القانون:

عرف المشرع الجزائري في المادة 2 فقرة 15من القانون 04/15 سياسة التصديق الإلكتروني على أنها: " مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين".[3]

كما يعرف التصديق الإلكتروني على انه وسيلة آمنة للتحقق من صحة التوقيع أو المحرر حيث يتم نسبه إلى شخص أو كيان معين. [4]

ويفهم من التصديق الإلكتروني مجموعة التقنيات المستعملة المتمثلة في الأدوات والوسائل الآلية التي تستخدم للتأكد من صحة وأصالة طرفي المعاملة، وتشمل العديد من الأدوات والوسائل التي يتم من خلالها إنشاء التوقيع الإلكتروني وضمان سلامته وأمنه. [5]

ومن خلال التعريف يتبين أن التصديق الإلكتروني هو عملية متكاملة تتداخل فيها عدة آليات اصطلح عليها بجهات التوثيق أو التصديق الإلكتروني وشهادة التصديق الإلكتروني.

---

[1]– موقع سلطة الضبط للبريد والواصلات السلكية واللاسلكيةWWW.ARPT.DZ/ar/gd/ce

[2]– مرجع سابق:WWW.ARPT.DZ

[3]– القانون 04/15 المؤرخ في 10 فيفري 2015، مرجع سابق.

[4]– حمد حسين منصور، الاثبات الإلكتروني، دار الفكر الجامعي، الاسكندرية 2006، ص209.

[5]– يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، الجزائر 2016، ص189

1. مفهوم جهات التصديق الإلكتروني:

يعرف مقدم خدمة التوثيق بأنه:" جهة أو منظمة عامة، أو خاصة مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية بإصدار شهادات إلكترونية". [1]

ويطلق على الغير الذي يتولى عملية التصديق: " مقدم خدمات التصديق " ويرمز لهم إختصارا (PSC).

وقد عرفه المشرع الجزائري في القانون 04/15 المؤرخ في 10 فيفري 2015[2]، في مادته الثانية الفقرة 11 و12 حيث أطلق مصطلح الطرف الثالث الموثوق كتعبير عن إقتصار أداء خدمات التصديق الإلكتروني على الشخص المعنوي، ومؤدي خدمات التصديق الإلكتروني الذي نص عليه صراحة في الفقرة 12 الموالية فجاء التعريف كما يلي:

- **الطرف الثالث الموثوق:** شخص معنوي يقوم بمنح شهادات تصديق موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.
- **مؤدي خدمات التصديق الإلكتروني:** شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجلات الصديق الإلكتروني.

وقد عرفت قواعد قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية مقدم خدمات التصديق الإلكتروني في المادة (E/2) بأنه:" شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية".[3]

كما عرف القانون الإماراتي هذه الجهة بأنها:" أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية، أو أي خدمات أو مهمات متعلقة بها أو بالتواقيع الإلكترونية". [4]

---

[1]– سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة 2006 ص75

[2]– القانون 04/15 المؤرخ في 10 فيفري 2015، السالف ذكره.

[3]– المادة E/2 من القانون الاونسترال بشأن التوقيعات الإلكترونية.

Le terme prestataire de service de certification designe une personne qui emet des certificats et peu fournir d'autres services lie x s ausignatures électronique.
2J.O.C.E.L 13-19 Janvier 2000p12 ets s:

[4]– المادة 20/2 من قانون المعاملات والتجارة الإلكترونية الاماراتي رقم 12 لسنة 2002.

وعليه فان دور جهات التوثيق أو التصديق الإلكتروني يتمثل في التأكد من صحة التوقيع الإلكتروني، ومن سلامته، كما يتمثل في تحديد هوية المتعاملين الإلكترونية، ومن أهليتهم القانونية للتعامل والتعاقد، كما تعمل أيضا على التحقق من مضمون هذا التعامل وسلامته وجديته، كما تقوم هذه الجهات كذلك بإصدار المفاتيح الإلكترونية سواء المفتاح الخاص أو العام[1].

ثانيا: مفهوم شهادات التصديق الإلكتروني:

تقوم شهادات التصديق الإلكتروني بدور فعال في مجال المعاملات الإلكترونية، فمن شأنها التأكد من شخصية المرسل ومن سلامته وصحة البيانات المدونة بالمحرر، وعدم قابليتها للتعديل، وهو من شأنه أن يرسخ الثقة، الأمان لدى المتعاملين عبر الأنترنت.[2]

وقد عرفها المشرع الجزائري في القانون 04/15 لسنة 2015 الفقرة السابعة بأنها وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع. [3]

وعرفت المادة 2 من قانون الأونسترال النموذجي الصادر عن الأمم المتحدة بأنها تعني " رسالة بيانات أو سجلا آخر يؤكد الارتباط بين الموقع وبين إنشاء التوقيع"[4]

كما عرفت المادة الثالثة من التوجيه الأوربي شهادة التصديق الإلكتروني بأنها:" تلك التي تربط بين التوقيع وبين شخص معين وتؤكد شخصية الموقع".[5]

وعرفها البعض من الناحية الفنية بأنها، عملية إلكترونية تربط بين شخص معين (شخص طبيعي أو معنوي) بخصائص معينة تسمح بتمييزه عن غيره[6]، فهي بمثابة بطاقة إثبات الهوية الإلكترونية تصدر أثناء عملية التوقيع الإلكتروني. [7]

---

[1]– بلحسين حمزة، الحماية القانونية والفنية للتوقيع الإلكتروني، مرجع سابق ص 84

[2]– لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار هومة، الجزائر 2012، ص 182.

[3]– القانون 04/15 السالف ذكره.

[4]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق ص 261

[5]– لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، مرجع سابق، ص 183.

[6]–Tulienesnault,lasignatureelecto nique.publié sur: www.signelec.com-le 21juillet 2003 ,p.11

[7]– أيمن سعد، التوقيع الإلكتروني، دار النهضة العربية، القاهرة 2013، ص93

وتختص في اغلب التشريعات جهة معينة بإصدار هذه الشهادة والتصديق على التوقيع الإلكتروني في نفس الوقت، وبمقتضى هذه الشهادة يمكن للجهة المختصة أن تشهد بصحة التوقيع وبالتالي تحديد هوية الموقع.

فالغرض من شهادة التوثيق الإلكتروني التأكيد على أن هناك ارتباط بين الموقع وبيانات إنشاء التوقيع، كما تشهد بان الكتابة الإلكترونية (أو ما يطلق عليه رسالة البيانات في بعض التشريعات العربية) كتابة صحيحة ولم يتم التلاعب فيها، [1] وبالتالي صحة التوقيع الإلكتروني ونسبته إلى من أصدره لاستفائه الشروط والضوابط والمعايير الفنية والتقنية المنصوص عليها قانونا، ليكتسب في الأخير حجية في الإثبات شأنه شأن التوقيع الكتابي أو التقليدي.

المطلب الثاني:

أحكام التوقيع والتصديق الإلكترونيين في التشريع الجزائري

تم إدراج التوقيع الإلكتروني من قبل المشرع الجزائري للمرة الأولى سنة 2005 من خلال القانون 10/05 المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر 58/75 المتضمن القانون المدني[2]، الذي تم من خلاله الاعتراف بالكتابة الإلكترونية والتوقيع الإلكتروني في مجال الإثبات.

وجاء المرسوم التنفيذي 162/07 المؤرخ في 30 ماي 2007[3] لينظم نشاط التصديق الإلكتروني من خلال إخضاعه إلى نظام الترخيص الوارد في المادة 39 من القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية.[4]

---

[1]– محمد امين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر 2007، ص 57.

[2]–تنص المادة 323 مكرر 1 " يعتبر الاثبات في الشكل الإلكتروني كالإثبات بالكتابة على الورق شرط إمكانية التأكد من هوية الشخص الذي اصدرها وان تكون معدة ومحفوظة في ظروف تضمن سلامتها

[3]– المرسوم التنفيذي 162/07المؤرخ في 30 ماي 2007 المعدل والمتمم المتعلق بنظام الاستغلال المطبق على كل نوع من انواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، الجريدة الرسمية عدد37

[4]– القانون 03/2000 المؤرخ 05 اوت 2000 المتعلق بالقواعد العامة بالبريد والمواصلات السلكية واللاسلكية، ملغى بموجب القانون 04/18 المؤرخ في 2018/05/10، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية المشار اليه سابقا

ومع صدور القانون 04/15 المؤرخ في 01 فيفري 2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، تم البدء فعليا لهذه الآلية وفق ثلاث مبادئ أساسية هي: التوثيق، السلامة، عدم الإنكار، ما يجعل التوثيق الإلكتروني موثقا وغير قابل للتزوير، ولا يمكن إعادة استعماله، وسيتم التطرق إلي كل ذلك على النحو التالي:

- **الفرع الأول:** آليات عمل التوقيع والتصديق الإلكترونيين.
- **الفرع الثاني:** الآثار القانونية للتوقيع الإلكتروني.
- **الفرع الثالث:** المسؤولية المدنية الناشئة عن المعاملات الإلكترونية الحاملة لتوقيعات إلكترونية.

الفرع الأول: آليات عمل التوقيع والتصديق الإلكترونيين.

إنتهج المشرع الجزائري وفق القانون 04/15المتعلق بالتوقيع والتصديق الإلكترونيين سياسة التصديق الإلكتروني التي تمثل مختلف القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين، وبدأ بآليات الإنشاء والتشفير كوسيلة حماية تقنية، إلى جانب آليات التصديق الإلكتروني بمختلف مراحله، والسلطات المشرفة عليه، وهو ما يطلق عليه بمنظومة التوقيع والتصديق الإلكترونيين.

أولا: منظومة إنشاء التوقيع الإلكتروني.

1. آلية إنشاء التوقيع الإلكتروني:

يتضمن إستخدام التوقيع الإلكتروني عمليتين، الأولى يتم انجازها من قبل الموقع والثانية من قبل مستلم التوقيع الإلكتروني على النحو التالي:

- **المرحلة الأولى:** وتتمثل في إنشاء التوقيع الإلكتروني من خلال جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني، وهو ما أوردته المادة 2 من القانون 04/15 السالف الذكر[1] في فقرتها الثالثة والرابعة حيث عرفت بيانات إنشاء التوقيع الإلكتروني على

[1]–القانون 04/15.

أنها:" بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني".

- **المرحلة الثانية:** التثبت من صحة التوقيع الإلكتروني: وهو ما جاء في الفقرتين الخامسة والسادسة من المادة 02 من القانون 04/15 حيث عرفت آلية التحقق من التوقيع الإلكتروني على أنها:" جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني المتمثلة في الرموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى مستعملة من اجل التحقق من التوقيع الإلكتروني".

وتستخدم التوقيعات الإلكترونية ما يعرف بنظام مفتاح التشفير، والذي يستخدم منهجا معينا مستعينا بمفتاحين مختلفين ولكنهما مرتبطين حسابيا، أحدهما لإنشاء التوقيع الإلكتروني، أو لتحويل البيانات إلى أشكال تبدو وكأنها غير مفهومة، والآخر للتبيين من صحة التوقيع الإلكتروني. [1]وقد عرف المشرع الجزائري مفتاح التشفير الخاص في الفقرة الثامنة من المادة 02 من القانون 04/15[2]على أنه: "عبارة عن سلسلة من الإعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي".

وعرف مفتاح التشفير العمومي في الفترة التاسعة من المادة 02 من القانون 04/15[3]"على انه:" عبارة عن سلسلة من الإعداد تكون موضوعة لمتناول الجمهور يهدف لتمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".

ورغم أن العديد من الأشخاص يمكن أن يكونوا على علم بالمفتاح الشفري العام أو ما أسماه المشرع الجزائري بمفتاح التشفير العمومي لموقع ما، ويستخدمونه للتثبت من صحة توقيعات موقع معين، إلا أنهم لا يستطيعون اكتشاف مفتاح التشفير الخاص لذلك الموقع واستخدامه في تزوير توقيعه الإلكتروني. [4]

---

[1]–ايمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق ص8.

[2]–القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

[3]–القانون 04/15.

[4]–ايمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق ص9.

2. التوقيع الإلكتروني الموصوف:

نصت المادة 10 من القانون 04/15 على وجوب تأمين آلية إنشاء التوقيع الإلكتروني والآلية المؤمنة حسب نص المادة 11 بإعتماد وسائل تقنية وإجراءات مناسبة تضمن سريتها وحمايتها من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد وإلزامية عرضها على الموقع قبل عملية التوقيع وفق آلية موثوقة للتحقق من التوقيع الإلكتروني.[1]

3. آلية التصديق الإلكتروني:

يعرف التصديق الإلكتروني على انه:" وسيلة آمنة للتحقق من صحة التوقيع أو المحرر حيث يتم نسبه إلى شخص أو كيان معين"[2]، ويتولى هذه الخدمة جهة ثالثة محايدة موثوق بها يتأكد بطرقه الخاصة من صحة صدور التواقيع الإلكترونية وكذا الإرادة التعاقدية ممن تنسب إليه ومن جدية هذه التواقيع والإرادة وبعدها عن الغش والاحتيال، ويتمثل هذا الطرف الثالث المحايد في أفراد أو شركات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين يطلق عليها اسم سلطات التوثيق أو مقدمي خدمات التصديق. [3]

وقد أوردها المشرع الجزائري في المادة الثانية من القانون 04/15 في فقرته 11 تحت اسم الطرف الثالث الموثوق، وفي الفقرة 12 بمؤدي خدمات التصديق الإلكتروني، تصدر هذه الهيئات شهادة التصديق الإلكتروني المنصوص عليها في الفقرة 7 وهي الوثيقة الإلكترونية التي تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع. وقد اعترف المشرع الجزائري بجهات التوثيق الإلكتروني في نص المادة 3 مكرر من المرسوم التنفيذي 162/07 الصادر في 30 ماي 2007 والمتعلق بنظام استغلال الشبكات بما فيها السلكية بأنها: " كل شخص في مفهوم المادة 8/8 من

---

[1]–انظر المادة 11، 12، 13، 14 من القانون 04/15.

[2]–محمد حسين منصور، الاثبات الإلكتروني، دار الفكر الجامعي، الاسكندرية، 2006، ص209.

[3]–بلحسين حمزة، المرجع السابق، ص83.

القانون 02/2000 المؤرخ في 05 أوت 2000 المذكور أعلاه، يسلم شهادات أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني".[1]

واخضع المشرع الجزائري في القانون 04/15 استغلال خدمات التصديق الإلكتروني إلى نظام الترخيص الذي تمنحه السلطة الاقتصادية للتصديق الالكتروني في شكل شهادة تأهيل، يتجسد في الوثيقة الرسمية الممنوحة لمؤدي الخدمات بطريقة شخصية تسمح له بالبدء الفعلي في توفير خدماته.

4. شهادة التصديق الإلكتروني الموصوفة:

شهادة التصديق الإلكتروني هي رسالة إلكترونية تسلم من شخص ثالث موثوق، وتكون لها وظيفة الربط بين شخص طبيعي أو معنوي وزوج من المفاتيح (الخاص، العام)، وتسمح بتحديد حائز المفتاح الخاص الذي يتطابق مع المفتاح العام المذكور فيها، وتحتوي الشهادة على معلومات عن المتعامل (اسم، عنون، أهلية، عناصر تعريفية أخرى)، والممثل القانوني بالنسبة للشخص المعنوي، واسم مصدر الشهادة والمفتاح العمومي للمتعامل، والرقم التسلسلي، وتاريخ تسليم الشهادة، وتاريخ انتهاء صلاحيتها. [2].

وقد ميز المشرع الجزائري بين نوعين من شهادة التصديق الإلكتروني، وهما شهادة التصديق الإلكتروني العادية، هذه الأخيرة التي أورد لها تعريفا في نص المادة الثانية الفقرة 07 من القانون 04/15، أما النوع الثاني المستحدث فهو يتمثل في شهادة التصديق الإلكتروني الموصوفة، ونظم أحكامها في نص المادة 15 من هذا القانون واشترط فيها ضرورة توفر بعض المتطلبات وبعض البيانات نجملها كالآتي:

- أن تمنح من طرف ثالث موثوق أو من قبل مؤدي خدمات التصديق الإلكتروني.
- أن تمنح للموقع دون سواه.

---

[1]–المرسوم التنفيذي 07–162 مؤرخ في 30 ماي 2007، يعدل ويتمم المرسوم التنفيذي رقم 01–123 المؤرخ في 09 ماي 2001 والمتعلق بنظام الاستغلال المطلق على كل نوع من انواع الشبكات بما فيها السلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

[2]–زهيرة كيسي، النظام القانوني لجهات التوثيق (التصديق الإلكتروني) مجلة دفاتر السياسة والقانون، المركز الجامعي بتمنراست الجزائر ص 216 العدد السابع، جوان 2012.

- ضرورة أن تتضمن بعض البيانات من بينها التأشير فيها بأنها شهادة تصديق إلكتروني موصوفة.
- تحديد هوية الطرف الذي أصدرها سواء كان طرفا ثالثا موثوق أو مؤدي خدمات التصديق الإلكتروني، وكذا تحديد البلد الذي يقيم فيه.
- إدراج اسم الموقع وصفته عند الاقتضاء وذلك حسب الغرض من استعمال تلك الشهادة.
- تضمينها البيانات المتعلقة بالتوقيع الإلكتروني، كتلك الذي تتعلق بالتحقق من هذا التوقيع.
- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني. [1]

كما نص المشرع الجزائري على صاحب شهادة التصديق الإلكتروني في القانون 04/15 السالف الذكر المادة الثانية فقرة 14 على أنه: " شخص طبيعي أو معنوي تحصل على شهادة التصديق الإلكتروني من طرف مؤدي خدمات التصديق الإلكتروني أو طرف ثالث".

ثانيا: سلطات التصديق الإلكتروني

إستحدث المشرع الجزائري بموجب القانون 04/15 المذكور آنفا ثلاثة سلطات للتصديق الإلكتروني، وقد نظم أحكامها في الباب الثالث من هذا القانون أسماه بسلطات التصديق الإلكتروني، وتتمثل هذه السلطات في: السلطة الوطنية للتصديق الإلكتروني، السلطة الحكومية للتصديق الإلكتروني، والسلطة الاقتصادية للتصديق الإلكتروني.

وحدد مهام كل سلطة بصورة تضمن ترقية استعمال التوقيع والتصديق الإلكترونيين وتطورهما وتضمن موثوقية استعمالهما. [2]

1. السلطة الوطنية للتصديق الإلكتروني:

وهي سلطة إدارية تنشأ لدى الوزير الأول مستقلة وتتمتع بالشخصية المعنوية والاستقلال المالي حسب نص المادة 16 من القانون 04/15 المذكور أعلاه، وتتمثل مهمتها الأساسية في إعداد

[1]–للمزيد من التفاصيل انظر المادة 15 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2]– بلحسين حمزة، مرجع سابق، ص86.

سياسة للتصديق الإلكتروني والسهر على تطبيقها، وكذا إعداد واقتراح ما تراه مناسبا من مشاريع تمهيدية للنصوص التشريعية والتنظيمية ذات العلاقة بالتوقيع والتصديق الإلكترونيين. [1]

2. السلطة الحكومية للتصديق الإلكتروني:

وهي سلطة تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والإتصال، تتمتع بالاستقلال المالي والشخصية المعنوية حسب نص المادة 26من القانون 04/15، من مهامها متابعة ومراقبة التصديق الإلكتروني وضمان توفير هذه الخدمة لفائدة المتدخلين في الفرع الحكومي وكذا إعداد القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع الإلكتروني والسهر على تطبيقها وذلك بعد الحصول على موافقة من السلطة الوطنية. [2]

3. السلطة الاقتصادية للتصديق الإلكتروني:

تعتبر أهم سلطة من سلطات التصديق الإلكتروني، باعتبارها هيئة تحكمية تتبع سلطة الضبط للبريد والمواصلات السلكية واللاسلكية، وقد وسع المشرع الجزائري من مهامها بموجب القانون 04/15 حيث أعطى لها الحق في منح التراخيص لمؤدي خدمات التصديق الإلكتروني، واتخاذ كل التدابير الضرورية لضمان استمرارية الخدمات في حالة عجز مؤدي خدمات التصديق عن تقديم خدماته، وكذا صلاحية التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين وإبلاغ النيابة العامة عن كل فعل جزائي تكتشفه وهي تقوم بتأدية مهامها. [3]

الفرع الثاني: الآثار القانونية للتوقيع الإلكتروني:

إن الهدف الأول من التوقيع سواء كان تقليديا أو إلكترونيا هو تحديد هوية الموقع والتزامه، كما انه أداة للتعبير عن إرادة الشخص الموقع وموافقته على المعلومات الواردة في المحرر الذي يرتبط به وبالالتزامات الواردة فيه.

وفي مجال التوقيع الالكتروني فإنه يثبت سلامة المحرر الإلكتروني، ومن ثم ينتج الآثار القانونية، أو ما يسمى فقها بحجية التوقيع الإلكتروني في مجال الإثبات.

---

[1]–انظر المادة 188 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2]–انظر المادة 28 من القانون 04/15.

[3]–بلحسين حمزة، مرجع سابق، ص88.

وعليه سيتم التطرق إلى مبادئ المماثلة وعدم التمييز تجاه التوقيع الإلكتروني كما نص عليها المشرع الجزائري في القانون 04/15 السالف الذكر، وأثر ذلك الاعتراف من حيث حجيته في الإثبات.

أولا: مبادئ المماثلة وعدم التمييز تجاه التوقيع الإلكتروني:

تبنى المشرع الجزائري مبدأ المماثلة وعدم التمييز تجاه التوقيع الإلكتروني بموجب القانون 04/15، وهو تحصيل حاصل لمبدأ التعادل الوظيفي بين التوقيع التقليدي والتوقيع الإلكتروني بكافة أشكاله الوارد في نص المادة 323 مكرر 1 من القانون المدني الجزائري والتي يستلخص منها نتيجتان:

- **الأولى:** عدم التميز بين الكتابة بسبب الوسيط الذي تتم من خلاله، سواء تمت الكتابة على وسيط ورقي أو عبر وسيط إلكتروني، فان هذا الأمر لا يحول دون قوتهما في الإثبات.
- **الثانية:** المسأواة الوظيفية بين المحرر الإلكتروني والمحرر التقليدي، وبالنتيجة المساواة بين التوقيع التقليدي والتوقيع الإلكتروني. [1]

كما اشترطت المادة 8 من القانون 04/15 السالف الذكر أن يكون التوقيع الإلكتروني موصوفا[2]، حيث نصت على انه: "يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي".

ولا يمكن في نظر المشرع الجزائري تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب شكله أو انه لا يعتمد على شهادة تصديق إلكترونية موصوفة أو انه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني. [3]

[1]–زهدور كوثر، حجية التوقيع الإلكتروني في الإثبات والمسؤولية المدنية المتولدة عنه في التشريع الجزائري، مجلة الدفاع، العدد الثاني، ص 105.

[2]–انظر المادة 07 من القانون 04/15.

[3]–انظر المادة 09 من القانون 04/15 .

ثانيا: حجية التوقيع الإلكتروني في الإثبات:

لا شك أن احد أهم عناصر الحماية للتوقيع الإلكتروني هو تنظيم التزامات قانونية على عاتق الأطراف ذات الصلة به، سواء تعلق الأمر بطرفي المعاملة أو بالجهات التي تلعب دورا في إنشائه وإدارته. [1]

وقد اتفقت جميع التشريعات التي أضفت الحجية القانونية على التوقيع الإلكتروني على ضرورة توافر شروط معينة تعزز من هذا التوقيع وتوفر فيه الثقة حتى يتمتع بالحجية.

وتدور هذه الشروط حول كون التوقيع مقصورا على صاحبه، وخاضعا لسيطرته المطلقة وقابلية التحقق من صحته، هذا بالإضافة إلى ارتباطه بالبيانات التي يثبتها. [2]

- **موقف المشرع الجزائري:**

عدل المشرع الجزائري وتمم بموجب المادة 46 المادة 327 من القانون المدني الجزائري وأورد في الفقرة الثانية من المادة ما يلي:"...ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر أعلاه". وعليه فقد اعتد المشرع الجزائري بالتوقيع الإلكتروني، ولكن اقرن قبوله في الإثبات بتوفر شروط نصت عليها المادة 323 ف1 من ذات القانون[3]انه: " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق شرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

ومع صدور القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين نص المشرع الجزائري صراحة على القوة القانونية للتوقيع الإلكتروني في الإثبات مثله مثل التوقيع المكتوب في نص المادة 8 منه شريطة خضوعه لمتطلبات أوردها في المادة 7 من نفس القانون وهي:

أ. أن ينشأ التوقيع الإلكتروني على أساس شهادة تصديق إلكتروني موصوف.

---

[1]–ايمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق، ص61.

[2]–سليم سعداوي، عقود التجارة الإلكترونية، دار الخلدونية، الجزائر 2008، ص103.

[3]– المادة 44 من القانون 10/05 المؤرخ في 2005/06/20 تممت الأمر 58/75 المؤرخ في 1975/09/26 المتضمن القانون المدني بالمادتين 323 مكرر و323 مكرر.

ب. أن يرتبط بالموقع دون سواه.

ج. أن يمكن تحديد هوية الموقع.

د. أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

هـ. أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

و. أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

الفرع الثالث: المسؤولية المدنية الناشئة عن المعاملات الإلكترونية الحاملة لتوقيعات إلكترونية:

تقوم المسؤولية المدنية طبقا للنظرية التقليدية بالإخلال بالتزام سابق، وبناء على طبيعة الالتزام المخل به تنقسم المسؤولية المدنية إلى نوعين: مسؤولية عقدية ومسؤولية تقصيرية، ولقيام كلا المسؤوليتين لابد من توافر أركان انعقادهما هي: الخطأ، الضرر، والعلاقة السيئة بينهما، ومع ظهور شبكة الأنترنت إنتقلت المعاملات المدنية من الدعامات الورقية إلى الدعامات الإلكترونية، أي أصبحت المعاملات تتم عبر وساطة إلكترونية[1].

أولا: المسؤولية العقدية لمقدمي خدمات التصديق الالكتروني

تقوم المسؤولية العقدية لوقوع الإخلال بالالتزام العقدي، ومن الطبيعي أن يستوجب هذاأولا وجود عقد صحيح لم يلتزم أحد الطرفين بتنفيذ إلتزام يتعلق به، والعقد الصحيح كما عرفه المشرع الجزائري بالمادة 54 من القانون المدني[2]، وهو: "اتفاق يلتزم بموجبه شخص أو عدة أشخاص نحو شخص أو عدة أشخاص آخرين بمنح أو فعل أو عدم فعل شيء يترتب على العقد إنشاء التزامات تقع على كاهل كل من طرفيه والقوة الملزمة للعقد تقضي بأن يقوم كل طرف بتنفيذ التزامه العقدي "[3] . فالمسؤولية العقدية هي جزاء لعدم قيام المتعاقد بتنفيذ التزامه، أو تأخره في هذا التنفيذ وهي تؤدي إلى

---

[1]–زهدور كوثر، حجية التوقيع الإلكتروني في الاثبات والمسؤولية المدنية المتولدة عنه في التشريع الجزائري، مرجع سابق، ص 107.

[2]– المادة 54 من الأمر رقم 75–58المؤرخ في 26سبتمبر 1975، المعدل والمتمم بالقانون رقم 05–10المؤرخ في 20يونيو 2005.

[3]–محمد صبري السعدي، الواضح في شرح القانون المدني، الطبعة الرابعة، دار الهدى، الجزائر، 2009، ص310–311.

تعويض المتعاقد لما أصابه من ضرر بسبب عدم تنفيذ العقد، [1]طبقا للقانون المدني الجزائري الذي يجبر المتعاقد على تنفيذ إلتزاماته التعاقدية . ومن النصوص القانونية التي تفيد هذا المعنى المادة106التي تنص على أن: "العقد شريعة المتعاقدين"[2]، والمادة 107: "يجب تنفيذ العقد طبقا لما اشتمل عليه وبحسن النية"[3]، والمادة 164[4] التي تجبر المدين بعد إعذاره –وفقا للمادتين 180 و181–[5]على تنفيذ التزاماته عينيا متى كان ذلك ممكنا، وعلى ذلك إن لم يقم المدين بتنفيذ التزاماته العقدية، فإن الركن الأول للمسؤولية العقدية يكون قد توفر ألا وهو الخطأ العقدي.

1) أركان المسؤولية العقدية لمقدمي خدمات التصديق الإلكتروني:

تفترض المسؤولية العقدية وجود عقد صحيح واجب التنفيذ فتقوم هذه المسؤولية عن عدم الوفاء بالالتزام المفروض، مما يلحق الضرر بالمتعامل، فلهذا لا تقوم المسؤولية إلا عند قيام الأركان الثلاث والمتمثلة فيما يلي :

أ. ركن الخطأ العقدي

نصت المادة 176 من القانون المدني الجزائري على القاعدة العامة للعقود التي تجعل المدين مسؤولا بمجرد عدم الوفاء ما لم يثبت أن سببا أجنبيا هو الذي حال بينه وبين الوفاء، وبتالي فإن هذه المادة هي التي تحكم الخطأ العقدي في القانون المدني الجزائري.

أما المادة 172 من القانون المدني الجزائري فهي تختص بتحديد مدى الإلتزام ببذل عناية في الوفاء بالإلتزام، فالخطأ العقدي كما سبق وأن أشرنا هو السبب فيما أصاب الدائن من ضرر، ويبقى المدين مسؤولا لنص المادة 2/172 عن غشه وسوء نيته أو إهماله أو خطئه الجسيم.

---

[1]–نبيل إبراهيم سعد، النظرية العامة للالتزام، مصادر الالتزام، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 296.

[2]–انظر المادة 106من القانون المدني الجزائري

[3]–انظر المادة 107من القانون المدني الجزائري

[4]–انظر المادة 164من القانون المدني الجزائري

[5]– انظر المادتين 180و 181 من القانون المدني الجزائري.

فإن الخطأ العقدي هو انحراف إيجابي أو سلبي في سلوك المدين يؤدي إلى مؤاخذته ومعيار الانحراف[1]، هنا هو معيار الرجل العادي وهذا المعيار يستفاد من نص المادة 172 من القانون المدني الجزائري، وهذه الفكرة مجردة يرجع في تحديدها إلى الرجل العادي في طائفة الناس التي ينتمي إليها المدين في نفس الظروف والملابسات.

يتحقق الخطأ العقدي لجهة التصديق الإلكتروني في حالة الإخلال بأي من الالتزامات الملقاة على عاتقه، بموجب عقد التصديق وهو ما يعرف بالركن المادي والمتمثل في ما يلي:

- الإهمال في حماية البيانات الخاصة بالتوقيع الإلكتروني.
- عدم التحقق من صحة البيانات أي عدم الإلتزام ببذل عناية فيتحقق الخطأ العقدي بعدم بذل العناية اللازمة والكافية من جانب مقدم خدمات التصديق الإلكتروني.
- عدم الإلتزام بسرية المعلومات يتحقق الخطأ العقدي وهذا لعدم تحقيق النتيجة، أو الغاية المطلوبة ويصبح مقدم خدمات التصديق الإلكتروني مجبر على التعويض بقوة القانون نتيجة تسرب المعلومات الخاصة .

إن المسؤولية العقدية لمقدم خدمة التصديق الإلكتروني تجاه الغير المتضرر من تعويله على الشهادة، لا تقوم إلا إذا كان هناك عقد يربط الغير المتضرر مع جهة التصديق، حيث تضمن هذه الجهة بموجب العقد صحة المعلومات التي تتضمنها شهادة التصديق الإلكتروني، وفي حالة ثبوت تقصير أي طرف من أطراف التعاقد بهذه الإلتزامات، ونتج عنه ضرر أصاب الطرف الأخر فان المسؤولية العقدية هي التي تطبق هنا عند توافر باقي أركانها.

ب. ركن الضرر

الضرر هو الأذى الذي يلحق شخص في حق من حقوقه أو مصلحة مشروعة له، سواء كان ذلك الحق أو تلك المصلحة ذات قيمة مالية أو أدبية، والضرر روح المسؤولية المدنية وعلتها التي تدور معها وجودا وعدما فلا مسؤولية مدنية دون ضرر مهما بلغت درجة جسامة الخطأ، والتعويض

[1]– محمد صبري السعدي، الواضح في شرح القانون المدني الجزائري، النظرية العامة للالتزامات، مصادر الالتزام، الجزء الأول، الطبعة الأولى، دار الهدى للنشر والتوزيع، الجزائر، 2007 – 2008، صفحة 313.

عن الضرر وفقا للمادة 176 ق. م. ج يكون عن عدم تنفيذ الإلتزام وقد يكون عن التأخر في تنفيذه.[1]

يعد الضرر الركن الأساسي في قيام المسؤولية المدنية، فهو السبيل نحو المساءلة المدنية فلا مسؤولية عند انتفاء الضرر لتخلف هذا الركن الجوهري، ويقع عبء إثبات الضرر على من يدعيه، والضرر بوجه عام هو الأذى الذي يصيب حقا أو مصلحة مشروعة للشخص المتعاقد معه، وهذا الأذى أو التعدي قد ينشأ عن الإخلال بالتزام يفرضه القانون.[2]

ولا يكفي أن يكون هناك خطأ عقدي فقط حتى تقوم مسؤولية مقدم خدمات التصديق الإلكتروني، إنما يجب أن يكون هناك ضرر لحق بصاحب الشهادة جراء هذا الخطأ، فإذا توافر سبب موجب لتعليق العمل بشهادة التصديق أو إلغائها ولم يقم مقدم الخدمات التصديق بهذين الإجرائيين، يكون قد أخل بالتزام مفروض عليه إذا لحق ضرر بصاحب الشهادة نتيجة لهذا الإهمال، وتتم مسائلة مقدم خدمات التصديق الإلكتروني عن ذلك ويلتزم بالتعويض للمتضرر وفقا لأحكام المسؤولية العقدية، فإذا فقد صاحب الشهادة مفتاحه الخاص وطلب من جهة التصديق إلغاء العمل بشهادة التصديق ولم يستجيب لطلبه وترتب عن ذلك إستعمال غير مشروع لهذا المفتاح باسم صاحب المفتاح دون ترخيص منه أو علم به تقوم المسؤولية العقدية في حق مقدم خدمة التصديق لتعويض صاحب الشهادة عن الضرر الذي لحق به، لأن القاعدة العامة في التعويض هي أن الضرر المباشر المتوقع هو الذي يعوض عنه المسؤولية العقدية، فالضرر غير المباشر لا يعوض عنه مطلقا سواء في المسؤولية العقدية أو المسؤولية التقصيرية.[3]

ويرتبط شرط التعويض بتحقق الضرر، حيث يلتزم مسبب الضرر الذي هو مقدم خدمة التصديق الإلكتروني بالتعويض بقدر حجم الضرر، أما في حالة العكس إذا أثبت مقدم خدمات التصديق أن إلتزاماته لا يجوز مساءلته بها لحق يفرضه القانون، كصدور حكم قضائي يجيز نشر

---

[1]– حسن علي الذنون، ومحمد سعد الرحو، الوجيز في النظرية العامة للالتزام– مصادر الالتزام– الجزء الأول، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن، 2000، ص 208

[2]– منذر الفضل، النظرية العامة للالتزامات، الجزء الأول، دار الثقافة، عمان، الأردن، 1996، ص 299–300.

[3]– لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص181.

البيانات أو الإعلان عن المعلومات الخاصة بصاحب شهادة التصديق، فتنتفي المسؤولية العقدية لمؤدي خدمة التصديق الإلكتروني، فلا ضرورة لها بالتعويض وهو ما تضمنه نص المادة127من القانون المدني الجزائري "إذا اثبت الشخص أن الضرر قد نشا عن سبب لا يد له فيه كحادث مفاجئ أو قوة قاهرة أو خطا صدر من المضرور كان غير ملزم بتعويض هذا الضرر"، والمادة 176من القانون المدني الجزائري .

أما فيما يخص التعويض عن الضرر الأدبي، وعلى الأخص فيما يتعلق بالمسؤولية العقدية فقد أثار خلافا كبيرا في الفقه والقضاء، فذهب القضاء الفرنسي في بداية الأمر إلى عدم تعويض عن الضرر الأدبي لعدم إمكانية تقويمه بنقود، كما ذهب إلى ذلك بعض الفقهاء إلى أن الضرر المعنوي الذي يترتب وحده على الإخلال بالالتزام عقد لا ينشأ حقا في التعويض عنه غير أنه استقر في الفقه والقضاء المعاصرين جواز التعويض عن الضرر الأدبي في المسؤولية العقدية.[1]

وقد جاء نص المادتين 124 و176 من القانون المدني الجزائري المتعلقتين بالمسؤولية العقدية والتقصيرية بشكل عام وبصفة مطلقة وكلية، مما يفيد أن التعويض يشمل الضرر الأدبي أيضا.

مما لاشك فيه أنه لا يكفي تحقق الضرر حتى تقوم المسؤولية العقدية لمقدم خدمات التصديق الإلكتروني وإنما على المضرور أي صاحب شهادة التصديق إثبات أن الضرر نتيجة لإهمال هذا الأخير وإخلاله بالتزاماته.[2]

ج. علاقة السببية بين الخطأ والضرر:

إن علاقة السببية هي الركن الثالث لقيام المسؤولية العقدية، فإذا انتفت علاقة السببية انقطعت انتفت معها المسؤولية، ولا يخرج هذا الضرر من حيث المبدأ عما قررته القواعد العامة في المسؤولية المدنية في مجال الضرر.

---

[1]– حمدي باشا عمر، القضاء المدني، ط4، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009، ص83.

[2]–لينا إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة (دراسة مقارنة)، دار الراية للنشر والتوزيع، ط1، الأردن عمان.

العلاقة السببية هي تلك الصلة التي تربط الضرر بالخطأ، فتجعل الضرر نتيجة للخطأ فإذا انعدمت انتفت المسؤولية لانعدام ركن من أركانها، وتنتفي الرابطة السببية عموما إذا تدخل سبب أجنبي، ليفصل بين الضرر الذي أصاب صاحب الشهادة، وبين الخطأ الذي صدر من مقدم خدمات التصديق الإلكتروني، فالضرر الذي يصيب صاحب الشهادة، يجب أن يكون سببه الخطأ الذي ارتكبه مقدم خدمات التصديق الإلكتروني، والمتمثل بإخلاله بالتزاماته العقدية كأن يصدر شهادة تصديق معيبة مما يؤدي إلى تفويت الصفقة على صاحب الشهادة ومنه تعرضه إلى خسارة مادية واجبة التعويض من الجهة المسؤولة كما أن الضرر الناتج عن خطا ارتكبه مقدم خدمات التصديق الالكتروني يجب أن يكون ضررا مباشر ينحصر داخل الالتزامات التي تقع على عاتق مقدم خدمات التصديق الإلكتروني، كالالتزام ببذل عناية، مثل التحقق من صحة البيانات والمعلومات الشخصية والحفاظ على سرية المعلومات التي مكنت منها، لأنه المبدأ الأساسي الذي يعطيها مصداقية العمل في مجال التصديق الإلكتروني والغاية المرجوة من المتعاملين، كذلك الإلتزام بتحقيق نتيجة والتي تتمثل في إصدار شهادة تصديق مراعية للغاية التي صدرت من أجلها مستوفية لجميع الشروط اللازمة لإصدارها وتكون ذات حجية للمتمسك بحجيتها بما يخدم صاحبها.[1]

ثانيا: المسؤولية التقصيرية لمقدم خدمات التصديق الإلكتروني:

تقوم المسؤولية التقصيرية على الإخلال بالتزام قانوني واحد لا يتغير، هو الإلتزام بعدم الإضرار بالغير ولا ترتبط جهة التصديق مع الغير المتضرر بأي عقد رسمي.[2]

قد لا تكون مسؤولية مقدم خدمات التصديق الإلكتروني عقدية، وهذا بالطبع عند عدم وجود علاقة عقدية بين مركز التصديق وأولئك المتضررين من طرف أخر، ويعتبر من الغير كل شخص لا تربطه أية علاقة عقدية مع مركز التصديق يشترط لقيام المسؤولية التقصيرية أن يكون الفعل من قبيل

[1]– عبد الرزاق احمد ا السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني، ط3، منشورات الحلبي الحقوقية، بيروت، لبنان، 1998ص 241.

[2]– عبد الرزاق احمد ا السنهوري، مرجع سابق، ص241.

الخطأ حيث نصت المادة 124 من القانون المدني الجزائري: "أن كل فعل أيا كان يرتكبه الشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"[1].

وللمسؤولية التقصيرية بصفة عامة ثلاثة أركان هي:

1. ركن الخطأ

إن أي إهمال أو تقصير يسجل على مستوى مقدم خدمات التصديق الإلكتروني يخل بإلتزاماته من شأنه أن يقيم مسؤولية المركز وفقا لأحكام المسؤولية المدنية التقصيرية، متى توفر الثالوث الشهير الخطأ، الضرر، والعلاقة السببية بينهما، إن قيام هذه المسؤولية يتطلب توافر أركان لهذه المسؤولية، أولها وأهمها الخطأ التقصيري، أي الإخلال بالالتزام القانوني العام المتمثل في احترام حقوق الآخرين وعدم الإضرار بهم، وهذا الإلتزام هو إلتزام ببذل عناية، فالإخلال به يشكل خطا يوجب المسؤولية إذا لم يبذل مقدم خدمات التصديق الإلكتروني العناية اللازمة من الحيطة والتبصر، وهو ما يجب على الغير المتضرر إثباته وإقامة البينة عليه وذلك بإقامة الدليل على أن مقدمات خدمات التصديق الإلكتروني لم يبذل العناية اللازمة المعتادة، ولا شك أن ذلك ليس بعمل يسير على الغير المتضرر من سلوكه، لأنه إذا اثبت هذا الأخير أنه قام بالعناية المعتادة والمطلوبة منه، يسقط حق المضرور في مسائلة جهة التصديق وبالتالي يسقط حقه بالتعويض. إن الخطأ في المسؤولية التقصيرية، هو إخلال الشخص بالتزام قانوني مع إدراكه بان هذا الإخلال قد يضر بالغير، ويتمثل الإلتزام القانوني الذي يعتبر الإخلال به خطأ يبرر المسؤولية التقصيرية، في ضرورة أن يصطنع الشخص في سلوكه قدرا من اليقظة والتبصر حتى لا يضر بالغير، فإذا انحرف عن السلوك الواجب، وكان من القدرة على التمييز بحيث يدرك أنه قد انحرف فان انحرافه هذا يعد خطأ يستوجب المسؤولية التقصيرية.

2. ركن الضرر:

الضرر هو الركن الثاني للمسؤولية التقصيرية، لا يكفي لتحقق هذه المسؤولية أن يقع الخطأ بل يجب أن يحدث ضرر نتيجة للخطأ، والمضرور هو الذي يثبت وقوع الضرر به ويجوز إثبات الضرر بأي وسيلة ممكنة، كونه واقعة مادية والضرر نوعان ضرر مادي، وضرر أدبي:

---

[1]– المادة 124من الأمر رقم: 75/ 85المؤرخ في 26سبتمبر 1975المعدلة والمتممة بالقانون رقم 10/05المؤرخ في 20 يوليو 2005 .

الضرر المادي هو إخلال بمصلحة المضرور ذات القيمة المالية ويجب أن يكون هذا الإخلال محققا ولا يكفي أن يكون محتمل الحدوث.

الضرر الأدبي هو الضرر الذي لا يصيب الشخص في ماله وإنما يصيب مصلحة غير مالية والضرر الأدبي قابل للتعويض بالمال.[1]

3. ركن العلاقة السببية

لقيام علاقة السببية بين الضرر والخطأ، يجب أن يكون الخطأ هو السبب في حصول الأذى للمتضرر، فإذا لم يتحقق هذا الشرط لا تقوم المسؤولية التقصيرية لانتفاء هذه الرابطة، فإذا تدخلت عوامل أخرى قطعت ارتباط الضرر بالخطأ، فلا تتحقق هذه السببية لأن النتيجة ليست مرتبطة بالسبب ارتباطا طبيعيا.[2]

العلاقة السببية هي الركن الثالث للمسؤولية التقصيرية، تتمثل في العلاقة السببية بين الخطأ والفعل الضار والضرر بان يكون الفعل هو السبب في حدوث الضرر فإذا انتفت علاقة السببية لأي سبب لا يد للمدين فيه فلا تقوم المسؤولية التقصيرية.[3]

ثالثا: مسؤولية مقدم خدمات التصديق الإلكتروني وفقا للقواعد الخاصة

تنبهت بعض التشريعات المنظمة لعمل مقدم خدمات التصديق الإلكتروني، للأهمية المترتبة على تنظيم مسؤولياته في حال إخلاله بالإلتزامات المترتبة عليه، فأفردت له نصوصا قانونية خاصة نظمت فيها الحالات التي تنعقد بها مسؤولية هذه الجهات وكذلك إعفائها من المسؤولية وجواز تقييدها، تمثلت هذه التشريعات في قانون المبادلات والتجارة الالكترونية التونسي، وقانون المعاملات والتجارة الالكترونية لإمارة دبي، [4]وقد سلك المشرع الجزائري ذات النهج .

---

[1]–عبد الرزاق السنهوري، المرجع السابق، ص 984–982

[2]–منذر الفضل، المرجع السابق، ص 449

[3]–لينا إبراهيم يوسف، مرجع سابق، ص 166.

[4]– تقوم مسؤولية مقدم خدمات التصديق الإلكتروني وفقا للقانون التونسي في الحالات التالية:

أ– إخلالها بالضمانات المنصوص عليها في قانون المبادلات التونسي، وتتمثل هذه الضمانات في:

- ضمان صحة المعلومات المصادق عليها التي تضمنتها الشهادة من تاريخ تسلمها.

- ضمان الصلة بين صاحب الشهادة ومنظومة التدقيق في الإمضاء الخاصة به، انفراده بمسك منظومة إحداث إمضاء مطابقة لأحكام القرار المنصوص عليه بالفصل الخامس من هذا القانون ومتكاملة مع منظومة التدقيق في الإمضاء المعرفة في الشهادة في تاريخ تسلمها.
- التحقق من الشخص الطبيعي عند إصدار وتسليم شهادة المصادقة إليه بوصفهم مثلا للشخص المعنوي والتحقق من صحة تمثيله للشخص المعنوي.

ب- إخلال مقدم خدمات التصديق الإلكتروني بالتزاماته بتعليق أو إلغاء الشهادة متى توافرت الأسباب الموجبة لهما، فإنه يكون مسؤولا عن تعويض الضرر الناشئ عن إخلاله بالتزامه، لكن إذا كان التعليق أو الإلغاء بناء على طلب صاحب الشهادة وترتب عليه ضرر للغير، فإن صاحب الشهادة هو المسؤول عن تعويض الضرر وليس مقدم الخدمة، وإذا كان التعليق أو الإلغاء بناء على قرار من مقدم الخدمة نفسه وترتب عليه ضرر للغير إذا توافرت إحدى حالاته فهنا نفرق بين ما إذا كان الضرر أصاب صاحب الشهادة أو الغير فإذا كان الضرر أصاب صاحب الشهادة نفسه فإن مزود الخدمة يسأل وفق القواعد المسؤولية العقدية لوجود علاقة عقدية بينه وبين صاحب الشهادة، أما إذا كان الضرر لحق بالغير فإن مقدم الخدمة يسأل وفق القواعد المسؤولية التقصيرية متى توافرت عناصرها، وفي جميع الأحوال فإن مقدم الخدمة الذي يخلب أي من الواجبات المفروضة عليه فإنه يعرض نفسه لعقوبة سحب الترخيص وإيقاف نشاطه، تجدر الإشارة في هذا الصدد إلى أنه لا تقوم مسؤولية مزود الخدمة وفق القانون المبادلات التونسي عند عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث إمضاءه الإلكتروني أولا، وعند قيام مقدم الخدمة بتعليق العمل بشهادة المصادقة أو إلغائها بناء على طلب صاحب الشهادة وحصول ضرر للغير نتيجة هذا التعليق أو الإلغاء ثانيا، وفي كلتا الحالتين لا يكون أمام المتضرر سوى الرجوع على صاحب الشهادة بالتعويض عن الضرر وفق الأحكام المسؤولية التقصيرية وليس على مزود الخدمة.

كما تقوم مسؤولية مقدم خدمات التصديق الإلكتروني وفقا لقانون المعاملات والتجارة الإلكترونية لإمارة دبي:

- إذا حدثت أية أضرار نتيجة لعدم صحة الشهادة أو نتيجة لأي عيب فيها يكون مقدم خدمات التصديق الإلكتروني مسؤولا على خسائر التي يتكبدها :
- كل طرف تعاقد مع مقدم خدمات التصديق الإلكتروني حول تقديم الشهادة.
- أي شخص اعتمد بصورة معقولة على الشهادة التي أصدرها مقدم خدمات التصديق، وفقا لهذا القانون تقوم مسؤولية مقدم الخدمة في حالة عدم صحة شهادة المصادقة ووجود عيب في الشهادة، وهذه المسؤولية تكون إما عقدية في مواجهة أي شخص ارتبط معه بعقد، وهو في هذه الحالة صاحب الشهادة، وإما أن تكون تقصيرية في مواجهة أي شخص لم يرتبط معه بعلاقة عقدية، ولحقه ضرر نتيجة إهماله وخطئه وتقوم هذه المسؤولية في مواجهة أي شخص اعتمد بصورة معقولة على الشهادة التي أصدرها مقدم الخدمة، إلا أن المشرع لم يحدد معيار الفصل الأول الإطار المؤسساتي للتصديق الإلكتروني الاعتماد المعقول بموجب نص المادة24، غير أن نص

الفقرة الثانية من المادة21 من نفس القانون حدد بعض الاعتبارات التي يمكن بموجبها تحديد ما إذا كان الاعتماد معقولا أم لا وهي:

- طبيعة المعاملة المعنية والتي قصد تعزيزها بالتوقيع الإلكتروني:
- إذ أن مدى التأني والتدقيق في التوقيع الإلكتروني، يختلف باختلاف طبيعة المعاملة إذا كانت مدنية أو تجارية أو إدارية.
- قيمة أو أهمية المعاملة متى كان ذلك معروفا: فالمعاملات كبيرة القيمة أو ذات أهمية خاصة تحتاج إلى التأني والتدقيق أكثر مما تحتاج إليه في معاملات أخرى.
- إذا كان الشخص الذي اعتمد على التوقيع الإلكتروني أو الشهادة قد اتخذ خطوات مناسبة ليقرر مدى إمكانية الاعتماد على التوقيع الإلكتروني أو الشهادة.
- إذا كان الشخص الذي اعتمد على التوقيع الإلكتروني قد اتخذ خطوات مناسبة للتحقق من أن التوقيع الإلكتروني معزز بشهادة، أو من المتوقع أن يكون كذلك.
- ما إذا كان الطرف الذي اعتمد على التوقيع الإلكتروني أو الشهادة قد عرف أو كان عليه أن يعرف أن التوقيع الإلكتروني أو الشهادة قد عُدلت أو ألغيت.
- أي اتفاقية أو سياق تعامل بين المنشئ والطرف الذي اعتمد على التوقيع الإلكتروني أو الشهادة أو أي عرف تجاري سائد؛ فقد يتم الاتفاق بينهما على آلية معينة يتم من خلالها اعتماد التبادلات الإلكترونية، وكذلك قد يكون هناك عرف تجاري يوجب على العملاء أخذ بعض الخطوات للاعتماد على التوقيع الإلكتروني أو الشهادة بصورة معقولة.
- أي عامل ذي صلة، كسمعة صاحب الشهادة، ومدى تمتعه بأهلية إبرام التصرفات القانونية، وتجدر الإشارة في هذا الصدد أنه تنتفي مسؤولية مقدم خدمات التصديق الإلكتروني وفقا لنص الفقر ة الخامسة من المادة 24 من قانون المعاملات والتجارة الإلكترونية لإمارة دبي، إذا أدرج في الشهادة بيان يقيد نطاق ومدى مسؤوليته تجاه أي شخص ذي صلة، ومدى ذلك القيد، و إذا أثبت أنه لم يقترف أي خطأ أو إهمال، أو أن الضرر نشأ عن سبب أجنبي لا يد له فيه.

وفي جميع الأحوال لابد أن لا نوسع من حالات إعفاء مقدم خدمات التصديق أو إعفاءهم كليا من المسؤولية، مما قد يؤثر سلبا على المعاملات الإلكترونية وعدم التشجيع على التعامل بموجبها، ونفي الثقة فيها، في الوقت التي هي بأشد الحاجة إلى الثقة والأمان. راجع :- لينا إبراهيم يوسف، مرجع سابق، ص 166.

- الفصل الثامن عشر من قانون المبادلات والتجارة الكترونية التونسي .
- زهرة الكبسي، مرجع سابق، ص 220-221.

- المادتين (21-24) من قانون المعاملات والتجارة الالكترونية لإمارة دبي سنة 2002.

- لينا إبراهيم يوسف حسان، مرجع سابق، ص 146-152.-https://www.dc.gov.ae

رابعا: مسؤولية مؤدي خدمات التصديق الكتروني وفقا لقانون رقم 15-04

يكون مقدم خدمات التصديق الالكتروني الذي سلم شهادة التصديق الالكتروني موصوفة مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي كان أو معنوي اعتمد على هذه الشهادة وذلك من خلال:

- التأكد من صحة المعلومات الواردة في شهادة التصديق الالكتروني الموصوفة ضمن الشهادة.
- التأكد عند منح شهادة التصديق الالكتروني أن الموقع الذي تم تحديد هويته في شهادة التصديق يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدم، والمحدد في شهادة التصديق الإلكتروني والتحقق منها بدقة.[1]
- يكون مقدم خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن عدم إلغاء شهادة التصديق الإلكتروني هذه والذي يلحق بكل شخص طبيعي أو معنوي اعتمدوا على تلك الشهادة إلا إذا قدم مقدم خدمات التصديق الإلكتروني ما يثبت انه لم ير تكب أي إهمال.
- يمكن لمقدم خدمات التصديق الإلكتروني أن يشير في شهادة التصديق إلى الحدود المفروضة على استعمالها بشرط أن تكون الإشارة واضحة ومفهومة من طرف الغير، في هذه الحالة لا يكون مسؤولا عن الضرر الناتج لاستعمالها عند تجاوز الحدود المفروضة على استعماله.
- يمكن لمقدم خدمات التصديق الإلكتروني أن يشير في الشهادة إلى الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها شهادة التصديق الإلكترونية شريطة أن تكون واضحة ومفهومة للمتلقي، وفي هذه الحالة لا يكون مقدم خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن تجاوز ذلك الحد الأقصى.
- يجب على مقدم خدمات التصديق الإلكتروني إعلام السلطة الاقتصادية للتصديق الإلكتروني برغبته فيوقف نشاطه المتعلق بتأدية خدمات التصديق الإلكتروني أو بأي فعل يؤدي إلى ذلك.
- يجب على مقدم خدمات التصديق الإلكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته أن يعلم السلطة الاقتصادية للتصديق الإلكتروني بذلك فورا كما تقوم هذه الأخيرة بإلغاء شهاداته للتصديق الإلكتروني بعد تقديره الأسباب المقدمة، في هذه الحالة يتخذ مؤدي

[1]- http://www.moj.gov.bh/default.asp?action=cate

الخدمات التدابير اللازمة من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الممنوحة له[1]، على الرغم مما نظمته تشريعات الدول المختلفة من التزامات تقع على عاتق جهات التوثيق الإلكتروني، وما يترتب عليه من مسؤولية عن إخلالها بالتزاماتها.

إلا أنني أرى أنه من واجب الأطراف التي تعوّل على شهادات التوثيق الإلكترونية أن تبذل عناية معقولة للتحقق من صلاحية الشهادة، وفيما إذا كان العمل بها موقوفا أو ما إذا كانت ملغاة، أو في ما لو وجد أي قيد على استعمالها، فكما نلاحظ فقد أجمعت التشريعات المدروسة على أن جهات التصديق الالكتروني تلتزم ببذل عناية وتحقيق نتيجة، فيما يخص بذل العناية تتمثل في التحقق من البيانات وحفظها فإذا أخلت بهذا الالتزام تقوم عليها مسؤولية قد تكون عقدية وقد تكون تقصيرية يتحدد نوعها بحسب من تعرض للإخلال بالالتزام في حقه، أكان المتعاقد أم الغير، أما فيما يخص الالتزام بتحقيق نتيجة هو التزام مقدم خدمات التصديق الإلكتروني بسرية المعطيات والبيانات الشخصية إلى جانب إصدار شهادة تصديق موافية للشروط التنظيمية المفروضة على مقدم خدمات التصديق الإلكتروني.[2]

[1]– المواد من المادة 53 إلى المادة 60 من القانون رقم 04/15.

[2]– القانون رقم 15–04.

المبحث الثاني:

النموذج القانوني لجرائم التوقيع الإلكتروني

تعتبر الحماية التكنولوجية الرامية إلى الحد من الإعتداءات المختلفة على التوقيع والتصديق الإلكترونيين ذات أهمية كبيرة، تتجسد كما سبق تناوله في آلية إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني عن طريق تقنية تشفير المعلومات، والتي تعطي القوة للوثيقة الإلكترونية من جهة الحجية والإثبات.

وقد لا تمنع في الغالب تلك الحماية من ارتكاب الجرائم التقليدية أو المستحدثة ذات الصلة بالتوقيع والتصديق الإلكترونيين، والتي تدخل في عداد الجرائم المعلوماتية، إلا أن لهذه الجرائم ذاتية خاصة اضفت الطابع القانوني الخاص لها، ويظهر ذلك من خلال المصلحة المحمية قانونا عند إقتراف هذه الجرائم والتي تتمثل في حماية الحق في خصوصية وسرية تداول بيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني، وكذا حماية الثقة في التوثيق الإلكتروني، أو من حيث المجالات التي تشملها الحماية الجزائية للتوقيع والتصديق الإلكترونيين وهي على الخصوص مجالات الحكومة الإلكترونية، والتجارة الإلكترونية، وباقي المعاملات المدنية على اختلاف أنواعها، أو من خلال خصائص الجرائم المذكورة وطبيعتها وتصنيفاتها الفقهية والقانونية وخصوصية أركانها مقارنة بغيرها من الجرائم المقترفة في الوسط الرقمي.

وفي ضوء ما تقدم قسم المبحث إلى مطلبين اثنين على النحو التالي:

- **المطلب الأول:** المصلحة المحمية قانونا في جرائم الإعتداء على التوقيع الإلكتروني.
- **المطلب الثاني:** خصائص جرائم الإعتداء على التوقيع الإلكتروني.

المطلب الأول:

المصلحة المحمية قانونا في جرائم الإعتداء على التوقيع الإلكتروني.

من المتعارف عليه أن أي سلوك مكون لواقعة إجرامية يحمل بالتأكيد صفة الأضرار بمصلحة محمية جنائيا[1]. ولجوء المتضرر إلى حماية حقه برفع دعوى أمام القضاء يجب أن يكون مرتبطا بمصلحة في ذلك، والمصلحة تعني حق أو مركز قانوني تم الإعتداء عليه.

ولأن الدعوى وسيلة لحماية ذلك الحق أو المركز القانوني، فإنه يجب أن يكون الحق أو المركز القانوني قائما، ولذلك يعبر الفقه عن هذا الشرط بقانونية المصلحة و–أو قانونية الدعوى، فلا بد أن يكون القانون معترفا بالحماية المجردة لنوع المصلحة التي يطلبها المدعي.

لذلك فالجريمة في نطاق التوقيع والتصديق الإلكترونيين تضر بأطراف عديدة، وتصيب مصلحة كل منهم سواء كان الموقع أو المتعامل معه أو الشخص الاعتباري الذي رخص بعمل برامج هدفها استخراج توقيعات الإلكترونية تخص مختلف المتعاملين في البيئة الرقمية. [2]

وهو ما يحتم بطبيعة الحال الوقوف على وجه الدقة على المصلحة محل الحماية في جرائم الإعتداء على التوقيع والتصديق الإلكترونيين، هذا من جهة، ومن جهة أخرى الوقوف على مجالات هذه الحماية سواء ما تعلق منها بالحكومة الإلكترونية، أو في نطاق التجارة الإلكترونية، ومختلف المعاملات المدنية الأخرى عبر الأنترنت.

وعلى ذلك قسم المطلب إلى ثلاثة فروع على النحو التالي:

- **الفرع الأول:** تعريف جرائم الإعتداء على التوقيع الإلكتروني
- **الفرع الثاني:** حماية الحق في خصوصية وسرية تداول بيانات التوقيع الإلكتروني
- **الفرع الثالث:** مجالات الحماية الجزائية للتوقيع الإلكتروني.

---

[1]–عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأول "الجريمة"، ديوان المطبوعات الجامعية، الجزائر 2009.

[2]– عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول، دار الكتب القانونية، مصر 2007، ص268، ص269.

الفرع الأول: تعريف جرائم الإعتداء على التوقيع الإلكتروني

اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية والتي من ضمنها الجرائم الواقعة على التوقيع الإلكتروني بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وعرفها بموجب أحكام المادة (02/أ) من القانون رقم: 04-09 مؤرخ في :05أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[1]على انها:" جرائم المساس بانظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية..."

وانطلاقا من فحوى هذه المادة والمواد من (394 مكرر-394 مكرر7) من قانون العقوبات الجزائري يمكن تعريف جرائم الإعتداء على التوقيع الإلكتروني بأنها: " كل فعل أو امتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلومات، ويكون محلها الإعتداء على التوقيع الإلكتروني، إما بإتلافه أو استنساخه أو تزويره وتقليده أو استعماله مزورا مع علم الجاني بذلك، أو إفساد بياناته أو استعمالها في غير الغرض المقدم من أجله".

وتصنف هذه الجرائم ضمن الجرائم الشكلية أي أنها تعد من جرائم الخطر أو جرائم السلوك المحض الذي لا يتوقف على تجريم السلوك فيها المتمثل في الحصول على التوقيع الإلكتروني على تحقق نتيجة معينة، وإنما يكفي تمام صناعة البرنامج أو النظام المعلوماتي لذلك. [2]

ويجرم المشرع في هذا المجال نوعين من الانتهاكات الواقعة ضد التواقيع والمستندات الإلكترونية ومختلف المحررات الإلكترونية الأخرى، يتمثل الأول في أفعال الإتلاف والتزوير في المجال المعلوماتي، والثاني هو الحصول بدون حق على المحررات الإلكترونية والتواقيع الإلكترونية وشهادات التصديق الإلكترونية.

---

[1]- القانون رقم: 09-04 مؤرخ في: 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، (ج.ر) رقم: 47 المؤرخة في: 2009/08/16، ص ص 5-9

[2]- نبيلة هروال، جرائم الأنترنت، اطروحة دكتوراه، جامعة ابي بكر بلقايد، تلمسان، 2014، ص 304.

الفرع الثاني: حماية الحق في خصوصية وسرية تداول بيانات التوقيع الإلكتروني:

إن أكثر ما يهدد المعاملات الإلكترونية وبالأخص في نطاق التجارة الإلكترونية هو المساس بأمن المعلومات وعدم تأمين التوقيع الإلكتروني، مما يؤدي إلى تهديد سلامة عملية تداول المعلومات من طرف ثالث أو أي جهة أخرى غير المتعاقدين، لذلك كان لابد من إيجاد وسيلة لحفظ سرية البيانات وحمايتها حتى لا يستطيع أي شخص بإستثناء المتعاقدين أو من يصرح له القانون بذلك الاطلاع عليها. [1]

وإفشاء المعلومات أو الأسرار يعني إذاعتها أو نقلها أو إطلاع الغير عليها وإعلانها لكثير من الناس وخروجها من حيز الكتمان أو السرية بعد أن كان العلم بها قاصرا على أصحابها أو الذين انتموا عليها بحكم وظيفتهم وهم مزودي خدمة المصادقة الإلكترونية ومعاونيهم. [2]

وترتبط حماية الخصوصية في مجال التوقيع الإلكتروني بمنظومة متكاملة تحدد عناصر الحماية ونطاقها، تتجسد في خمسة مبادئ أساسية تحكم ما يسمى بالممارسات العادية والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية وهي: الإبلاغ(الإخطار)، الاختيار، الوصول إلى البيانات، تطبيق القانون، الأمن.[3]

1. **الإبلاغ(الإخطار):** يراد بهذا المبدأ إلتزام مزود الخدمة أو الموقع إخطار مستخدمي المواقع بها إذا كان الموقع أو مقتضيات الخدمة ينطويان على جمع بيانات شخصية، وبيان إلى أي مدى تجمع هذه البيانات وتستخدم.
2. **الاختيار:** وهو إلتزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بخصوص إستخدام بياناته في غير الغرض المخصص من اجله. [4]

---

[1]- بلحسين حمزة، مرجع سابق ص 75.

[2]- عبد الفتاح البيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر 2007، ص89، ص90.

[3]- ايمن رمضان محمد احمد، مرجع سابق ص 101.

[4]- المرجع نفسه، ص 101.

3. **الوصول للبيانات:** ويوجب هذا المبدأ منح القدرة للمستخدمين للوصول إلى بياناتهم والتثبت من صحتها وتحديثها. [1]
4. **الأمن:** مضمون هذا المبدأ الإلتزامات المترتبة على مزودي الخدمات والمواقع، المتمثلة في معايير الأمن، وسرية البيانات، وسلامة الإستخدام، وحظر الوصول غير المصرح به لهذه البيانات، وتتضمن أيضا كلمات السر والتشفير وغيرها من وسائل أمن المعلومات.
5. **تطبيق القانون:** يتعلق هذا المبدأ بفرض العقوبات على الجهة التي لا تلتزم بالمبادئ السالفة الذكر. [2]

وفي هذا السياق حظيت أنظمة المعالجة الآلية للمعطيات بما فيها التوقيع الإلكتروني وشهادة التصديق الإلكتروني بالحماية الجزائية من قبل المشرع الجزائري في إطار حماية الخصوصية وسرية المعلومات.

بداية بالدستور، نصت المادة 46 منه في فقرتها الرابعة على ما يلي: "سرية المراسلات والاتصالات الخاصة بكل إشكالها مضمونة. حماية الأشخاص الطبيعيين في معالجة

المعطيات ذات الطابع الشخصي يضمنه القانون ويعاقب على انتهاكه"[3]، وفي قانون العقوبات بموجب المادة 394 مكرر وما يليها لاسيما المادة 394 مكرر2 المتعلقة بحيازة أو إفشاء أو استعمال لأي غرض كان تلك المعطيات، فبنوك المعلومات التي تحتوي أسرار أصحابها من معطيات منظمة التي لها طابع الخصوصية مجرم الاطلاع عليها أو كشفها أو نشرها حماية للحق في الخصوصية.

وفي نفس السياق جاءت المواد 61 و68 و73من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني المذكور سابقا لتجرم حيازة أو اقتناء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير، وهي نوع من حماية الخصوصية السرية، تضمن سلامة التوقيع الإلكتروني وكذا المواد 42، 43 فيما يخص مؤدي خدمات التصديق.

---

[1]– ياسر محمد الكومي محمود ابو وحطب، الحماية الجنائية الامنية للتوقيع الإلكتروني، منشأة المعرف الاسكندرية 2014، ص 102.

[2]– ياسر محمد الكومي محمود ابو وحطب، مرجع سابق، ص 102.

[3]– القانون 01/16 المؤرخ في 06 مارس 2016، ج، رقم 14 المتضمن تعديل الدستور.

تداخل الحماية المقررة للتوقيع الإلكتروني والحماية الجزائية للأسرار:

يتجسد ذلك من خلال إمكانية التفرقة بين الجرائم الماسة بالمستند الإلكتروني[1]، وإفشاء الأسرار، ففعل إفشاء السر يجب أن يتم من شخص مؤمن على الحفاظ على هذا السر، بخلاف الإعتداء على المستند الإلكتروني، إذ يجوز أن يقع من أي شخص، هذا من جهة ومن جهة أخرى فانه حتى لو كانت الجريمة لا تتطلب إفشاء السر من أشخاص مؤتمنين عليه فان الفارق يبقى أيضا بين الفكرتين، فمدلول " السر" في جرائم إفشاء الأسرار أضيق نطاقا من مدلول سرية المستند، فالقانون يحمي السر أيا كان الشكل الذي حفظ فيه هذا السر.[2]

من خلال كل ذلك يتضح أن فكرة البيانات الإلكترونية أوسع نطاقا من فكر السر المرتبطة أساسا بالعمل المهني أو الوظيفي لمن اؤتمن عليه.

وتقتصر مختلف التشريعات على تجريم وسيلة المساس بالحق في سرية التوقيع الإلكتروني تاركة تحديد مضمون هذا الحق للمجني عليه، بينما يذهب الفقه والقضاء المقارنين إلى وضع ضوابط لمدلول السر الذي يعد إفشائه إخلالا بواجب حفظه.

ويتفرع عن الحماية الجزائية لخصوصية وسرية تداول بيانات التوقيع الإلكتروني:

أولا: حماية الثقة في التوقيع الإلكتروني

يتعلق مبدأ مصداقية التوقيع الإلكتروني بمسالة مدى حجيته في المعاملات الإلكترونية على اختلاف صورها في ظل الأخطار الماسة بأمن المعلومات وعدم تأمين عملية التوقيع الإلكتروني وبالتالي عدم ضمان سلامة عملية تداول المعلومات الخاصة بإتمام التعاقدات الإلكترونية.

ويرجع سبب ذلك إلى إمكانية اختراق أنظمة الكمبيوتر وإكتشاف التوقيع الإلكتروني أو فك شفرته أو الاستيلاء أو إستخدامه دون موافقة صاحب و– أو علمه بذلك، ويزيد ذلك ما يجري من

---

[1]– يعرف المستند المعلوماتي أو المحرر المعلوماتي بأنه: كل جسم منفصل أو يمكن ان يتم فصله عن نظام المعالجة الالية للمعلومات، وقد سجلت عليه معلومات معينة سواء اكان معد للاستخدام بواسطة نظام المعالجة الالية للمعلومات ام مشتق من هذا النوع – ايمن عبد الله فكري، مرجع سابق، ص382

[2]– Sophie Bardou, Les Traitements de donnees biometriques en entreprise, thése pour le doctorat en droit, faculte de droit, universite monpellier 1, novembre, 2010,p111.

تزوير لبطاقات الائتمان وما يتم تطويره من ابتكار الفيروسات والتي تهدد بإتلاف الملفات المحفوظة في نظم المعلومات أو تشويهها الأمر الذي يؤدي إلى اضطراب التعامل وضياع المصداقية. [1]

هذا إلى جانب تركيز الجهود على تذليل المعوقات التي تعترض التعاملات الإلكترونية بإعتماد الكتابة الإلكترونية التي ترتكز أساسا على المستندات الإلكترونية بالإضافة إلى الاعتراف بالتوقيع الإلكتروني ومساواته بالتوقيع الخطي.

وفي هذا الشأن يأتي اصدار قانون الأونسترال النموذجي في شأن التجارة الإلكترونية الذي وصفته لجنة الأمم المتحدة بالقانون التجاري الدولي في 1 ديسمبر 1966 ليمنح الرسائل والبيانات الإلكترونية حجية في الإثبات، كما اعترف بالتوقيع الإلكتروني وساوى بينه وبين التوقيع اليدوي. [2]

كما قامت لجنة الأمم المتحدة للقانون التجاري الدولي في دورتها الرابعة وثلاثون بوضع قانون الأونسترال النموذجي في شأن التوقيعات الإلكترونية لعام2001، الذي تعرض بالتنظيم للتوقيع الإلكتروني الموثق به، والجهة التي تقوم بتحديده، والتزامات الموقع، وكذا تنظيم خدمات توثيق التوقيع الإلكتروني وشهادات التصديق الالكتروني والاعتراف بالشهادات والتوقيعات الالكترونية الاجنبية.

كما اهتم المشرع الجزائري بالتوقيع الالكتروني ونص على مساواته في الحجية مع التوقيع التقليدي بإصداره للقانون 04/15 السالف الذكر والمتعلق بالتوقيع والتصديق الإلكترونيين، وأقر فيه العديد من الضوابط بما يكفل إسباغ الثقة اللازمة لكل المتعاملين الإلكترونيين في التوقيع الإلكتروني ويحول دون تقليد التوقيعات أو تزويرها أو التلاعب فيها.

وحتى تتحقق الثقة ويتوفر الأمان في التوقيع الإلكتروني يقتضي الأمر وجود جهتين:

- **الأولى:** سلطة إصدار الشهادات تمنح صلاحية إصدار شهادات للتوقيع الإلكتروني وتحتفظ تحت سلطتها بمراقبة المفتاح الخاص بصاحب التوقيع".[3]

---

[1]– ايمن رمضان محمد احمد، مرجع سابق ص 102، ص 103.

[2]– ياسر محمد الكومي محمود ابو حطب، مرجع سابق ص 105.

[3]– محمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، مصر 2014، ص 355، ص356.

- **الثانيـة:** السلطة التـي تـودع لـديها مفـاتيح الشـفرات، والتـي علـى أساسـها يمكـن إعـادة تخليـق المفتـاح الخـاص لحـائزه بنـاء علـى طلبـه فـي حالـة فقده أو تلفه أو بنـاء علـى طلـب السلطات المختصة بموجب أمر قضائي[1]، وهو ما انتهجه المشرع الجزائري من خلال التنصيص على هـذه السـلطات فـي القـانون الخـاص بـالتوقيع والتصـديق الإلكترونـي 04/15 لسـنة 2015 باستحداث ثلاثة سلطات للتصديق الإلكتروني، تتمثل في السلطة الوطنية للتوقيع الإلكتروني والسلطة الحكومية للتصديق الإلكتروني والسلطة الاقتصادية للتصديق الإلكتروني .

وحدد مهام كل سلطة على نحو تكمل كل منها عمل الأخرى بصورة تضمن موثوقية استعمال كل من التوقيع والتصديق الإلكترونيين.[2]

ثانيا: شرعية تداول بيانات التوقيع الإلكتروني

من مقتضيات مشروعية تداول البيانات في مجال التوقيع والتصديق الإلكترونيين أن يتم تداولها عن طريق مزود الخدمة الإلكترونية المصرح له بذلك، وهو ما نص عليه المشرع الجزائري في القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين في المواد 33 وما بعدها بإخضاعها لنظام الرخصة، حيث نصت المادة 33 على ما يلي: " يخضع نشاط تأدية خدمات التصديق الإلكتروني الى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني ".

وألزم المشرع الجزائري في هذا الصدد مؤدي خدمات التصديق الإلكتروني إعلام السلطة الاقتصادية للتصديق الإلكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني أو بأي فعل قد يؤدي إلى ذلك وفق ما أشارت إليه المادتين 58 و59 من القانون 04/15 المذكور أنفا، ويلتزم مؤدي الخدمة باستمرارية الخدمة، ويترتب عن وقف نشاطه سحب الترخيص الممنوح له كما هو وارد في المواد 67، 71، 72، 74 من القانون ذاته، وان أي إخلال بهذه الإجراءات يترتب عليه المساءلة الجزائية. وقد تتشابه الحماية المقررة للتوقيع والتصديق الإلكترونيين مع تلك المقررة لنظم تشغيل الحاسب الآلي، ووجه هذا الشبه أن محل الإعتداء في الحالتين ينصب على البيانات التي يتضمنها كل من التوقيع أو شهادة التصديق

[1]–محمود ابراهيم غازي، مرجع سابق ص 357.

[2]–سليم سعداوي، مرجع سابق، مرجع سابق ص75.

الإلكتروني أو برنامج التشغيل، ولعل هذا التشابه هو الذي دفع برأي في الفقه إلى القول بان البيانات المدخلة إلكترونيا لا تنفصل على البرامج التي تنظمها، وأنهما لذلك لا تختلفان في الطبيعة باعتبارهما كيانا معنويا واحدا، وأن حماية هذه البرامج تعد في الوقت ذاته حماية للبيانات المعالجة إلكترونيا. [1]

الفرع الثالث: مجالات الحماية الجزائية للتوقيع الإلكتروني

تتصل فكرة التوقيع والتصديق الإلكترونيين بالعديد من المجالات الحيوية داخل أجهزة الدولة ذاتها أو بباقي المعاملات المدنية والتجارية الأخرى، والتي تتطلب حتما حماية قانونية ردعية تتداخل مع الحماية المقررة للتوقيع والتصديق الإلكترونيين، وهو ما سيتم تناوله من خلال التعرض إلى الحماية الجزائية لكل من الحكومة الإلكترونية، والتجارة الإلكترونية، وباقي المعاملات المدنية ذات الصلة.

أولا: الحماية الجزائية للحكومة الإلكترونية

من الأهمية بما كان توفير حماية جزائية للتوقيع والتصديق الإلكترونين من شتى الإعتداءات التي تقع عليهما، وتظهر هذه الأهمية في توجه الجزائر نحو تطبيق شامل للحكومة الإلكترونية في السنوات المقبلة كون هذا المشروع يمثل الوسيلة الأفضل للتخلص من البيروقراطية والإجراءات الروتينية، وتخفيف العبء على المؤسسات الحكومية المختلفة مما يؤدي إلى زيادة كفاءتها.

وبإستقراء مختلف التعريفات للحكومة الإلكترونية، والتي جاءت بها بعض المنظمات الدولية مثل البنك الدولي والأمم المتحدة وبعض الدول التي بدأت بتطبيق هذه التقنيات المعلوماتية، ومختلف التعريفات الفقهية، التي أجمعت على أن الحكومة الإلكترونية هي: " تحول الإجراءات الحكومية الداخلية أو الخارجية والمتمركزة حول توفير أو إيصال الخدمات للمتعاملين معها بفاعلية وكفاءة بصورة أفضل من خلال تقنيات المعلومات والإتصالات الحديثة".[2]

وتقوم فكرة الحكومة الإلكترونية على عدة ركائز هي تجميع الأنشطة والخدمات المعلوماتية والتفاعلية والتبادلية كلها في موقع الحكومة الرسمي على شبكة الأنترنت في نشاط أشبه ما يكون بفكرة

[1]–ياسر محمد الكومي ابو حطب، مرجع سابق، ص 101.

[2]– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن، 2010، ص61.

مجمعات الدوائر الحكومية، وصولا الى تحقيق حالة إتصال دائم بالجمهور مع القدرة على تأمين الاحتياجات الاستعلامية والخدمية كلها للمواطن. [1]

والمطلب الأساسي والهام في هذا الشأن ضرورة وجود إطار تشريعي وقائي رادع يحيط بكل متعلقات الحكومة الإلكترونية يضمن أمن المعلومات وسريتها وخصوصيتها، وهنا تظهر العلاقة الوطيدة بين التوقيع والتصديق الإلكترونيين والحكومة الإلكترونية، كون الحماية المقررة لأحدها تنطوي بطريق اللزوم على حماية الآخر، ذلك ان الإعتداء على التوقيع الإلكتروني أو شهادة التصديق الإلكتروني أو أي محرر إلكتروني بالإتلاف أو التعيين أو التعطيل وكذا تزوير المحرر الإلكتروني الحكومي من شأنه ان ينال من ثقة الأفراد فيها، ومن ثم فإنه فضلا عن خضوع الجاني في تلك الأحوال لنصوص قانون التوقيع الإلكتروني الجزائية، فانه يخضع أيضا بذات القدر للقواعد العامة في قانون العقوبات من حيث اعتبار المال المعتدى عليه من الأموال العامة.

إلا أن مجال الحماية المقررة للتوقيع والتصديق الإلكترونيين أوسع نطاقا، حيث أن التوقيع الإلكتروني هو محور العلاقة بين المتعاقد الإلكتروني والإدارة الإلكترونية أثناء إبرام مختلف التعاملات الإلكترونية ومع مختلف الشركات والمؤسسات الخاصة أو حتى الأشخاص الطبيعيين.

وفي هذا الصدد تبنى المشرع الجزائري سياسة تشريعية جنائية لتأمين الحكومة الإلكترونية من خلال تجريم كل السلوكيات والأفعال التي تعتدي على أنظمة المعالجة الآلية للمعطيات التي يقترفها المجرم الإلكتروني وزجره بعقوبات ردعية لقمع الجرائم الإلكترونية بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، وأدرج هذا القانون ضمن القسم السابع مكرر من المواد 394 مكرر إلى 394 مكرر من قانون العقوبات، وألحق هذا القانون بصدور القانون 04/09 المؤرخ في 05 سبتمبر 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والذي تشكل الإعتداءات الواقعة على التوقيع والتصديق الإلكترونيين بإعتبارها النوع المستحدث من الجرائم الإلكترونية إحدى محاوره الأساسية.

[1]–ايمن رمضان محمد احمد، مرجع سابق ص107.

وهو ما عجل بصدور القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، الذي جرم مختلف الإعتداءات على التوقيع الإلكتروني وشهادة التصديق الإلكتروني حماية للإدارة الإلكترونية التي أصبحت خيارا لا رجعية فيه بالنسبة للجزائر.

ثانيا: الحماية الجزائية للتجارة الإلكترونية:

عرفت منظمة التجارة العالمية التجارة الالكترونية بأنها:" مجموعة عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات عبر وسائل إلكترونية". [1]

ويمكن تعريف التجارة الإلكترونية على انها المعاملات التجارية التي تتم بإستخدام تكنولوجيا المعلومات وشبكات الإتصال.

ويعد التوقيع الإلكتروني للأطراف المتعاقدة أحد الوسائل الأساسية في تنظيم الخدمات المصرفية الإلكترونية المطلوبة في إبرام مختلف عقود التجارة الإلكترونية، وإعطائها الأثر القانوني.

وبوصف التجارة الإلكترونية نظام معلوماتي تتدفق خلاله السلع والخدمات والمقابل المالي لها، فهي تحتاج إلى حماية جزائية، والتي تكون أساسا من خلال حماية بيانات التجارة الإلكترونية، والتي يترتب على المساس بها إهدار الأموال المتداولة في هذه التجارة، ومن ذلك الجرائم التي تقع على التوقيع الإلكتروني، وكذلك فض الشفرات الخاصة بهذا التوقيع، بما يتضمنه من بيانات تتعلق بالبائع أو المستهلك في عقد التجارة الإلكترونية.[2]

وهي جرائم تقع على مضمون التجارة الإلكترونية ذاتها، وليس على البيانات الخاصة بها، ذلك أن عقد التجارة الإلكترونية سواء كان عقد بيع أو استيراد أو غيره من العقود يستلزم لصحته تمام توقيع الطرفين عليه كما في عقود التجارة الإلكترونية، ليس توقيعا تقليديا إنما هو توقيع إلكتروني. [3]

---

[1]–صالح شنين، مرجع سابق ص1.

[2]– عبد الفتاح بيومي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الكتب القانونية، مصر 2007، ص9

[3]– عبد الفتاح بيومي حجازي، مرجع سابق ص 294.

وتتداخل أفعال المساس بالتوقيع الإلكتروني والذي يعتبر كمستند إلكتروني مع فعل سرقة الأسرار التجارية إذا كانت هذه الأسرار مودعة في مستند إلكتروني، ومن ثم يكون الاطلاع غير المأذون به على هذا المستند ونقل محتواه إلى الغير مشكلا لجريمة سرقة الأسرار التجارية، إلا أن الاختلاف يقع في المحل الذي ينصب عليه الفعل المرتكب وهو ما يميز بين الجريمتين، فالمساس بالمستند الإلكتروني يتحقق بأفعال الاطلاع أو النسخ أو النقل غير المأذون بها دون أن يتطلب تحقق أي نتيجة أخرى، فهو بهذه المثابة من جرائم الخطر، أما سرقة الأسرار التجارية فتقتضي أن ينصب الفعل المرتكب على الاستيلاء على هذه الأسرار لحساب الغير أي تحقق نتيجة معينة الأمر الذي يجعلها من جرائم الضرر، ويترتب على التفرقة بين نوعي الجريمتين انه قد تتوافر إحداهما دون الأخرى. [1]

ثالثا: الحماية الجزائية للتوقيع الإلكتروني في مختلف المعاملات الأخرى:

1. التوقيع الإلكتروني وحماية المستهلك:

تتدخل نصوص القانون الجنائي في هذا الإطار لحماية كافة المعاملات الإلكترونية التي يباشرها المستهلك أثناء أو بعد عملية التعاقد وهذا نظرا لعجز القانون المدني في توفير الحماية الأنجع من الغش والخداع التي تعترض المستهلك، فهي حماية محدودة قياسا إلى الحماية الجزائية التي تذهب إلى ابعد حد تذهب إليه النظرية التقليدية لعيوب الرضا في القانون المدني، هذا إلى جانب أن الحماية المدنية لا تخرج عن إطار المتعاقدين، أي المنتج والمستهلك عكس الحماية الجزائية التي تتوجه بحمايتها إلى جميع الأطراف المتدخلة في عملية التعاقد الإلكتروني.

فهناك علاقة وطيدة بين آلية التوقيع والتصديق الإلكترونيين وحماية المستهلك، فإذا كانت علة الأخذ بتطبيقات التوقيع والتصديق الإلكترونيين هو تسهيل التعامل وسرعة انجازه فان هذه الاعتبارات لا يجب ان تتجاوز حقوق المستهلك وحمايته من أي تحايل قد يترتب كنتيجة لإتمام التصرفات من خلال الوسائل الإلكترونية. [2]

---

[1]– ايمن رمضان محمد احمد، مرجع سابق ص 113.

[2]– ياسر محمد الكومي ابو حطب، مرجع سابق ص107.

2. التوقيع الإلكتروني وحقوق الملكية الفكرية:

في سبيل تقرير حماية جنائية فعالة في مستوى الدور المنوط بها، عدد المشرع الجزائري مجموعة من الأفعال الماسة بالمصنفات وبحقوق مؤلفيها وجرمها وجعل مرتكبيها يشكلون خرقا لحقوق المؤلف تجب معاقبة من اقترفه وتتمثل في مختلف السلوكيات المادية المشكلة لجنحة التقليد.[1]

وقد وردت هذه السلوكيات في الأمر 05/03 المتعلق بحماية حقوق المؤلف والحقوق المجاورة في المواد 151 و152 أو 155 وتتمثل فيما يتعلق بالبرمجيات أو المصنفات المعالجة إلكترونيا في أفعال الكشف غير المشروع عن البرمجية، واستنتاج البرمجيات بأي أسلوب في شكل نسخ مقلدة، إستيراد وتصدير نسخ مقلدة للبرمجيات، بيع نسخ مقلدة من البرمجية، تأجير برمجية مقلدة أو عرضها للتداول.

ويتماثل التوقيع الإلكتروني وشهادة التصديق الإلكتروني مع المصنف في أحقية صاحب التوقيع أو الشهادة في الاستئثار به، ويتماثلان كذلك في أن المشرع يبسط حمايته لمحتوى كل منهما، فالمساس بحقوق الملكية الفكرية للمصنفات المعالجة إلكترونيا قد تنتمي بالمعنى الواسع إلى المساس بالبيانات الإلكترونية ومن ثم تصبح الحماية المقررة لهذه البيانات هي في نفس الوقت حماية لحقوق الملكية الفكرية. [2]

إلا ان محل الحماية الجزائية للمصنف يرتكز على حماية حق المؤلف على أفكاره، والذي يأخذ الإعتداء عليه غالبا صور المساس ماديا بمحتواه وهو ما يختلف عن مدلول الحماية الجزائية للتوقيع والتصديق الإلكترونيين. [3]

3. التوقيع الإلكتروني والحق في الإعلام:

يقصد بالحق في الإعلام الإلكتروني على شبكة الأنترنت الإلتزام القانوني لمزودي الخدمات الإلكترونية بتقديم البيانات والمعلومات الجوهرية فيما يخص العقد المزمع إبرامه بالوسائط الإلكترونية، وقد نص المشرع الجزائري على حماية حق المستهلك في الإعلام من خلال القانون 03/09 المتعلق

---

[1]– بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر 2007، ص76.

[2]– ياسر محمد الكومي محمود ابو حطب، مرجع سابق، ص 108.

[3]– ايمن رمضان محمد احمد، مرجع سابق ص 110.

بحماية المستهلك وقمع الغش، وفي القانون 02/04 المتعلق بالقواعد المحددة للممارسات التجارية، بوجوب إتصال المعلومات محل الالتزام بالمستهلك، وقرر زيادة على ذلك عقوبات جزائية ردعية جراء مخالفة تلك القواعد.

وللتوقيع والتصديق الإلكترونيين صلة وثيقة بالحق في الإعلام، ذلك انه إذا كان هذا الحق الأخير يعني أن للفرد حق تلقي المعلومات والإطلاع عليها ونقلها، فإن هذه المعلومات قد يحويها مستندا إلكتروني يتضمن التوقيع الإلكتروني، غير ان نطاق المعلومات والبيانات الإلكترونية أوسع من نطاق المستند الإلكتروني. [1]

المطلب الثاني:

خصائص جرائم الإعتداء على التوقيع الإلكتروني

تدخل جرائم الإعتداء على التوقيع والتصديق الإلكترونيين ضمن الإطار الواسع للجرائم المعلوماتية أو جرائم التكنولوجيا الحديثة التي يتدخل فيها الحاسب الآلي كوسيلة أساسية لإنشاء ودمج وإرسال التوقيع الإلكتروني وشهادة التصدبق الإلكتروني، فمحل الإعتداء في كلا النوعين من الجرائم يبدو واحدا وهي الوسائل التقنية الخاصة بمعالجة المعطيات والبيانات والتي تعطي التكييف القانوني للجريمة بتوافر اركانها مجتمعة، ليظهر التطابق الكامل بين الجرائم المعلوماتية وجرائم الإعتداء على التوقيع والتصديق الإلكترونيين .

لذا كان لزاما التعرض إلى الخصائص الجوهرية التي تتصف بها هذه الجرائم سواء من حيث طبيعتها وخصائصها وتقسيماتها الفقهية والقانونية، وكذا السمات الخاصة بأركانها قياسا بباقي الجرائم المعلوماتية وذلك على النحو التالي:

- **الفرع الأول:** طبيعة جرائم الإعتداء على التوقيع الإلكتروني.
- **الفرع الثاني:** السمات الخاصة لأركان جرائم التوقيع الإلكتروني

[1]– ايمن رمضان محمد احمد، مرجع سابق، ص 110.

الفرع الأول: طبيعة جرائم الإعتداء على التوقيع الإلكتروني

تعرف الجرائم المعلوماتية بصفة عامة على أنها سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها. [1]

وعرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) على أنها: " كل فعل أو امتناع من شأنه الإعتداء على الأحوال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[2]

وإلى جانب هذين التعريفين فهناك تعريف شامل للجريمة المعلوماتية والتي تشكل جرائم الإعتداء على التوقيع والتصديق الإلكترونيين إحدى صورها بأنها تتضمن كافة السلوكيات غير المشروعة التي ترتكب إعتداءا على الحاسب الآلي وتلعب فيها البيانات والمعطيات الإلكترونية والبرامج الإلكترونية وبرامج المعلومات دورا رئيسيا، أو أي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية، أو أي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف المعلومات المخزنة داخل الحاسب، أو أي جريمة اختراق لبرامج معلوماتية تتطلب لدى الفاعل معرفة تقنية لكل فعل أو إمتناع من شأنه الإعتداء على الأحوال المادية أو المعنوية يكون ناتجا مباشرة أو غير مباشرة من تدخل التقنية المعلوماتية. [3]

وتتميز جرائم التوقيع والتصديق الإلكترونيين على غرار الجرائم المعلوماتية أنها:

- جرائم مستحدثة، بحيث ظهرت تبعا للتطور الهائل في مجال التقنية العالمية، وهو ما جعل أمر تحديد هذا النمط من الجرائم وإدراجه ضمن طائفة الجرائم التقليدية المعروفة يكتنفه

---

[1]–عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف، المصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت 2007، ص32.

[2]– يذكر في هذا الشأن ان فريقا من هذه المنظمة خلصت إلى تعريف شامل لهذه الجريمة اتخذته اساسا للمناقشات التي جرت في اجتماع عقدته في باريس سنة 1983، ارجع في هذا الشأن عفيفي كامل عفيفي، مرجع سابق، ص32.

[3]– مؤتمر تأمين المعلومات والدليل الرقمي وكيفية اثباته في الجرائم الإلكترونية، مصر 10–16 ديسمبر 2010، المركز القومي للبحوث الاجتماعية، مصر.

صعوبات ترجع إلى الطبيعة الخاصة بها باعتبارها تطال المعلومات والبيانات المعالجة إلكترونيا عبر شبكة الأنترنت .

- استعمال الشفرات السرية والتي لا تشكل في ظاهرها عملا خاطئا مما يسمح بالدخول بدون إذن إلى برامج التوقيع وشهادة التصديق الإلكترونيين، مع أنها تشكل جريمة بحد ذاتها. [1]
- استعمال الحاسب الآلي كأداة ارتكاب جرائم الإعتداء على التوقيع والتصديق الإلكترونيين عبر شبكة الأنترنت، ويقصد بالحاسب الآلي وفقا للموسوعة الشاملة لمصطلحات الحاسب الإلكتروني: " كل جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليا إدخال (data input) أو إخراج معلومات (information output) أو إجراء عمليات حسابية أو منطقية. وهو يقوم بالكتابة على أجهزة الإخراج (output devices) أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب (operator) عن طريق وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية، وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج".[2]
- ويتكون الحاسب الآلي من كيانين الأول مادي (Hardware)والثاني معنوي (Software) بحيث يضم الأول الأجهزة المادية المختلفة والتي تشمل وحدات الإدخال وكذا الإخراج، ووحدات التشغيل المركزية، أما الثاني فيضم البرمجيات الجاهزة ومختلف البيانات والمعلوماتية المنطقية. [3]
- تعتبر شبكة الأنترنت حلقة الوصل بين كافة الأهداف المحتملة لجرائم الإعتداء على التوقيع والتصديق الإلكترونيين باعتبارها البيئة الطبيعية والوحيدة لإقتراف هذه الجرائم.

ومن هذا المنطلق وجب التعرف على الجاني والمجني عليه في هذه الجرائم أولا، ثم التعرف ثانيا على صعوبة اكتشافها بعد كل عملية إعتداء.

أولا: الجاني والمجني عليه في جرائم الإعتداء على التوقيع الإلكتروني

[1]– نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلب الحقوقية، بيروت 2006، ص 218.

[2]– هلالي عبد الاله احمد، تفتيش نظام الحاسب الالي وضمانات المتهم المعلوماتي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة 1997، ص 16 و17.

[3]– نبيلة هبة هروال، الجوانب الاجرامية لجرائم الأنترنت، دار الفكر الجامعي، الاسكندرية 2007، ص37.

إن أي إعتداء يقع على آليتي التوقيع والتصديق الإلكترونيين يحتاج إلى طرف فاعل أو جاني وطرف مجني عليه يمثلان أطراف الجريمة، إلا أنهما يختلفان عند باقي أطراف الجرائم الأخرى، إذ أن المجرم المعلوماتي له دراية ومعرفة بالحاسب الآلي كشرط أساسي، الى جانب معرفته بآلية إنشاء التوقيع الالكتروني، ويستخدم في ذلك أدوات خاصة وأجهزة متطورة لإتمام جريمته.

1. الجاني في جرائم التوقيع الإلكتروني:

الجاني في جرائم التوقيع والتصديق الإلكترونيين قد يكون شخصا طبيعيا أو شخصا معنويا (كمؤسسة تسعى لإلحاق الضرر بمؤسسة منافسة لها)، يتوفر لديه كشرط أساسي معرفة بآليات عمل وتشغيل كل من الحاسب الآلي والتوقيع والتصديق الإلكترونيين[1] يقوم بعمله إما بحسن نية أو سوء نية كأعمال الإتلاف والغش وفك الشفرات، كما هو الحال في مجال جرائم الحواسيب من خلال سلوكيات غير مشروعة كالإعتداء على مواقع الأنترنت، أو تخريب البيانات والمعلومات الموجودة على جهاز آخر أو سرقتها.

ويمكن إجمال سمات المجرم المعلوماتي في مجال الإعتداءات الواقعة على التوقيع والتصديق الإلكترونيين أنه:

أ. **مجرم متخصص:** فقد بينت العديد من القضايا أن عددا من المجرمين لا يرتكبون إلا جرائم الكمبيوتر بما فيها فك الشفرات المتعلقة بآلية إنشاء التوقيع الإلكتروني أو شهادة التصديق الإلكتروني، أي أنهم متخصصون في هذا النوع من الجرائم.

ب. **مجرم عائد إلى الإجرام:** ويرجع سبب عودتهم إلى إقتراف هذا النوع من الجرائم لرغبتهم في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، مما يجرهم إلى المتابعة الجزائية للمرة الثانية.

ج. **مجرم محترف:** باعتبار آلية إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني معقدة، فهي تحتاج إلى شخص ذو دراية وتخصص دقيق في مجال المعلوماتية ليتمكن من اختراق الأنظمة.

[1]– ياسر محمد الكومي محمود أبو حطب، مرجع سابق، ص 27.

د. **مجرم غير عنيف:** أي انه لا يحتاج إلى استعمال العنف عند إقترافه للجرائم باعتبار الإجرام المعلوماتي إجرام حيلة.

ويمكن تصنيف المجرم المعلوماتي في مجال التوقيع والتصديق الإلكترونيين إلى الفئات التالية:

أ. **القراصنة** (Pirates)(Hackers): بما فيهم الهواة الفضوليين الذين يتسببون في إحداث أضرار كبيرة بدافع الحصول على أعمال، أو بغرض الشهرة أو إثبات تفوقهم العلمي دون تحريف للمعطيات الموجودة داخل النظام المعلوماتي، أي بدون دوافع إجرامية. [1]

ب. المخادعون(Fraudeurs): يتمتعون بقدرات فنية عالية في إخفاء دليل الجريمة باعتبارهم من المتخصصين في المعلوماتية، وتنصب معظم جرائمهم في شبكات تحويل الأموال، والتلاعب بحسابات المصارف، أو فواتير الكهرباء والهاتف، أو تزوير بطاقات الاعتماد، والتي يشكل فيها الإعتداء على التوقيع الإلكتروني المحور الأساسي في الوصول إلى النتيجة الإجرامية.[2]

ج. الجواسيس(Espions): يهدف هؤلاء إلى جمع المعلومات من خلال اختراق آلية التوقيع والتصديق الإلكترونيين لمصلحة دولة معينة أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس بينها.

2. المجني عليه في جرائم التوقيع الإلكتروني:

يمكن تحديد نطاق جرائم التوقيع والتصديق الإلكترونيين في أن ضحايا هذا الإعتداء هم جميع الأشخاص سواء كانت طبيعية أو معنوية أو خاصة. ويرتبط هذا النوع من الجرائم بالأنشطة التجارية والمالية الإلكترونية وكذا مجال الإدارة الإلكترونية ومختلف المعاملات المدينة الإلكترونية[3]، وبالتالي تستهدف هذه الجرائم في الواقع المؤسسات العمومية والإدارت والمؤسسات المالية التي تسيطر على ما يعرف بالقيم الرأسمالية، فالهدف الرئيسي لهذه الجرائم يتمثل في الأموال، وتليها المعلومات باعتبارها

---

[1]–باطلي غنية، مرجع سابق، ص38.

[2]–نصر شومان، التكنولوجيا الإجرامية الحديثة وأهميتها في الإثبات الجنائي، الطبعة الأولى، ب–ت–ن، وبدون دار النشر، ص31.

[3]–Abbas Youssef Jaber, Les contrats conclus par voie electronique : étude comparée, these pour le doctorat en droit privé, ecole doctorale droit er science politique, universite monpellier 1, juin, 2012, p25.

الطريق إلى اقتصاد السوق، ومن هذا المنطلق تأتي أهمية المعلومات لمجتمع الأعمال، هذه الفئة التي تسعى إلى الحصول على المعلومة بطرق قد تكون مشروعة وقد تكون في الغالب غير مشروعة.

ثانيا: صعوبة اكتشاف جرائم التوقيع الإلكتروني

إكتشاف الإعتداءات الواقعة على آليتي التوقيع والتصديق الإلكترونيين ليس بالأمر السهل، وفي حال اكتشافها والإبلاغ عنها فان إثباتها والتحقيق فيها أمر يحيط به الكثير من الصعاب، وهذه خاصية أخرى تميزها عن غيرها من الجرائم الأخرى وهي صعوبة الإثبات، حيث يكون من الصعب إثبات أركانها لأنها لا تترك آثارا مادية. [1]

والإثبات في هذا المجال ينطبق عليه المفهوم العام، وهو بذلك يواجه العديد من الصعوبات التي تتعلق بالبحث عن الدليل وجمعه ومشكلات قبوله إن وجد، ومدى موثوقيته أو مصداقيته في إثبات وقائع الجريمة.

وأهم العقبات التي تواجه عملية البحث عن الأدلة هي:

- إعاقة الوصول إلى الدليل حيث يلجأ المجرم المعلوماتي إلى التمويه بإستخدام التشفير وكلمات السر والأسماء المستعارة التي تمكنه من إخفاء الأدلة التي قد تكون قائمة ضده، هذا من جهة، ومن جهة أخرى قد يلجا إلى محو الأدلة أو تدميرها في زمن قصير جدا، باعتبارها معلومات معنوية غير مرئية تعتمد في موضوعها على الشفرة والرموز السرية والنبضات والتخزين الإلكتروني، فالجهة المكلفة بالتحريات القضائية في هذه الجرائم لا تستطيع تطبيق إجراءات الإثبات التقليدية عليها نتيجة صعوبة فهم الدليل المتحصل عليه من الرسائل الإلكترونية، والضخامة البالغة لكم البيانات المتعين فحصها. [2]
- تمتاز جرائم التوقيع والتصديق الإلكترونيين باعتبارها جرائم التقنية بالتباعد الجغرافي بين الجاني والمجني عليه، يظهر فيها سلوك المجرم والذي يشكل الركن المادي عمل سريع قد لا

[1]– غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية، الجزائر 2015، ص 43.

[2]–أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، دار النهظة العربية، مصر، 2015، ص419.

يستغرق أكثر من بضع ثوان، بالإضافة إلى سهولة محو الدليل والتلاعب فيه، مع إمكانية تنفيذ كل ذلك عن بعد دون اشتراط التواجد في مسرح الجريمة. [1]

ويمكن إجمال صعوبات إثبات أو اكتشاف جرائم التوقيع والتصديق الإلكترونيين فيما يلي:

1. من حيث أركان الجريمة:

أ. **الركن الشرعي:** هناك العديد من الإعتداءات التي تطال التوقيع الإلكتروني وشهادة التصديق الإلكتروني والتي لا ينطبق عليها أي وصف قانوني، فكان لزاما على أي مشرع أن يأخذ هذا التقدم التكنولوجي بعين الاعتبار، بتطوير الوسائل اللازمة أهمها قواعد التجريم ردعا للإجرام الإلكتروني.

ب. **الركن المادي:** تقوم جرائم التوقيع والتصديق الإلكترونيين في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والأنترنت وبالتالي فالسلوك المجرم الذي يقوم به الجاني غير ملامس لأرض الواقع مما يصعب معه الوقوف على الركن المادي لهذه الجرائم المستحدثة والتي يكون موضوعها المال المعلوماتي المعنوي. [2]

ج. **الركن المعنوي:** من المتصور غالبا أن لا تقع الإعتداءات التي تطال آليتي التوقيع والتصديق الإلكترونيين إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق أو فك الشفرة أو إتلاف أو تزوير البيانات والمعلومات، والأصل في هذه الجرائم هو العمدية إلا ما استثني بنص، وهناك من الجرائم ما يتطلب المشرع إرادة ارتكاب السلوك وتحقق النتيجة، حيث يكتفي بتوافر القصد الجنائي العام بصورتيه العلم والإرادة كالدخول إلى آليات إنشاء التواقيع الإلكترونية وشهادات التصديق الإلكترونية من اجل طمس الدليل، وفي نفس الوقت قد يشترط المشرع إضافة إلى القصد الجنائي العام قصدا جنائيا خاصا، كضرورة توافر نية التملك للأموال المحصل عليها من سرقة التوقيع الإلكتروني ونسبته إليه باستعماله في سرقة بطاقات الائتمان وغير ذلك من الإعتداءات .

---

[1]– اسامة احمد المناعسة، جلال مهد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان 2014، ص 45.

[2]– غنية باطلي، الجريمة الإلكترونية، مرجع سابق ص 45.

2. من حيث وصف الجريمة:

ويظهر ذلك في أن مجمل الإعتداءات التي تطال آليتي التوقيع والتصديق الإلكترونيين هي:

- جرائم ذات طابع دولي .
- صعوبة تنفيذ العقاب على مرتكبي جرائم التوقيع والتصديق الإلكترونيين .
- جرائم فادحة الأضرار.

وسيأتي تفصيل كل ذلك في الفرع اللاحق بعنوان أركان جرائم التوقيع والتصديق الإلكترونيين.

ثالثا: أصناف جرائم التوقيع الإلكتروني

يخضع تصنيف جرائم التوقيع والتصديق الإلكترونيين إلى معايير فقهية متعددة، باعتبارها جرائم التقنية المستحدثة تتداخل فيها آليات متعددة بدءا بالحاسب الآلي المستعمل في الإعتداء، وكذا البيئة الرقمية واستعمال شبكة الأنترنت، وقد وردت هذه الأفعال المجرمة في الإتفاقيات والمؤتمرات التي عنت برصد الظاهرة وضبطها، كإتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001. [1] ومنظمة التعاون الاقتصادي، أو في القوانين الجزائية الداخلية.

[1]–الإتفاقية الدولية لمكافحة الجريمة المعلوماتية في 23 من نوفمبر 2001: في مدينة بودابست عاصمة المجر قامت 26 دولة بالتوقيع على تلك الإتفاقية فيما بينها لمكافحة الجريمة المعلوماتية، وقد كانت تلك الإتفاقية نتاج لتعاون وعمل لجان قانونية وفنية من تلك الدول، ورغم اختلافها في نظمها القانونية الا انه وبالنظر لخطورة الموضوع وجسامة المخاطر المترتبة عليه في حالة عدم التكاتف في مواجهته تغاضت الدول عن تلك الاختلافات وذلك حتى تتمكن من تنظيم العمل أو الاستفادة من مجتمع المعلومات وثورة الاتصالات فهذه المعاهدة اسهمت في تقنين العديد من المجهودات الدولية التي بذلت في هذا المجال وهي المعاهدة الاوروبية بشأن حماية البيانات الشخصية وكذلك استندت إلى الميثاق الدولي لحماية الحقوق المدنية والسياسية الصادرة عن الامم المتحدة 1966، كما تأثرت بمعاهدة التعاون الدولي في مكاقحة الجريمة المعلوماتية الصادرة عن الامم المتحدة، ومنظمة التعاون الاقتصادي والتنمية OECD ودول الاتحاد الاوروبي، ومجموعة G8 وكذلك التوصية الاوروبية رقم 10/85 والتوصية رقم 2/88 والتوصية رقم 9/89 والتوصية رقم 13/95، د/أيمن عبد الله فكري، الجرائم المعلوماتية، مرجع سابق ص148، ص 149.

1. **تصنيف إتفاقية بودابست:**

يمكن إجالها في الجرائم التالية:

أ. الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية ذات الصلة بالتوقيع الإلكتروني وشهادة التصديق الإلكتروني[1]:

- الولوج غير القانوني.
- الإعتراض غير القانوني.
- الإعتداء على سلامة البيانات.
- الإعتداء على سلامة النظام.
- إساءة إستخدام أجهزة الحاسب الآلي.

ب. الجرائم المعلوماتية:

- التزوير المعلوماتي.
- الغش المعلوماتي.
- الجرائم المتصلة بالإعتداءات على الملكية الفكرية.

2. تصنيف المشرع الجزائري:

تدخل جرائم التوقيع والتصديق الإلكترونيين ضمن طائفة الجرائم المعلوماتية التي ورد النص عليها في القسم السابع مكرر من القانون 15/04 المؤرخ في 2004/11/10 المتمم والمعدل لقانون العقوبات تحت مسمى "المساس بأنظمة المعالجة الآلية للمعطيات". ويحتوي هذا القسم على المواد من 394 مكرر إلى 394 مكرر7 بمحورين أساسيين لتصنيف الجرائم، الأول يتمثل في الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع في كل جزء من نظام المعالجة الالية للمعطيات، ويشدد العقوبة في حالة دخول أو تعديل المعطيات الموجودة داخل النظام، والمحور الثاني المتمثل في الجرائم المترتبة عن جريمة الدخول أو البقاء غير المشروع، كالإعتداء العمدي على المعطيات ونظام المعالجة، وجرائم التعامل غير المشروع في المعطيات سواء الصالحة لارتكاب الجريمة أو المتحصلة منها .

[1]– انظر المادة الثانية وما بعدها من الإتفاقية المشار اليها.

ومع تنامي الإعتداءات على المعلومات الرقمية، صدر القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث ضم 18 مادة موزعة على 6 فصول تناولت تصنيف الجرائم الإلكترونية وإجراءات التحري فيها، وهي الجرائم المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

وقد خص المشرع الجزائري مؤخرا جرائم التوقيع والتصديق الإلكترونيين بنصص خاصة وردت في الفصل الثاني من القانون 04/15 المؤرخ في 2015/02/01 المحدد للقواعد العامة المتعلقة بالتوقيع الإلكتروني، وكذا الفصل الخامس من القانون 03/15 المؤرخ في 2015/02/01 المتعلق بعصرنة العدالة، والقانون 04/18 المؤرخ في 2018/05/10، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، والقانون 05/18 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية، والقانون 07/18 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ويمكن إجمالها كالآتي:

- الإعتداءات على آلية إنشاء التوقيع الإلكتروني.
- الإعتداءات على شهادة التصديق الإلكتروني.
- جرائم مؤدي خدمات التصديق الإلكتروني.

سيتم التعرض لهذه الجرائم بالتفصيل في الفصل الثاني من هذه الدراسة.

الفرع الثاني: السمات الخاصة لأركان جرائم التوقيع الإلكتروني

تبعا للقاعدة الراسخة في القانون الجنائي فإن قيام أي جريمة ما يتطلب كأصل عام ركن مادي وركن معنوي، وبإنعدام هذين الركنيين تنعدم الجريمة ولا وجود لمبرر للعقاب.

فالركن المادي لازم لوجود النشاط الإجرامي بعناصره الثلاث: (السلوك، العلاقة السببية للجريمة، النتيجة)، وهو يمثل العمل العضلي للجاني، والركن المعنوي يمثل العمل الفكري له بأشكاله المتعددة من قصد جنائي، وخطأ غير عمدي، وتجاوز في القصد، وقصد احتمالي، حسب ما يطلبه المشرع في كل جريمة.

أولا: الركن المادي في جرائم التوقيع الإلكتروني

إن قيام أي جريمة مهما كانت طبيعتها يتطلب وجود ركن مادي، وهو الفعل أو العمل الخارجي الذي يعبر عن النية الإجرامية أو الخطأ الجزائي[1]، فالركن المادي هو سلوك إجرامي يحقق نتيجة معينة تجمعها رابطة سببية، وهذا التعريف ينصرف إلى الركن المادي للجريمة عامة بما فيها جرائم التوقيع والتصديق الإلكترونيين، [2]إلا أن أهم ما يميز هذه الجرائم خصوصية ركنها المادي وهي على العموم:

1. **النشاط المادي في جرائم التوقيع الإلكتروني:**

يتمثل الفعل أو النشاط المادي في جرائم التوقيع والتصديق الإلكترونيين في الحركة العضوية الصادرة عن الإرادة الإنسانية تستهدف المساس بآلية التوقيع الإلكتروني وبيانات إنشاءه، أو شهادة تصديق إلكتروني بما تحتويه من معلومات وبيانات أطراف التعاقد الإلكتروني، قد تكون في بعض الأحيان سرية.

- **النشاط التقني:**

يأخذ هذا الفعل المادي صورة النشاط التقني باستخدام الحاسب الآلي أو شبكة الأنترنت، وتعد هذه الأفعال من الجرائم الايجابية المعاقب عليها سواء في قانون العقوبات أو باقي القوانين الخاصة ذات العلاقة، والعلة من تقريرها هي معاقبة الإقدام عليها بفعل ايجابي وليس الإحجام عن ارتكابها، وهو ما يميزها عن الجرائم السلبية.[3]

والسلوك الإجرامي قد يأتي بصورة بسيطة وقد يتضمن سلسلة سلوكيات معقدة كالاحتيال في جرائم شهادة التصديق الإلكتروني من قبل مؤدي خدمات التصديق الإلكتروني، أو الإخلال بالتزاماتهم تجاه السلطة سواء الحكومية أو الاقتصادية، وكذا احتيال صاحب شهادة التصديق الإلكتروني خلال استعماله غير المشروع لها .

---

[1]–B.Bouloc , Droit Penalegeneral ; 22 edition , Da 1102,2011 , N169 , p 169.

[2]– احمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، مرجع سابق، ص145

[3]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 2016/2015، دار هومة، الجزائر 2016. ص 116

وقد يلعب الزمن دورا هاما في ارتكاب بعض الجرائم ذات الصلة بالتوقيع والتصديق الإلكترونيين وتحديد طبيعتها، كما يوجد السلوك الإجرامي بصفة وقتية محددة، فقد يوجد بصورة مستمرة ومثالها في هذا المجال برامج الحاسب الآلي المدرجة لإتلاف البيانات، وهذا الإتلاف يعرف باسم (الفيروسات) (Viruses) وتكون الاستمرارية للنتيجة الإجرامية. [1]

وتقوم النتيجة الإجرامية في جرائم التوقيع والتصديق الإلكترونيين على فكرة الخطر والضرر والمصلحة الجديرة بالحماية، وقد سبق شرح ذلك في بداية الدراسة، وهي في معظمها من جرائم الضرر التي تتطلب حدوث النتيجة الإجرامية، اي الضرر الناتج عن وقوع الفعل المادي، بينما تكون جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية لبيانات التوقيع الإلكتروني وبيانات شهادة التصديق الإلكتروني من قبيل جرائم الخطر الذي تتحقق النتيجة الإجرامية فيه بمجرد الدخول حتى ولو لم يحدث ضرر. [2]

ويلزم لكي يتم ثبوت الركن المادي بعناصره كافة أن تكون هناك علاقة سببية بين السلوك الإجرامي الذي أتاه الجاني والنتيجة الحاصلة، بحيث يمكن القول أن تحقق النتيجة كان بفعل السلوك المجرم وإلا انتفت العلاقة السببية، فلا مجال لمساءلة الجاني.

وعدم تحقق النتيجة يعود بنا إلى الشروع أو محاولة إرتكاب الجريمة، والأصل في القانون الجزائري أن الشروع يعاقب عليه حسب نص المادة 30 من قانون العقوبات، في حين لا يعاقب على المحاولة في الجنحة إلا بنص صريح (المادة 1/31ق ع) [3]، وينطبق ذلك على جرائم التوقيع والتصديق الإلكترونيين بإعتبارها من الجرائم المعلوماتية المنصوص عليها في قانون العقوبات أو في قانون التوقيع والتصديق الإلكترونيين أو القوانين الأخرى، لا يتصور فيها الشروع، ويرجع ذلك إلى طبيعة الركن المادي لهذه الجرائم وهي معظمها في مصاف الجنح.

---

[1]– أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق ص 54.

[2]– أحمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، مرجع سابق ص 155.

[3]– الأمر 156/66المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات المكمل والمتمم.

ثانيا: الركن المعنوي في جرائم التوقيع الإلكتروني

الركن المعنوي للجريمة بصفة عامة هو الرابطة المعنوية أو الصلة النفسية أو العلاقة الأدبية التي تربط بين ماديات الجريمة ونفسية فاعلها، بحيث تتدخل الإرادة في حصول النتيجة. [1]

وتظهر أهمية الركن المعنوي من حيث انه يكمل أركان الجريمة ويعطي لها الوصف القانوني الموجب للجزاء الجنائي المناسب. وإسقاطا على جرائم التوقيع والتصديق الإلكترونيين، فان الركن المعنوي بصورته التقليدية من قصد جنائي وخطأ جنائي يتفق مع باقي الجرائم، لكنها تختلف في بعض النقاط لعل أهمها من حيث عنصري العلم والإرادة، فالجاني يعلم أنه يرتكب فعل غير مشروع، لكن في الوسط الرقمي بالتحديد وليس في الوسط المادي التقليدي، زيادة إلى إرادته في إتيان السلوك وتحقق النتيجة التي قد يمتد أثرها إلى الوسط المادي الملموس.

وبصورة عامة فان جرائم التوقيع والتصديق الإلكترونيين من الجرائم العمدية التي يتوافر لها القصد الجنائي لإلحاق الأذى والخسارة بالمجني عليه، سواء أكان ذلك بالنفس، أو بالأموال، أو البيانات أو المعطيات ذات العلاقة بالتوقيع الإلكتروني أو شهادة التصديق الإلكتروني. [2]

هذا وقد اشترط المشرع الجزائري لقيام الجريمة العمدية توافر الركن المعنوي في كثير من مواده[3]، وبتطبيق هذه المبادئ العامة على جرائم التوقيع والتصديق الإلكترونيين، ينبغي أولا أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية تتدخل في تكوين هذه الجريمة، فلكي يتوافر القصد الجنائي يجب أن يعلم الجاني بعناصر الركن المادي للجريمة، ولعل أول هذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني أن فعله ينصب على معلومات وبيانات توقيع إلكتروني أو شهادة تصديق إلكتروني محمية جزائيا باعتبارها محلا للحق الذي يحميه المشرع. [4]

---

[1]– عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام)، ديوان المطبوعات الجامعية، الجزائر 2009، ص231.

[2]–م.م.لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد للنشر والتوزيع، عمان 2015، ص164.

[3]– راجع مواد قانون العقوبات التي تشير صراحة إلى ضرورة توافر العمد في ارتكاب الجريمة ومنها على سبيل المثال المواد: 73و 155و 160و 180و 254و 264...الخ

[4]– أحمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، مرجع سابق، ص172.

إلا أنه عند الاطلاع على بعض القوانين المقارنة التي جاءت لمكافحة الجريمة المعلوماتية نلاحظ بأن بعض صور الجرائم لم يكتف فيها المشرع بالقصد العام (العلم والإرادة)، وإنما أضاف مشاركة القصد الخاص، كما هو الحال في نص المادة 22 من قانون الإمارات الخاص بمكافحة الجريمة المعلوماتية رقم 02 لسنة 2006، حيث جاءت هذه المادة لتجرم الحصول على معلومات سرية من خلال اختراق المواقع، فلابد أن تتجه إرادة الجاني إلى فعل الاختراق وعلمه بأن البيانات الموجودة فيه هي بيانات سرية وهامة، بالإضافة إلى توافر القصد الخاص المتمثل وهو الحصول على بيانات ومعلومات حكومية سرية. [1]

وفي المملكة المتحدة، يتضمن قانون إساءة إستخدام الحاسبات الآلية لعام 1990 في مادته الثانية نصا يجرم الدخول غير المصرح به متى توافر لدى الفاعل قصد خاص يتمثل في نية ارتكاب جريمة أخرى لاحقة على هذا الدخول، وجاءت المادة الثانية لتجرم الدخول غير المصرح به إلى نظام الحاسب الآلي بنية ارتكاب أو تسهيل ارتكاب جرائم أخرى. [2]

وفي المادة السابعة من القانون البرتغالي لجرائم المعلوماتية الصادر عام 1991، تتطلب جرائم الدخول غير مصرح به لنظام المعالجة الآلية قصدا خاصا يتمثل في نية الحصول له أو للغير على ربح أو فائدة غير مشروعة[3] .

وهو ما انتهجه المشرع الجزائري مؤخرا في القانون 04/15 السالف الذكر أثناء تناوله لمختلف الإعتداءات التي تطال آلية التوقيع الإلكتروني أو شهادة التصديق الإلكتروني، وكذا في القوانين ذات الصلة وهو ما سيأتي تفصيله في الفصل الثاني من هذه الدراسة.

---

[1]–م.م.لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، مرجع سابق، ص166.

[2]–Bain bbridge (David) , Hacking. T Access of computer systems ,Thelegal Implications , Wiley , 1989 ,P 237.

[3]–احمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، مرجع سابق، ص173.

الفصل الثاني:

صور الجرائم الواقعة على التوقيع الالكتروني

تمهيد:

تشكل مختلف الإعتداءات الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني تحديا كبيرا يواجهه القاضي الجزائي الملزم بمبدأ شرعية الجرائم والعقوبات، من حيث انه لا يستطيع من جهة أولى تجريم أفعال لم ينص عليها المشرع، ومن جهة ثانية التزايد الهائل للجرائم المستحدثة ذات العلاقة بآليتي التوقيع والتصديق الإلكترونيين.

بناء على ذلك اتجه الفقه والقضاء في البداية إلى الاستعانة بالنصوص التقليدية المتعلقة بجرائم الأموال وجرائم التزوير، مما تسبب في جدل فقهي وقضائي كبير، الأمر الذي أدى إلى تدخل المشرع في بعض الدول بتعديل النصوص القائمة تماشيا مع الطبيعة الخاصة لجرائم التوقيع والتصديق الإلكترونيين، فيما اتجهت بعض التشريعات لاستحداث نصوص خاصة، وهو ما تبناه المشرع الجزائري من خلال القانون 03/15 المتعلق بعصرنة العدالة في خطوة أولى، ثم القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

وعليه سيتم تقسيم الفصل إلى مبحثين، يتناول الأول جرائم التوقيع الإلكتروني وشهادة التصديق الإلكتروني التقليدية، وهي الجرائم الواردة في قانون العقوبات كأصل للتجريم، كالتزوير والإتلاف، وجرائم الأموال، وكذا الإعتداءات في إطار المساس بأنظمة المعالجة الآلية للمعطيات، ثم يتناول المبحث الثاني جرائم التوقيع والتصديق الإلكترونيين المستحدثة في القانون 04/15 والقوانين الخاصة ذات العلاقة على النحو التالي:

- **المبحث الأول:** جرائم التوقيع والتصديق الإلكترونيين في إطار القواعد العامة لقانون العقوبات.
- **المبحث الثاني:** جرائم التوقيع الإلكتروني في إطار القانون 04/15 وبعض النصوص الخاصة.

المبحث الأول:

جرائم التوقيع الإلكتروني في إطار القواعد العامة لقانون العقوبات

يتعلق موضوع الجريمة الإلكترونية بالبرامج والمعلومات التي تشكل محلا يضفي نوعا من الخصوصية على هذه الجرائم، ولما كانت أغلب الدول ومن بينها الجزائر تفتقر لقوانين تحمي التوقيع الإلكتروني وشهادة التصديق الإلكتروني باعتبارهما آليتين أساسيتين في نطاق الحكومة أو الإدارة الإلكترونية، أو في مجال التجارة الإلكترونية ومختلف التطبيقات الالكترونية الأخرى، حاول الفقه والقضاء في البداية تفسير النصوص العامة المتعلقة بجرائم الأموال ونصوص جرائم التزوير مسايرة لمبدأ شرعية الجرائم والعقوبات، وعدم جواز تجريم أفعال لم ينص المشرع عليها مهما كانت خطورتها ثم انتقل في مرحلة ثانية إلى الحماية الجزائية تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

وعليه سيتم التطرق في هذا المبحث إلى الإعتداءات التي تطال آليتي التوقيع والتصديق الإلكترونيين في إطار جرائم الأموال وجرائم التزوير في المطلب الأول، وفي إطار المساس بأنظمة المعالجة الآلية للمعطيات في مطلب ثان على النحو التالي:

المطلب الأول:

الإعتداء على التوقيع الإلكتروني في إطار جرائم الأموال وجرائم التزوير

يقصد بجرائم الأموال: تلك الأفعال التي تشكل إعتداء حالا أو محتملا على الحقوق ذات القيمة المالية، أو على أحد عناصر الذمة المالية للشخص، وبحكم أن المحررات الإلكترونية التي ينتمي إليها التوقيع الإلكتروني وشهادة التصديق الإلكتروني ذات طبيعة خاصة، تثور إشكالية مدى إعتبار المحرر الإلكتروني مالا بصدد جرائم الأموال، وكذلك مدى انطباق جرائم الأموال كالسرقة والنصب وخيانة الأمانة وحيازة المحررات الإلكترونية المتحصلة من جريمة على آليتي التوقيع والتصديق الإلكترونيين[1]، إلى جانب ما تثيره جريمة التزوير وفقا للقواعد العامة بتزوير التوقيع الإلكتروني.

على ضوء ذلك سيتم تناول هذا المطلب في فرعين على النحو التالي:

[1]– أحمد عاصم عجيلة، مرجع سابق ص 271.

- **الفرع الأول:** الإعتداءات باعتبارها جرائم أموال.
- **الفرع الثاني:** جرائم تزوير التوقيع الإلكتروني.

الفرع الأول: الإعتداءات باعتبارها جرائم أموال:

من المقرر أن جرائم الأموال في التشريعات المختلفة تقع على مال منقول مملوك للغير، حيث تنص المادة 350 من قانون العقوبات الجزائري انه: " كل من إختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100000دج إلى 50000دج وتطبق نفس العقوبة في حالة اختلاس المياه والغاز والكهرباء "، أسوة بنص المادة 2/311 من قانون العقوبات الفرنسي. أما المشرع المصري فقد استعمل مصطلح "منقول" عندما نصت المادة 311 على أنه: " كل من اختلس منقولا مملوكا للغير فهو سارق"، وهذا ما أثار مدى إمكانية إدراج البرامج والمعلومات ذات الصلة بالتوقيع الإلكتروني وشهادة التصديق الإلكتروني ضمن موضوع السرقة باعتبارها من الأشياء أو من المنقولات.[1]

ويثور التساؤل كذلك حول مدى اعتبار تلك البرامج والمعلومات ضمن التعداد الوارد في المادة 376 من قانون العقوبات الجزائري المتعلق بخيانة الأمانة، وكذا المادة 372 فيما تتعلق بجريمة النصب.

أولا: التوقيع الإلكتروني وجريمة السرقة:

ذهب جانب من الفقه الجزائي بفرنسا إلى إمكانية تطبيق الأحكام الخاصة بالسرقة على الإستخدام غير المشروع لمختلف البرمجيات الرقمية، ويستند أصحاب هذا التوجه إلى المفهوم القانوني لفكرة السرقة كما حددها إميل غارسون[2]، والتي اخذ بها القضاء الفرنسي في بعض أحكامه، ويمثل فعل السرقة عنده مجرد الإعتداء على حيازة الشيء محل السلوك الإجرامي دون اقتضاء إنتقاله

[1]– باطلي غنية، مرجع سابق ص 85.

[2]– بخلاف أصحاب النظرية المادية لا يشترط اميل غارسون في السرقة ان تصدر عن الجاني حركة مادية ينقل بها الشيء من موضعه. فقد عرف السرقة بأنها الاستيلاء على الحيازة الكاملة للشيء بعنصريها المادي والمعنوي دون علم وإرضاء المالك أو الحائز. لمزيد من التفصيل راجع: علي عبد القادر القهوجي، قانون العقوبات القسم الخاص، منشورات الحلبي الحقوقية، بيروت 2002، ص 632.

المادي[1]، ويرى جانب آخر من الفقه أن محل السلوك الإجرامي لا علاقة له بالبرامج الإلكترونية أو الرقمية إنما بالوظيفة أو الخدمات التي تؤديها هذه البرامج، وهو ما يخرج عن الإطار العام لجريمة السرقة. [2]

وبالعودة إلى تعريف السرقة في القانون والفقه والتي تمثل اختلاس الشيء المملوك للغير، يظهر جليا أن مدلول الكلمة واسع يشمل الأشياء المادية وغير المادية، وهو ما يجعل المعلومات والبيانات الخاصة بآليتي التوقيع والتصديق الإلكترونيين تدخل في نطاق هذه الكلمة.

بالمقابل فان أي تفسير لكلمة شيء ينبغي ألا يكون بمعزل عن العنصر الثاني في السرقة ألا وهو فعل الاختلاس، فالاختلاس هو الركن المادي في جريمة السرقة، وهو يبدأ عادة بفعل مادي يتمثل في نقل الشيء أو أخذه أو نزعه من مالكه، متضمنا تغييرا في الحيازة القانونية لهذا الشيء، وهو ما يقتضي أن يكون هذا الشيء ماديا بطبيعته[3]، وتطبيق ذلك جريمة السرقة على أنواع الطاقة الكهربية أو الكهرومغناطيسية.

ومن ثم فانه يمكن وبالقياس على ذلك إدخال أنواعا جديدة من الأموال غير المادية مثل التوقيع الإلكتروني وشهادة التصديق الإلكتروني بما تحتويه من برامج ومعلومات داخل نطاق مفهوم الشيء ليشمل الأشياء المادية وغير المادية.

وتنطبق في هذا السياق شروط سرقة التوقيع الإلكتروني وشهادة التصديق الإلكتروني على سرقة بطاقات الائتمان من حيث أن كل منهما عبارة عن صندوق يتضمن كمية من المعلومات والبيانات الخاصة ويغلق عليها ببرنامج تشفير، إلا أن بطاقة الائتمان هي لحفظ الأموال وتأمينها، بينما التوقيع الإلكتروني وشهادة التصديق الإلكتروني آليتين لحفظ المعلومات. [4]

---

[1]– عبد الجبار الحنيص، الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية – المجلد 27– العدد الأول، 2011، ص195.

[2]– عبد الجبار الحنيص، مرجع سابق ص 196.

[3]– احمد عاصم عجيلة، مرجع سابق ص273.

[4]– ضياء مصطفى عثمان، السرقة الإلكترونية دراسة فقهية، الطبعة الأولى، دار النفائس، الاردن 2011.

ويمكن إجمال الاتجاهات الفقهية المختلفة بشأن سرقة المحررات الإلكترونية عامة والتوقيع والتصديق الإلكترونيين خاصة كما يلي:

1. **الاتجاه الأول:** صلاحية التوقيع الإلكتروني وشهادة التصديق الإلكتروني كمحل يقبل السرقة:

يذهب الاتجاه المؤيد لكون المعلومة أو البرنامج يدخل في عداد الأموال إلى الأخذ بمعيار القيمة بدلا من المعيار المادي الذي اخذ به الفقه التقليدي في نظرته للمال فالمعيار في اعتبار الشيء مالا ليس على أساس حاله من كيان مادي وإنما على أساس ما له من قيمة اقتصادية، وأن الحائز الذي يرفض إسباغ وصف المال على شيء له قيمة اقتصادية هو قانون ينفصل عن الواقع.[1]

وهو ما ذهب إليه أحد الفقهاء بالقول أن مفهوم المال أو الشيء هو مفهوم ينبع من تصور الذهن بهما وليس ما طبيعة الشيء. [2]

وبناء على هذا المفهوم من المقبول أن يكون موضوع المال شيئا غير مادي متى كانت له قيمة اقتصادية، مثل البرامج والمعلومات التي تتضمنها آليتي التوقيع والتصديق الإلكترونيين والتي يجب معاملتها على أنها مال. [3]

2. **الاتجاه الثاني:** عدم صلاحية التوقيع الإلكتروني وشهادة التصديق الإلكتروني كمحلان يقبلان السرقة.

يرى هذا الاتجاه أن آليتي التوقيع الإلكتروني وشهادة التصديق الإلكتروني باعتبارهما محررين إلكترونيين لا يمكن أن تكونان محلا يقبل السرقة، ذلك أن غالبية النصوص التشريعية المقارنة التي عرفت جريمة السرقة لا تجرم سرقة المعلومات في ذاتها منفصلة من وسيطها المادي مما يتعارض مع تطبيق نصوص جريمة السرقة التقليدية على المحررات الإلكترونية والمعلومات والبيانات المخزنة إلكترونيا.

---

[1]– انظر: Carbonnier , Droit Civil P.U.F Paris 1973 T3 Les biens No 17 , 18 , p54 et 55.

[2]–Planial (M) Et Ripert (G) , Traitépratique de droit civil Français , L.G.D.T Paris 1926 T3 Les biens N° 50, p 55 et 56.

مشار اليه / علي عبد القادر القهوجي، المرجع السابق، ص 50.

[3]– ايمن عيد الله فكري، مرجع سابق، ص 588.

وقد أيد الفقه الجنائي في مصر وفرنسا هذا الرأي لأسباب عدة منها:

أ. عدم تناسب طبيعة المحل في جريمة سرقة المحررات الإلكترونية مع فعل الاختلاس كون المعلومات والبيانات التي تتضمنها آليتي التوقيع والتصديق الإلكترونيين تخرج من مجال السرقة إذا كانت منفصلة عن إطارها المادي، وهو ما ذهبت إليه بعض التشريعات في نصها صراحة على أن يكون المحل ماديا، كقانون العقوبات المصري والاسباني والسويسري والتي رأت أن إتصال البيانات والمعلومات بشيء مادي كوسيلة لتسجيلها والاحتفاظ بها يعطي لها كيان مادي، ومن ثم تصلح موضوعا للسرقة. [1]

ب. تنافي سرقة المعلومات مع قابلية التملك في الشيء محل جريمة السرقة تماشيا مع إجماع الفقه على القول بأن جريمة السرقة من فئة جرائم الأموال التي يكون من شأنها أن تهدر حقا من الحقوق المتصلة بالذمة المالية للغير أو تعرضه للخطر، وهي كلها إعتداءات على حق الملكية، لان جوهر السرقة الإعتداء على المال بقصد تملكه.[2]

وبهذا فالمعلومات والبيانات ليست موضوعا لحق الملكية، مما يخرجها عن دائرة فعل الاختلاس المشكل لجريمة السرقة ويدخلها تحت طائلة جريمة التقليد في إطار قوانين محددة كحق الملكية الفكرية وبراءات الاختراع.

ج. سلب الحيازة بإخراج المال من حيازة الحائز الشرعي وإدخاله في حيازة الجاني بطرق غير مشروعة.[3]

وبالنسبة للتوقيع الإلكتروني وشهادة التصديق الإلكتروني فلا يتصور ذلك بالنسبة لها إلا إذا إنصب فعل الاختلاس على الدعامة المادية التي تحمله والتي تم تسجيل التوقيع الإلكتروني وشهادة التصديق الإلكتروني عليها، فإختلاس البيانات والمعلومات المخزنة إلكترونيا من جانب الغير لا يؤدي إلى إنتقالها من حيازة الحائز الشرعي سواء أتم ذلك بطريقة مشروعة أو غير مشروعة. [4]

---

[1]– احمد عاصم عجيلة، مرجع سابق ص 271.

[2]– محمد زكي ابو عامر، قانون العقوبات، القسم الخاص، دار الجامعة الجديدة للنشر، الإسكندرية 2015، ص799.

[3]– ايمن عبد الله فكري، مرجع سابق ص 625.

[4]– احمد عاصم عجيلة، مرجع سابق، ص 272.

د. انتقال الشيء محل فعل الاختلاس من حيازة إلى أخرى: تعتبر جريمة سرقة بيانات التوقيع الإلكتروني أو شهادة التصديق الإلكتروني من الجرائم الرقمية تتم بفعل الاختلاس الذي يؤدي إلى خروج الشيء من حيازة المجني عليه وإدخاله في حيازة السارق. [1]

وينصب فعل الاختلاس على الوسيط المادي الذي يحمله المحرر الإلكتروني بما يتضمنه من بيانات ومعلومات مخزنة إلكترونيا والتي تم تسجيلها عليه، وهو ما يختلف عن فعل الاختلاس للبرامج أو المعلومات عن طريق الالتقاط الذهني، والذي يخرج عن دائرة العقاب بوصفه مكون لجريمة السرقة.[2]

وتبنى المشرع الجزائري في هذا السياق المفهوم الواسع للمال وصلاحية المال المعنوي خصوصا لإن لا يكون محلا لجريمة السرقة سواء من خلال المادة 2/350 من قانون العقوبات بتطبيق عقوبة السرقة على اختلاس الكهرباء باعتبار أن المعلومات والبرامج طاقة ذهنية تقبل التملك والحيازة من خلال دعامتها، كما أنها تقبل الإنتقال بموافقة حائزها، وهذه الموافقة يترجمها نظام التشفير الذي يعد بمثابة المفتاح، والمادة 372 حيث أورد المشرع الجزائري أيضا مصطلحي الأموال والمنقولات بدون تقيد لطبيعتهما.

ثانيا: التوقيع الإلكتروني وجرائم النصب وخيانة الأمانة

1. جرائم النصب الواقعة على التوقيع الإلكتروني:

يذهب رأي في الفقه إلى تعريف النصب بأنه: " الغش والإحتيال ويكون هو الوسيلة لسلب كل مال الغير أو بعضه، ويجب أن يكون له مظهر خارجي، فلا يكون كذب مجرد أو كتمان، وإنما يجب أن يكون مدعوما بما يعرف بالحبكة المسرحية أو التمثيلية ".[3]

---

[1]– فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، الاسكندرية، 2012، ص 227.

[2]– صالح شنين، مرجع سابق ص 18.

[3]–أحمد حسام طه، الجرائم الناشئة عن إستخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة، دار النهضة العربية، 2000، ص670.

وقد حدد المشرع الجزائري أحكام جريمة النصب في المادة 372 من قانون العقوبات[1]وأدرجها ضمن جرائم الأموال المنقولة وتقوم على ثلاثة أركان هي: الركن المادي ويتمثل في سلوك خداع المحتال للمجني عليه، ونتيجة إجرامية تتمثل في تسليم المجني عليه مالا معينا للمحتال، ورابطة سببية مادية تربط بين السلوك والنتيجة الإجرامية، يضاف إليه ركن المحل وهو مال منقول أو عقار حدده المشرع مملوك للمجني عليه، ويضاف إلى هذين الركنيين ركن ثالث وهو الركن المعنوي بتوافر القصد العام والقصد الخاص وهو نية التملك كون جريمة النصب جريمة عمدية. [2]

وقضى القضاء الفرنسي بأنه من الجائز إستخدام نظم المعلومات في تحقيق جريمة النصب، إذ أن" إستخدام الكمبيوتر في اصطناع إيصالات وطبعها نظرا لما له من إمكانيات في إجراء الحسابات يمثل الإيهام بوجود دين غير حقيقي تقع به جريمة النصب".[3]

بينما ذهب جانب آخر في الفقه الفرنسي إلى القول بأن الحصول على المعلومات بطرق احتيالية تمثل إحتيالا من اجل الحصول على المنفعة، مستندا في هذا الرأي إلى بعض التشريعات المقارنة كالمادة 146 من قانون العقوبات السويسري، والمادة 1/1 من قانون السرقات الصادر عام 1968 في انجلترا والتي تعتبر أن المنفعة يمكن أن تكون موضوعا ينصب عليه النشاط الإجرامي في جريمة النصب. [4]

وباعتبار التوقيع الإلكتروني وشهادة التصديق الإلكترونيين آليتين تتضمنان معلومات وبيانات مخزنة إلكترونيا لا تتم أي صفقة تعاقدية عبر الأنترنت بدونهما مما يضفي عليها طابع الأموال المتداولة في نطاق التعاملات الإلكترونية وفي التجارة الإلكترونية خاصة، فإنه يمكن حمايتهما بنصوص النصب والاحتيال.

---

[1]– انظر المادة 372 من العقوبات الجزائري.

[2]–نبيل صقر، مرجع سابق، ص90، ص92، ص108.

[3]–مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 200ص144و ما بعدها.

[4]–حمد عاصم عجيلة، مرجع سابق، ص287.

2. التوقيع الإلكتروني وجرائم خيانة الأمانة:

تتفق خيانة الأمانة مع السرقة والنصب في كونها من جرائم الإعتداء على ملكية المال المنقول، ويكمن الاختلاف عن السرقة التي تفترض فعل اختلاس مال المجني عليه بإرادته الحرة تسليما صحيحا بناء على سند قانوني، وتختلف خيانة الأمانة عن النصب الذي يفترض تسليم المجني عليه ماله برضاء معيب نتيجة التدليس الذي قام به المتهم. [1]

ويعرف الفقه خيانة الأمانة بأنها: " إختلاس مال منقول مملوك للغير أو استعماله أو تبديده، سلم إلى الجاني بناء على عقد من عقود الأمانة إضرارا بمالكه أو صاحبه أو واضع اليد عليه مع توافر القصد الجنائي".[2]

من التعريف السابق لخيانة الأمانة تتضح الأركان الأربعة للجريمة:

- **الركن الأول:** محل الجريمة، وهو المال المنقول المملوك للغير المسلم إلى الجاني وفق عقود محددة.
- **الركن الثاني:** الركن المادي، ويتخذ صورة اختلاس أو استعمال أو تبديد محل الجريمة.
- **الركن الثالث:** الإضرار بمالك الشيء أو صاحبه أو وضع اليد عليه.
- **الركن الرابع:** الركن المعنوي، ويتخذ صورة القصد الجنائي.

وقد ترد خيانة الأمانة على الأموال الإلكترونية المادية كجهاز الكمبيوتر أو الشرائط الممغنطة، إلا أن الإشكال يثور حول الأموال الإلكترونية المعنوية، وهي البيانات المبرمجة ذات الصلة بآلية التوقيع والتصديق الإلكترونيين، وجواز أن تكون محلا لخيانة الأمانة، وذلك مع الازدياد الهائل كما وكيفا لهاته الأموال في معظم التعاملات الإلكترونية.

يرى جانب من الفقه والذي يمثل الاتجاه الرافض لتطبيق نصوص خيانة الأمانة على الاختلاس المعلوماتي وفقا لنص المادة 408 من قانون العقوبات الفرنسي والمادة 341 من قانون العقوبات المصري انه إذا كان القصد هو اختلاس المال المعلوماتي المادي سواء كان حاسب

[1]–فتوح عبد الله الشاذلي، مرجع سابق، ص351.

[2]–أيمن عبد الله فكري، مرجع سابق، ص695.

إلكتروني أو شريط أو اسطوانة ممغنطة فلا يختلف المفهوم في المال التقليدي عنه في المجال المعلوماتي، فالمفهوم واحد والتطبيق واحد وهو أن محل جرائم الأموال عامة هو المال المادي ويطبق ذلك على المجال المعلوماتي بدون أي تغيير. [1]

وقد قضى القضاء الفرنسي بأن من تسلم برنامج معالجة معطيات خاصة بالمشروع الذي يعمل به، وإستخدم هذا البرنامج في المعالجة الآلية الخاصة بالغير فلا نكون هنا بصدد جريمة خيانة الأمانة لانفصال البرنامج عن الدعامة المادية مما يخرجه من فئة الأموال المنقولة. [2]

فيما يؤيد جانبا آخر من الفقه والذي يمثل الاتجاه الغالب تطبيق نصوص خيانة الأمانة على الاختلاس المعلوماتي، فقد قضت محكمة النقض الفرنسية بتوافر خيانة الأمانة بخصوص رقم كارت السحب من البنك على سند حيث أن" أحكام المادة 314 فقرة 1 من قانون العقوبات تسري على كل مال أيا كانت طبيعته وليس فقط على المال المادي" فيكفي لوقوع جريمة خيانة الأمانة أن يكون المال المسلم قد خصصه صاحبه لإستعمال معين فيخرجه الأمين عن ذلك الاستعمال مستوليا على مال الغير، ومما لا شك فيه أن رقم كارت الائتمان هو مال له قيمة مالية.[3]

كما قضت محكمة جنح بروكسل بتوافر جريمة خيانة الأمانة بشأن متهم قام باختلاس عدد 50 دعامة ممغنطة إضرارا بالمبرمج الذي كان يقوم بتسجيل معلومات عليها لصالح الشركة التي كان يعمل بها المتهم، وقد أسست المحكمة حكمها على أن المتهم قام بحيازة أو إستعمال البرامج المسجلة على الاسطوانات المملوكة للشركة. [4]

وإجمالا فان قيام الجاني بنسخ المعلومات والبرامج المسلمة إليه على سبيل الأمانة وإستعمالها أو تبديدها أو اختلاسها لحسابه الخاص متجاوزا الإتفاق الذي يربطه وصاحب هذه المعلومات أو البرامج يحقق جريمة خيانة الأمانة لتحقق فعل الاستعمال المؤدي إلى استنزاف قيمة المال كلها أو

---

[1]–أيمن عبد الله فكري، مرجع سابق، ص116.

[2]–انظر: باطلي غنية، مرجع سابق، ص116.

[3]–شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظامين اللاتيني والانجلو أمريكي، مصر 2013، ص71، ص72.

[4]–انظر: أيمن عبد الله فكري، مرجع سابق، ص716.

بعضها مع بقاء مادته على حالها، وهو ما ينطبق مع آليتي التوقيع الإلكتروني وشهادة التصديق الإلكتروني اللتان تقومان بوظيفة النقود الإلكترونية بسداد الالتزامات المالية عبر شبكة المعلومات.

ثالثا: فكرة التوقيع الإلكتروني كبديل للنقود الإلكترونية في مجال جرائم الاموال:

أدى التطور التكنولوجي إلى إبتكار وسائل مساعدة لتداول الأموال كبديل للأموال النقدية الورقية والشيكات، وهو ما يطلق عليه بالنقود الإلكترونية ممثلة في البطاقات الممغنطة[1] (cartes manitiques)، لإستعمالها لدفع الاموال عند الشراء، أو سحبها من خلال منافذ التوزيع الآلي للعملة الورقية[2](Distributeurs automatiques de billets). وقد ورد تعريفها بمشروع قانون التجارة الإلكترونية المصري بأنها: " وفاء بإلتزام نقدي بوسيلة إلكترونية مثل الشيكات الإلكترونية والكمبيالات الإلكترونية وبطاقات الدفع الممغنطة ".[3]

ويتفق التوقيع الإلكتروني مع النقود الإلكترونية من حيث الشكل والآليات الفنية والتقنية اللازم توافرها للاعتداد بهما، إلا أن التوقيع الإلكتروني يمكنه القيام بوظيفة النقود الإلكترونية بسداد الإلتزامات المالية كما نصت عليه المادة 158 من القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين أن شهادة التصديق الإلكتروني الممنوحة على توقيع الشخص الإلكتروني يجب أن تتضمن حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني عند الاقتضاء. [4]

---

[1]– ظهرت البطاقات الائتمانية لأول مرة في الولايات المتحدة الأمريكية قبيل الخرب العالمية الأولى، ثم انتقلت إلى فرنسا في أواخر العشرينيات ومن ثم انتشرت في أرجاء الكرة الأرضية بسبب سهولة استخدامها والميزة التي تساعد حاملها على الاستغناء عن حيازة الشيك أو الأوراق النقديةأثناء تجواله، وهي عبارة عن بطاقات مصنوعة من البلاستيك تصدر عن مؤسسة ما إلى عميل يتعامل مع تلك المؤسسة يحملها فتسمح له بتسديد ثمن مشترياته من نوع معين من السلع أو من مختلف السلع المتوفرة أو بسحب النقود عند الحاجة (بحسب الحال ووفقا للأوضاع الفنية والقانونية للمؤسسة مصدرتها وللتجار أصحاب السلع المزمع شراؤها).

Soussi Roubi , Carte de crédit , Le Guide juridique Dalloz ,p215 Et W. Jeandidier, Les trucage et usages frauduleux de cartes magnétiques , Cahiers de droit de l’entreprise, /1986/.

[2]– نصر شومان، مرجع سابق، ص52

[3]– انظر أيمنعبد الله فكري، مرجع سابق، ص 719.

[4]– انظر المادة 15 من القانون 04/15 السالف الذكر.

وهو الأمر الذي يمكن من خلاله أن يقوم التوقيع الإلكتروني بسداد الالتزامات المالية عبر شبكة المعلومات دون الحاجة إلى المطالبة بالنص على النقود الإلكترونية طالما أن التوقيع الإلكتروني يقوم بدورها. [1]

ومن ثم اتجهت مختلف التشريعات إلى تجريم الحصول بغير حق على التوقيع الإلكتروني سواء كان ذلك بالسرقة أو النصب أو بخيانة الأمانة، مثلما جرمت نشاط الاستيلاء غير المشروع على المعلومات أو البيانات، من خلال جرائم الاختلاس أو الاستيلاء عن طريق الاحتيال.

ومن خلال ما سبق فقد ظهر واقعيا إمكانية إعمال آلية التوقيع الإلكتروني كبديل عن النقود الإلكترونية في مجال جرائم الأموال مادام أن التوقيع الإلكتروني يحقق وظيفته كوسيلة للتعبير عن التزام الشخص بما وقع عليه من معاملات تم توثيقها بمحرر إلكتروني، هذا إلى جانب وظيفة الوفاء بالالتزامات المالية الناشئة عن تلك المعاملات، ذلك أن العبرة هي بحقيقة الدور والوظيفة التي يقوم بها المصطلح لا بالمصطلح في ذاته. [2]

الفرع الثاني: جرائم تزوير التوقيع الإلكتروني:

جريمة التزوير من الجرائم المضرة بالمصلحة العامة كونها تستهدف الثقة التي أودعها المشرع في المحررات، مما يحتم المعاقبة على كل الأفعال الماسة بتلك المحررات سواء كانت رسمية أو عرفية أو توقيع إلكتروني أو شهادة تصديق إلكتروني لضمان عدم وقوع تغيير لحقيقتها.

ويختلف التزوير التقليدي عن التزوير الإلكتروني، حيث يتضمن التزوير إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو بالإضافة، وكل سلوك غير مشرع يتعلق بالكيان المادي للحاسب الآلي أو البرامج المعالجة معلوماتيا.

---

[1]– عرف القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية قانون 83 لسنة 2000 وسيلة الدفع الإلكتروني بأنها:"الوسيلة التي تمكن صاحبها من القيام بعمليات الدفع المباشر عن بعد عبر الشبكة العمومية للاتصالات".انظر هذا القانون على الموقع التالي:

www.arablaw.org/donload/EC_Tunisia.doc http: //

[2]–أيمن عبد الله فكري، مرجع سابق، ص 721.

أولا: التزوير المعلوماتي:

تدخل جرائم تزوير التوقيع الإلكتروني ضمن جرائم التزوير المعلوماتي الذي عرفته إتفاقية بودابست بأنه: "التزوير المرتبط بالحاسب الآلي والذي يتكون عند خلق أو تعديل غير مصرح به للبيانات في سياق المعاملات القانونية، بتغيير صحة البيانات المستخرجة التي تكون موضوعا لخداع المصالح القانونية المحمية".[1]

واتفق الفقه على أن التزوير المعلوماتي هو أخطر صور الغش التي تتصل بالمعلوماتية، وذلك بسبب حلول هذا النظام محل المحررات في تسجيل التصرفات والأعمال القانونية التي ترتب الحقوق وتنشأ الالتزامات، وبالتالي زيادة الثقة في المحررات المعلوماتية. [2]

وهو الأمر الذي أدى بالفقهاء إلى دراسة الظاهرة ووضع تعريف لها أنها: " تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في ورقة مكتوبة أو مرسومة عن طريق الرسم بأية لغة كانت وربما تتمثل في صورة مخرجات غير ورقية بشرط أن تكون محفوظة على دعامة معلوماتية كبرنامج منسوخ على اسطوانة، وبشرط أن يكون المحرر المعلوماتي ذا أثر قانوني في إثبات حق أو التزام وان يكون قابلا للإستخدام".[3]

تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي ولم يساير في ذلك المشرع الفرنسي الذي اخضع في مرحلة أولى أفعال التزوير المعلوماتي للقواعد العامة لجريمة التزوير التقليدية، إلا أن قانون العقوبات الفرنسي بعد تعديله أصبح ينص على أن موضوع التزوير هو الدعامة المادية التي تحوي البيانات والمعلومات، ولم يقتصر على المحرر في شكل كتابة أو عبارات خطية[4]، عكس المشرع الجزائري الذي إستحداث نصوصا تعاقب المساس بنظام المعالجة الآلية للمعطيات تضمنت بعض أفعال التعديل والمحو والإدخال كما سيأتي تفصيله

---

[1]– عمر محمد يونس، الإتفاقية الأوربية حول الجريمة الافتراضية، دار النهضة العربية، القاهرة 2007، ص 85

[2]– ايمن عبد الله فكري، مرجع سابق، ص 362

[3]–عبد الفتاح بيومي حجازي، مرجع سابق، ص306، وانظر هذا التعريف أيضا لذات المؤلف، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص170، ص 171.

[4]– احسن بوسقيعة، مرجع سابق، ص408

لاحقا، إلا أنه أغفل التطرق للتزوير في مجال المعلوماتية، مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي.

وبالنظر لتمتع التوقيع الإلكتروني بالحجية في الإثبات في القانون الجزائري، من خلال نص المادة 327 مكرر 1 من القانون المدني، والمواد 6 و8 و9 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، فان التوقيع الإلكتروني يكون محلا للحماية الجنائية تبعا للقاعدة العامة التي تنص على أن التوقيع الإلكتروني الذي لا يتمتع بالحجية في الإثبات ليس محلا للتزوير. [1]

ثانيا: أركان جريمة تزوير التوقيع الإلكتروني

اتجهت غالبية الفقه والتشريعات إلى معارضة فكرة تطبيق نصوص قانون العقوبات على المحرر المعلوماتي، وحصرت صورة المحرر في ضرورة إدراك مضمونه بالنظر أو اللمس، وذلك مالا يتوفر في المحرر المعلوماتي والذي يعتبر التوقيع الإلكتروني وشهادة التصديق الإلكتروني إحدى صوره، مما إستدعى إستحداث نصوص خاصة بالتزوير المعلوماتي مثلما ذهب إليه المشرع الفرنسي حيث نصت المادة 5/462 من قانون الغش المعلوماتي لسنة 1988 على انه: " كل من يقوم بتزوير مستندات معالجة آليا ...." والمادة 1/441 من قانون العقوبات الفرنسي الجديد لسنة 1994 التي عرفت التزوير بأنه " كل تغيير للحقيقة في محرر أو أي وعاء آخر بأي طريقة"[2]، وهو ما يفيد إمتداد مفهوم المحرر ليشمل المحرر المعلوماتي والمحررات التقليدية.

---

[1]– انظر: Rapport du coseil d'etat français, intrnet et les reseaux numerique, les documentation français, 1988, p.17,

Alain Ben soussan et Yves le roux, cryptologie et signature électronique, aspects juridiques, E, Hermes, 1999.p.79.

[2]– Art 441-1: « constitue un Faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. » codepenale Français, p94

كما جرم المشرع المصري في مشروع قانون التجارة والمعاملات الإلكترونية[1]، فعل تزوير التوقيع الإلكتروني، والمشرع الإماراتي في قانون المعاملات والتجارة الإلكترونية رقم 2 لعام 2002أفعال تزوير البيانات المقدمة لمزود خدمات التصديق الإلكتروني. [2]

1. الركن المادي لجريمة تزوير التوقيع الإلكتروني

قوام الركن المادي في جريمة تزوير التوقيع الإلكتروني هو تغيير حقيقة بيانات إنشاء التوقيع الإلكتروني وكذا شهادة التصديق الإلكتروني عن طريق الدخول إلى قاعدة البيانات وتعديلها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك بإحدى طرق التزوير التي يقرها القانون.

وقد ادخل المشرع الفرنسي تعديلا جوهريا على كل من مفهوم تغيير الحقيقة والمحرر في جريمة التزوير، حيث قام بإدماج المادة 5/462 و6 المتعلقة بتزوير المحررات المعالجة آليا واستعمالها داخل إطار النص العام للتزوير، وكذا المادة 1/441 التي أعطت المفهوم الحديث للتزوير في التشريع الجنائي الفرنسي. [3]

وإستنادا إلى ذلك يمكن تقسيم النشاط الإجرامي في جرائم تزوير التوقيع الإلكتروني إلى أربعة عناصر هي: تغيير الحقيقة، التوقيع محل التزوير، طرق التزوير، وعنصر الضرر.

أ. المفهوم المستحدث لتغيير الحقيقة:

تغيير الحقيقة في جرائم التزوير التقليدية يقصد به استبدالها بما يخالفها وفقا لإحدى الطرق التي نص عليها القانون، وهي بهذا المعنى من الجرائم المحددة الشكل. وهو التعريف الذي ينأى عن شموله صورة التزوير الإلكتروني بالتلاعب بالمعطيات. [4]

---

[1]–مشروع قانون التجارة والمعاملات الإلكترونية المصري، مركز المعلومات ودعم اتخاذ القرار، رئاسة مجلس الوزراء، القاهرة 2000.

[2]–قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 2 لسنة 2002، حكومة دبي، الجريدة الرسمية العدد 277، فيفري 2002.

[3]– ايمن عبد الله فكري، مرجع سابق، ص475.

[4]– نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر 2012، ص229.

وتحول هذا المفهوم من القالب المقيد إلى المفهوم المرسخ ليشمل جميع طرق تغيير الحقيقة دون تحديد الطريقة بعينها، لتصبح جريمة التزوير من الجرائم ذات القالب الحر[1]، واستخدم في ذلك المشرع الفرنسي مصطلح "الغش المعلوماتي" الذي يشمل جميع أنواع تغيير الحقيقة، وهو ما يفيد الفصل بين التلاعب في بيانات النظام المعلوماتي وتلك التي تقع على المحرر المعلوماتي.

وعليه فتغيير الحقيقة هو الأساس الذي تقوم عليه جريمة تزوير التوقيع الإلكتروني، لكن بشرط أن لا يكون هذا التغيير ماسا بحقوق الغير، فإذا كان محل التغيير توقيع إلكتروني خاص بالشخص نفسه وقام بكتابة بياناته هو ثم أضاف أو عدّل في حقوق له فلا يعتبر تزويرا طالما انه لم يمس بحقوق الغير أو بمراكزهم القانونية. [2]

ب. طرق تزوير التوقيع الإلكتروني:

يسري التزوير المادي للتوقيع الإلكتروني وشهادة التصديق الإلكتروني بتغيير البيانات (الحذف، الإضافة، الاصطناع) على غرار التزوير المادي في المحررات التقليدية.

غير أن المشرع قد يخرجهما (التوقيع الإلكتروني وشهادة التصديق الإلكتروني) وكذا في حالة بطاقات الائتمان الممغنطة من إطار القواعد العامة لجريمة التزوير لكي تحكمها نصوص خاصة، وهو ما تبناه القانون الفرنسي الصادر في 30 ديسمبر 1991، عند معاقبته لأفعال الاصطناع أو تزوير كروت الدفع أو السحب الإلكتروني، وهو نص خاص يجب إعماله تقييدا للنص العام. [3]

ويتم التلاعب بالنظام المعلوماتي للتوقيع الإلكتروني وغيرها من أنظمة المعلومات التي أفرزتها التعاملات المختلفة مع البنوك والهيئات والمؤسسات المالية من خلال شبكة المعلومات، عن طريق أساليب جديدة هي:

---

[1]– ايمن عبد الله فكري، مرجع سابق، ص 476.

[2]– احمد عاصم عجيلة، مرجع سابق، ص189.

[3]– شيماء عبد الغني محمد عطا الله، مرجع سابق ص 90.

- **التلاعب ببيانات إنشاء التوقيع الإلكتروني في مرحلة الإدخال المعلوماتي:**

ينصب نشاط الجاني في هذه المرحلة على المعلومات المدخلة إلى نظام التوقيع الإلكتروني والتي تتمثل في بيانات إنشاء التوقيع الإلكتروني[1]، دون إحداث تلاعب في البرنامج، مما يؤدي في النهاية إلى إخراج معلومات مزورة وغير مطابقة لحقيقة المعلومات الواجب تخزينها في منظومة إنشاء التوقيع الإلكتروني .

- **تزوير بيانات التوقيع الإلكتروني في مرحلة المعالجة المعلوماتية:**

خلافا لمرحلة الإدخال فان الجاني يُبقي على بيانات إنشاء التوقيع الإلكتروني كما هي من غير تغيير، ويقوم بالتدخل في برنامج المعالجة المتمثل في آلية إنشاء التوقيع الإلكتروني[2]، سواء بتعديل النتائج أو وضع برنامج جديد، مما يؤدي إلى تغيير حقيقة البيانات المطلوب إخراجها وفقا للبرنامج ببيانات أخرى غير مطابقة للحقيقة، ونكون في هذه الحالة أمام توقيع إلكتروني مزور وبالتالي شهادة تصديق إلكتروني مزورة .

- **التلاعب بتطبيقات التوقيع الإلكتروني المزور (إنتحال الشخصية في التعامل عبر النظم المعلوماتية).**

وتتمثل في قيام الجاني بنسبة التوقيع الإلكتروني إلى نفسه بعد تغيير حقيقة البيانات والمعلومات وصولا إلى تزوير هوية المستخدم الشرعي للتوقيع الإلكتروني (الموقع) [3]، وإجراء التصرفات المختلفة بإستخدام توقيع إلكتروني مزور، خاصة ما تعلق بالصفقات المالية المبرمة

---

[1]–عرف المشرع الجزائري بيانات إنشاء التوقيع الإلكتروني في الفقرة 3 من المادة 2 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين على أنه " بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني ".

[2]–عرف المشرع الجزائري آلية إنشاء التوقيع الإلكتروني في الفقرة 4 من المادة 2 من القانون 04/15 السالف الذكر على أنها " جهاز أو برنامج معلومات معد لتطبيق بيانات إنشاء التوقيع الإلكتروني".

[3]–الفقرة من المادة 2 من القانون 04/15 عرفت الموقع على انه" شخص طبيعي يحوز بيانات إنشاء توقيع إلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمتلكه".

وعمليات الدفع والتسويات المالية لصالح عملاء البنوك والمؤسسات المالية التي تستخدم شبكة المعلومات الدولية. [1]

كما توجد صور أخرى لتزوير التوقيع الإلكتروني وإستعماله في مختلف التطبيقات الحديثة، مثل انتحال المواقع الإلكترونية عبر شبكة المعلومات، وتزوير وسائل الدفع الإلكترونية (التحويل الإلكتروني للأموال).

ج. التوقيع الإلكتروني محل التزوير:

إعترف المشرع الجزائري بحجية التوقيع الإلكتروني في الإثبات وفق شروط حددتها في البداية المادة 323 مكرر من القانون المدني، وكذا القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، وقد سبق تفصيل ذلك بإسهاب في الفصل الأول، مما يمنح التوقيع الإلكتروني الحماية الجزائية اللازمة إذ ما تم تزويره.

- **الضرر:** لا يكفي لاكتمال الركن المادي لجرائم تزوير التوقيع الإلكتروني أن يقع تغيير الحقيقة في بيانات إنشائه، وأن يقع هذا التغيير بإحدى الطرق التي ينص عليها القانون، وإنما ينبغي حصول ضرر للغير وبإنعدامه تنعدم الجريمة. [2]

وقد إنقسم الفقه في تحليله للضرر إلى اتجاهين:

- **الاتجاه الأول:** ارتباط الضرر بمدى قابلية التوقيع الإلكتروني للإثبات أي نظرية الضرر القانوني.
- **الاتجاه الثاني:** أن يكون الضرر مبني على فكرة الضرر الفعلي بعيدا عن ربط التوقيع الإلكتروني بقانون الإثبات.

2. الركن المعنوي لجريمة تزوير التوقيع الإلكتروني

يتمثل الركن المعنوي في جريمة التزوير في القصد الجنائي الذي يرتبط أساسا بعنصري العلم والإرادة، أي أن تتوجه إرادة الجاني العمدية إلى ارتكاب الجريمة مع العلم بأركانها.

---

[1]–أيمن عبد الله فكري، مرجع سابق، ص450.

[2]–أيمن رمضان محمد احمد، مرجع سابق، ص212.

وفي جريمة تزوير التوقيع الإلكتروني يضاف القصد الجنائي الخاص، حيث لابد أن تتوافر لدى الجاني إرادة القيام بفعل التزوير، أي إنصراف إرادته إلى ارتكاب الفعل المادي المكون للجريمة مع علمه بذلك[1]، ولذلك فان عدم علم الجاني أنه يغير الحقيقة في بيانات التوقيع الإلكتروني أو شهادة التصديق الإلكتروني اللتان تتمتعان بالحماية القانونية ينفي القصد الجنائي لديه.[2]

وتعتبر صيغة النص الجنائي الفرنسي في تجريم التزوير من الصيغ الواضحة في تطلب القصد الخاص في جرائم التزوير، حيث أشار النص إلى ضرورة وقوع التزوير بنية الغش التي تؤثر في إثبات حق أو واقعة قانونية. [3]

المطلب الثاني:

جرائم التوقيع الإلكتروني في إطار القانون (15/04) المعدل والمتمم لقانون العقوبات الجزائري

إستحدث المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 15/2004 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ضمن القسم السابع مكرر، يحتوي على ثمانية مواد، من المادة 394 مكرر إلى المادة 394 مكرر7، المعدل والمتمم بالقانون 23/06 المؤرخ في 2006/12/20.

ويدخل التوقيع الإلكتروني بالنظر لآلية إنشاءه– المنصوص عليها في الفقرة الرابعة من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين والتي إعتبرها المشرع الجزائري جهاز أو برنامج معلوماتي معد لتطبيق بيانات فريدة كالرموز أو مفاتيح التشفير المستعملة من الموقع لإنشاء التوقيع – ضمن الأنظمة المعالجة آليا التي تشملها نصوص القانون 15/04 السالف الذكر:

وتشمل الإعتداءات الواقعة على التوقيع الإلكتروني بمفهوم هذا القانون في:

---

[1]– حفصي عباس، جرائم التزوير الإلكترونية، أطروحة دكتوراه، جامعة وهران، 2015، ص76.

[2]– عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني، دار الكتب القانونية، مصر 2007، ص249.

[3]–براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، جامعة بسكرة 2015، ص 226.

جرائم الدخول والبقاء غير المشروع على قاعدة بيانات التوقيع الإلكتروني، والجرائم المترتبة عن جريمة الدخول والبقاء غير المشروع. [1]

وعليه سيتم تفصيل ما سبق على النحو التالي:

- **الفرع الأول:** جريمة الدخول والبقاء غير المشروع على قاعدة بيانات التوقيع الإلكتروني
- **الفرع الثاني:** الجرائم المترتبة عن جريمة الدخول أو البقاء غير المشروع

الفرع الأول: جريمة الدخول أو البقاء غير المشروع على قاعدة بيانات التوقيعالإلكتروني

تعد أنشطة الدخول أو التوصل غير المصرح به من الأنشطة الإجرامية الأكثر انتشارا بين جرائم الاعتداء على التوقيع الإلكتروني[2]، وقد جرم المشرع الجزائري هذه الأفعال المستحدثة تحت مسمى: الدخول أو البقاء في منظومة معلوماتية (Introduction dans un système informatique)عن طريق الغش، بنص المادة 394 مكرر من قانون العقوبات[3]، التي تقابلها المادة 26 من مشروع قانون التجارة الإلكترونية المصري، التي تنص على انه: " مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن 3000 جنيه أو بإحدى هاتين العقوبتين، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو بقاعدة بيانات تتعلق بالتوقيعات الإلكترونية..."

وتتمثل الجريمة في دخول شخص نظام خاص بالمعلومات أو البقاء فيه بغرض الاطلاع على المعطيات والبيانات دون أن يكون لديه نية التغيير أو الحذف دون نية التملك. [4]

---

[1]– انظر في هذا الإطار: باطلي غنية، مرجع سابق، ص134

[2]– ياسر محمد الكومي، مرجع سابق، ص116.

[3]– المادة 394 مكرر " يعاقب بالحبس من ثلاثة أشهرإلى سنة بغرامة من 50000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير معطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50000دج إلى 300000دج."

[4]–نبيل صقر، الوسيط في جرائم الأموال، مرجع سابق، ص217.

ويقصد بنظام معالجة البيانات في نطاق التقنية النظام الذي يحوي المعلومات والبيانات المعالجة آليا داخل نظام الحاسب الآلي.

أولا: الركن المادي للجريمة:

يتشكل الركن المادي لجريمة الدخول أو البقاء غير المشروع على قاعدة بيانات التوقيع الإلكتروني من أفعال تأخذ صور الدخول غير المصرح به، وفعل البقاء بطريقة غير مشروعة.

1. الدخول غير المصرح به:

تفيد كلمة الدخول غير المصرح به في إطار المعلوماتية كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي، بما يحتويه من معلومات وبيانات مخزنة داخل نظام الحاسوب دون رضاء المسؤول عن هذا النظام أو المعلومات والسيطرة على هذه البيانات والخدمات التي يقدمها.

والمقصود بالدخول هو الفعل الذي ينطوي على نشاط ذهني يقوم به الفاعل في ذاكرة النظام المعلوماتي وليس نشاطا ماديا[1]، كما تفترض هذه الجريمة أن نظام المعلومات المتعلق بالتوقيع الإلكتروني والمتمثل في آلية إنشاء التوقيع الإلكتروني غير متاح للجمهور، وإنما يكون الإذن فيه مقصور على الهيئات والأشخاص المخولين قانونا الاطلاع على هذه البيانات، ونذكر هنا الموقع الحائز لبيانات إنشاء التوقيع الإلكتروني (الموقع الشرعي) [2]، وصاحب شهادة التصديق الإلكتروني، إلى جانب الجهات العامة التي لها الحق في مراقبة أجهزة الحاسب الآلي المتواجدة لدى الأفراد في إطار مكافحة الجرائم المعلوماتية .

[1]– احمد عاصم عجيلة، مرجع سابق، ص303.

[2]– ورد مصطلح الموقع الشرعي في نص المادة 11 فقرة 1/ج من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين بنصها على ضرورة ان تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

وأحاط المشرع الجزائري آلية إنشاء التوقيع الإلكتروني بمجموعة من متطلبات الأمن باستعمال الوسائل التقنية المناسبة ضمانا لسريتها وفق الاعتماد، وضرورة عرض أي تعديل على الموقع قبل عملية التوقيع. [1]

وفي نفس السياق إشترط المشرع الفرنسي توافر الوسائل التقنية لحماية النظام المعلوماتي للتحقق من وجود القصد الجنائي للجاني، فمن خلال تفسير المادة 1/323 من قانون العقوبات والخاصة بالولوج أو البقاء غير المشروع، يقتضي لتحقق هذا التجريم أن يكون النظام المعلوماتي متمتع بحماية أمنية وأن يتم اختراق هذه النظم بالفعل. [2]

ويلاحظ أن المشرع لم يشرط تحقق نتيجة معينة على أثر الدخول إلى آلية إنشاء التوقيع الإلكتروني التي تمثل قاعدة البيانات، أو إلى النظام المعلوماتي من قبل الجاني، وكل ما اشترطه أن يكون الدخول قد تم بطريق الغش أو التدليس. [3]

2. فعل البقاء بطريقة غير مشروعة:

نص قانون العقوبات الجزائري على صورة أخرى لحماية المعالجة الآلية للمعطيات، وهي صورة البقاء داخل النظام، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عند الدخول إلى هذا النظام وقد يجتمعان منذ البداية[4]، ويكون البقاء معاقبا عليه بمعزل عن فعل الدخول إلى النظام والذي يكون مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى آلية إنشاء التوقيع الإلكتروني بالصدفة أو عن طريق الخطأ أو السهو[5]، وهو ما يستوجب على المتدخل قطع وجوده وانسحابه فورا، فإذا بقي رغم ذلك فانه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي، وقد يجتمع الدخول

---

[1]–المزيد من التفاصيل حول آلية إنشاء التوقيع الإلكتروني المؤمنة 11 وآلية التحقق من التوقيع الإلكتروني الموصوف انظر المواد 11، 12، 13، 14 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2]–أيمن عبد الله فكري، مرجع سابق، ص263.

[3]– عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، مرجع سابق، ص297.

[4]– عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية 1999، ص52.

[5]– ياسر محمد الكومي، مرجع سابق، ص124.

غير المشروع والبقاء غير المشروع معا وذلك في الحالة التي لا يكون فيها الحق للجاني الدخول إلى النظام ويدخل إليه فعلا ضد إرادة صاحب النظام ثم يبقى داخل هذا النظام بعد ذلك، ويتحقق في هذه الحالة الاجتماع المادي للجرائم وفقا للقانون الفرنسي[1].

3. الصورة المشددة:

نصت كل من المادة 394 مكرر، والفقرة 02 من القانون 15/04 السالف الذكر، والمادة 1/323 والفقرة 02 من قانون العقوبات الفرنسي على هذه الجريمة انه: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"

وتشير الفقرة 03 انه: " إذا ترتب عن الأفعال المذكورة تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر (6) إلى سنتين (2) والغرامة من 50000دج إلى 150000دج.

يُستشف من ذلك انه إذا نتج عن فعل الدخول أو البقاء غير المشروع حذف أو تغيير معطيات النظام أو عدم صلاحية النظام لأداء وظائفه، فإنهما يُعتبران ظرفا مشددا تتضاعف العقوبة على أساسه.

ووجود هذا الظرف المشدد يستلزم وجود علاقة سببية بين فعل الدخول أو البقاء غير المشروع وتلك النتيجة الضارة، سواء محو أو تعديل المعطيات التي يحتويها النظام، والمقصود من ذلك حماية المشرع للنظام المعلوماتي[2].

ثانيا: الركن المعنوي

جريمة الدخول أو البقاء غير المشروع على قاعدة بيانات تتعلق بالتوقيع الإلكتروني جريمة عمدية يتعين لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة[3]، أي أن يعلم الجاني أن

---

[1]–مدحت رمضان، مرجع سابق، ص51 وما بعدها.

[2]– باطلي غنية، مرجع سابق، ص168.

[3]– لم يقتصر الأمر في بعض التشريعات على توافر القصد العام فقط بل هناك من التشريعات من تتطلب توافر القصد الخاص في جريمة الدخول غير المشروع للنظام المعلوماتي، ففي اسراليا مثلا يوجد نص خاص يشدد العقوبة على مرتكب فعل الدخول غير المشروع إلى نظام الحاسب الالي بنية الاضرار بالغير. انظر: أيمن عبد الله فكري، مرجع سابق، ص314.

دخوله أو بقاءه غير مشروع، وأن تتجه إرادته إلى ارتكاب هذه السلوك، ولا تحتاج لتترتب عنها نتيجة أو اثر خاص لتتحقق الجريمة حتى لو كانت بدافع الفضول أو اثبات المهارة في هذا المجال[1]، فإذا أثبت الجاني إنتقاء العلاقة السببية كأن يثبت أن تعديل أو محو البيانات المتعلقة بآلية إنشاء التوقيع الإلكتروني يرجع إلى قوة قاهرة أو لحادث عرضي إنتفى السلوك الإجرامي، وكذلك القصد الجنائي لدى الجاني.

الفرع الثاني: الجرائم المترتبة عن جريمة الدخول أو البقاء غير المشروع

وتتجسد في صورتين الأولى جرائم المساس العمدي بالمعطيات، والثانية جرائم التعامل في معطيات غير مشروعة.

أولا: جرائم المساس العمدي ببيانات التوقيع الإلكتروني

وهي ما تسمى أيضا بجرائم التلاعب بمعطيات أنظمة المعالجة الآلية للمعطيات، التي تطرقت إليها المواد 03، 04، 08 من الإتفاقية الدولية للإجرام المعلوماتي على النحو التالي: " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية من 50.000 إلى 4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

أما المشرع الفرنسي فقد نص عليها بعدما نص على جريمة إعاقة سير النظام وإفساده التي لم ينص عليها المشرع الجزائري لتشابهها مع جريمة الإعتداء العمدي على المعطيات من جهة، ومن جهة أخرى أن أفعال الإدخال أو الإزالة أو التعديل بطريق الغش لبيانات مخزنة داخل النظام المعلوماتي تؤدي حتما إلى إعاقة النظام عن أداء وظائفه[2]، وتنص المادة 3/323 من قانون العقوبات الفرنسي على عقاب كل من ادخل– بسوء نية– بيانات في نظام معالجة البيانات، أو قام – بسوء نية – بإلغاء أو تعديل هذه البيانات بالحبس مدة لا تزيد عن ثلاث سنوات والغرامة لا تزيد عن 300 ألف فرنك.

---

[1]– نسيمة جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة ماجستير، جامعة وهران، 2014، ص55–60.

[2]– باطلي غنية، مرجع سابق، ص172

1. الركن المادي:

يتحقق الركن المادي في هذه الجريمة بفعل الإعتداء على بيانات إنشاء التوقيع الإلكتروني ويتخذ إحدى الصورتين:

- **الصورة الأولى:** أن يتم محو البيانات والمعلومات الخاصة بالموقع الشرعي وتدميرها كليا.
- **الصورة الثانية:** أن يتم تشويه المعطيات أو آلية إنشاء التوقيع الإلكتروني عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل انتقالها. [1]

أي أن الركن المادي لجنحة المساس بالمعطيات أو التلاعب بها فيما يتعلق بالتوقيع الإلكتروني يتحقق بإتيان الجاني لفعل من الصور التالية:

أ. إدخال معلومات وهمية:

ويكون التدخل في بيانات آلية التوقيع الإلكتروني بإدخال معطيات وهمية إلى آلية بيانات التوقيع الإلكتروني لم تكن موجودة من قبل، أو بقصد التشويش على صحة البيانات القائمة.

ب. المحو أو الإزالة أو التعديل (إدخال معلومات مزورة):

ويتم ذلك إما عن طريق إستبدال المعطيات، أو عن طريق المحو أو الإزالة أو التغيير الذي يقع على بيانات إنشاء التوقيع الإلكتروني، أي بإضافة بيانات غير صحيحة أو تغيير محتواها، أو قد يتم إصطناع بيانات ليس لها وجود ونسبتها إلى غير مصدرها[2]، أو أن يلجأ الجاني إلى إحدى طرق التزوير المعنوي لاقتراف جريمته، بإدخال بيانات لم تصدر عن المتعاقدين، أو إغفال معلومات أو إيرادها على وجه غير صحيح، مما يضعنا أمام تحريف حقيقة بيانات التوقيع الإلكتروني.

---

[1]–نبيل صقر، مرجع سابق، ص226

[2]– محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2011، ص 232، ص234، ص233.

ثانيا: الركن المعنوي

تُشكل مختلف الإعتداءات التي تطال آلية إنشاء التوقيع الإلكتروني بإحدى الصور سالفة الذكر جرائم مقصودة، سواءً بصورتها المادية التقليدية أو بصورتها المعنوية المستحدثة، مما يحقق القصد الجنائي الذي يقوم على عنصري العلم والإرادة، بغض النظر عن طبيعة وماهية السلوك أو حجم الضرر الناتج عنه. [1]

[1]–أسامة احمد المناعسة، جلال محمد الزعبي، مرجع سابق، ص 133.

المبحث الثاني:

جرائم الإعتداء على التوقيع الإلكتروني في إطار القانون 04/15، وبعض النصوص الخاصة

أورد المشرع الجزائري نصا خاصا بالعقوبات على الأفعال الإجرامية التي تنال من التوقيع الإلكتروني وكذا شهادة التصديق الإلكتروني في القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، وهي خطوة هامة واكبت التطور التكنولوجي في مجال تقنية المعلومات ووسائل الإتصال، وقد أشار المشرع إلى صور الإعتداء على التوقيع الإلكتروني وشهادة التصديق الإلكتروني في الفصل الثاني من القانون، بعنوان الأحكام الجزائية، إلى جانب الباب الرابع، الفصل الخامس من القانون 03/15 المتعلق بعصرنة العدالة، وهو ما سيتم تفصيلة على النحو التالي:

- **المطلب الأول:** الجرائم المتعلقة بتداول بيانات التوقيع الإلكتروني
- **المطلب الثاني:** جرائم التعامل غير المشروع في نشاط التصديق الإلكتروني

المطلب الأول:

الجرائم المتعلقة بتداول بيانات التوقيع الإلكتروني

نص المشرع الجزائري في القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني على تجريم الإعتداءات المختلفة الماسة بتداول بيانات التوقيع الإلكتروني وكذا شهادة التصديق الإلكتروني في المواد 68، 73، 74 والمواد 17، 18 من القانون 03/15 التعلق بعصرنة العدالة، وذلك على النحو التالي:

- **الفرع الأول:** جرائم إنتهاك سرية وخصوصية البيانات
- **الفرع الثاني:** جرائم الحصول بطريق الغش على شهادة تصديق إلكتروني

الفرع الأول: جرائم انتهاك سرية وخصوصية البيانات

عمد المشرع الجزائري إلى تبني التشفير كوسيلة لتأمين سرية التوقيع الإلكتروني ضمانا لسلامة عملية تداول المعلومات الخاصة بإتمام المعاملات والصفقات، وهو ما يتضح من نص المادة الثانية في فقرتها الثامنة والتاسعة من القانون 04/15، من خلال النص على آليتي مفتاح التشفير الخاص

ومفتاح التشفير العمومي، وأعطى تعريفا لكل منهما وأخضعها لضوابط تقنية وإجرائية عند إستخدامه.[1]

وحماية نظام المعلومات يعتمد أساسا على عوامل السرية، وتعني عدم علم غير المتعاقدين ببيانات العملية التعاقدية، بينما تنفي الخصوصية إرتباط هذه البيانات بالمتعاقدين أطراف العملية، مما يحتم عدم إطلاع الغير عليها، إلى جانب حرية تداول البيانات وإتاحتها، ثم سلامة البيانات. [2]

وفي هذا الصدد جرم المشرع كل سلوك يؤدي إلى كشف معلومات سرية تتعلق ببيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني، أو حيازتها أو إفشائها واستعمالها سواء من الغير أو المكلف بالتدقيق[3]، أو للاستعمال غير المشروع للعناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر.

أولا: جرائم إفشاء سرية بيانات التوقيع الإلكتروني وآلية إنشاءه

نصت المادة 68 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين على أنه " يعاقب بالحبس من (3) ثلاثة أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1000000دج) إلى خمسة ملايين دينار (5000000دج) أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.

كما نصت المادة 73 من القانون سالف الذكر أنه " يعاقب بالحبس من (3) ثلاث أشهر إلى (2) سنتين وبغرامة من عشرين ألف دينار (20000دج) إلى مائتي ألف دينار (200000دج) أو بإحدى هاتين العقوبتين فقط كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق".[4]

---

[1]– بلحسين حمزة، مرجع سابق، ص75، ص 77.

[2]– ايمن رمضان محمد احمد، مرجع سابق، ص139.

[3]– حيث عرف المشرع الجزائري التدقيق في المادة الثانية، الفقرة 10 من القانون 04/15 " التحقق من مدى المطابقة وفقا لمرجعية ما"

[4]– تقابلها المادة 28 من قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 01 لسنة 2006، نصت على انه " يعاقب بالحبس لمدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن عشرين ألفا ولا تزيد عن مائتي ألف درهم أو بإحدى هاتين العقوبتين كل شخص تمكن بموجب أي سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو

1. الركن المادي للجريمة:

يتمثل النشاط المادي في جريمة إنتهاك سرية بيانات التوقيع الإلكتروني في فعل الدخول غير المشروع من قبل الجاني لآلية إنشاء التوقيع الإلكتروني المشمول بالحماية دون أن يكون مأذونا له بذلك، ولا تتطلب الجريمة صفة خاصة في فاعلها، إذ ترتكب من أي شخص سواء توفرت له صفة الصلة الوظيفية في مجال أنظمة المعالجة الإلكترونية أم لم تتوفر، كما تقع الجريمة بأية وسيلة من وسائل الدخول سواء باستعمال أجهزة خاصة تمكن الجاني من كسر شفرة البرنامج المعلوماتي أو بإستخدام الشفرة الصحيحة لشخص آخر مأذون له بالدخول، حيث أن هذا الإذن بالإطلاع غير متاح للجمهور، وإنما يقتصر على عدد محدد من الأشخاص وهو ما يكون الركن المفترض للجريمة. [1]

كما تفترض الجريمة حسب نص المادة 60 من القانون 04/15 أن يكون التوقيع الإلكتروني محل الحماية موصوفا خاصا بالغير. [2]

هذا بالإضافة إلى أفعال الحيازة والاستعمال لبيانات التوقيع الإلكتروني الموصوف الخاص بالغير، والتي تشكل نشاط مادي مجرم بنص المادة السابقة، إلى جانب الاستعمال غير المشروع للعناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع إلكتروني آخر. [3]

مستندات أو مرفقات إلكترونية أو أفشى أيا من هذه المعلومات " . وكذا نص المادة 22 من قانون تقنية المعلومات الإماراتي رقم 05 لسنة 2012 بأنه " يعاقب بالحبس لمدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استخدم بدون تصريح أي تقنية معلوماتية أو موقعا إلكترونيا أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه"، كما تقابلها المواد 21، 23 من القانون المصري بشأن التوقيع الإلكتروني لسنة 2004، والمادة 52-10 من قانون المعاملات الإلكترونية العماني رقم 2008/69.

[1]- احمد عاصم عجيلة، مرجع سابق، ص330، ص331.

[2]- انظر المادة 07 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.

[3]- حيث نصت المادة 17 من القانون 03/15 المتعلق بعصرنة العدالة على انه " يعاقب بالحبس من سنة إلى خمس (5) سنوات وبغرامة تتراوح بين 100000دج إلى 500000دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع إلكتروني اخر".

كما عاقب المشرع الجزائري بنص المادة 73 من القانون 04/15 انتهاك سرية المعلومات الخاصة بالتوقيع الإلكتروني من قبل المكلف بالتدقيق أثناء قيامة بهذه الوظيفة واطلاعه على هذه المعلومات.

أ. حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير

نصت على هذه الجريمة المادة 68 من القانون 04/15 ويتكون الركن المادي لهذه الجريمة من ثلاث صور هي:

- حيازة بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير
- إفشاء بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير
- استعمال بيانات إنشاء توقيع إلكتروني خاصة بالغير

ويتمثل السلوك الإجرامي في الصورة الأولى حينما يتحصل الجاني على بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير بطريقة غير مشروعة، ويمكن الإستيلاء على هذه المعلومات عن طريق النصب المعلوماتي أو خيانة الأمانة. [1]

وتتمثل الصورة الثانية في فعل الإفشاء العمدي لبيانات إنشاء توقيع إلكتروني خاصة بالغير، أي وضع هذه البيانات في متناول أي شخص يحتمل أن يعتمد عليها لتحقيق أغراض احتيالية، أو أي غرض غير مشروع[2]، في الوقت الذي يفترض أن يكون الإطلاع على هذه البيانات قاصر على أصحابها أو الأشخاص المؤتمنين عليها بحكم وظيفتهم، وهم في هذه الجريمة مؤدي خدمات التصديق الإلكتروني، أو الطرف الثالث الموثوق.

[1]– عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة 2002، ص321.

[2]– محمد امين الخرشة، نائف عبد الجليل الحمايدة، الحماية الجنائية للتوقيع الإلكتروني في التشريعيين الاماراتي والبحريني " دراسة مقارنة "، مجلة جامعة الأزهر غزة، سلسلة العلوم الإنسانية 2014، المجلد 16، العد الأول، ص342.

أما الصورة الثالثة فهي الإستعمال غير المشرع لبيانات إنشاء توقيع إلكتروني خاصة بالغير، ويرتكز الاستعمال غير المشروع بصورة رئيسية على الخدمات التي يؤديها التوقيع الإلكتروني في مجال الحكومة الإلكترونية، أو التجارة الإلكترونية، أو مختلف التعاقدات الأخرى. [1]

ب. كشف معلومات سرية من قبل المكلف بالتدقيق

ورد النص على هذه الجريمة كما سبق بيانه في المادة 73 من القانون 04/15، ويظهر السلوك الإجرامي في قيام المكلف بالتدقيق أثناء تأديته لمهامه– المتمثلة في مطابقة إنشاء التوقيع الإلكتروني على إثر التحقق من التوقيع الإلكتروني وفقا لمرجعية ما حسب نص المادة نفسها– بكشف معلومات سرية إطلع عليها خلال هذه العملية.

ونظرا لسهولة ارتكاب هذه الجريمة من قبل المؤتمن على تلك البيانات فإن المشرع الجزائري قد حدد العقوبة بالنظر إلى الخطورة البالغة لجرائم إفشاء السر المهني.

ثانيا: جرائم إفشاء سرية بيانات شهادة التصديق الإلكتروني

أحاط المشرع الجزائري البيانات والمعلومات المحتوات في شهادة التصديق الإلكتروني الممنوحة، بالحماية القانونية وأخضعها للموافقة الصريحة والقبلية للمعني، كونها تتعلق ببيانات شخصية تتصف بالسرية، وذلك حسب نص المادتين 42 و43 من القانون 04/15. [2]

وجرمت المادة 75 من القانون ذاته كل إخلال بالسرية المطلوبة يقوم به مؤدي خدمات التصديق الإلكتروني أثناء جمعه للبيانات الشخصية المتعلقة بشهادة التصديق الإلكتروني، حيث نصت على أنه: " يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مائتي ألف

[1]– عبد الجبار الحفيص، الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول 2011، ص191.

[2]– تنص المادة 42: يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.

وتنص المادة 43: لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة.

دينار (200.000دج) إلى مليون دينار (1.000.000 دج) أو إحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون".

كما عاقبت المادة 71 من نفس القانون مؤدي خدمات التصديق الإلكتروني عند إخلاله بأحكام المادة 43، التي تفرض الموافقة الصريحة لصاحب شهادة التصديق الإلكتروني قبل جمع بياناته الشخصية الضرورية، ومنعت أي تلاعب بها أو إستعمالها في غير الأغراض الممنوحة لأجلها.

1. الركن المادي:

يتحقق الركن المادي للجريمة بمجرد إنتهاك سرية البيانات وخصوصيتها حتى ولو لم يترتب عن الفعل أي نتيجة، لأن الجريمة سلوكية، إكتفى المشرع فيها بتحقق السلوك الإجرامي دون تحقيق النتيجة، وغايته في ذلك تحقق الغرض من التجريم وهو الحفاظ على سرية وخصوصية البيانات الشخصية.

كما يتحقق الركن المادي بنص المادة، 71 في فعل الإهمال العمدي لطلب الموافقة الصريحة لصاحب شهادة التصديق الإلكتروني من قبل مؤدي خدمات التصديق الإلكتروني عند جمعه للبيانات الشخصية الضرورية لمنح الشهادة، وكذا فعل التلاعب العمدي بهذه البيانات، بإستعمالها في أغراض غير مشروعة.

وعليه يمكن إدراج جريمة الكشف عن البيانات الشخصية المتعلقة سواء بالتوقيع الإلكتروني أو بشهادة التصديق الإلكتروني من قبل مؤدي خدمات التصديق الإلكتروني أو المكلف بالتدقيق مع جريمة الكشف عن الأسرار المهنية المنصوص عليها في المواد من 311 إلى 303 قانون العقوبات الجزائري، من حيث أنها تشترك في عنصر الكشف عن المعلومات السرية من طرف أشخاص تحصلوا عليها بمناسبة تأديتهم لمهامهم أو وظائفهم.

2. الركن المعنوي:

جرائم إفشاء سرية بيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصريه العلم والإرادة، فالجاني في هذه الجرائم هو المكلف بالتدقيق الذي يكشف المعلومات السرية التي قام بالاطلاع عليها أثناء قيامه بالتدقيق، وكذا مؤدي

خدمات التصديق الإلكتروني الذي يخل بواجب السرية أثناء جمعه للبيانات الشخصية لصاحب شهادة التصديق الإلكتروني مع علمهما(المكلف بالتدقيق ومؤدي خدمات التصديق الالكتروني) بأنها أفعال محظورة ومعاقب عليها قانونا وأن تتجه إرادة كل منهما لإقتراف الفعل المجرم. [1]

ومتى تمت جريمة الإفشاء بركنيها المادي والمعنوي وجب إنزال العقوبة على الجاني دون نظر للباعث الذي دفعه لذلك، ويستوي أن يكون هذا الإفشاء قد نتج عنه وقوع ضرر بالمجني عليه من عدمه، ذلك أن هذه الجرائم تنتمي إلى جرائم الخطر لا الضرر.

3. العقوبة:

قرر المشرع الجزائري عقوبة الحبس والغرامة أو بإحدى هاتين العقوبتين على جريمة إفشاء بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير بنص المادة 68 من القانون 04/15 " الحبس من (3) ثلاثة أشهر إلى (3) ثلاث سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين (5.000.000دج) أو بإحدى هاتين العقوبتين فقط".

كما عاقبت المادة 73 من نفس القانون المكلف بالتدقيق بالحبس من (3) ثلاثة أشهر إلى (2) سنتين وبغرامة مالية من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين.

وعاقبت المادة 70 من القانون 04/15 مؤدي خدمات التصديق الإلكتروني على جريمة الإفشاء بالحبس من (3) أشهر إلى (2) سنتين وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار(1.000.000دج) أو بإحدى هاتين العقوبتين.

وفي هذا السياق عاقبت المادة 71 من القانون 04/15 مؤدي خدمات التصديق الإلكتروني عند اخلاله بأحكام المادة 43 من نفس القانون بالحبس من (6) ستة أشهر إلى (3) ثلاث سنوات وبغرامة مالية من مائتي ألف دينار (200.000دج) إلى مليون دينار(1.000.000دج) أو بإحدى هاتين العقوبتين فقط.

[1]– بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، أطروحة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، 208، ص148.

ويعاقب الشخص المعنوي بنص المادة 75 من نفس القانون الذي ارتكب إحدى الجرائم المنصوص عليها سابقا بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

الفرع الثاني: جرائم إساءة استخدام شهادة التصديق الإلكتروني:

تعتبر شهادة التصديق الإلكتروني حلقة وصل بين بيانات التوقيع الإلكتروني– بعد مرور هذه الاخيرة بآلية التحقق– والشخص الطبيعي الحائز لهذه البيانات، والتي تمكنه من التصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله. [1]

ويقع الإضرار بشهادة التصديق الإلكتروني، عند إعطاء بيانات غير صحيحة لغرض احتيالي أو أي غرض غير مشروع، كما نص عليه المشرع الجزائري في القانون 04/15 من خلال المواد 66 و74 التي جرمت أفعال التصريح الكاذب للحصول على شهادة التصديق الإلكتروني الموصوفة، وكذا إستعمال الشهادة لأغراض غير مشروعة.

أولاً: جريمة الإدلاء بإقرارات كاذبة:

يتحقق السلوك الإجرامي في هذه الجريمة بالإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة، حيث نصت المادة 66 من القانون 04/15، على أنه: "يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من عشرين ألف دينار (20.000دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة".

1. الركن المادي:

يتخذ الركن المادي لهذه الجريمة صورة وحيدة هي إعطاء بيانات متعارضة مع الحقيقة لمؤدي خدمات التصديق الإلكتروني من أجل الحصول على شهادة تصديق إلكتروني موصوفة.

ويجب أن تكون الغاية من الشهادة أو البيانات الكاذبة هو إستخدامها في غرض إحتيالي أو أي غير مشروع أي هدفها خداع المجني عليه.

[1]– راجع الفقرات الثانية، الخامسة، السادسة، السابعة من المادة الثانية (2) من القانون 04/15 السالف الذكر.

وفي هذا السياق لم يكتف المشرع الإماراتي بتجريم التصريح الكاذب مثلما فعل المشرع الجزائري، وإنما مد نطاق التجريم إلى تقديم بيانات ومعطيات خاطئة عن الهوية بغرض طلب استصدار أو إلغاء أو ايقاف شهادة التصديق الإلكتروني، حيث نصت المادة 40 من قانون المعاملات والتجارة الإلكترونية على انه:" مع عدم الإخلال بأية عقوبة اشد ينص عليها أي قانون آخر، يعاقب كل من قدم متعمدا بيانات غير صحيحة عن هويته أو تفويضه إلى مزود خدمات التصديق بغرض طلب إستصدار أو إلغاء أو ايقاف شهادة، بالحبس لمدة لا تزيد عن ستة أشهر وبغرامة لا تتجاوز 100000 درهم أو بإحدى هاتين العقوبتين". [1]

2. الركن المعنوي:

جريمة الإدلاء بإقرارات كاذبة من الجرائم العمدية، يتحقق الركن المعنوي فيها بتوافر القصد العام بعنصريه وهما العلم والإرادة، بأن يعلم الجاني أن شهادة التصديق الإلكتروني غير صحيحة، وأن البيانات التي سلمها لمؤدي خدمات التصديق الإلكتروني غير صادقة، ومع ذلك تنصرف إرادته إلى الحصول غير المشروع عليها، وبالتالي قبوله بالنتائج المترتبة عن فعله الاحتيالي.

كما لا تتطلب الجريمة قصداً جنائياً خاصا حيث لا يتصور وجود باعث معين من ارتكابها سواء أكان فعل الإدلاء بالإقرارات الكاذبة لمؤدي خدمات التصديق الإلكتروني عبثيا أو بصفة جدية، وكانت الغاية الحصول على شهادة تصديق إلكتروني موصوفة.

3. العقوبة:

عاقب المشرع الجزائري على جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة بنص المادة 66 من القانون 04/15 بعقوبة الحبس والغرامة، أو بإحدى هاتين

---

[1]– قانون رقم (2) سنة 2002 بشأن المعاملات والتجارة الإلكترونية (صدر في تاريخ 12 فيفري 2002)، انظر عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، نظام التجارة الإلكترونية وحمايتها مدنيا (2005)، ص520 وص522.

– وفي نفس الاتجاه جرم المشرع التونسي هذه الافعال تحت عنوان جريمة التصريح عمدا بمعطيات خاطئة بنص المادة 47 من القانون المتعلق بالمبادلات والتجارة الإلكترونية بانه: " يعاقب كل من صرح بمعطيات خاطئة لمورد خدمات التوثيق الإلكتروني لكافة الأطراف التي طلب منها ان تثق بإمضائه للسجن لفترة تتراوح بين ستة اشهر وعامين، وبغرامة تتراوح من 1000 إلى 10.000 دينار أو باحدى هاتين العقوبتين.

العقوبتين، هادفا من وراء ذلك الحفاظ على الثقة المطلوبة في جميع المعاملات الإلكترونية وحماية حقوق المتعاملين خاصة ما تعلق بالتجارة الإلكترونية وباقي المعاملات المدنية الأخرى، وإنطلاقا من ذلك كانت العقوبات على الشكل الآتي:

- عقوبة أصلية تتمثل في الحبس من (3) ثلاثة أشهر إلى (3) ثلاث سنوات، وبغرامة مالية تتراوح من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار (200.000دج)، أو بإحدى هاتين العقوبتين فقط.
- يعاقب الشخص المعنوي في هذه الجريمة طبقا لنص المادة 75 من القانون 04/15 بغرامة تعادل (5) مرات الحد الأقصى للغرامة النصوص عليها بالنسبة للشخص الطبيعي، أي انه يعاقب بغرامة مالية تقدر بمليون دينار جزائري (1.000.000دج)

ثانيا: جريمة الإستخدام غير المشروع لشهادة التصديق الإلكتروني

تعد جريمة الإستعمال غير المشروع لشهادة التصديق الإلكتروني الموصوفة المنصوص عليها بموجب المادة 74 من القانون 04/15 من بين الإعتداءات التي تقع على التوقيع الإلكتروني من قبل صاحب التوقيع نفسه، على خلاف المادة 71 من نفس القانون خاصة، وباقي الجرائم الواردة بنفس القانون عامة. [1]

وتنص المادة 74 على انه: " يعاقب بغرامة مالية من ألفي دينار (2000دج) إلى مائتي ألف دينار (200.000دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها".

1. الركن المادي:

يتحقق الركن المادي للجريمة عن طريق استعمال صاحب التوقيع الإلكتروني لشهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من اجلها. وبالرجوع لأحكام المادة 15 من القانون 04/15 السالف الذكر[2]، والتي توضح المتطلبات الضرورية المتوفرة في شهادة تصديق إلكتروني موصوفة، يمكن تكييف أفعال الإساءة من قبل الموقع على الشكل الآتي بيانه:

[1]– راجع في هذا الصدد جرائم افشاء سرية بيانات شهادة التصديق الإلكتروني فيما سبق، صفحة 105 وما بعدها.

[2]–راجع المادة 15 من القانون 04/15 السالف الذكر.

أ. **إستعمال شهادة تصديق إلكتروني موصوفة من قبل شخص غير ذي صفة خاصة أو من قبل الغير:** ويقصد بالغير أو غير ذي صفة من لم تمنح شهادة التصديق الإلكتروني الموصوفة بإسمه دون سواه أو بالإسم المستعار الذي يسمح بتحديد هويته، ويتحقق الإستخدام غير المشروع من قبل الغير لشهادة التصديق الإلكتروني الموصوفة باحدى الطرق الاتية:

- إستخدام شهادة تصديق إلكتروني موصوفة مسروقة أو مفقودة، وهي الحالة التي يتم فيها سرقة الشهادة من مالكها الأصلي أو العثور عليها في حال فقدها، ويتعين في هذه الحالة على صاحب شهادة التصديق الإلكتروني إخطار الجهة المصدرة لهافي حالة الضياع أو عند سرقة مفتاح التشفير الخاص التي يحوزها الموقع.
- تزوير شهادة تصديق إلكتروني موصوفة: أي بتغيير الحقيقة سواء في بيانات إنشاء التوقيع الإلكتروني أو بيانات التحقق من التوقيع الإلكتروني، وهو ما يؤدي إلى قيام الركن المادي لجرائم الدخول أو البقاء غير المشروع على قاعدة بيانات التوقيع الإلكتروني والجرائم المترتبة عن هذه الجريمة.

ب. **استعمال شهادة تصديق إلكتروني موصوفة بعد انتهاء مدة صلاحيتها:** تعتبر العلاقة بين مؤدي خدمات التصديق الإلكتروني وصاحب الشهادة علاقة عقدية، تنقضي بإنتهاء المدة المتفق عليها، إلا أن صاحب الشهادة قد يحتفظ بها لاستخدامها رغم إنتهاء صلاحيتها .

ج. **إستعمال شهادة تصديق إلكتروني موصوفة خارج الحدود الممنوحة من أجلها:** ويتحقق هذا الفعل غير المشروع في حالة تعسف صاحب شهادة التصديق الإلكتروني الموصوفة في إستعمال الشهادة، وعدم إحترامه لبنود العقد المبرم بينه وبين مؤدي خدمات التصديق الإلكتروني، خاصة فيما تعلق بالنشاطات المسموح التعامل بها عن طريق الشهادة الممنوحة.

د. **إستعمال شهادة تصديق إلكتروني خارج حدود قيمة المعاملات التي تستعمل من أجلها:** ويتحقق ذلك عند تجاوز صاحب شهادة التصديق الإلكتروني الموصوفة لقيمة المعاملات التي تم ذكرها أثناء إصدار الشهادة.

2. الركن المعنوي:

يلزم لقيام هذه الجريمة توافر الركن المعنوي في حق الفاعل أي القصد الجنائي، بعنصريه العلم والإرادة، وذلك بأن يعلم الجاني أنه يستعمل شهادة تصديق إلكتروني موصوفة بصفة غير مشروعة، من خلال إستعمالها لغير الأغراض التي منحت من اجلها، ومع ذلك تتجه إرادته إلى هذا

السلوك الإجرامي، فالجريمة عمدية ولا مجال لقيامها عن طريق الخطأ غير العمدي، ولا يشترط لقيام القصد الجنائي أي باعث دفع إلى إساءة إستخدام شهادة تصديق إلكتروني موصوفة.

3. العقوبة:

مقارنة بباقي الجرائم، عاقب المشرع الجزائري على جريمة إساءة إستخدام شهادة تصديق إلكتروني موصوفة ماليا دون اللجوء إلى عقوبة سالبة للحرية، حيث نصت المادة 74 من القانون 04/15 عل عقوبة الغرامة التي تتراوح بين ألفي دينار جزائري (2000دج) إلى مائتي ألف دينار (200.000دج) إذا كان الجاني شخصا طبيعيا، أما إذا كان شخصا معنويا فإنه يقع تحت طائلة المادة 75 من القانون السالف الذكر، حيث يعاقب بغرامة تعادل (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وتتمثل في مليون دينار جزائري (1000.000دج).

المطلب الثاني:

جرائم مؤدي خدمات التصديق الإلكتروني:

باستقراء نصي المادتين11و12 من القانون 04/15 السالف الذكر فإن المشرع الجزائري قسم مزودي خدمات التصديق الإلكتروني إلى نوعين[1]: الأول هو الطرف الثالث الموثوق حسب المادة 11، وتوكل له مهمة منح شهادات التصديق الإلكتروني الموصوفة وخدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المنخرطين في الفرع الحكومي، أما الفئة الثانية حسب المادة 12 فإنها قد تكون شخص طبيعي أو معنوي توكل له نفس المهام في إطار التصديق الإلكتروني، تقوم في حقهم مجموعة من الالتزامات القانونية، من شأن كل مخالفة لها ترتيب مسؤولية جزائية قد تأتي في صورة جرائم وردت على سبيل الحصر في القانون 04/15، وهي جريمة التقاعس عن إعلام السلطة بوقف نشاط التصديق الإلكتروني، وجريمة الإخلال بإلتزام تحديد هوية صاحب شهادة التصديق الإلكتروني، وجريمة مباشرة خدمات التصديق الإلكتروني دون الحصول على رخصة.

[1]– مع صدور القانون 05/18، المتعلق بالتجارة الإلكترونية وبنص المادة (06) في فقرتها الرابعة اصبح التعريف شاملا على النحو التالي: " المزود الإلكتروني: كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توزيع السلع أو الخدمات عن طريق الاتصالات الإلكترونية."

الفرع الأول: جريمة التقاعس عن إعلام السلطة بوقف نشاط التصديق الإلكتروني

ألزم المشرع الجزائري في المادة 67 من القانون 04/15 جهات التصديق الإلكتروني أو المورد الإلكتروني بضرورة إعلام السلطة الاقتصادية بالتوقف عن نشاط التصديق الإلكتروني في الآجال المحددة في المادتين 58 و59 من نفس القانون. [1]

وتنص المادة 67 على انه: " يعاقب بالحبس من شهرين إلى سنة واحدة وبغرامة من مائتي الف دينار (200000دج) إلى مليون دينار (1000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون".

أولا: الركن المادي:

يتحقق السلوك المادي في هذه الجريمة بتوقف مؤدي خدمات التصديق الإلكتروني والمرخص لهم من الهيئة الاقتصادية للتصديق الإلكتروني، [2]عن نشاط التصديق الإلكتروني دون إعلام هذه الهيئة في الآجال المحددة في سياسة التصديق للسلطة الإقتصادية، والمتعلقة باستمرارية الخدمة بحسب نص المادة 58 من القانون 04/15، والمادة 59 من نفس القانون، فقد ألزمت مؤدي خدمات

---

[1]–تنص المادة 58 من القانون 04/15 السالف ذكره على أنه: " يجب على مؤدي خدمات التصديق الإلكتروني، اعلام السلطة الاقتصادية للتصديق الإلكتروني، في الاجال المحددة في سياسة التصديق لهذه السلطة، برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني أو بأي فعل قد يؤدي إلى ذلك.

وفي هذه الحالة، يلتزم مؤدي خدمات التصديق الإلكتروني بأحكام سياسة التصديق الإلكتروني المتعلقة باستمرارية الخدمة.

يترتب عن وقف النشاط سحب الترخيص".

كما تنص المادة 59 من نفس القانون على انه: " يجب على مؤدي خدمات التصديق الإلكتروني الذي يوقف نشاطه لأسباب خارجة عن ارادته ان يعلم السلطة الاقتصادية للتصديق الإلكتروني بذلك فورا، وتقوم هذه الاخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة بعد تقدير الاسباب المقدمة.

وفي هذه الحالة، يتخذ مؤدي الخدمات التدابير اللازمة، والمنصوص عليها في سياسة التصديق الإلكتروني للسلطة الاقتصادية، من اجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة "

[2]–انظر المادة 29 وما بعدها من القانون 04/15 السالف الذكر.

انظر في ما يخص نظام الترخيص لتأدية نشاط التصديق الإلكتروني في المادة 33 وما بعدها من القانون 04/15.

التصديق الإلكتروني بإعلام السلطة الإقتصادية بالتوقف عن النشاط فورا إذا كان التوقف راجع إلى أسباب خارجة عن إرادته.

وتبلغ مدة الترخيص الممنوح لمؤدي خدمات التصديق الإلكتروني خمس سنوات قابلة للتجديد بحسب المادة 40 من القانون 15/، 04 وبالتتالي فإن أي توقف عن النشاط قبل انتهاء هذه المدة القانونية سواء لأسباب إرادية أو غير إرادية من قبل مؤدي خدمات التصديق الإلكتروني دون إعلام السلطة الاقتصادية للتصديق الإلكتروني تضعهم تحت المسؤولية الجزائية، والغرض من ذلك المواءمة بين ما تستوجبه المعاملات التجارية الإلكترونية من سرعة، وما يجب أن تتمتع به شهادات التصديق الإلكتروني الممنوحة والضرورية للتحقق من صفة الموقع وإستمرارية أداء هذه الخدمة بثقة وأمان.

ثانيا: الركن المعنوي

جريمة التقاعس عن إعلام السلطة الاقتصادية للتصديق الإلكتروني بوقف نشاط التصديق الإلكتروني من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام بعنصريه: العلم والإرادة، فيجب أن يكون الجاني وهو مؤدي خدمات التصديق الإلكتروني عالما بإخلاله بالتزام إعلام السلطة الاقتصادية بوقف نشاطه في الاجال المحددة في المادتين 58 و59 من القانون 15/، 04 وإتجاه إرادته عن وعي وإدراك إلى هذا السلوك، ولا عبرة في قيام الجريمة بالباعث الذي دفع الجاني إلى الاخلال بهذا الالتزام.

ثالثا: العقوبة

عاقبت المادة 67 من القانون 04/15 على جريمة التقاعس عن إعلام السلطة الاقتصادية للتصديق الإلكتروني بوقف نشاط التصديق الإلكتروني بالحبس من شهرين (2) إلى سنة واحدة (1) وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1000.000دج) أو باحدى هاتين العقوبتين فقط، هذا في حالة ما إذا كان الجاني شخصا طبيعيا، أما في حالة الشخص المعنوي فيعاقب بغرامة تعادل خمس مرات الحد الاقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي بنص المادة 75 من ذات القانون أي بغرامة قدرها خمسة ملايين دينار (5000.000دج).

الفرع الثاني: جريمة الاخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني

بالرجوع إلى أحكام المادة 44 من القانون 04/15 السالف ذكره، [1]يتبين أن المشرع الجزائري أخضع عملية منح شهادة التصديق الإلكتروني إلى إلزامية التحقق من هوية طالبها، سواء كان شخصا طبيعيا أو معنويا، وعند الاقتضاء التحقق أيضا من صفاته الخاصة، وأن أي إخلال بهذا الالتزام يترتب عنه المسؤولية الجزائية طبقا لأحكام المادة 69 من نفس القانون والتي تنص على انه: " يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من عشرين ألف (20.000دج) إلى مائتي ألف دينار (200.000دج) أو بإحدى هاتين العقوبتين فقط كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة".

وتقوم الجريمة على ركنيين أساسيين مادي، ومعنوي، على النحو الاتي:

أولا: الركن المادي

يتمثل الركن المادي في جريمة إخلال مؤدي خدمات التصديق الإلكتروني بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة، حسب الفقرة الثانية من المادة 44 من القانون 04/15.

وكما سبق تبيانه، فقد يكون صاحب شهادة التصديق الإلكتروني شخصا طبيعيا أو معنويا، كما نصت عليه المادة 14 من القانون نفسه، لذلك فان تحديد الهوية يأخذ صورتين: الأولى هي التحقق من هوية الشخص الطبيعي، وعند الاقتضاء التحقق من صفاته الخاصة، والثانية التحقق من هوية الشخص المعنوي عن طريق احتفاظ مؤدي خدمات التصديق الإلكتروني بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع الإلكتروني المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني، حسبما نصت عليه المادة 2/44 من القانون 04/15 السالف الذكر.

ويرجع الغرض من تجريم المشرع الجزائري لهذه الافعال، ما تشكله شهادة تصديق إلكتروني من أهمية، لما تحتويه من بيانات ومعلومات سرية من شأن أي استعمال غير مشروع لها من غير ذي

[1]– انظر المادة 44 من القانون 04/15 السالف ذكره.

صفة (صاحب شهادة التصديق الإلكتروني) الإضرار بالمعاملات الإلكترونية التي تستوجب الثقة والأمان.

وهذه الجريمة من جرائم الخطر التي لا يشترط لقيامها تحقق نتيجة معينة، فبمجرد الإخلال بالتزام تحديد الهوية تقع الجريمة، ولو لم يصب المجني عليه ضرر فعلي. [1]

ثانيا: الركن المعنوي

تعتبر جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام بصورتيه، الأولى: أن يعلم مؤدي خدمات التصديق الإلكتروني انه بصدد منح شهادة تصديق إلكتروني موصوفة دون التحقق من هوية طالبها وأن هذا الفعل يجرمه القانون، والثانية: أن تتجه إرادته إلى اقتراف هذا الفعل.

ثالثا: العقوبة

عاقبت المادة 69 من القانون 04/15 على جريمة الإخلال بالتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة بالحبس من شهرين إلى ثلاث (3) سنوات، وبغرامة مالية من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار (200.000دج)، أو بإحدى هاتين العقوبتين فقط، أما في حالة ما إن كان الجاني شخصا معنويا فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، أي أنها تقدر بمليون دينار (1000.000دج) حسب نص المادة 75 من نفس القانون.

الفرع الثالث: جريمة مزاولة نشاط التصديق الإلكتروني بدون رخصة

ورد النص على هذه الجريمة في المادة 72 من القانون 04/15 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين انه: "يعاقب بالحبس من سنة (1) واحدة إلى ثلاث سنوات (3) وبغرامة من مائتي ألف دينار (200.000دج) إلى مليوني دينار (2000.000دج) أو بإحدى

[1]– ياسر محمد الكومي، الحماية الجنائية الامنية للتوقيع الإلكتروني، مرجع سابق، ص180.

هاتين العقوبتين كل من يؤدي خدمات التصديق الإلكتروني للجمهور بدون ترخيص، أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه".[1]

وبالتالي فقيام الجريمة بنص المادة 72 يرتكز على ركنيين أساسيين: الركن المادي والركن المعنوي على النحو التالي:

أولا: الركن المادي

يتحقق السلوك الإجرامي في جريمة مباشرة نشاط التصديق الإلكتروني بدون رخصة في صورتين وردتا في المادتين 72 من القانون 04/15 السابق ذكره وهما:

- إنتحال الجاني صفة مؤدي خدمات التصديق الإلكتروني، ومباشرته لنشاط التصديق الإلكتروني للجمهور دون ترخيص من السلطة الاقتصادية للتصديق الإلكتروني.
- إستئناف أو مواصلة مؤدي خدمات التصديق الإلكتروني النشاط بالرغم من سحب الترخيص.

وقد نصت المادة 33 وما بعده من القانون 04/15 السابق ذكره[2]، على مجموعة من الإلتزامات على عاتق أي شخص طبيعي أو معنوي يرغب في ممارسة نشاط التصديق الإلكتروني، أهما نظام الترخيص الذي تمنحه السلطة الإقتصادية للتصديق الإلكتروني وفق شروط ومؤهلات يجبأن تتوفر في كل طالب ترخيص، وآجال قانونية للممارسة هذا النشاط، ويظهر جليا أن مخالفة المادة 72 يحيلنا إلى أحكام المواد من 33 إلى 40 من نفس القانون التي تشترط الحصول على رخصة لمزاولة النشاط، إضافة إلى مجموعة من المؤهلات المطلوبة، والعلة من تجريم كل هذه الأفعال هي الآثار

---

[1]– تقابلها المادة (23/د) من التشريع المصري رقم: 15 لسنة 2004 والتي عاقبت بالحبس وبغرامة لا تقل عن عشرة الاف جنيه ولا تتجاوز مائة الف جنيه أو بإحدى هاتين العقوبتين كل من يخالف أيا من أحكام المادتين 19، 21 من هذا القانون، وقد تضمنت المادة 19 من قانون التوقيع الإلكتروني مجموعة من الالتزامات على عاتق من يرغب في ممارسة نشاط إصدار شهادة التصديق الإلكتروني وهي:

-ضرورة الحصول على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات قبل ممارسة النشاط المذكور.

-سداد رسم الهيئة المذكورة مقابل هذا النشاط.

- عدم جواز التوقف عن النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير، سوى بعد الحصول على موافقة كتابية من الهيئة المذكورة.

[2]– انظر المواد من 33 إلى 40 من القانون 04/15 السالف ذكره.

البليغة التي تترتب عن إصدار شهادة تصديق إلكتروني في حق الغير، وأن مخالفة نص المادة 72 – الذي يُخضع نشاط التصديق الإلكتروني إلى ما أسماه المشرع الجزائري بالتأهيل والترخيص– من شأنه المساس بالثقة في التوقيع الإلكتروني.

وتدخل جريمة مباشرة نشاط التصديق الإلكتروني بدون رخصة في نطاق جرائم الخطر، التي يكتمل الركن المادي فيها بمجرد إقتراف الجاني لسلوك إصدار شهادة تصديق إلكتروني بدون ترخيص، ولا يشترط تحقق نتيجة معينة ولو لم يصب المجني عليه ضرر فعلي.

ثانيا: الركن المعنوي

تعد جريمة مزاولة نشاط التصديق الإلكتروني بدون ترخيص من الجرائم العمدية التي تقوم على عنصري العلم والإرادة، أي القصد الجنائي العام، فيجب أن يعلم الجاني انه يمارس نشاط غير مشروع، بإصدار شهادات تصديق إلكتروني في غير الأحوال المصرح بها قانونا، سواء إصداره أياها بدون ترخيص، أو استئناف أو مواصلة النشاط بالرغم من سحب الترخيص، ومع ذلك يقدم عليه وتنصرف إرادته إلى اقتراف الفعل، وبالتالي قبوله للنتائج المترتبة على نشاطه غير القانوني، إذ لا مجال للحديث عن وقوع الجريمة بطريق الخطأ.

ثالثا: العقوبة

قرر المشرع الجزائري حسب نص المادة 72 من القانون 04/15 لهذه الجريمة عقوبة أصلية تتمثل في الحبس من سنة (1) إلى ثلاث سنوات (3)، وبغرامة من مائتي ألف دينار (200.000دج) إلى مليوني دينار (2000.000دج)، أو بإحدى هاتين العقوبتين فقط في حالة ما إذا كان الجاني شخصا طبيعيا، أما إذا كان الجاني شخصا معنويا وفقا لأحكام المادة 73 من نفس القانون، فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، أي انه يعاقب بغرامة قدرها عشرة ملايين دينار (10.000.000دج).

كما تصادر التجهيزات التي استعملت لإرتكاب الجريمة طبقا للتشريع المعمول به.

المطلب الثالث:

صور الاعتداء على التوقيع الإلكتروني في بعض النصوص القانونية الخاصة (القانون 03/15 والقانون 07/18)

يشكل القانون 03/15 المتعلق بعصرنة العدالة، السند القانوني الذي يضع الإطار العام لضبط كيفية إستخدام وسائل التكنولوجيا والإتصال الحديثة وإضفاء الشرعية اللازمة لإستعمال الدعائم الإلكترونية[1]، وقد تضمن في شقة الجزائي جريمة إساءة استعمال العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بشخص آخر، وجريمة مواصلة إستعمال شهادة إلكترونية ملغاة أو منتهية الصلاحية من قبل حائزها.

وفي هذا السياق جاءت أحكام القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، لتدعيم الحماية القانونية للبيانات الشخصية عن طريق فرض الإلتزامات الواجب إحترامها أثناء جمع ومعالجة وحفظ هذه البيانات، خاصة فيما تعلق بالتوقيع والتصديق الإلكتروني، والتدخل جزائيا لقمع أي إعتداء عل هاتين الآليتين.

وهو ما سيتم تفصيله في فرعين إثنين، الأول: يعالج صور الإعتداء على التوقيع الإلكتروني في القانون 03/15، بينما يخصص الفرع الثاني لأشكال الإعتداءات المحتملة على ضوء القانون 07/18.

الفرع الأول: صور الإعتداء على التوقيع الإلكتروني في القانون 03/15

بالرجوع إلى أحكام المادة (4) من القانون 03/15 المتعلق بعصرنة العدالة يظهر الدور الهام للتوقيع الإلكتروني في إضفاء الحجية القانونية لمختلف الوثائق والمحررات القضائية التي تسلمها مصالح وزارة العدل والمؤسسات التابعة لها، والتي ترتبط إلكترونيا بالمحرر الأصلي بواسطة وسيلة تحقق موثوقة وهي آلية التصديق الإلكتروني، التي تضمن سلامة العقد الرابط بين الموقع والبيانات

[1]– تدخل وزير العدل حافظ الاختام وكذا تدخلات النواب أثناء مناقشة مشروع قانون عصرنة العدالة المنقول عبر الإذاعة الوطنية، الموجود في الموقع الرسمي للإذاعة الوطنية: www.radioalgerie.dz/news/arتم الاطلاع عليه بتاريخ 07 اوت 2018 الساعة 17: 57.

المنشئة للتوقيع الإلكتروني، وهذا ما يستوجب توفير حماية جزائية لكل تلاعب بهذه الآليات القانونية[1].

أولا: جريمة إساءة إستخدام العناصر الشخصية المتعلقة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر

تنص المادة 17 من القانون 03/15 المتعلق بعصرنة العدالة انه: " يعاقب بالحبس من سنة إلى خمس (5) سنوات وبغرامة تتراوح من 100.000دج إلى 500.00دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر".

يتطلب لقيام هذه الجريمة وفقا للمادة 17 من القانون السابق الذكر توافر ركنين: ركن مادي، وركن معنوي زيادة إلى تحديد الجزاء المقرر لمرتكب هذه الجريمة.

1. الركن المادي:

يتمثل الركن المادي في هذه الجريمة في الإستعمال غير القانوني للعناصر الشخصية التي تدخل في إنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر. ويقصد بالعناصر الشخصية المتصلة بإنشاء توقيع إلكتروني البيانات والمعلومات الشخصية التي تعرف بهوية الموقع أو صاحب التوقيع بمفهوم المادتين 6و7 من القانون 03/15 السالف الذكر، والتي يمكن التحقق منها عن طريق آلية التحقق من التوقيع الإلكتروني.[2]

وهي كلها بيانات سرية لا يطلع عليها إلا صاحب التوقيع وهي بيانات مؤمنة عن طريق آلية التشفير وقد سبق التطرق إلى ذلك عند دراستنا لأنواع الحماية التي سنها القانون 04/15حفاظا على التوقيع الالكتروني وشهادة التصديق الإلكتروني.

[1]– خصص المشرع الجزائري الفصل الخامس من القانون 03/15 المتعلق بعصرنة العدالة للأحكام الجزائية وذلك في المادتين 17 و18

[2]– انظر المواد 4، 5، 6، 7، 8 من القانون 03/15 المتعلق بعصرنة العدالة.

2. الركن المعنوي:

جريمة إساءة إستخدام العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصرية العلم والإرادة، فيجب أن يعلم الجاني بأن فعل إستعمال العناصر الشخصية للتوقيع الإلكتروني والذي يتعلق بتوقيع شخص آخر فعل غير مشروع ومعاقب عليه قانونا، وأن تتجه إرادته لإقتراف الفعل المجرم.

3. العقوبة:

على عكس باقي جرائم الإعتداء على التوقيع الإلكتروني، شدد المشرع الجزائري العقوبة في جريمة إساءة إستخدام العناصر الشخصية المتمثلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر، ومرد ذلك تعزيز الثقة في المعاملات الإلكترونية، التي يشكل فيها عامل الثقة في التوقيع الإلكتروني الأهمية الكبرى، ولذلك نصت المادة 17 من القانون 03/15 السالف الذكر على عقوبة الحبس من سنة إلى خمس سنوات، وبغرامة تتراوح من 100.000دج إلى 500.000دج.

ثانيا: جريمة الاستعمال غير المشروع للشهادة الإلكترونية

ورد النص على هذه الجريمة في المادة 18 من القانون 03/15 المتعلق بعصرنة العدالة على أنه: " يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة تتراوح بين 100.000دج إلى 500.000دج كل شخص حائز شهادة إلكترونية يواصل استعمالها رغم علمه بانتهاء مدة صلاحيتها أو إلغائها". تقوم الجريمة كما يستفاد من نص المادة 18 المذكورة على ركنين اثنين، ركن مادي، وركن معنوي يتم تفصيلهما على النحو التالي:

1. الركن المادي:

يتحقق السلوك الإجرامي في جريمة الإستعمال غير المشروع للشهادة الإلكترونية[1]، في فعل إستعمال الشهادة من قبل حائزها رغم علمه بإنتهاء مدة صلاحيتها، أو استعماله إياها بعد إلغائها. فمن

[1]– تنص المادة 6 من القانون 03/15 المتعلق بعصرنة العدالة في تعريفها للشهادة الإلكترونية انه: " يتم اثبات العلاقة بين معطيات التحقق من التوقيع الإلكتروني وصاحب التوقيع عن طريق شهادة إلكترونية موصوفة تصدرها وزارة العدل".

المعلوم أن العلاقة بين الوزارة مصدرة الشهادة الإلكترونية والعميل صاحب التوقيع علاقة عقدية، تنقضي بإنتهاء المدة المتفق عليها، وعليه يجب على حائز الشهادة الوقف الفوري عن أي استعمال لها بمجرد علمه بانتهاء صلاحيتها، أو علمه بتاريخ إلغائها لأنه قد يحتفظ بها لاستخدامها في أغراض غير مشروعة مما يجعله تحت طائلة المسألة الجزائية. [1]

2. الركن المعنوي:

تعتبر جريمة الاستعمال غير المشروع للشهادة الإلكترونية من الجرائم العمدية والتي يتحقق القصد الجنائي فيها بتوافر ركني العلم والإرادة، فيجب أن يعلم الجاني مواصلته استعمال شهادة إلكترونية يحوزها منتهية الصلاحية أو ملغاة رغم علمه المسبق بذلك، ما يشكل فعلا محظورا يعاقب عليه القانون، وأن إرادته اتجهت إلى اقتراف هذا الفعل.

3. العقوبة:

انتهج المشرع الجزائري نفس سياسة التشديد التي تبناها إزاء هذا النوع من الجرائم، مثلما ورد في المادة 17 من القانون 03/15 السابق ذكره، فقد قرر من خلال المادة 18 التالية عقوبة الحبس من سنة (1) إلى خمس (5) سنوات، وبغرامة تتراوح بين 100.000دج إلى 500.000دج.

الفرع الثاني: صور الاعتداء على التوقيع الإلكتروني في القانون 07/18

تنص المادة الأولى من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي على انه: " يهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي".

---

[1]– في هذا الاطار ذهبت محكمة النقض الفرنسية في حكم صادر في 19 مارس 2014 إلى اعتبار تصرف حامل بطاقة دفع إلكتروني منتهية الصلاحية سلوكا يكون جريمة خيانة الامانة على اساس ان البطاقة محرر يتم تسليمها إلى العميل على سبيل عادية الاستعمال ومن اجل وظيفة محددة وان استمرار التعامل بها على الرغم من اخطاره بسحبها من قبيل الاختلاس الذي يضر بالبنك.

Arret n 1193 du 19 mars 2014(12-87-416) de la chambre: Criminelle disponible en ligne cour de cassation: https: www.courdecassation.fr/uriprudence2/chambre_criminelle-578/dite_societe_28730.html

كما قضت محمكمة جنح باريس في حكم لها صادر في 16 اكتوبر 1984، بإدانة صاحب بطاقة الائتمان بتهمة جنحة النصب لقيامه بتقديم بطاقة مجردة من أي قيمة بفعل الغائها من قبل البنك مصدرها , T-corr, Paris 16 octobre 1984 T.C.P , ed 1967, p129.

وعرفت المادة الثالثة من نفس القانون المعطيات ذات الطابع الشخصي أنها:" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعية..."

وبإستقراء نص هذه المادة، تدخل بيانات إنشاء التوقيع الإلكتروني التي يحوزها الموقع[1]، وكذا شهادة التصديق الإلكتروني بما تتضمنه من معلومات معالجة إلكترونيا، ضمن المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين التي أشار إليها المشرع الجزائري في المادة 42 من القانون 07/18.[2]

على ذلك، يمكن إستخلاص أشكال الإعتداءات المحتملة على آليتي التوقيع والتصديق الإلكترونيين في إطار معالجة المعطيات ذات الطابع الشخصي، وهي الإخلال بالموافقة المسبقة للشخص المعني، وكذا عدم التصريح المسبق لدى السلطة الوطنية، أو عدم الترخيص، أي خرق أحكام المادتين 7 و12من القانون 07/18 وكلها أفعال جرمتها المادتين 55 و56 من نفس القانون.[3]

---

[1]– وهو في هذه الحالة "الشخص المعني" الذي عرفته المادة 3 فقرة2 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي على انه: " كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة".

[2]– تنص المادة 42 من نفس القانون على انه: " ما عدا في حالة مرافقتهم الصريحة يجب الحصول على المعطيات ذات الطابع الشخصي التي تتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص المعنيين بها مباشرة ولا يحوز معالجتها لاغراض غير تلك التي جمعت لاجلها".

[3]–في هذا السياق جرم المشرع الفرنسي من خلال قانون 6 جانفي 1978 بشأن الاطلاع على البطاقات ذات البيانات الشخصية قبل تعديله العديد من الافعال التي تمثل خروجا على أحكامه في المواد 41 في 44 وكذلك في المرسوم رقم 81–1142 الصادر في 22 ديسمبر 1981، الا انه وبمناسبة صدور القانون رقم 92– 1336 الصادر في 16 ديسمبر 1992 بشأن إصدار قانون العقوبات الجديد تم ادراج العديد من الجرائم التي كان ينص عليها قانون 6 يناير 1978 في صلب قانون العقوبات الفرنسي الجديد، حيث تم تخصيص المواد من 16/226 إلى 24/226 لهذا الغرض، واقتصرت المادة 50 من نفس القانون على مجرد الاحالة لمواد التجريم المنصوص عليها في قانون العقوبات الفرنسي.

أولا: جريمة الاخلال بشرط الموافقة الصريحة للشخص المعني لمعالجة معطياته الشخصية

تنص المادة 55 من القانون 07/18 السالف ذكره في فقرتها الأولى على انه:" يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة مالية تتراوح من 100.000دج إلى 300.000دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون".

فقد ألزم المشرع الجزائري مؤيدي خدمات التصديق الإلكتروني عند قيامهم بإجراءات المعالجة الآلية للمعطيات الشخصية للشخص المعني، وهو هنا الموقع أو صاحب التوقيع الإلكتروني، الحصول المسبق على موافقتهم الصريحة، وهو شرط أساسي تنجم عن مخالفته قيام المسؤولية الجزائية التي تستوجب العقاب. [1]

1. الركن المادي:

يقوم الركن المادي لهذه الجريمة بمجرد أن تتم المعالجة الآلية للبيانات الشخصية دون إتخاذ الإجراءات القانونية الواردة بالمادة 7 من القانون 07/18 السابق ذكره، أو بالرغم من إعتراض الشخص المعني على هذه المعالجة، وطبقا للمادة 7 فانه يتعين على الهيئات المخول لها معالجة المعطيات ذات الطابع الشخصي إن تحصل على الموافقة الصريحة للشخص المعني.

كما انه لا يجوز إطلاع الغير على المعطيات ذات الطابع الشخصي الخاصة للمعالجة، إلا من أجل الغايات المرتبطة بمهام المسؤول عن المعالجة والمرسل إليه، وبعد موافقة الشخص المعني مسبقا.

وأورد المشرع الجزائري الإستثناءات الواردة على شرط الموافقة المسبقة للشخص المعني على سبيل الحصر في الفقرة الأخيرة من المادة 7، حماية لمصالح الأطراف المتدخلة في عملية المعالجة.[2]

---

[1]– وقد سبق للمشرع الجزائري تجريم مثل هذه الافعال من خلال المادة 7 من القانون 03/15 المتعلق بالتوقيع والتصديق الإلكترونيين .

– راجع في هذا الصدد جرائم افشاء سرية بيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني، ص110

[2]–انظر الفقرة 5 من المادة 7 من القانون 18–07 السالف الذكر وكذا الفقرة 2 من المادة 55 من نفس القانون.

2. الركن المعنوي:

تعد جريمة الإخلال بشرط الموافقة الصريحة للشخص المعني قبل معالجة بياناته الشخصية من الجرائم العمدية، يتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، ويجب لقيام الجريمة أن يعلم الجاني أنه يعالج بيانات شخصية دون موافقة صريحة من صاحب الشأن، وأنه يعلم بأن هذا الفعل غير مشروع، ومع ذلك تتجه إرادته إلى ارتكاب هذا السلوك الإجرامي.

ولا عبرة بالباعث أو الغرض من ارتكاب الجريمة، ولا حتى بالقصد الجنائي الخاص، حيث إكتفى المشرع الجزائري بالقصد الجنائي العام.

3. العقوبة:

قرر المشرع الجزائري بنص المادة 55 من القانون 07/18 السالف ذكره عقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات، وبغرامة من 100.000دج إلى 300.000دج، كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من نفس القانون.

وهي نفس العقوبة المقررة لكل من قام بمعالجة المعطيات ذات الطابع الشخصي رغم اعتراض الشخص المعني.

ثانيا: جريمة الاخلال بشرط الترخيص المسبق للمعالجة

نصت المادة 56 من القانون 07/18 السابق ذكره على أنه: " يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000دج إلى 500.000دج، كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون". وبالرجوع إلى أحكام المادة 12 من نفس القانون فقد اشترط المشرع الجزائري التصريح المسبق لدى السلطة القضائية أو ترخيص منها، قبل مباشرة عملية معالجة المعطيات ذات الطابع الشخصي.[1]

[1]– تنص المادة 12 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي انه: " مالم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها طبقا لأحكام المنصوص عليها في هذا القانون".

1. الركن المادي:

لقيام الركن المادي لهذه الجريمة يجب أن تتم معالجة المعطيات ذات الطابع الشخصي دون اتخاذ الإجراءات القانونية الواردة في المادة 12 من القانون 07/18، وطبقا للمادة 12 فانه يتعين على الشخص أو الهيئة المخول لها معالجة المعطيات ذات طابع شخصي أن تباشر هذه المعالجة وفق تصريح مسبق، أو بترخيص من السلطة الوطنية. [1]

ويتحقق الركن المادي لهذه الجريمة بأي معالجة للمعطيات الشخصية دون اتخاذ الإجراءات المطلوبة قانونا (سواء تصريح مسبق أو ترخيص من السلطة الوطنية)، ولا يشترط توافر نتيجة إجرامية.

2. الركن المعنوي:

تعد جريمة الإخلال بشرط الرخيص المسبق للمعالجة من الجرائم العمدية، والتي تقوم على القصد الجنائي العام بعنصرية العلم والإرادة، فيجب أن يعلم الجاني أنه أخل بواجباته التي يفرضها عليه القانون في طلب التصريح المسبق أو الترخيص لدى السلطة الوطنية قبل عملية المعالجة، ويجب أن تتجه إرادته إلى إتيان هذه الأفعال غير المشروعة، وبالتالي قبوله بالنتائج التي تنجر عن ذلك، ولا عبرة في هذا الإطار بالباعث أو الغرض من ذلك.

3. العقوبة:

يعاقب المشرع الجزائري على جريمة الإخلال بشرط التصريح المسبق أو الترخيص قبل المعالجة حسب نص المادة 66 من القانون 07/18، بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000دج إلى 500.000دج

[1]– انظر في هذا الإطار المواد 13 وما بعدها من القانون 07/18 والتي تناولت إجراءات التصريح، وكذلك المواد 17 وما بعدها من نفس القانون والتي تناولت إجراءات الترخيص.

الباب الثاني:

الجوانب الإجرائية للحماية الجزائية للتوقيع والتصديق الإلكترونيين

لا شك أن الهدف الرئيسي الذي تسعى إلى تحقيقه إجراءات الخصومة الجنائية منذ نشأتها بتحريك الدعوى العمومية، وحتى إنقضائها بإصدار حكم نهائي، هو إثبات نسبة الجريمة إلى فاعلها.

ومع تزايد إستخدام آلية التوقيع الإلكتروني، تزايد معدل إستخدام مرتكبي الجرائم لهذه الآلية في الإيقاع بضحاياهم، مستغلين في ذلك الصعوبات الكبيرة التي تعترض أجهزة إنفاذ القانون، ورجال القضاء، والنيابة ورجال البحث الجنائي، أثناء كشفهم عن أدلة الإدانة. فكان من الضروري على الكثير من الدول إصدار تشريعات إجرائية مستحدثة بعيدا عن وسائل الإثبات التقليدية التي أظهرت عجزها في كثير من الأحيان عن إثبات جرائم التوقيع الإلكتروني، وأصبح التعامل مع أشكال مستحدثة من الأدلة الجنائية يمكن الإعتماد عليها في إثبات الجرائم الواقعة على التوقيع الإلكتروني.

إنطلاقا من كل ذلك، سيتم التعرف في هذا الباب على أحدث إجراءات الإثبات الجنائي لكشف الجرائم الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني، ومتابعة المجرمين وتقديمهم إلى القضاء ومحاكمتهم. وقد خصص الفصل الأول من هذا الباب لإجراءات التحقيق في الجرائم الواقعة على التوقيع الإلكتروني، فيما تناول الفصل الثاني إجراءات المحاكمة في هذا النوع من الجرائم.

الفصل الأول:

إجراءات التحقيق في الجرائم الواقعة على التوقيع الإلكتروني

تمهيد:

تكتسي مرحلة التحقيق الجنائي أهمية كبيرة في الكشف عن الجريمة والمجرمين، بما تتضمنه من جمع للإستدلالات من قبل أجهزة الضبط القضائي المختصة (مرحلة التحقيق التمهيدي) من جهة، ومرحلة التحقيق التي يتولاها قاضي التحقيق من جهة ثانية، يجمع فيها بين أعمال ضباط الشرطة القضائية وبين أعماله كقاضي تحقيق يصدر عنه مجموعة من الأوامر ذات الطبيعة القضائية.

ومع الطبيعة الخاصة لجرائم الإعتداء على التوقيع الإلكتروني، أصبح من الضروري إستحداث آليات وأساليب جديدة للبحث والتحري والإثبات، تماشيا مع التطورات التكنولوجية للإجرام المعلوماتي، وتضمن في الوقت ذاته إحترام الحق في الخصوصية المكفول دستوريا، مثلما نص عليه التعديل الدستوري الأخير لسنة 2016، في المواد (46) و(47) من القانون 01/16 المتضمن التعديل الدستوري.

لذا أصبح تعامل الجهات المكلفة بالتحري والتحقيق عن الجريمة مختلفا إزاء هذا النوع من الجرائم، وفقا للتشريعات الإجرائية المستحدثة، بداية بالقانون 22/06 المعدل لقانون الإجراءات الجزائية[1]، والقانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[2]وهو ما أتاح لهذه الجهات إعتماد أساليب تقنية جديدة للوصول إلى الدليل المناسب لإثبات الجرائم المعلوماتية عامة وجرائم التوقيع الإلكتروني خاصة.

وعليه تناولت الدراسة في هذا الفصل إجراءات جمع الاستدلالات في الجرائم الواقعة على التوقيع الإلكتروني في مبحث أول، ثم التعرف على الإجراءات التقنية للإثبات الجنائي في الجرائم الواقعة على التوقيع الإلكتروني في مبحث ثاني.

---

[1]–القانون 06–22 المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 155/66 المؤرخ في 1966/06/08، والمتضمن قانون الإجراءات الجزائية (ج.ر) رقم 84 المؤرخة في 2006/12/24.

[2]–القانون 04/09 المؤرخ في 2009/08/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (ج.ر) رقم 47 المؤرخة في 2009/08/16.

المبحث الأول:

إجراءات جمع الاستدلالات في الجرائم الواقعة على التوقيع الإلكتروني

جمع الاستدلالات مرحلة إجرائية شبه قضائية تساعد على الوصول إلى الحقيقة[1]، وتتمثل في مباشرة التحريات الجنائية لإستقاء المعلومات الموثوق بها تبعا لإجراءات بحثية شرعية يقوم بها موظفون مختصون من سلطة استدلال لكشف واقعة جنائية ونسبتها إلى فاعلها. [2]

وأوكل المشرع الجزائريهذه المهمة لأجهزة الضبط القضائي[3]، تمهيدا لعرض القضية أمام النيابة العامة. وعليه تشكل هذه المرحلة الخطوة الأساسية لمواجهة جرائم الإعتداء على التوقيع الإلكتروني مما يستوجب معه تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجرائم الماسة بسلامة الأنظمة المعلوماتية عبر شبكة الأنترنت.

نتيجة لذلك اتجهت معظم الدول إلى إعداد وتجهيز فرق خاصة لمواجهة هذا النوع من الإجرام الإلكتروني كشرطة الأنترنت أو فرق التحري الخاصة، وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات للتعرف على أحدث أساليب التحري لمكافحة الإجرام المعلوماتي، وهو ما سيتم التعرف عليه على النحو التالي:

- **المطلب الأول:** دور الضبطية القضائية في الكشف عن الجرائم الواقعة على التوقيع الإلكتروني.
- **المطلب الثاني:** أساليب التحري المستحدثة في الكشف عن الجرائم الواقعة على التوقيع الإلكتروني.

---

[1]– عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، الطبعة الثالثة، دارهومة، الجزائر 2012، ص 193.

[2]– مصطفى محمد الدغيدي، التحريات والإثبات الجنائي، مطابع جامعة المينا، مصر، 2002، ص 21.

[3]– حسب المادة 14 من قانون الإجراءات الجزائية الجزائري، حيث يشمل الضبط القضائي: ضباط الشرطة القضائية، أعوان الضبط القضائي، الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي.

المطلب الأول:

دور الضبطية القضائية في الكشف عن الجرائم الواقعة على التوقيع الإلكتروني.

قد لا يظهر ذلك الإختلاف الكبير بين سلطة الضبطية القضائية في حالة التحري عن الجرائم التي تقع إعتداءا على آليتي التوقيع والتصديق الإلكترونيين، والقاعدة العامة في إجراءات الاستدلال عن الجرائم التقليدية، إلا أن لجرائم التوقيع الإلكتروني ذاتية خاصة تتمثل في لامادية التواقيع الإلكترونية وشهادات التصديق الإلكترونية، وتحتاج بذلك إلى خبرات من نوع خاص في رجال الضبط القضائي.

على هذا الأساس، وتنفيذا للسياسة الإجرائية المستحدثة من قبل الدولة لمكافحة أساليب الإجرام المعلوماتي لاسيما في مجال البحث والتحري، فتحت المادة (16فقرة7) من قانون الإجراءات الجزائية الجزائري الباب واسعا أمام الضبطية القضائية لمباشرة عملية البحث والمعاينة، ليمتد إختصاص ضباط الشرطة القضائية إلى كافة الإقليم الوطني.[1]

---

[1]–من اجل التجسيد الفعلي وتسهيل مهام السلطات الضبطية القضائية، وفي اطار مكافحة الجريمة المعلوماتية والتي تتطلب كفاءة مهنية عالية، تناسب وخصوصيات هذه الجرائم المستجدة، قام المشرع الجزائري بادخال تعديلات جوهرية على قانون الإجراءات الجزائية بالقانون 14/04 المؤرخ في 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66–155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ع 71 _الصادرة في 10 نوفمبر 2004، والقانون 06–22 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم –155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ع 84 الصادرة في 24 ديسمبر 2006، حيث وسع بموجبها الاختصاص الاقليمي لاعضاء الضبطية القضائية، كلما تعلق الأمر ببحث ومعاينة احدى الجرائم المنصوص عليها في المادة 7/16 من ق.ا.ج.ج وحصرتها فيما يلي: "جرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بانظمة المعالجة الالية للمعطيات وجرائم تبييض الاموال والجرائم المتعلقة بالتشريع الخاص بالصرف"، وبناء على المواد 16 و16 مكرر من ق.ا.ج.ج فان الاختصاص الاقليمي للنشاط ضباط الشرطة القضائية، اتسع اقليميا فيما يخص الجرائم الماسة بانظمة المعالجة الالية للمعطيات ليشمل كامل الاقليم الوطني، كما انه طبقا للمواد من 40 مكرر 1 إلى 40 مكرر 3 ق.ا.ج، فان الاختصاص الاقليمي لنشاط ضباط الشرطة القضائية اتسع اقليميا ليشمل اختصاص اقليمي لمحاكم أخرى غير المحكمة التي يباشرون مهامهم في دائرة اختصاصها، حيث حدد هذا الاختصاص الاقليمي الموسع وفقا لأحكام المرسوم التنفيذي رقم (06_348) المؤرخ في 2006/10/05، المتضمن تمديد الاختصاص المحلي لبعض المحاكم، ووكلاء الجمهورية وقضاة التحقيق.

غير أن التحري في البيئة الإلكترونية يستوجب بالإضافة إلى تمديد الاختصاص، إستحداث أجهزة متخصصة لمكافحة هذا النوع من الجرائم بالتنسيق مع مؤدي خدمات التصديق الإلكتروني[1]وكذا سلطات التصديق الإلكتروني[2]، و إعمال أساليب البحث والتحري الخاصة توازيا مع تنامي الإعتداءات التي تطال تقنية التوقيع والتصديق الإلكترونيين.

وإنطلاقا من كل ذلك، تم تقسيم هذا المطلب إلى فرعين، يتناول الفرع الأول أجهزة الضبط القضائي المختصة في مكافحة الجرائم الواقعة على التوقيع الإلكتروني، ثم التعرف على مدى إستعانة الضبطية القضائية بمؤدي خدمات التصديق الإلكتروني في الفرع الثاني.

الفرع الأول: أجهزة الضبط القضائي المختصة في الجرائم الواقعة على التوقيع الإلكتروني

تماشيا مع إستراتيجية الدولة إلزامية إلى تطبيق مشروع الجزائر الإلكترونية الذي بدا عام 2013، ومجابهة مخاطر الإعتداءات الإجرامية التي تطال شبكة المعلومات الإلكترونية المتداولة، والتي تشكل حجر الزاوية بالنسبة لهذا المشروع، كان من الضروري تخصيص آليات على مستوى جهازي الشرطة والدرك الوطني، بالإضافة إلى هيئة متخصصة في مكافحة هذه الجرائم المتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

وتبعا للإجراء المستحدث بتوسيع إختصاص أجهزة الضبط القضائي، كان تقسيم الوظائف كالتالي:

---

[1]– انظر الفصل الثاني من الباب الثالث من القانون 15–04 المتعلق بالتوقيع والتصديق الإلكترونيين المذكور آنفا، الذي نص على سلطات التصديق الإلكتروني وهي:

- السلطة الوطنية للتصديق الإلكتروني .
- السلطة الحكومية للتصديق الإلكتروني .
- السلطة الاقتصادية للتصديق الإلكتروني .

[2]– انظر المادة (2) من القانون 15–04 الفقرة (11) و(12) في تعريفها لمؤدي خدمات التصديق الإلكتروني والطرف الثالث الموثوق.

أولا: أجهزة الأمن الوطني (الشرطة) المختصة:

تتوفر المديرية العامة للأمن الوطني على هياكل وأجهزة متطورة في مجال مكافحة جرائم نظم المعلومات وجرائم الأنترنت، في إطار تفعيل العمل المشترك مع الأجهزة الجنائية الدولية، وإستجابة لمتطلبات مشروع تكنولوجيا الانتربول وقاعدة البيانات المتعلقة بذلك، يتقدمها المعهد الوطني للشرطة الجنائية الذي تم إنشاءه سنة 1999[1]، مهمته الأساسية التحقيق والتحري إلى جانب اربع (4) مخابر جهوية موزعة على التراب الوطني بكل من: قسنطينة، وهران، بشار، تمنراسنت، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الالي تعمل بالتنسيق مع الفرق المتخصصة في البحث والتحري عن الجريمة المعلوماتية المتواجدة على مستوى كل مديريات الامن الولائي .

[1]– المعهد الوطني للشرطة الجنائية أو المخبر المركزي للشرطة العلمية والتقنية، هو احد مراكز تكوين الشرطة الجزائرية تم انشاؤه سنة 1999، لتلبية الحاجات التكوينية التخصصية للشرطة الجزائرية مقره الجزائر العاصمة يضم 15 مصلحة يحتل المرتبة الثانية إفريقيا والأولى عربيا بين مخابر الشرطة .

– سجلت مصالح المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال خلال الـ 08 أشهر الأولى من السنة الجارية، 567 قضية تتعلق بجرائم المساس بالانظمة المعلوماتية وجرائم الأنترنت، تورّط فيها 543 شخصا.

حيث تمكنت الفرق المتخصصة في مكافحة الجرائم الإلكترونية للأمن الوطني ومن خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر، من معالجة 385 جريمة إلكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها اهمها:

- 23 قضية تتعلق بنسخ البرامج دون حق وجرائم القرصنة، عولج منها 21 قضية وتورط فيها 39 شخصا بنسبة معالجة وصلت إلى 92%
- 57 قضية تتعلق بجرائم الاعتداء على سلامة الأنظمة المعلوماتية، عولج منها 31 قضية وتورط فيها 39 شخصا بنسبة معالجة وصلت إلى 55%
- 25 قضية تتعلق بجرائم الاحتيال عبر الأنترنت، عولج منها 17 قضية وتورط فيها 32 شخصا بنسبة معالجة وصلت إلى 68 %
- الموقع الرسمي للشرطة الجزائرية بتاريخ:2019/06/02 /http.//www.dgsn.dz

ثانيا: أجهزة الدرك الوطني المختصة

تم إستحداث مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها (ببئر مراد رايس) التابع لمديرية الأمن العمومي للدرك الوطني[1]، إلى جانب المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للقيادة العامة للدرك الوطني الذي يضم من بين أقسامه قسم الإعلام والإلكترونيك حيث

---

[1]– وهو جهاز متخصص تابع لقيادة الدرك الوطني، يقع مقره بالجزائر العاصمة بالدائرة الإدارية لبئر مراد رايس، ولممارسة صلاحياته، تم تقسيمه إلى ما يلي: قسم اليقظة المعلوماتية، قسم التحقيقات المعلوماتية، قسم الامن الرقمي، مصلحة التقنية والاستغلال، مصلحة الإدارة والوسائل.

ومن صلاحيات مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ما يلي:

- ضمان يقظة عامة ومستمرة على شبكة الانترنيت،
- الوقاية من كل أنواع الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها،
- مساعدة السلطات القضائية وإجراء الخبرة التقنية المتعلقة بالجرائم المرتبطة بتكنولوجيات الاعلام والاتصال،
- تقديم المساعدة للتنظيمات العمومية الوطنية , في ما يتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والتصال ومكافحتها،
- تقديم المساعدة لوحدات الدرك الوطني المكلفة بالشرطة القضائية لمعاينة الجرائم التي سهل ارتكابها أو المرتبطة باستعمال انظمة الاعلام الالي وتكنولوجيات الاعلام والاتصال، جمع ادلتها والبحث عن مرتكبيها،
- اعداد وتفعيل الاستراتيجية الرقمية للدرك الوطني،
- المشاركة في اعداد وتفعيل الاستراتيجية الرقمية الوطنية،
- التمكن والتحكم في قواعد امن التكنولوجيات وأنظمة الإعلام،
- المشاركة في تقوية امن أنظمة الإعلام الوطنية وحماية فضاء المعلومات الوطني،
- المشاركة في إعداد القوانين والنظم المسيرة لمجال تكنولوجيات الإعلام والاتصال،
- إنشاء علاقات تنسيق وتعاون مع مختلف المتدخلين في مجال تكنولوجيات الإعلام والاتصال.الرائد حلاب منير، دور الدرك الوطني في ميدان محاربة جرائم المعلوماتية، مداخلة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، السابق الذكر، ص 3. وفي هذا الإطار صرح الرائد من خلال المداخلة على عدد القضايا المعالجة من طرف مركز الوقاية من الجرائم المعلوماتية للدرك الوطني، من سنة 2009 إلى 2016 وهي تتراوح مابين 18 قضية إلى 465 قضية في سنة 2016، وهذه الجرائم تنصب على: التهديد، جرائم المساس بالنظام العام، الارهاب جرائم المساس بانظمة المعالجة الالية للمعطيات (الاختراق)، تحرض القصر على الفسق والدعارة.

يختص بالبحث والتحري في الجرائم المعلوماتية[1]، هذا إلى جانب المهام الموكلة لمصلحة التحقيق القضائي والأمن على مستوى مديرية الأمن الداخلي بدائرة الاستعلام والأمن بوزارة الدفاع الوطني، بموجب المرسوم الرئاسي رقم 183/14 المؤرخ في 11 جوان 2014، المتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن.[2]

---

[1]– المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني استحدث بموجب المرسوم الرئاسي رقم 04–183 المؤرخ في 8 جمادى الأولى عام 1425 هـ الموافق 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الاساسي ج.رعدد: 41 الصادرة في 27 جوان 2004.

ومن مهام المعهد حسب المادة 6 من المرسوم الرئاسي السالف ذكره ما يلي:

- إجراء، بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، الخبرات والفحوص العلمية التي تخضع لاختصاص كل طرف في اطار التحريات الأولية والتحقيقات القضائية بغرض اقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح،

– تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة، المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل إشكال الاجرام ...الخ .

– وفي هذا الاطار وأثناء تدخله في اشغال الندوة الدولية حول الامن السيبيراني ومكافحة الجرائم الإلكترونية المنعقدة يومي 27 و28 من شهر مارس 2018، اكد قائد الدرك الوطني ان من أولويات الدولة الجزائرية وان اختيار موضوع الندوة: الخدمات الإلكترونية والامن العمومي يتزامن مع المصادقة على عدة قوانين من اهمها قانون التجارة الإلكترونية سنة 2018 والذي سبقه صدورقانون التوقيع الإلكتروني سنة 2015، هاته النصوص من شانها اعطاء دفعة قوية لتطوير الخدمات الإلكترونية وكشف قائد الدرك الوطني ان مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية ومكافحتها قام خلال سنة 2017 بمعالجة ما يقارب الف جريمة رقمية في إطار مساعدة الوحدات الإقليمية للدرك الوطني, وهو مايمثل زيادة بنسبة 68 بالمائة مقارنة بالسنة السابقة".

وفي ذات الصدد, حذر قائد الدرك الوطني من أن "المساس بالخدمات الإلكترونية يمكن أن يكون له عواقب وخيمة على الأفراد والممتلكات والأمن العمومي, خاصة في حال كانت هذه الخدمات حيوية لعمل قطاعات حساسة مثل الأمن, الصحة, الطاقة والمالية".

– مأخوذ من موقع وكالة الانباء الجزائرية على الأنترنت بتاريخ 2019/06/03 www.aps.dz/ar

[2]– المرسوم الرئاسي رقم 14–183 المؤرخ في 15شعبان عام 1435 هـ الموافق لـ 11 جوان 2014، يتضمن انشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والامن ومهامها وتنظيمها ج.ر. عدد: 32 الصادر في 12 جوان 2014.

ثالثا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، يوجد مقرها بالجزائر العاصمة، وضعت تحت سلطة وزارة الدفاع الوطني، تم إنشاؤها بموجب المرسوم الرئاسي رقم 172/19[1]، تطبيقا لأحكام القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لا سيما المادتين (13) و(14) منه.

[1]– المرسوم الرئاسي رقم 172/19 المؤرخ في 06يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج. ر العدد37 بتاريخ09يونيو 2019، تضم الهيئة من حيث تشكيلتها مجلس توجيه ومديرية عامة.

- مجلس التوجيه: يرأس مجلس التوجيه وزير الدفاع الوطني أو من يمثله وتتشكل من ممثلي الوزارات الاتية:
  - وزارة الدفاع الوطني
  - الوزارة المكلفة بالداخلية
  - وزارة العدل
  - الوزارة المكلفة بالمواصلات السلكية واللاسلكية
  - تتولى المديرية العامة امانة المجلس.

ويكلف على الخصوص بممارسة المهام التالية: التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنسيق ذلك مع المؤسسات والهيئات الوطنية المعنية بهذا النوع من الاجرام، وتوجيه عمل الهيئة والإشراف عليه ومراقبته بالإضافة لدراسة كل مسالة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر اللجوء للمراقبة الوقائية للاتصالات الإلكترونية وضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه .

- يجتمع المجلس في دورة عادية مرتين (2) في السنة، بناء على استدعاء من رئيسه، ويمكنه ان يجتمع في دورة غير عادية كلما كان ذلك ضروريا، بناء على طلب من رئيسه أو بطلب من احد اعضائه أو من المدير العام للهيئة.
- المديرية العامة: يتولى إدارتها مدير عام وتتولى العديد من الصلاحيات تتمثل أهمها في العمل على حسن سير الهيئة الوطنية عن طريق ضمان تنفيذ برنامج عملها وتنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها وقيامه بتحضير اجتماعات مجلس التوجيه، بالإضافة لقيامها بتمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية ناهيك عن ممارسة السلطة السلمية على مستخدمي الهيئة والعمل على احترام قواعد حماية السر في الهيئة والقيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين

تمارس الهيئة العديد من المهام والمسؤوليات في ظل إحترام الأحكام التشريعية في مجال حقوق الانسان وحرياته الأساسية، تتمثل أساسا في إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

ومع صدور قانون التوقيع الإلكتروني وقانون التجارة الإلكترونية سنتي 2015 و2018 على التوالي، أصبح للهيئة دورا كبيرا في الكشف عن الجرائم المستحدثة التي قد تطال المعاملات الإلكترونية الإدارية والمالية الاقتصادية، وتداخل ذلك مع جرائم الفساد المالي والإداري، وهو ما عجل بصدور المرسوم 172/19 المذكور آنفا.

المعنيين في الهيئة مع إعداد التقرير السنوي لنشاطات الهيئة وعرضه على مجلس التوجيه للمصادقة عليه كما يعمل على ضمان التسيير الإداري والمالي للهيئة، وتضم المديرية العامة الأجهزة التالية:

- المديرية التقنية: تتكفل بالقيام بالعديد من المهام لضمان فعالية الهيئة نذكر منها على وجه الخصوص القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الإلكترونية من اجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، وإرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة بالإضافة لتنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم .

تتولى أيضا مهمة جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والعمل على تنظيم أو المشاركة في عمليات التوعية حول كيفية استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها ناهيك عن تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرة وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيره والحفاظ على الحالة الجيدة لمنشاته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة.

- مديرية الادارة والوسائل: تكلف على الخصوص بتسيير الموارد البشرية والوسائل والمالية الخاصة بالهيئة.

*- انظر المواد 4 وما بعدها من المرسوم الرئاسي 19-172 المشار اليه سابقا.

وتضطلع الهيئة في إطار مهمتها الأساسية في مكافحة الجرائم الماسة بالأنظمة والبرامج المعلوماتية بما يلي:[1]

- تنشيط وتنسيق عمليات المراقبة الوقائية لهذه المعاملات، إلى جانب مساعدة السلطات القضائية ومصالح الشرطة القضائية، من خلال جمع المعلومات والتزويد بها، ومن خلال الخبرات القضائية وتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم وتحديد مكان تواجدهم. [2]

---

[1]– أنظر المادة 14 من القانون 09–04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الاعلام والاتصال.

[2]–جرائم الاعتداء على التوقيع الإلكتروني إحدى ابرز صور الاجرام المعلوماتي المستحدث والتي تتميز بانها عابرة للحدود الوطنية، حيث يمكن ان يتعدى اثرها إلى عدة دول، لذا كان لا بد من وجود تعاون دولي لمكافحة هذا النوع من الاجرام، بحيث يسمح لأجهزة الشرطة في مختلف الدول بالاتصال المباشر بينها، لذلك اصبحت الحاجة ماسة إلى وجود كيانات دولية واقليمية تأخذ على عاتقها مهمة تبادل المعلومات المتعلقة بالجريمة والمجرمين وتعقب الجناة الفارين من العدالة، ومن اهم صور هذا التعاون الامني الأجهزة التالية:

– على المستوى الدولي: تعد المنظمة الدولية للشرطة الجنائية "الانتربول" من اهم الأجهزة على المستوى الدولي لمكافحة الاجرام بصفة عامة ومنها الجرائم المعلوماتية، تم انشاء هذه المنظمة سنة 1923، تحت اسم اللجنة الدولية للشرطة الجنائية وذلك للتنسيق بين أجهزة الشرطة في الدول الاوروبية في مجال مكافحة الجريمة، وتم ايقاف نشاطها إبان الحرب العالمية الثانية، ثم اعيد فتحها خلال مؤتمر فيينا تحت اسم " منظمة الشرطة الجنائية الدولية" سنة 1956، وهي تضم 177 دولة عضوا، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف عبر وسيلتين:

الأولى: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الموجودة في اقاليم الدول الأطراف.

= الثانية: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وفي مجال الجرائم المعلوماتية، تقوم المنظمة الدولية للشرطة الجنائية باعداد قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في مثل هذه القضايا، كما توفر هذه المنظمة للدول الأطراف المعلومات

- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجريمة المعلوماتية، وتكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال، وتحديث المعايير القانونية في مجال اختصاصها.

إجراءات سير وممارسة الهيئة لمهامها:

تجتمع الهيئة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها، إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه، حيث يتم تزويدها بقضاة وضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني، كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل.

اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين، ولقد انشات هذه المنظمة وحدة متخصصة في الجرائم المعلوماتية تقوم لتزويد أجهزة الشرطة التابعة للدول الاعضاء بارشادات حول التحقيق في هذا النوع من الاجرام وكيفية التدريب على مكافحته.

إلى جانب الانتربول، هنالك منظمات لها دور فعال في مواجهة هذا النوع المستحدث من الاجرام على المستوى الدولي، كمنظمة التعاون الاقتصادي والتنمية " OECD" ومجموعة الثمانية الاقتصادية (G8)، حيث قامت باعداد مؤتمر دولي في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية، تتمثل مهامها في تحقيق امن تكنولوجيا المعلومات.

–على المستوى الإقليمي: – الشرطة الأوروبية أو الانتربول: وهو جهاز على مستوى الاتحاد الاوروبي تم انشاؤه عام 1992 ومقره في مدينة لاهاي بهولندا لكي يكون حلقة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة لملاحقة الجناة في الجرائم العابرة للحدود، ومنها جرائم الاعتداء على التوقيع الإلكتروني.

وفي سنة 2010 استحدث جهاز على مستوى الاوروبول بمبادرة من الشرطة القضائية (Internet Crime Repportinge Online System)، بغرض التنسيق اكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الاعضاء.

– الاورجست: وهو جهاز يعمل على المستوى الاوروبي إلى جانب الاوروبول في مجال مكافحة الجرائم الخطيرة، تم انشاؤه عام 2002، وينعقد اختصاصه عندما تمس جريمة دولتين على الاقل من الدول الاعضاء في الاتحاد الاوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي. ويعد الاورجيست دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية، وخصوصا فيما يتعلق بالجرائم المعلوماتية، للتفصيل اكثر انظر:

Harmonisation des moyens de lute contre la cybercriminalité, revue de web, réalisé le 22-04-2004, disponible en ligne à l'adresse suivante: //www.finances.gouv.fr.

– بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، مرجع سابق، ص198.

يشارك في عملية مراقبة الاتصالات وغيرها من المعاملات الإلكترونية أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة، كما يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة بالاتصال مع المسئولين المعنيين في الهيئة من اجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.

يتم حفظ المعلومات المستقاة أثناء عملية المراقبة خلال حيازتها من الهيئة بالإضافة لتسجيل الإتصالات الإلكترونية التي تكون موضوع مراقبة وتحرر وفق الشروط والأشكال المنصوص عليها قانونا خاصة في إطار قانون الإجراءات الجزائية، إذ تسلم التسجيلات والمحررات إلى السلطات القضائية ومصالح الشرطة القضائية المختصة حيث تحتفظ دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع، إذ يجب عدم إستخدام المعطيات والمعلومات التي تستلمها أو تجمعها الهيئة لأية أغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. [1]

وفي إطار ممارستهم لوظائفهم أو بمناسبتها، يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعين للهيئة طبقا للتشريعات المعمول بها[2]، بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الإتصالات الإلكترونية، و في حال معاينة أفعال يمكن وصفها جزائيا تخطر الهيئة النائب العام المختص للقيام بالمتابعات المحتملة، إذ يمكن في هذا الصدد أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجالات تكنولوجيات الإعلام والإتصال.[3]

الفرع الثاني: مدى إستعانة الضبطية القضائية بمؤدي خدمات التصديق الإلكتروني

تطرقنا سابقا إلى مفهوم مقدمي الخدمات حسب نص المادة 2 فقرة د من القانون 09-04، ويدخل ضمن هذا التعريف مقدمي خدمات التصديق الالكتروني، الذين يقدمون خدماتهم إلى الجمهور

[1]- المواد من 11إلى14 من المرسوم الرئاسي 19-172، المنوه عنه سابقا.

[2]- حيث تنص المادة13 من المرسوم 19-172 أن :" تمارس المديرية التقنية مهامها المرتبطة بالشرطة القضائية وفقا لأحكام التشريع المعمول به، لا سيما الأمر 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية".

[3]- انظر المادة 13 من المرسوم 19-172.

في مجال المعاملات الإلكترونية المتنوعة، سواء في قطاع الإتصالات الإلكترونية أو في القطاع المالي الإقتصادي والإداري[1]، وهو ما يعكس من جهة، الأهمية البالغة لمقدم الخدمة الإلكترونية في مكافحة الجرائم الإلكترونية عن طريق تسهيل الوصول إلى الدليل الرقمي، ومن جهة ثانية، إتجاه المشرع إلى إلزام الأطراف المتدخلة في توفير الخدمات بتقديم المساعدات الضرورية للجهات القضائية المكلفة بالتحريات والتحقيقات تطبيقا لنص المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[2]، تحت عنوان: " التحفظ العاجل على البيانات المحزنة في تقنية المعلومات"، مما دفع بالدول الأطراف إلى تبني الإجراءات الضرورية لتمكين السلطات المخولة بالبحث والتحري من الحصول العاجل على المعلومات المخزنة لدى مزود الخدمة الموجودة تحت حيازته، وإلزامه في نفس الوقت بضرورة حفظ تلك المعلومات وصيانتها. [3]

وقد عرفت الإتفاقية الأوروبية لمكافحة الإجرام المعلوماتي مقدمي الخدمات بموجب المادة01/ج التي نصت على: " يقصد بمزودي الخدمات:

---

[1]– في تقرير نشرته سلطة الضبط البريد والاتصالات الإلكترونية سنة 2018منحت سلطة الضبط عدد كبير من التراخيص لمزودي خدمة النفاذ لشبكة الأنترنت لتغطية الطلب المتزايد على خدمة الشبكة العنكبوتية، لأكثر تفاصيل يرجى زيارة الموقع على الرابط الآتي:

https://www.arpce.dz/ar/obs/prest/?c=voipتاريخ الاطلاع: 2020/08/28 على الساعة:18.00.

[2]–الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 2010/12/21، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم: 14–252 المؤرخ في: 2014/09/08، ج.ر رقم: 57 المؤرخة في: 2014/09/28.

[3]–تنص المادة (23) من (ا.ع.م.ج.ت.م) على:

"1– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة منى إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين، والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد ان تلك المعلومات عرضة للفقدان أو التعديل .

2– تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من اجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن اجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من اجل تمكين السلطات المختصة من البحث والتقصي.

3– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي ".

- أي كيان عام أو خاص الذي يوفر لمستخدميه القدرة على التواصل من خلال النظام المعلوماتي.
- أي كيان آخر يقوم بمعالجة أو تخزين البيانات الحاسوبية لخدمة الإتصالات أو لحدمة مستخدميه...". [1]

كما عرف المشرع الجزائري مقدمي الخدمات من خلال المادة 02/د من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها:"

- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام إتصالات.
- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها ".

وأشار القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين إلى مؤدي خدمات التصديق الإلكتروني كما سبق تفصيله في بداية البحث، من خلال المادة (2) فقرة 11و12 وهم على التوالي:

- **الطرف الثالث الموثوق:** " شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي".
- **مؤدي خدمات التصديق الإلكتروني:** " شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني".[2]

---

[1]–Article 1-Definitions

Aux fins de la présente Convention, l'expression…

c. « fournisseur de service » désigne:

i. Toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

ii. Toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs, convention européenne de la cybercriminalité, Op.Cit,p.3.

[2]–اكثر تفاصيل، راجع الباب الأول من البحث عند دراستنا لمفهوم مؤدي خدمات التصديق الإلكتروني، ص 27.

وفي نفس السياق عرفت المادة 6 من قانون التجارة الإلكترونية الجزائري 05/18 في فقرتها الرابعة عند تعريفها للمورد الإلكتروني بأنه: " كل شخص طبيعي أو معنوي يقوم بتسويق أو إقتراح توفير السلع أو الخدمات عن طريق الإتصالات الإلكترونية".

وتضمن قانون الحياة الخاصة في مجال الإتصالات الإلكترونية الأمريكي أو ما يسمى بقانون الخصوصية لسنة 1974[1]، نوعين من مزودي الخدمات، الأول مزودوا خدمة الإتصالات الإلكترونية، وهم من يقدمون خدمة إلى مستخدمي الشبكة، مثل تسهيل وإرسال واستقبال الإتصالات السلكية واللاسلكية والإلكترونية، والثاني مزودوا خدمة معالجة المعلومات عن بعد. ويثار التساؤل عن مدى التزام مزودي الخدمات الذين يقدمون خدماتهم للجمهور ألا يقوموا بإفشاء أية معلومات إلى الغير، إلا أن هذا الالتزام ليس على إطلاقه من الحذر، إذ أوجبت بعض التشريعات المقارنة إلتزامهم بالتعاون مع رجال القضاء.[2]

أولا: طرق إلزام مؤدي الخدمات بالكشف عما لديهم من بيانات لرجال الضبط القضائي:

1. الالتزام بالاحتفاظ بالبيانات وتقديم المعلومات:

أوكل المشرع الجزائري مهمة الاحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق ومؤدي خدمات التصديق الإلكتروني إلى السلطة الحكومية للتصديق الإلكتروني، والسلطة الاقتصادية للتصديق الإلكتروني على التوالي، بغرض

[1]– سوزان عدنان، إنتهاك الحياة الخاصة عبر الأنترنت، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد29، العدد الثالث، 2013.

[2]– في الولايات المتحدة الأمريكية يوجب قانون حماية الحياة الخاصة في مجال الاتصالات الإلكترونية على مزودي الخدمات الذين يقدمون خدماتهم للجمهور الكشف عما لديهم من معلومات للجهات العامة في بعض الحالات ومن هذه الحالات تعلق تلك المعلومات بارتكاب جريمة أو حالة الاستعجال مثل خطر الموت أو إيذاء جسمي يهدد الأشخاص كما يوجب قانون الإجراءات الجنائية الفرنسي على الجهات العامة أو الأشخاص المعنوية الخاصة ان تضع تحت تصرف رجال الضبط القضائي البيانات التي تساعد في الكشف عن الحقيقة، راجع ياسر ابو حطب، مرجع سابق، ص229.

تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء طبقا للأحكام التشريعية والتنظيمية المعمول بها. [1]

وفي السياق ذاته ألزم المشرع مقدمي الخدمات تقديم المساعدة للسلطات القضائية المكلفة بالتحريات القضائية وفقا للمادة (10) من القانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، التي نصت على: " في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

وتشمل المساعدات المقدمة من قبل مؤدي خدمات التصديق الإلكتروني في مجال التوقيع الإلكتروني، المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات والبرامج المعلوماتية المستعملة في إنشاء آلية التوقيع الإلكتروني، وبيانات التحقق من التوقيع الإلكتروني، وتاريخ ومدة صلاحية كل شهادة تصديق إلكترونيةبالإضافة إلى الموقع وصاحب شهادة التصديق الإلكتروني. [2]

---

[1]–انظر المواد (27) و(28) و(29) و(30) من القانون 15–04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[2]–يجيز قانون الإجراءات الجنائية الأمريكي لسلطات البحث والتحري تكليف مزودي الخدمات تقديم المعلومات، ولكن قد يسبق ذلك توجيه إخطار إلى المشترك والمتعامل معه قبل إلزام مزودي الخدمات بتقديم تلك المعلومات، فإذا كان من شان هذا الإخطار التأثير على سير التحقيق فان القانون أجاز لسلطات الضبط القضائي بتأخير هذا الإخطار. وإذا كان هذا هو الوضع في القانون الأمريكي فان التشريعات ذات الاصل اللاتيني لا تجيز هذا الحق لسلطات الضبط القضائي وانما تجيزه لسلطة التحقيق، وكذلك في القانون المصري وفقا لما نصت عليه المادة 99 إجراءات جنائية على انه: " لقاضي التحقيق ان يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه..."، ومن ثم تطبق في شانه حكم المادة 284 إذا ما خالف هذا الأمر، كما ان للنيابة العامة ذات السلطة وللمحكمة أيضا ان تصدر هذا الأمر فالمادة 281 من قانون الإجراءات الجنائية المصري تنص على ان للمحكمة ان تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة.

وحسنا فعل المشرع الجزائري، لأن من شأن تقديم المساعدات من قبل مؤدي الخدمات تسهيل مهمة أجهزة البحث والتحري لكشف أي اعتداء يقع على آليتي التوقيع والتصديق الإلكترونيين وكشف المجرمين في هذه البيئة الافتراضية.

2. الحصول على إذن تفتيش:

يتم ذلك من خلال حصول ضابط الشرطة القضائية على إذن بالمراقبة وفق أحكام قانون الإجراءات الجزائية[1]، ويلزم مزود الخدمات في هذه الحالة بالتعاون معه في إجراء تلك المراقبة، وله أيضا ان يستصدر إذنا للاطلاع على البيانات والاتصالات المخزنة لدى مزودي الخدمة وضبطها . ولكن هل يجوز لمزودي الخدمات مراقبة آليتي التوقيع والتصديق الإلكترونيين كنظام معلوماتي دون إذن قضائي مسبق؟

إن الإجابة على هذا التساؤل وجد صداه في بعض التشريعات المقارنة بنصوص صريحة والأخرى تركت الأمر للقواعد العامة. وفي هذا الصدد لم تتم الإشارة من المشرع الجزائري إلى إمكانية الاطلاع على النظام المعلوماتي الخاص بآليتي التوقيع والتصديق الإلكترونيين من قبل مؤدي خدمات التصديق الإلكتروني أو من قبل الطرف الثالث الموثوق بعد منح التوقيع الإلكتروني أو شهادة التصديق الإلكتروني، تاركا للسلطتين الحكومية والاقتصادية للتصديق الإلكتروني ضبط نشاط التصديق الإلكتروني[2]، بينما أعطى المشرع الأمريكي فيما يتعلق بالمراقبة المعتادة للمعاملات الإلكترونية على شبكة الأنترنت إستثناءا لمزودي الخدمات الحق في مراقبة المشتركين في خدماتهم من خلال معرفة ما يقوم هؤلاء المشتركون من نشاط الاطلاع غير المشروع على أجهزة الآخرين أو تخزين مواد مخالفة للقانون.

---

[1]– ادرج المشرع الجزائري قواعد إجرائية جديدة على قانون الإجراءات الجزائية بهدف جعله يتطابق مع ما جاء في المواثيق والاتفاقيات الدولية في هذا المجال، تتمثل اساسا في أساليب واليات حديثة للبحث والتحري عن الجرائم الإلكترونية، وهذا بموجب القانون رقم: 06–22 المؤرخ في: 2006/12/22 يعدل ويتمم قانون الإجراءات الجزائية، لاسيما المادة (65مكرر05– 65مكرر10)، وسيتم تفصيل ذلك عند تناول أساليب البحث والتحري في الجرائم الواقعة على التوقيع الإلكتروني في قادم البحث.

[2]–انظر المواد (28) و(30) من القانون 15–04 السالف ذكره.

والقانون الأمريكي عندما يقرر هذا الإستثناء فانه يراعي حقوق مزودي الخدمات في مواجهة المشتركين في الخدمات التي يقدمونها بمقابل أو الذين يستعملون تلك الخدمات حتى يمكنهم من الأداء اليومي لأجهزتهم ومعداتهم، ومن ثم فان القانون الأمريكي يسمح لهم بتسجيل هذه التجاوزات والتبليغ عنها لرجال الضبط القضائي، ولا يجوز لرجال الضبط القضائي ان يقوموا بتلك المراقبة دون بلاغ من مزودي الخدمات أو سبق حصولهم على إذن بذلك. [1]

وإذا كان القانون الأمريكي قد أعطى لمزودي الخدمات الحق السالف إستثناءا، فانه لا يطلقه على عنانه إذ يتعين إقامة التوازن ما بين مصالح متعارضة وهي مصلحة مزود الخدمات ومصلحة المشتركين والمستعملين لتلك الخدمات، مما حذا بالمحاكم الأمريكية إلى إعمال معيار المعقولية كلما توفرت ظروف معقولة تدعو إلى الاعتقاد بوجود تهديد لمصالح مزودي الخدمات، كما أجاز لهم القانون تلك الرقابة، ويستبين من تلك الأحكام أن القانون الأمريكي يجيز لمزود خدمات الإتصالات السلكية هذه السلطة في الرقابة والكشف عن محتوى الإتصال بالإضافة إلى مزودي خدمات الكمبيوتر. [2]

ويتضح مما سلف انه من حق مزودي الخدمات الرقابة المعتادة لمتابعة العمل اليومي لشبكتهم وإصلاح ما بها من أعطال دون سبق الحصول على إذن بذلك نظرا لطبيعة الخدمات التي يؤدونها، وبالتالي فان إكتشافهم وقوع جريمة يعطيهم الحق في إبلاغ رجال الضبط القضائي عنها ولا يشوب الإجراءات عندئذ بطلان يصيب الحكم السابق بالإدانة. [3]

هذا من ناحية ومن ناحية أخرى فهل يجوز لمقدمي الخدمات إذا ما إشتكى اليهم أحد المشتركين من مشكلات تخل بعمل الجهاز الخاص به أن يقوم بمراقبة الرسائل الواردة إلى هذا الجهاز محل الشكوى دون إذن؟

في الواقع إنه إذا كان الأصل عدم جواز مراقبة الإتصالات الإلكترونية والإتصالات السلكية إلا بإذن قضائي، حسب أحكام المادة (119) من القانون 04/18 المحدد للقواعد العامة المتعلقة

---

[1]–ياسر محمد ابو حطب، مرجع سابق، ص230.

[2]– حسن إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه، دار النهضة العربية، 2006، ص137.

[3]–ياسر محمد أبو حطب، مرجع سابق، ص231.

بالبريد والإتصالات الإلكترونية[1] التي نصت على: " يلزم متعاملوا الإتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض إعتراض الإتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقا للتشريع المعمول به، ويجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها وعلى العقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام"، فان القانون الأمريكي يسمح بالخروج على هذا في حالة الطلب الصادر من صاحب الجهاز محل الإعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي وبالتالي فان هذا الإستثناء يسمح لمقدم الخدمات بأن يقوم بذلك شريطة توافر أربع شروط مجتمعة هي[2]:

- أن يسمح المالك لرجل الضبط بوضع الجهاز الخاص به تحت المراقبة .
- أن يتم ذلك في إطار تحقيق جنائي قائم .
- أن تتوافر دلائل كافية على أن تسجيل الإتصالات القادمة من الجهاز الصادر منه الإعتداء يفيد في كشف الحقيقة.
- أن يقتصر رجال الضبط القضائي على اعتراض الإتصالات الصادرة من وإلى الأجهزة محل التحقيق.

وفي تحديد مفهوم "المعتدي على النظام"، يستبعد القانون الأمريكي من هذا المفهوم كل من تربطه علاقة تعاقدية مع مقدم الخدمة، والذي يتجاوز الحدود التي تسمح بها تلك العلاقة (المادة (21) &U.S.C 2511). [3]ومثال ذلك مستخدمو شركة معينة لا يعتبرون في عداد المعتدين على النظام إذا استغلوا أجهزة الشركة في غير أغراض مشبوهة أو في غير أوقات العمل بالمخالفة لنظام الشركة، على عكس القانون الكندي الذي اعتبر أنعمل مقدمي الخدمات يدخل ضمن أعمال السلطة العامة التي

[1]–القانون 18– 04 المؤرخ في 10ماي2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، (ج.ر) عدد: 27 المؤرخة في 13ماي2018.

[2]–شيماء عبد الغني عطا لله، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص260 وما بعدها.

[3]–United State Code Sec.2511. – Intrception and disclosure of wire , oral, or electronic communications prohibited

يشترط فيها الإذن المسبق من السلطة القضائية لمباشرة أي رقابة أو تسجيل، وأن القيام بذلك دون إذن فيه مخالفة لأحكام المادة (42 فقرة 2) من ميثاق الحقوق والحريات الكندي. [1]

المطلب الثاني:

أساليب البحث والتحري المستحدثة في الكشف عن جرائم التوقيع الإلكتروني

لم يكتف المشرع الجزائري في إطار سياسته الجنائية لمكافحة الإجرام المعلوماتي بإستحداث الأجهزة الشرطية المختصة في هذا المجال وإحاطة أفرادها بالتكوين اللازم، بل دعم هذه السياسة بتطوير إجراءات التحقيق والتحري التقليدية وتمكن رجال الشرطة القضائية من جمع الأدلة والتوصل إلى مرتكبي الجريمة بالسرعة والدقة اللازمتين[2]، وهي الإجراءات المنصوص عليها في القانون

---

[1]–الميثاق الكندي للحقوق والحريات هو تشريع دستوري في كندا، ألحِق بالدستور الكندي على شكل الفصل الأول منه واعتبرت بنود الدستور السابقة كفصل ثاني وذلك في 17 نيسان 1982. وقد تبنى الميثاق وعمل إلى إخراجه إلى النور السياسي ورئيس الوزراء الكندي آنذاك بيير ترودو، للتفصيل اكثر في بنود الميثاق يرجى الاطلاع على موقع ويكيبيديا: https: //ar.wikipedia.org

[2]– يمكن إجمالها فيما يلي:

– إجراء تلقي الشكوى والبلاغات سواء بالطرق التقليدية أو عبر الأنترنت، حيث نصت المادة (17) من قانون الإجراءات الجزائية على: " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية ...".

– كما نصت المادة (18) من نفس القانون على: " يتعين على ضباط الشرطة القضائية ان يحرروا محاضر بأعمالهم وان يبادروا بغير تمهل إلى اخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى عملهم...".

في هذا الاطار قامت قيادة الدرك الوطني بإطلاق خدمة عمومية جديدة عبر 48 ولاية باستعمال تكنولوجيات الاعلام والاتصال تحت اسم " الشكوى المسبقة والاعلام عن بعد ". تدخل هذه الخدمة في اطار عصرنة وسائل تنفيذ مهام وحدات الدرك الوطني والتكفل الجيد بشكاوي المواطنين . وتأتي بهدف تعزيز العمل الجواري المنفذ من طرف الدرك الوطني لصالح المواطنين مستعملي الأنترنت خاصة في ظل الانتشار المتزايد للجرائم الإلكترونية بالاستفادة من تطور تكنولوجيات الاعلام والاتصال. حيث يمكن هذا التطبيق المنجز من طرف مهندسي الاعلام الالي للدرك الوطني المواطنين من ايداع البلاغات والشكاوي المسبقة عن طريق الأنترنت وتأكيدها بعد ذلك لدى وحدة الدرك الوطني المعنية في غضون 30 يوما، مما يمكن أجهزة الضبطية القضائية من ربح الوقت والسرعة في البدء في إجراءات البحث والتحري بخصوص الكشف عن الجريمة الإلكترونية قبل ان يتمكن المجرم الإلكتروني من تدمير الدليل والافلات من

06_22 والقانون 09_04 السالف ذكرهما وبعض القوانين الخاصة تمحورت حول إجرائين هامين يتم تناولهما في فرعين اثنين على النحو التالي:

- **الفرع الأول:** اعتراض المراسلات وتسجيل الاصوات والتقاط الصور.
- **الفرع الثاني:** التسرب.

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

إستحدث المشرع الجزائري إجراء إعتراض المراسلات[1]، وتسجيل الأصوات والتقاط الصور في الفصل الرابع من القانون 22/06 المؤرخ في 2006/09/20 المعدل والمتمم لقانون الإجراءات الجزائية، تناول فيه تنظيم هذا الإجراء من حيث مجالات تطبيقه وضمانات إستخدامه .

وتندرج بيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني ضمن المراسلات محل عملية الاعتراض والمراقبة الإلكترونية، بالنظر إلى تعريف الإتصالات الإلكترونية الوارد في القانون 04/18 المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية في مادته (10 فقرة 1) والتي نصت على: "إتصالات إلكترونية: كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة

العقاب، للاطلاع اكثر على تفاصيل هذه الخدمة، يرجى الدخول على الموقع الرسمي لقيادة الدرك الوطني على الرابط التالي: https://ppgn.mdn.dz/prep.php، تاريخ الاطلاع: 2019/07/04 الساعة: 18:30.

– اجرء المعاينة والخبرة التقنية في البيئة الإلكترونية وفقا للمادتين (42) و(79) من (ق.ج.ج).

– إجراء الشهادة وفقا لأحكام القسم الرابع من الفصل الأول من الباب الثالث تحت عنوان: " سماع الشهود المواد: (88–99) من (ق.ا.ج.ج)، والتي تتلخص حول استدعاء الشهود وحضورهم وكيفية تلقي افادتهم وحلف اليمين والحالات التي لا يجوز فيها سماع الشخص كشاهد ونصاب الشهادة...الخ.

– إجراء التلبس في مجال الجرائم الإلكترونية وفقا لأحكام المواد: (41)، (49)، (50)، (61) من (ق.ا.ج.ج).

– راجع الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات _ قانون العقوبات _ قانون الإجراءات الجزائية _ قوانين خاصة، مرجع سابق، ص 311 ص 358 .

[1]–عرفت لجنة خبراء البرلمان الاوروبي بمناسبة اجتماعها المنعقد بسترسبورغ في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها " عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في اطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة".

كهرومغناطيسية "، وهو نفس ما جاءت به أحكام المادة (2 فقرة 9) من القانون 04/09 التي عرفت الاتصالات الإلكترونية بأنها: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صدور أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، وكذا المادة (65 مكرر 5) من (ق.ا.ج.ج) التي تنص على: " إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجرائم المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من اجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...".

أولا: إجراءات اعتراض المراسلات

- تنفذ هذه الإجراءات بموجب إذن مسلم من وكيل الجمهورية ويخص فقط التحري في الجريمة المتلبس بها أو التحقيق الابتدائي الخاصة بالجرائم المتعلقة بالمخدرات، الجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال وتمويل الإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.
- يسمح هذا الإذن الممنوح من قبل وكيل الجمهورية لغرض وضع الترتيبات التقنية، بالدخول إلى المحلات السكنية أو غيرها خارج المواعيد القانونية، وبغير علم أو رضا الأشخاص الذين لهم الحق على تلك الأماكن، وذلك تحت المراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي يتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة، على عكس المشرع الفرنسي الذي أورد إستثناءات في هذا الشأن بموجب المادة (96/706) من قانون الإجراءات الجزائية الفرنسي نذكر من بينها: المؤسسات الإعلامية والمحلات ذات الطابع المهني للأطباء وسيارات النواب والمحامين وغيرها من المؤسسات الرسمية. [1]

[1]– Article 706-96 du (CPPF):

- يسلم الإذن سواء الممنوح من طرف وكيل الجمهورية أو قاضي التحقيق لمدة أقصاها أربعة (04) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق. [1].
- يؤهل الإذن المشار إليه ضباط الشرطة القضائية تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات[2]، وكذا مترجم لترجمة المكالمات التي تتم باللغات الأجنبية، كما يلزم القانون ضابط الشرطة القضائية المأذون له بإجراء هذه العمليات تحرير محضر عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية والالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري كما يجب على ضابط الشرطة القضائية وصف أو نسخ المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة على محضر يودع بملف القضية. [3]

"Losque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application des articles 706/73 et 706/73/1 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et les agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressées, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction…

La mise en place du dispositif technique mentionné au premier alinéa ne peut concerner les lieux visés aux articles 56/1,56/2 et 56/3 ni être mise en œuvre dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100/7… ".

[1]–تنص المادة (65مكرر7) من (ق.ا.ج.ج) على: " يجب ان يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها . يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

[2]–حيث تنص المادة (65 مكرر 8) من نفس القانون على: " يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي إذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه، ان يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالعمليات التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه".

[3]–انظر المادتان (65 مكرر9– 65 مكرر10) من نفس القانون.

ثانيا: تسجيل الأصوات

يعرف تسجيل الأصوات بأنه 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 للإستماع إليه مرة أخرى. [1]

وهو إجراء تحقيقي تأمر به السلطة القضائية خلسة وينتهك سرية الأحاديث الخاصة بغية الحصول على دليل غير مادي للجريمة. [2]

وبالرجوع إلى نص المادة (65 مكرر 5) من (ق.إ.ج.ج) التي أوردت الوقائع التي يجوز فيها تسجيل الأصوات على سبيل الحصر في إطار ممارسة عملية البحث والتحري والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تتضح أهمية الإجراء في كشف أي إعتداء على البيانات الرقمية للتوقيع الإلكتروني أو شهادة التصديق الإلكتروني، حيث أجاز المشرع وضع الترتيبات التقنية دون علم وموافقة المعنيين من أجل تسجيل الحديث المتفوه به في الأماكن العامة أو الخاصة.

وتتمثل إجراءات تسجيل الأصوات وفق المادة (65 مكرر 5) سالفة الذكر في:

- منح الإذن القضائي من قبل وكيل الجمهورية أو قاضي التحقيق حسب الحالة. [3]
- تتم عملية تسجيل الأصوات بتسخير أعوان مصالح الإتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية وفقا لنص المادة (65 مكرر 8) السابق ذكرها وإلزام ضابط الشرطة القضائية المختص بتحرير محضر عن كل عملية تسجيل الأصوات.

---

[1]–جميلة محلق، مرجع سابق، ص 178.

[2]–حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث متوفر على الموقع الرسمي لمجلة القانون والأعمال لسنة 2015 على الرابط الاتي: http: //w.w.w.droitentreprise.com تاريخ الاطلاع 2019/07/09 على الساعة 16: 15.

[3]–انظر المواد (65 مكرر 5) و(65 مكرر 7) من (ق.إ.ج.ج).

ثالثا: التقاط الصور

لم يتطرق المشرع الجزائري إلى تعريف إجراء التقاط الصور إنما عبر عن هذه العملية في المادة (65 مكرر 5) بعبارة الالتقاط. [1]ويقوم هذا الإجراء على المعاينة المادية المرئية لحالة شخص أو عدة أشخاص مشتبه فيهم، على الحالة التي كانوا عليها وفق التصوير وإستعمال محتوى الفيلم كدليل مادي للإثبات، على خلاف إجراء تسجيل الأصوات الذي أخذ فيه المشرع الجزائري بمعيار طبيعة المكان، سمح المشرع لعملية التصوير أن تصل إلى الأماكن الخاصة والسرية للمعنيين بالمراقبة من أجل إجلاء الحقيقية وكشف المجرمين.[2]

وتجدر الإشارة إلى أن إجراءات التقاط الصور لا تختلف عن باقي الإجراءات كاعتراض المراسلات وتسجيل الأصوات إن من حيث تحديد مجال التصوير أو الإذن القضائي أو سيرورة العملية.

الفرع الثاني: التسرب الإلكتروني:

استحدث إجراء التسرب في قانون الإجراءات الجزائية الجزائري بموجب المواد من 65 مكرر 11 إلى 65 مكرر 18من القانون 22/06، حيث خول ضباط وأعوان الشرطة القضائية إمكانية قيامهم تحت مسؤولية ضابط الشرطة قضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم بأنه فاعل معهم أو شريك لهم أو خاف. [3]

---

[1]–حيث نصت المادة (65 مكرر 5) على ما يلي: "... التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ...".

[2]–تتم عملية التقاط الصور بتسخير اعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة، من بينهم مزودوا خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق وكذا السلطة الاقتصادية للتصديق الإلكتروني للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية التقاط الصور، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها، وهذا بموجب المادتين (10/9) من (ق.ا.ج.ج).

[3]– تنص المادة (65 مكرر12) من (ق.ا.ج.ج) على: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك لهم أو خاف. يسمح لضابط أو عون الشرطة القضائية ان يستعمل لهذا الغرض

وتتسم عملية التسرب بالتعقيد، بإعتباره من إجراءات البحث والتحري الخاصة، يمكن تصورها في نطاق الجرائم الإلكترونية عامة وجرائم الإعتداء على التوقيع الإلكتروني بصفة خاصة، حيث ينخرط ضابط أو عون الشرطة القضائية في مجموعات أو نوادي الهاكر المتخصصة في إختراق شبكات الإتصالات الإلكترونية والنظم المعلوماتية بإستخدام أسماء وصفات مستعارة وهمية قصد الإيقاع بالمجرم المعلوماتي. [1]

وفي هذا الإطار أحاط المشرع الجزائري هذا الإجراء بمجموعة من الضوابط الشكلية والموضوعية نظرا لخطورته على حرمة الحياة الخاصة للأفراد يمكن إجمالها فيما يلي:

- يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد. [2]
- إن عملية التسرب تخضع تحت طائلة البطلان لإذن كتابي من طرف وكيل الجمهورية أو قاضي التحقيق حسب الحالة تذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية

هوية مستعارة وان يرتكب عند الضرورة الافعال المذكورة في المادة (65 مكرر 14) ادناه، ولا يجوز تحت طائلة البطلان، ان تشكل هذه الأفعال تحريضا على ارتكاب الجرائم".

– في هذا الصدد تطرقت العديد من التشريعات إلى إجراء التسرب باعتباره وسيلة فعالة في مجال البحث والتحري عن الجرائم، من بينها القانون الفرنسي الذي نص عليه بموجب المواد من (706/81) إلى (706/87) من (ق.ا.ج.ف) نذكر على سبيل المثال:

Article 706/81 du (cppf):

"Lorsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champ d'application des articles 706/73 et 706/73/1 le justifient, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leur contrôle respectif, à une opération d'infiltration dans les conditions prévues par la présente section".

[1]–براهيمي جمال، التحقيق في الجرائم الإلكترونية، اطروحة دكتوراه، جامعة مولود معمري تيزي وزو، كلية الحقوق، 2018، ص85.

[2]–انظر المواد من (65 مكرر 11) و(65 مكرر 15) من (ق.ا.ج.ج)

ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته ويحرر بهذا الإذن مدة عملية التسرب والتي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن تجديدها حسب مقتضيات التحري والتحقيق كما يجوز للقاضي الذي رخص بها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب

- إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديدها يمكن للعون المتسرب مواصلة المهمة للوقت الضروري الباقي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن لا يتجاوز ذلك مدة أربعة 04 أشهر، وإذا انقضت مدة أربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه يجب إخبار القاضي المرخص الذي يستطيع أن يرخص بتمديدها لمدة أربعة أشهر أخرى على الأكثر، للإشارة فإنه يجوز سماع ضابط الشرطة القضائية الذي تجري العملية تحت مسؤوليته دون سواه لوضعه شاهد عن العملية، كما يرتب القانون عقوبات جزائية على كل من يكشف هوية ضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. [1]

يسمح القانون لضابط أو لعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأعمال التالية:

- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها.
- إستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين أو الإيداع أو الحفظ أو الإتصال. [2]

[1]–انظر المادة (65 مكرر16) من (ق.ا.ج.ج).

[2]–انظر المادة (65 مكرر14) من (ق.ا.ج.ج).

المبحث الثاني:

الإجراءات التقنية للإثبات الجنائي في الجرائم الواقعة على التوقيع الإلكتروني

يخضع التحقيق الجنائي في الجرائم المعلوماتية إلى قواعد علمية ثابتة، تحكمه إجراءات قانونية تستلزم الامتثال والتطبيق الحرفي، وقواعد تقنية متزنة تحتم على المحقق إضفاء خبرته ومهاراته، مواكبا في ذلك التطور السريع للجريمة الإلكترونية وتطور أساليب ارتكابها.

وبإعتبار الجرائم الواقعة على التوقيع الإلكتروني من الجرائم المستحدثة التي تتطلب إعمال إجراءات تقنية يتطلبها التحقيق الجنائي حتى يتحقق الدليل اللازم للإثبات، وجب التعرض إلى الإجراءات التقنية للإثبات الجنائي في هذه الجرائم من خلال مطلبين، يتناول المطلب الأول مبادئ وإجراءات جمع الدليل الجنائي في جرائم التوقيع الإلكتروني، بينما يعالج المطلب الثاني وسائل الإثبات التقنية في الجرائم الواقعة على التوقيع الإلكتروني.

المطلب الأول:

مبادئ وإجراءات جمع الدليل الجنائي في جرائم التوقيع الإلكتروني

تتسم إجراءات الاستدلال في مجال جرائم التوقيع الإلكتروني بذاتية خاصة، ويبدو ذلك من خلال الطابع الخاص لهذه الجرائم وتطور أساليب ارتكابها، مما يضع سلطة التحقيق أمام تحدي مواكبة تطور وسائل التحقيق والإثبات الجنائي وضرورة الاستعانة بالأساليب العلمية الحديثة واستخدام الحاسب الآلي وشبكة الأنترنت، سواء عند المعاينة الأولية للظروف المحيطة بالجريمة الإلكترونية المرتكبة، أو ما يتبع ذلك من تحفظ فوري على الدليل الإلكتروني المستمد من بيانات التوقيع الإلكتروني في هذه المرحلة من التحقيق، وفيما يلي نعرض لكيفية جمع الاستدلالات في جرائم التوقيع الإلكتروني من خلال التعرف على العناصر الأساسية لجمع الاستدلالات في جرائم التوقيع الإلكتروني في الفرع الأول، ثم تتناول إجراءات المعاينة التقنية في هذه المرحلة في الفرع الثاني ونتعرف في الفرع الثالث على إجراءات التحفظ على الأدلة والقرائن ذات الصلة بالاعتداء الحاصل على التوقيع الإلكتروني .

الفرع الأول: العناصر الأساسية لجمع الاستدلالات في جرائم التوقيع الإلكتروني

يتعين قبل مباشرة أي تحقيق جنائي يتعلق بمختلف الإعتداءات الإجرامية الواقعة على آلية التوقيع الإلكتروني الموصوف أو شهادة التصديق الإلكتروني الموصوفة مراعاة جهات التحقيق لإجراءات وقواعد أساسية قبل أو أثناء هذا التحقيق[1]، تتمثل في جمع اكبر قدر من المعلومات عن السلوك المكون للجريمة وأسلوب وظروف ارتكابها، ووسيلة الحصول على تلك المعلومات يمكن أن يتم عن طريق مقابلات مع المجني عليه، وبناء على طبيعة السلوك الإجرامي المرتكب يتحدد نطاق وتوقيت هذا التحري والوقت الذي يستلزمه، إلا أن هناك من الاعتبارات ما يتعين وضعها في الحسبان عند تنفيذ ذلك وأهمها ما يلي: [2]

- أن الدليل المستند إلى المعالجة الآلية للبيانات يمكن أن يكون متاحا لفترة قصيرة من الزمن .
- أن الجريمة التي يجرى التحري بشأنها يمكن أن تكون مستمرة من حيث نتائجها أو تنفيذها.
- أن الجريمة التي يجرى التحري بشأنها يمكن أن تكون تغطية لفعل إجرامي آخر.

وإذا ما توافرت أدلة أن هذا هو الوضع، فقد يكون من الضروري البدء على الفور في إجراء تحقيق أكثر دقة حول الواقعة والحقائق المفترض إسهام التحري الأول في إظهارها وهي:

- التثبت من وقوع الجريمة.
- نمط وطبيعة الجريمة المرتكبة.
- التقنيات المستخدمة في ارتكابها.
- الجاني (أو الجناة) المحتملون أو المشتبه فيهم.
- الأسباب والدوافع المحتملة لارتكاب الجريمة.
- الاستدلال على الشهود في حالة وجودهم.
- طبيعة الأدلة الجنائية ومصادرها.

---

[1]–جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص119

[2]– هشام محمد فريد رستم، الجوانب الإجرائية للجريمة المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط 1994 ص 106، 105 .

وعند بدء التحقيق مع الأشخاص ذوي العلاقة بجرائم التوقيع الإلكتروني تتبع الخطوات التالية:[1]

- قبل البدء في اخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين يقوم ضابط الشرطة القضائية وخبير الحاسب الآلي بتبادل المعلومات فيما بينهم بحيث يشرح الضابط للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم.
- يتم حصر النقاط المطلوب استيضاحها من قبل الخبير والضابط المحقق ومن ثم يتولى الضابط ترتيب تلك النقاط.
- يقوم ضابط الشرطة القضائية بالحصول على كافة المصطلحات التي يمكن إستخدامها مع بيان لمعاني تلك المصطلحات للاستفادة منها عند الضرورة.
- يضع الضابط خطة التحقيق على ضوء المعطيات الأخرى التي يراها.
- مباشرة إجراءات اخذ أقوال الشهود واستجواب المتهمين من قبل الضبطية القضائية، وبحضور الخبير والذي يجوز له توجيه الأسئلة التقنية أثناء الاستجواب وذلك وفق كيفية تم الإتفاق عليها ويفضل أن يكتب الخبير السؤال التقني على ورقة يضعها أمام ضابط الشرطة القضائية ليحدد الأخير الوقت الذي يوجه فيه ذلك السؤال، كما أنه من الممكن إتاحة الفرصة للخبير بعد انتهاء الضبطية القضائية من إستجوابه.
- مراعاة القوانين الوطنية فيما يتصل بسلطة التحقيق، والمدى المسموح به للخبير في مشاركة الضبطية القضائية وحضور الاستجواب، ومن الأنسب في حالة الدول التي لا تسمح قوانينها بمثل هذه المشاركة إستصدار قرارات بتشكيل لجان تحقيق تضم في عضويتها الخبرات الفنية المطلوبة في كل حالة.
- مراعاة التنسيق بين الضابط المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالمتهم أو الشاهد الذي يتم التحقيق معه إذ أن المجرم المتخصص في جرائم الحاسب الآلي يحتفظ بمعلوماته وخططه في الحاسب الآلي أو على أقراص مدمجة أو اسطوانة مرنة، ويمكن للمحقق والخبير أن يتوصلا إلى تلك البيانات وأساليب فتحها من

[1]– محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر "القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، العين في الفترة ما بين 1 و3 ماي 2000، " ص358 وما بعدها.

خلال التحقيق مع الأشخاص ذوي العلاقة بجرائم التوقيع الإلكتروني، علما بان اقل خطا في مثل هذه الحالات يقضي على كافة البيانات المخزنة في الحاسب الإلكتروني. [1]

وهناك قواعد عامة ينبغي مراعاتها لضمان نجاح التحقيق مع الأشخاص ذوي العلاقة بالحاسب الآلي وهي:

- مراعاة التعامل بين ضابط الشرطة القضائية وخبراء الحاسب الآلي العاملين في المؤسسة المتضررة من الجريمة فقد يكون خبراء المؤسسة شهود، أو متهمين، أو مساهمين في الجريمة عن قصد، أو جهل، أو إهمال.
- التركيز في البحث عن البرامج اللازمة لكشف البيانات المخزنة ووضع تدابير للمحافظة عليها وحسن استخدامها.
- مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغير ذلك من الحقوق الخاصة تفاديا لأي طعن بعدم مشروعية الأدلة التي يحصل عليها المحقق.
- العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها (Softwear) وبرامجها.
- مراعاة حفظ الأدلة الجنائية بالطرق المناسبة لكل حالة وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها إذ أن أي تأثير أو تعديل للأدلة قد ينهي القضية لصالح المتهم الذي يفسر الشك لصالحه كقاعدة عامة. [2]

الفرع الثاني: المعاينة التقنية في مرحلة جمع الاستدلالات

لم يحدد المشرع الجزائري المقصود بالمعاينة مكتفيا بالنص عليها في العديد من مواد قانون الإجراءات الجزائية[3]، وبالرجوع إلى تعريفات الفقه الجنائي تعتبر المعاينة :" إثبات حالة الأماكن

---

[1]–بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، مرجع سابق، ص215

[2]–ياسر محمد أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، مرجع سابق، ص240.

[3]– حيث تنص المادة 79 من (ق.ا.ج.ج) على: " يجوز لمقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها.."

– وفي نفس السياق نصت المادة 42 من (ق.ا.ج.ج) على: " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات

والأشخاص وكل ما يفيد في كشف الحقيقة[1]"، أو هي: " إثبات حالة الأشياء والأشخاص وغيرها وهي تستلزم الانتقال إلى محل وجود الشيء أو الشخص الذي ينبغي معاينته".[2]

فالمعاينة إجراء من إجراءات التحقيق، يتم بقصد جمع الأدلة وفحصها لكشف حقيقة الجريمة، ويتطلب ذلك أن ينتقل المحقق من مقر عمله إلى مكان محدد قد يشكل مسرحا للجريمة.

وتكمن أهمية المعاينة وفعاليتها في التيسير على سلطة التحقيق في الأحوال التي تقتضيها الضرورة، ذلك أن المبادرة بالإنتقال إلى مكان الجريمة لمعاينته وضبط ما قد يوجد به من أشخاص أو أشياء، من شأنها أن تؤدي إلى المساعدة في جمع الأدلة المترتبة على ارتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها .

ويثار التساؤل حول كيفية الانتقال إلى مسرح جرائم الإعتداء على التوقيع الإلكتروني؟ وكيف يمكن معاينتها؟ في ظل انصراف أغلب النصوص المنظمة لإجراء المعاينة والانتقال إلى الجرائم التقليدية وإمكانية تطبيقها بخصوص معاينة مكونات الحاسب الآلي ذات الطابع المادي، والتي بإمكان ضابط الشرطة القضائية التحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة وضبطها ونسبتها إلى الفاعل مع إخطار النيابة العامة بذلك[3].

اللازمة وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة..." .

– كما نصت المادة 235 (ق.إ.ج.ج) على أنه: " يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة والمدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة..." .

– راجع في هذا الإطار المواد: (47) و(50) و(62)من(ق.ا.ج.ج)

[1]–فؤاد حسن العزيزي، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، مصر، 2015، ص 195 .

[2]– نصر شومان، التكنولوجيا الجرمية الحديثة، وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة في الكتاب، طرابلس، لبنان، ط1، 2011، ص 151.

[3]–عبد الفتاح بيومي حجازي، الجوانب الإجرائيةلأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط1، 2003.

وهو ما سيتم التعرف عليه فيما يلي:

أولا: القواعد التقنية لإجراء المعاينة في جرائم التوقيع الإلكتروني

تقوم المعاينة على الملاحظة واثبات الحالة[1]، ويستطيع المحقق أن يقوم بذلك بنفسه أو عن طريق من يندبه لذلك من ضباط الشرطة القضائية المختصين قانونا، وأهم ما يميز المعاينة كإجراء من إجراءات التحقيق في جرائم التوقيع الإلكتروني هو معاينة مسرح الجريمة واثبات الحالة فيه، وليس هناك ما يمنع من استعانة ضابط الشرطة القضائية بخبير في ذلك كما في إستعانته لرفع البصمات مثلا[2]، غير أن الإنتقال لا يتم بالضرورة عبر العالم المادي، إنما عبر العالم الافتراضي (Cyber Space). وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الإعتداءات الواقعة على التوقيع الإلكتروني سواء من مكتبه أو من مقهى الأنترنت أو اللجوء إلى مؤدي خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق أو لمزود خدمة الأنترنت (Intrnet Server Provider).[3]

1. **الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة المعلوماتي:**

يجب على المحقق الجنائي قبل الانتقال لإجراء معاينة لمسرح الجريمة المعلوماتي إتباع الخطوات التالية[4]:

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد أجهزة الكمبيوتر المتوقع مداهمتها وشبكات الاتصال الخاصة بها، لتحديد إمكانيات التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات.

---

[1]– عمر سالم، الوجيز في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2011–2012، ص219.

[2]–مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، مكتبة رجال القضاء، الطبعة الثانية، 2005، ص 643.

[3]– نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2013، ص218.

[4]–محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للمعاملات الإلكترونية، دبي، 2004.

- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.
- قطع التيار الكهربائي عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير أو محو أثار الجريمة.
- إعداد فريق تفتيش من المتخصصين والفنيين.
- إعداد الأمر القضائي اللازم للقيام بالتفتيش، سواء كان ذلك إذن من النيابة العامة أم أمر من القاضي الجزائي المختص وذلك في الحالات التي حددها القانون.

2. إجراءات المعاينة والتحفظ على مسرح الجريمة في جرائم التوقيع الإلكتروني:

يختلف الأمر بالنسبة إلى المسرح الافتراضي عن ما هو متعارف عليه في عملية الإنتقال إلى المسرح التقليدي التي تتم بطريقة مادية، حيث يستطيع عضو النيابة أو قاضي التحقيق أو ضابط الشرطة القضائية أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال جهاز الكمبيوتر الموضوع على مكتبه[1]، أو من خلال الاستعانة بالخبراء المتخصصين في المعلوماتية، على نحو ما سيتم تفصيله لاحقا في إجراء الخبرة التقنية بالنسبة لجرائم التوقيع الإلكتروني.

ونتيجة لاختلاف مسرح الجريمة في الجرائم الواقعة على التوقيع الإلكتروني عن غيره من الجرائم، لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، وحتى تصبح معاينة مسرح الجريمة في مجال جرائم التوقيع الإلكتروني لها فائدة في كشف الحقيقة عنها وعن مرتكبها، ينبغي إتباع قواعد وإرشادات فنية أهمها[2]:

- تحديد نقطة البدء في المعاينة ونقطة الانتهاء منها بحيث تجرى المعاينة بصورة مرئية يلم فيها المحقق بكافة الجوانب التي يريد الوصول إليها من المعاينة.

[1]– عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص 895.

[2]– احمد عاصم عجيلة، الحماية الجنائية للمحررات الإلكترونية، مرجع سابق، ص438.

- تصوير شاشة الحاسب الآلي[1]، والأجهزة الطرفية المتصلة به والمحتويات صور شمسية مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته لكي تظهر المعلومات أو الصور المطلوب معاينتها.
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام أو الموقع أو الدخول معه في حوار. [2]
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالتوقيع الإلكتروني محل الجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.
- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة القريبة من الحاسب والشرائط والأقراص الممغنطة غير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تؤدي إلى التعرف على المتهم مرتكب الواقعة.
- الإستعانة عند مباشرة المعاينة بالخبراء والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم المعلوماتية. [3]
- عدم نقل أية محررات إلكترونية وأية معلومات مسجلة على الحاسب من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أية مجالات لقوى مغناطيسية يمكن إن تتسبب في محو البيانات المسجلة على الوسيط المادي.

---

[1]–جميل عبد الباقي الصغير، جرائم الأنترنت، الأحكام الموضوعية والجوانب الإجرائية، طبعة نادي القضاة، 2010، ص 24.

[2]–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 104.

[3]–هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص60.

- الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل مثل برنامج معالجة الملفات (Xtree pro Gold)، وبرنامج (Encase) الذي ينتج صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدرالية الأمريكية ويسميها الخبراء "حقيبة الأدلة الرقمية".[1]
- السيطرة على الدائرة المحيطة بمكان المعاينة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة أو لإمكان العودة لإجراء معاينة أخرى فيما بعد حتى يتم الانتهاء من التحقيق.

الفرع الثالث: إجراءات التحفظ على بيانات التوقيع الإلكتروني

يقصد بالتحفظ الفوري في قانون الإجراءات الجزائية: " وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[2]. ويعد التحفظ الفوري على المستند الإلكتروني المتضمن التوقيع الإلكتروني من أهم الإجراءات التقنية اللازمة لتعقب الدليل في جرائم الإعتداء على التوقيع الإلكتروني والمحافظة عليه من خطر الضياع أو التعديل، [3]فضلا عما يستلزمه المحافظة على المستند الإلكتروني من ضرورة تخويل السلطة القائمة على جمع الاستدلالات صلاحية التحفظ الفوري على تلك البيانات المخزنة على الحاسب الآلي وصولا للتحري الدقيق عن مرتكب الجريمة وملاحقته.

---

[1]–عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع السابق، ص 85.

[2]–هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مرجع سابق، ص93

[3]–Jean-François HENROTTE, L´importance de la collaboration internationale dans l´échange d´informations policières et de coopération judiciaire, in La cybercriminalité, Programme des Nations Unies pour le Développement, Casablanca, Royaume du Maroc, 19-20 juin, 2007.p 100.

– وفي دراسة مسحية حول انتحال الشخصية لعام 2006 اظهرت النتائج ما يلي: ضحايا انتحال الشخصية: 8,9 مليون من البالغين الأمريكيين، (9,3) مليون شخص في، 2004 المبالغ المستخدمة في انتحال الشخصية: 56,6 مليار دولار أمريكي (ارتفع المبلغ عن عام 2004 حيث بلغ حينئذ 54,4 مليار دولار)، معدل الخسارة الناتجة عن الاحتيال لكل ضحية: 6,383 دولارا أمريكيا (بارتفاع بنسبة 21,6 بالمائة عن عام 2000)، انظر هلالي عبد الله احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية في ضوء إتفاقية بودابست، دار النهضة العربية، الطبعة الأولى، 2003، ص 201 – 205.

وفي هذا الإطار نصت المادة (06) من القانون رقم: 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على انه: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية. غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للإستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات".

وتطبيقا لذلك، نصت المادة (16) من إتفاقية بودابست على التزام الدول الأطراف في تلك المعاهدة بسرعة المحافظة على بيانات المستند الإلكتروني والبيانات المخزنة على الحاسب الآلي وان يكون لجهة التحقيق أن تأمر أو تحصل فورا على بيانات المستند الإلكتروني، بما في ذلك خط سير البيانات التي يتم تخزينها بواسطة منظومة الحاسب الآلي، وخاصة إذا كان هناك ما يدعو للاعتقاد بإمكانية تعرض بيانات الكمبيوتر بصفة خاصة للضياع أو التعديل. وقد أكد التشريع الأمريكي ذات المعنى حيث نص البندان (1702) و(1703) من القسم الثامن عشر من قانون الإجراءات الجنائية الإلكترونية الأمريكي لسنة 2000 على انه يتطلب قانون فيدرالي آخر بوجه عام أو وجود إذن تفتيش، أو أمر محكمة، أو أمر بالحضور أمام القاضي لإنفاذ القانون حال الوصول إلى الاتصالات الإلكترونية المحفوظة، اعتمادا على: [1]

- إذا ما كانت جهة إنفاذ القانون تسعى إلى بيانات ذات محتوى من عدمه.
- وما إذا تم إستعادة الإتصال الإلكتروني من عدمه.

[1]–Better Business Bureau/javelin strategy and research , 2006 identity fraud surveyy report, http: //www.javelinstartegy.com.

ومن ثم، فان التشريع الأمريكي يفرق بين ما إذا كانت البيانات محل التحفظ لها محتوى من شأنه المساس بالخصوصية من عدمه. ويرتب على ذلك ضرورة استصدار إذن قضائي قبل التحفظ.[1]

أولا: ضمانات المتهم عند التحفظ الفوري على بيانات المستند المتضمن للتوقيع الإلكتروني

ينطوي إجراء التحفظ على بيانات المستند الإلكتروني المتضمن للتوقيع الإلكتروني على مساس بسرية المعلومات وحرمة الحياة الخاصة لما يتضمنه ذلك الإجراء من تحفظ على جميع بيانات الحاسب الإلكتروني، وهو ما أدى إلى تقييد سلطة التحقيق المختصة بهذا الإجراء بقيود تضمن التوازن بين حق المجتمع في إنزال العقاب على المتهم، وحق هذا الأخير في عدم المساس بسرية المعلومات المخزنة على الحاسب الآلي الخاص به[2]، وهذا ما نصت عليه المادة (09) من القانون 04/09 السالف ذكره: " تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، الا في الحدود الضرورية للتحريات أو التحقيقات القضائية".

وفي السياق ذاته نصت المادة (85) من (ق.ا.ج.ج) على: " يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 2000 إلى 20.000 دينار لكل من أفشى أو أذاع مستندا متحصلا من تفتيش شخص لا صفة له قانونا في الاطلاع عليه، وكان ذلك بغير إذن من المتهم أو من خلفه أو من الموقع بإمضائه على المستند أو الشخص المرسل إليه وكذلك كل من استعمل ما وصل إلى علمه ما لم يكن ذلك من ضروريات التحقيق القضائي".

كما نصت المادة 16 من اتفاقية بودابست بشأن جرائم الحاسب الآلي على الضمانات التي يجب توافرها لاستعمال تلك السلطة حيث اشترطت:

---

[1]–جوناثان ج. روش. الأطر التشريعية والقانونية لمكافحة الجرائم الإلكترونية، استراتيجية قضائية لتطبيق قانون التوقيع الإلكتروني، مؤتمر التواقيع الإلكترونية، القاهرة، مصر، الفترة ما بين 8 و9 مارس 2006.

[2]–ياسر محمد أبو حطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، مرجع سابق، ص250

1. توافر حالة الضرورة التي تبرر إصدار أمرا بالتحفظ على بيانات الحاسب الآلي:

وذلك كلما كانت تلك بيانات التوقيع الإلكتروني أو شهادة التصديق الإلكتروني محل الاعتداء عرضة لخطر الإتلاف أو التلاعب، وتقدير ما إذا كان التحفظ على تلك البيانات ضروريا من عدمه يتوقف على مدى جدية المبررات التي تعتد بها سلطات التحقيق لإصدار الأمر بالتحفظ عليها.

وقد أكد المشرع الأمريكي على ضرورة التحفظ على بيانات المستند الإلكتروني، فقد نص القسم 101/د من قانون الإجراءات الجنائية الإلكترونية الأمريكي لسنة 2000 على انه إذا تطلب أي تشريع أو تنظيم أو قاعدة قانونية أخرى أن يتم الاحتفاظ بأي عقد أو سجلات أخرى ترتبط بأي معاملات أو تؤثر على التجارة بين الولايات أو التجارة الخارجية، فان هذا المطلب سيتم استيفائه عن طريق الاحتفاظ بسجل إلكتروني أو أي سجل آخر من شأنه أن:

- يعكس بدقة المعلومات الموضحة في العقد أو أي سجل آخر.
- يظل ممكن الحصول عليه من جانب جميع الأشخاص الذين لهم حق الحصول عليه، بموجب لائحة أو تنظيم أو قاعدة قانونية، وذلك للمدة المطلوبة، بموجب هذه اللائحة أو التنظيم أو القاعدة القانونية وبالصيغة التي توفر إعادة النسخ بشكل دقيق للمراجعة اللاحقة سواء بواسطة الإرسال أو الطبع أو خلاف ذلك. [1]

ومؤدى ذلك أنه متى وقعت جريمة من جرائم الإعتداء على التوقيع الإلكتروني، يجوز لمكتب التحقيقات المختص بمقتضى القانون التحفظ على المستند الإلكتروني.

2. أن يكون الغرض من التحفظ جمع الأدلة أو التحقق من هوية الجاني

أن يكون الهدف من التحفظ على بيانات الحاسب الآلي الوصول إلى الدليل الإلكتروني وتحديد هوية مرتكب الجريمة، حتى يصبح الإجراء ذا قيمة، وتحديد البيانات التي يمكن أن تكون محلا للتحفظ يتوقف على ارتباطها بالمستند الإلكتروني محل الاعتداء. [2]

---

[1]–PUBLIC LAW 106-229- JUNE 30. 2000 Article no 101/D

[2]–هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 266 .

وقد أكد قانون التوقيع الإلكتروني الأمريكي سالف الذكر على أن حالة الضرورة تبرر اتخاذ ذلك الإجراء، فقد نص القسم 104 على انه: " يجوز لأي هيئة رقابية فدرالية أو هيئة رقابية تابعة للدولة أن تفسر القسم 101 (د) للمطالبة بالاحتفاظ بسجل في صيغة مطبوعة أو ورقية حقيقية ملموسة إذا:

- كان هناك فائدة حكومية ملزمة تتعلق بتنفيذ القانون أو الأمن القومي لغرض هذا المطلب .
- كان فرض هذا المطلب ضروريا للحصول على هذه الفائدة الحكومية" .

ولما كانت معظم جرائم الإعتداء على التوقيع الإلكتروني من شأنها المساس باقتصاد الدولة وكان الحصول على الدليل الإلكتروني أمرا لا غنى عنه، فانه يمكن القول انه لا صعوبة في تحقيق هذا الشرط في غالب الأحيان .

3. تسبيب الأمر الصادر بالتحفظ الفوري على بيانات المستند الإلكتروني

نصت المادة (19) من اتفاقية بودابست على وجوب تسبيب الأمر الصادر بالتحفظ الفوري على بيانات المستند الإلكتروني حيث اشترطت انه في حالة قيام الدولة الطرف بالاتفاقية بتفعيل الفقرة (ا) بإصدار أمر إلى شخص للمحافظة على بيانات المستند الإلكتروني المخزونة بحوزة الشخص أو تحت سيطرته، تقر الدولة الطرف بالاتفاقية هذه الإجراءات التشريعية وغيرها من الإجراءات الأخرى، لإلزام ذلك الشخص بالمحافظة على وحدة وسلامة بيانات التوقيع الإلكتروني طيلة هذه الفترة طالما كان ذلك ضروريا.

4. إلزام الأطراف المتدخلة بالتحفظ الفوري على بيانات المستند الإلكتروني

يقتضي التحفظ الفوري على بيانات المستند الإلكتروني أن تلتزم الأطراف المتدخلة في منظومة إنشاء التوقيع الإلكتروني الموصوفة بأن تتيح في الحال للجهة المعنية بجمع الاستدلالات، المعلومات اللازمة للتعرف على أجهزة الخدمة الأخرى، وعناصر سلسلة الاتصال المستخدمة، ومن ثم تبدو أهمية تفويض السلطة المختصة لجهات أخرى بالقيام بالتحفظ على بيانات المستند الإلكتروني

لحمايتها من المحو أو الإتلاف[1]وقد حددت المادة 18 من إتفاقية بودابست الجهات التي يجوز إلزامها بتنفيذ الأمر بالتحفظ وهي:

- أحد الأشخاص يحوز ويسيطر على بيانات المستند الإلكتروني المخزنة على حاسبه أو دعامة مادية متى كانت متصلة بالمستند الإلكتروني محل التجريم .
- أجهزة الخدمة المختصة بإرسال ما تحوزه أو تسيطر عليه من بيانات المشتركين. [2]

و يقصد بمصطلح (بيانات المشتركين): أية معلومات موجودة في صورة بيانات بالبيانات أو أية صورة أخرى يتم حفظها بأحد أجهزة تقديم الخدمة المعلوماتية، والتي تتعلق، بالمشتركين في الخدمات الخاصة به خلاف خط سير البيانات أو مضمونها والتي بموجبها يمكن التوصل إلى:

- نوعية خدمة الإتصال أو المراسلة المستخدمة، والشروط الفنية التي يتم اتخاذها في ذلك، والفترة الزمنية المستخدمة للخدمة .
- البيانات الشخصية للمشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع، والتي تكون متوافرة بموجب الإتفاق على الخدمة أو الترتيبات الخاصة بذلك .
- أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الإتصالات، والتي تتوافر بموجب الإتفاق على الخدمة أو الترتيبات الخاصة بذلك .

ويترتب على عدم مراعاة الالتزام المنصوص عليه أعلاه مسؤولية قضائية بموجب القانون، ويقصد بمصطلح " بيانات المستخدمين: " اية معلومات يمكن أن تؤدي إلى التعرف على مستخدم ما، بما في ذلك نوع الاتصال والخدمة المستخدمة، وكذلك أية بيانات أخرى يمكن أن تؤدي إلى كشف عن المستخدم. ولا شك أن إلزام الغير بالتحفظ على المستند الإلكتروني المتضمن لأدلة الإثبات في جريمة

[1]–jean – François Henrotte l' importance de la collaboration internationale et l'expérience belgedans l'échange d'informations policières et de coopération judiciaireprojet sur la Modemisation des Ministères Publics "Conférence régionale sur la Cybercriminalité Casablanca , Royaume du Maroc 19-20 juin , 2007 p 102

[2]–convention sur la cybercriminalité Budapest, 23XL . article no 18

من جرائم الاعتداء على التوقيع الإلكتروني وضبطه، وتعدد الجهات التي تلتزم بالتحفظ وتحديد فئاتها على ذلك النحو يوفر قدرا من التنوع يمكن من خلاله تسهيل عملية ضبط الدليل الإلكتروني. [1]

ثانيا: تصنيف بيانات المستند المتضمن للتوقيع الإلكتروني:

يحتفظ مؤدو خدمات التصديق الإلكتروني في إطار تأدية خدمات التصديق الإلكتروني بشهادات التصديق الإلكتروني بما تتضمنه من بيانات ومعلومات سرية[2]، ونظرا لتعدد وتنوع هذه البيانات فقد بات من الضروري تصنيفها من قبل رجال الضبط القضائي عند التنقيب على الدليل الإلكتروني في جرائم الإعتداء على التوقيع الإلكتروني. وقد تضمن القسم الثاني عشر من قانون الإجراءات الجنائية الإلكترونية الأمريكي لسنة 2000 تقسيما لأنواع المعلومات والبيانات محل البحث المصري حيث قسمها إلى نوعين:

1. بيانات تتعلق بمضمون المستند الإلكتروني:

حيث نصت الفقرة 8 من القسم الثاني عشر من قانون الإجراءات الجنائية الإلكترونية الأمريكي لسنة 2000، على تعريف تلك البيانات بأنها البيانات أو المحتوى أو المضمون الذي يتضمنه الإتصال الإلكتروني[3]. وترتيبا على ذلك يمكننا القول ان جميع البيانات الجوهرية التي يتضمنها المستند الإلكتروني والتي تكون محلا للإعتداء أو تلك التي تستخدم في تزوير التوقيع الإلكتروني أو إعداد برنامج لإتلافه أو تعييبه هي بيانات جوهرية يتعين على رجال الضبط إلزام مقدمي خدمات التصديق ومقدمي خدمات الحاسب الالي بتقديمها حتى يتسنى تحليلها والوصول من خلالها للدليل الإلكتروني المؤدي لإدانة المتهم في تلك الجرائم. وقد حرصت إتفاقية بودابست على تخويل سلطات التحقيق ذلك الحق عندما نصت المادة 19 على تفويض سلطة التحقيق القيام

---

[1]–convention sur la cybercriminalité Budapest, 23XL . article no 18

[2]–حيث نصت المادة (41) من القانون 15–04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني على انه: "يكلف مؤدي خدمات التصديق الإلكتروني بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني، وفقا لسياسة التصديق الإلكتروني الخاصة به، التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني".

ونصت المادة (42) على انه: "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة".

[3]–U.S. codetitle 18. crimes and criminal procedure. part i. crimeschapter 119. wire and electronic communications interception and interception of oral communications section 2510. definitions:

بالإجراءات اللازمة لضمان قيام سلطاتها بعمليات البحث أو الدخول على منظومة كمبيوتر بعينها أو على جزء منها، متى كان لديها أسباب للاعتقاد بان البيانات المطلوبة مخزنة بداخل منظومة كمبيوتر أخرى أو بداخل جزء منها على أراضيها، وأن هذه البيانات يمكن الدخول عليها قانونا من المنظومة الرئيسية أو المتوافرة لها، فتصبح السلطات قادرة على توسيع عملية البحث بسرعة ونشاط أو الدخول بالمثل على المنظومة الأخرى. [1]

2. بيانات تتعلق بالمشترك والمستهلك في المستند الإلكتروني المتضمن للتوقيع الإلكتروني:

وهي المتطلبات الواجب توافرها في شهادة تصديق إلكتروني موصوفة، ورد النص عليها في المادة (15) من القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين على انه: " شهادة التصديق الإلكتروني الموصوقة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني، طبقا لسياسة التصديق الإلكتروني الموافق عليها.
- أن تمنح للموقع دون سواه،
- يجب أن تتضمن على الخصوص:
- إشارة تدل على انه تم منح هذه الشهادة على أنها شهادة تصديق إلكتروني موصوفة،
- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه،
- إسم الموقع أو الاسم المستعار الذي سمح بتحديد هويته،
- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني،
- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني،
- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني،

[1]–jean- François Henrotte l'importance de la collaboration internationale et l'experiencebelgedans l'échange d'information policiéres et de cooperationjudiciaire Projet sur la modernisation des ministere Publics "Conférance régionale sur la cybercriminalité Casablaca, Royaume du maroc 19-20 juin, 2007 p 103

- رمز تعريف شهادة التصديق الإلكتروني،
- التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني
- حدود استعمال شهادة التصديق الإلكتروني، عند الاقتضاء،
- حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، عند الاقتضاء،
- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر، عند الاقتضاء.

وكذا المادة (42) من القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين على انه: "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة".

وفي نفس السياق نصت الفقرة الثالثة من المادة الثانية من القسم الثامن عشر من القانون الأمريكي والتي من شأنها الوقوف على شخصية المشترك مثل الاسم، أو العنوان المؤقت على الشبكة، وسجلات البيانات التي تقدم المشترك عند اشتراكه[1].

وتطبيقا لذلك، اعتبر القضاء الأمريكي ان أي بيانات تخص المشترك أو المستهلك يلزم التعامل معها بمنتهى السرية، متى كان من شأنها الربط بين المستند الإلكتروني محل التزوير وشخصية مرتكب الجريمة[2].

وقد ألزمت المادة 21 من إتفاقية بودابست كل دولة طرف بالإتفاقية بإقرار الإجراءات التشريعية وغيرها من الإجراءات الأخرى، لإلزام (المسؤول) أو أي شخص آخر يحتفظ ببيانات الكمبيوتر بالمحافظة على سرية القيام بمثل هذه الإجراءات للفترة الزمنية المنصوص عليها في قانونها المحلي.

ولا شك أن الوقوف على تلك البيانات من شأنه ان يحدد المتهم في جريمة الإعتداء على التوقيع الإلكتروني ومن ثم، فان النص في القانون الأمريكي على التزام مقدم الخدمة بتقديمها من شأنه

---

[1]–See 18 u.s.c 27703/c/2.

[2]–Hill v MCI worldcom. 120F. SuPP.2d 1194 , 1195/96(S.Dlowa 2000) ،available at:
https: //law.justia.com/cases/federal/district-courts/FSupp2/120/1194/2499659/ Sunday,21july 2019 22.15

أن يؤدي إلى الربط بين المستند الإلكتروني محل التزوير وشخصية مرتكب الجريمة ويقود إلى دليل يمكن الركون إليه لإثبات جريمة الإعتداء على التوقيع الإلكتروني قبله.

وبالرغم من خلو التشريع المصري من نص مماثل، إلا أن التشريع العماني قد تضمن نصا يوجب على مقدم خدمات التصديق والعاملين لديه تقديم تسهيلات للسلطة المختصة أو لأي من موظفيها للقيام بالمراقبة أو الإشراف أو التفتيش على أي نظام حاسب الي أو جهاز بيانات أو مواد أخرى متصلة بنظام الحاسب الالي بمقر مقدم خدمات التصديق[1].

المطلب الثاني:

أدلة الإثبات التقنية في الجرائم الواقعة على التوقيع الإلكتروني

بالنظر إلى الطبيعة الخاصة لجرائم الإعتداء على التوقيع الإلكتروني، صارت عملية الكشف عن هذه الجرائم تتطلب إتباع استراتيجيات خاصة تتعلق بإكساب القائمين بجمع الدليل مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، بحيث تتعقد وتتنوع التقنيات المرتبطة بارتكاب تلك الجرائم، استخدام تقنيات تحقيق جديدة ومبتكرة لتحديد نوع الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجاني والحصول على أدلة إدانة .

على ذلك سيتم تقسيم المطلب إلى ثلاثة فروع على النحو التالي:

- **الفرع الأول:** تفتيش منظومة التوقيع الإلكتروني واستخلاص الدليل الرقمي
- **الفرع الثاني:** الدليل الرقمي ومجاله في الإثبات الجنائي

---

[1]–حيث نصت المادة 53 من قانون المعاملات الإلكترونية العمانى على انه مع عدم الاخلال بأية عقوبة اشد ينص عليها قانون الجزاء العماني او أي قانون اخر يعاقب بالسجن لمدة لا تتجاوز سنة واحدة وبغرامة لا تتجاوز (الف وخمسمائة ريال عماني) او بإحدى هاتين العقوبتين كل مقدم خدمات تصديق او احد العاملين لديه رفض تسهيلات للسلطة المختصة او أي من موظفيها للقيام بالمراقبة او الاشراف او التفتيش على أي نظام حاسب الي او جهاز بيانات او مواد أخرى متصلة بنظام الحاسب الالي بمقر مقدم خدمات التصديق (قانون المعاملات الإلكترونية العماني رقم 2008/69 الصادر في 18مايو2008م).

- **الفرع الثالث:** الشهادة الإلكترونية والخبرة في مجال الجرائم الواقعة على التوقيع الالكتروني

الفرع الأول: تفتيش منظومة التوقيع الإلكتروني واستخلاص الدليل الرقمي

يعتبر إجراء التفتيش الخطوة الأولى في مباشرة التحقيق الذي يتولاه قاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه كما نصت على ذلك المادة (84) من قانون الإجراءات الجزائية الجزائري في فقرتها الأولى على انه: " إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فان لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع ما تقتضيه ضرورات التحقيق وما توجبه الفقرة الثالثة من المادة 83...". [1]

وفي هذا الصدد نص القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على جملة من القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات، منسجما في ذلك مع نصوص الاتفاقية الأوربية لمكافحة الإجرام المعلوماتي والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وينصب التفتيش على المكونات المادية للحاسب بأوعيتها المختلفة للوصول إلى دليل يتصل بارتكاب جريمة من جرائم الاعتداء على التوقيع الإلكتروني وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها. [2]

أولا: تفتيش منظومة التوقيع الإلكتروني وحجز المعطيات

نصت المادة (05) من القانون 04/09 تحت عنوان " تفتيش المنظومات المعلوماتية " على: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو على بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية...

---

[1]–أضاف المشرع الفرنسي البحث عن البيانات المعلوماتية (Données informatiques) إلى البحث عن المستندات.

[2]–إبراهيم حامد مرسي، سلطات مأمور الضبط القضائي، دراسة مقارنة، رسالة دكتوراه، الطبعة الثانية، 1997، ص743، ص743 .

من خلال هذه المادة يجيز المشرع الدخول إلى المنظومة المعلوماتية دون إذن صاحبها ولو عن بعد بغرض التفتيش، ونظرا لصعوبة تنفيذ هذا الإجراء من الجانب التقني، انجاز المشرع بنص المادة (6/05) من القانون رقم: 04/09 سالف الذكر الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث والتفتيش أو بالتدابير المتخذة لحماية المعطيات المعلوماتية.

وخلاف الإجراء تفتيش المكونات المادية للحاسوب الذي يتطلب إذنا مكتوبا من طرف وكيل الجمهورية أو قاضي التحقيق وفقا لأحكام المادة (44) من (ق.ا.ج.ج)، فان إجراء تفتيش المنظومة المعلوماتية للتوقيع الإلكتروني كلها أو جزء منها تنصب حول الكيان المنطقي للحاسوب، أي ان التفتيش يستهدف اشياء غير مادية. [1]

1. حجز المعطيات المعلوماتية

يقصد بالحجز في قانون الإجراءات الجزائية: " وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[2] . يمكن تخزين المعطيات في ذاكرة الحاسوب أو في برامجه إذ تعتبر كيانات غير مادية مما شكل اختلافا في التشريعات العالمية حول مدى اعتبارها قابلة للحجز فلقد نص التشريع الألماني في المادة (94) من قانون الإجراءات الجنائية على أن البيانات المعالجة إلكترونيا لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي كنقلها على دعامة إلكترونية، في حين ذهب اتجاه آخر في فرنسا إلى اعتبار برامج الحاسوب كيانا ماديا ملموسا فهو عبارة عن نبضات وإشارات إلكترونية ممغنطة[3]، في حين أضفى المشرع الجزائري حماية قانوني لقواعد البيانات بموجب نص المادة (05) من الأمر رقم: 05/03 المؤرخ في 200/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة التي تنص على: " تعتبر أيضا مصنفات الأعمال الأتية:

---

[1]–Chaque partie adopte les mesures législative et autre qui se révèlent nécessaire pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les donner informatique qui contient de fournir toutes les information raisonnablement nécessaire , pour permettre l'application des mesures visées par les paragraphes 1 et 2 convention européenne de la cybercriminalité, Op.Cit,p.10.

[2]–هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص93

[3]– هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص 596.

- أعمال الترجمة والاقتباس، والتوزيعات الموسيقية، والمراجعات التحريرية، وباقي التحريرية الأصلية للمصنفات الأدبية والفنية .
- المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء ان كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الإشكال الأخرى، والتي تأتي أصالتها من انتقاء مواد أو تربيتها ...".

كما نصت المادة (06) من القانون رقم 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها التي تنص على: " عندما نكتشف السلطة التي تباشر التفتيش في منظمة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. يجب في كل الاحوال على السلطة التي تقوم بتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجرى بها العملية. غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط ان لا يؤدي ذلك إلى المساس بمحتوى المعطيات".[1]

2. الحجز عن طريق منع الوصول إلى بيانات إنشاء التوقيع الإلكتروني

تواجه أجهزة البحث والتحري صعوبات أثناء توقيع الحجز على المنظومات المعلوماتية سواء أكانت هذه المنظومات منفصلة أو متصلة ببعضها البعض عبر شبكة الأنترنت ومرد هذه الصعوبة التطورات التقنية المتلاحقة في مجال المعلوماتية، لذا تلجأ أجهزة البحث إلى طريقة الحجز عن طريق منع الوصول إلى المعطيات في حدود ما يسمح به القانون.

---

[1]–وفي السياق ذاته نصت المادة (27) من (ا.ع.م.ج.ت.م) تحت عنوان: " ضبط المعلومات المخزنة " التي تنص على تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول اليها حسب الفقرة(1) من المادة السادسة والعشرين من هذه الإتفاقية، هذه الإجراءات تشمل صلاحيات:

ا– ضبط وتأمين تقنية المعلومات او جزء منها او وسيط تخزين معلومات تقنية المعلومات.

ب– عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

3. الحجز عن طريق منع الوصول إلى المعطيات:

يصادف تتبع المجرم المعلوماتي أثناء التحقيق الذي تأمر به السلطة القضائية المختصة صعوبات تقنية بالغة تحول أحيانا دون الكشف عنه، محاولا محو آثار جريمته ليصعب على المحققين تعقبه، وبالتالي اختفاء الدليل الرقمي الذي يدينه وإفلاته من العقاب، لذلك نص المشرع في المادة (07) من القانون رقم: 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: " إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها...". حيث تتوافق هذه المادة مع نص المادة (3/19–د) من (إ.أ.م.ا.م) بخصوص حفظ المعطيات المخزنة أو ازالتها أو منع الوصول إليها[1]، وهو نفسه ما نصت عليه المادة (1/27–د) من (ا.ع.م.ج.ت.م) سالفة الذكر.

ولم يحدد المشرع الاسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، وذلك راجع إلى التحديثات المستمرة على نظم الحواسيب حيث اصبحت تشكل جزءا من شبكات واسعة ومعقدة يصعب على السلطات المختصة مباشرة الحجز دون تعاون كامل (full co-operation) من القائم على تشغيل النظام[2]، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات، وما يتطلبه ذلك من متابعة وتكوين دوري لأعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم المعلوماتي، ليتدخل المشرع بالنص على ضرورة إجراء تدابير احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة، والقصد من ذلك عدم تمكين المجرم من التلاعب بالمعطيات المخزنة في المنظومة المعلوماتية والتي تشكل محل الجريمة لاحتوائها على أدلة الإدانة.[3]

---

[1]–Article 19 – perquisition et saisie de données informatiques stockées

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes: …

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté…, convention européenne de la cybercriminalité, Op.Cit,p.10.

[2]–هشام محمد فريد رستم، الجوانب الاجرائية، المرجع السابق، ص98

[3]–زيدان زيبحة، المرجع السابق، ص153.

4. حدود استعمال المعطيات:

نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات مراقبة الإتصالات الإلكترونية منعا لأي مساس بحق الأشخاص في سرية مراسلاتهم ومنها المراسلات الإلكترونية، وهو حق مكفول دستوريا[1]، الا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة (09) من القانون رقم: 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها: " تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية".

الفرع الثاني: الدليل الرقمي ومجاله في الاثبات الجنائي

لا شك أن إحاطة القاضي في مجال الإثبات الجنائي بوقائع الدعوى يجب أن يتم من خلال ما يطرح عليه من أدلة، لا أن يحكم بعلمه الشخصي، ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته.

ونتيجة للتطور العلمي وانتشار التقنية الرقمية في التعاملات اليومية، أصبحت تستعمل تلك التقنية كوسيلة لارتكاب الجرائم تارة، وكموضوع للجريمة تارة أخرى، وبذلك اختلف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة، وهي الأدلة الرقمية أو ما يسمى بالأدلة الإلكترونية.[2]

---

[1]–انظر المادة (46) من الدستور الجزائري.

[2]–أثار الدليل الرقمي الكثير من التساؤلات التي يمكن إرجاعها إلى إشكاليتين رئيسيتين هما:

- الأولى: حداثة الدليل الرقمي، فهو من افرازات التطور التقني، وهو أيضا ذو طبيعة خاصة من حيث الوسط الذي ينشأ والطبيعة التي يبدو عليها، وهذا يثير التساؤل حول مشروعية الأخذ به، اذ انه يشترط في الدليل الجنائي بوجه عام ان يكون مشروعا من حيث وجوده ومن حيث الحصول عليه، فمشروعية الوجود تقتضي أن يكون الدليل قد قبله المشرع ضمن أدلة الإثبات الجنائي، فما هو الموقف من هذا النوع من الأدلة – أما مشروعية الحصول عليه فتقتضي أن يتم الحصول على الدليل بإتباع الإجراءات التي ينص عليها القانون، وبالنظر إلى الطبيعة الخاصة للدليل الرقمي والوسط الذي نشأ به، فانه تثور الكثير من الإشكاليات التي تتصل

أولا: التعريف بالدليل الرقمي

نظرا لحداثة وأهمية الدليل الرقمي، تعددت التعريفات واختلفت بخصوص وضع تعريف شامل له لعل من أبرزها أنه: " تلك الأدلة التي يمكن الحصول عليها بإحدى وسائل الإخراج"[1]، أو هو: " الدليل المأخوذ من أجهزة الكمبيوتر، يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الإشكال والرسوم، وذلك من أجل إعتماده أمام أجهزة إنفاذ وتطبيق القانون".[2]

وترجع تسمية الدليل الرقمي إلى أن البيانات داخل الوسط الإفتراضي سواء كانت صورا أو تسجيلات أو نصوص تأخذ شكل أرقام على هيئة الرقمين(1 أو 0) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل.[3]

بهذا الموضوع، كمدى إمكانية البحث عن الدليل الرقمي في الوسط الافتراضي وضبطه وفقا للقواعد التي تحكم التفتيش، وكذلك صفة الشخص الذي يقوم بجمع هذا الدليل.

- الثانية: انه ووفقا لمبداء قرينة البراءة التي تحكم إجراءات الاثبات الجنائي، يتعين دائما الحكم بالبراءة كلما كان الدليل محل شك، وهذا يحيلنا إلى تساؤل اخر حول مدى قبول الدليل الرقمي في إثبات الوقائع الجنائية، لاسيما إذا علمنا مقدار التطور في مجال تقنية المعلومات على نحو يتيح التلاعب بالمخرجات الرقمية بما يجعل مضمونها مخالفا للحقيقة دون أن يتسنى لغير المتخصص إدراك ذلك، فهل مفهوم اليقين الذي== يجب أن يتمتع به الدليل الجنائي يتعارض وهذه الطبيعة الخاصة للدليل الرقمي. ياسر محمد الكومي، الحماية الجنائية والامنية للتوقيع الإلكتروني، مرجع سابق، ص261.

[1]–سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي، دراسة مقارنة، دار الكتب القانونية، مصر، 2011، ص55.

[2]–ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص77.

[3]–ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشورضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية"، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من: 10 إلى 12 ماي لسنة 2004، المجلد الخامس، ص2238 .

- وتتجلى الطبيعة الخاصة للدليل الرقمي في الخصائص الاتية:

ثانيا: أنواع الدليل الرقمي

لا شك أن الحكم على القيمة القانونية للدليل الرقمي يمر عبر فهم الهيئة التي يتخذها، وهو ما يحتم علينا تحديد أنواعه وإشكاله، على النحو التالي:

1. أنواع الدليل الرقمي

يمكن تقسيم الدليل الرقمي إلى أدلة أعدت لتكون وسيلة إثبات وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي:

- السجلات التي تم إنشاؤها بواسطة الآلة تلقائيا، وتعتبر هذه السجلات من مخرجات الآلة التي لم يتدخل الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.
- سجلات تنقسم إلى جزئين: جزء منها تم حفظه بالإدخال، وجزء تم إنشاؤه بواسطة الآلة، ومن أمثلة ذلك المعطيات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص. [1]

والنوع الثاني هو الأدلة التي لم تعد لتكون وسيلة إثبات وهذا النوع من الأدلة الرقمية نشا دون إرادة الشخص، أي أنها اثر يتركها الجاني دون أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميته أيضا بالآثار المعلوماتية الرقمية[2]، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة

- يعتبر الدليل الرقمي دليلا غير ملموس أي هو ليس دليلا ماديا، فهو –أي الدليل الرقمي – تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فان ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني ان هذا التجمع يعتبر هو الدليل، بل ان هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة.
- يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية، وهو من طائفة ما يعرف بالأدلة المستمدة في الآلة.
- ان فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلا رقميا، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، مما يعدم قيمته التدليلية في إثبات الجريمة ونسبتها إلى الجاني، ياسر الكومي، مرجع سابق، ص263، ص264.

[1]–خالد ممدوح إبراهيم، مرجع سابق، ص 2

[2]–ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص2238 .

الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية[1].والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجرى عبر الأنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.[2]

وتبدو أهمية التمييز بين هذين النوعين فيما يلي:

- يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه لكونه قد اعد أصلا لان يكون دليلا على الوقائع التي يتضمنها، في حين يكون الحصول على النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.[3]
- النوع الثاني من الأدلة الرقمية هو الأكثر أهمية من النوع الأول لكونه لم يعد أصلا ليكون أثرا لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.
- لأن النوع الأول قد أُعد كوسيلة إثبات لبعض الوقائع فإنه عادة ما يُعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه، وعلى عكس النوع الثاني حيث لم يعد ليحفظ مما يجعله عرضة للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز على سبيل المثال.

---

[1]–ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 2238.

[2]–حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول IP والذي يمكن من ضبط تحركات مستخدم الشبكة تحدي الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة، راجع في ذلك: عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والأنترنت، دراسة معمقة في جرائم الحاسب الآلي والأنترنت، مرجع سابق، ص 63 – 64.

[3]–وهذا النظام لا يحدد شخصية مرتكب الجريمة وإنما يحدد الجهاز الذي استعملت منه، ويرى البعض أن ذلك يصلح كقرينة لاعتبار صاحب الجهاز مرتكب الجريمة إلى أن يثبت العكس، راجع ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب الوطنية، 2006، ص 108، ص 109.

2. أشكال الدليل الرقمي:

يتخذ الدليل الرقمي ثلاثة إشكال رئيسة هي:

أ. **الصور الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطورا ولكنها ليست بالضرورة أفضل من الصور التقليدية.[1]

ب. **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية عبر الأنترنت والهاتف ... الخ.

ج. **النصوص المكتوبة:** وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي، ... الخ.

ثالثا: مجالات إعمال الدليل الرقمي في الإثبات الجنائي

أدى إنتشار إستخدام تقنية المعلومات الرقمية وتعاظم دورها مع دخول الأنترنت شتى مجالات الحياة إلى الاهتمام بالدليل الرقمي قياسا بغيره من الأدلة الأخرى المستمدة من الآلة، وأصبح بذلك هذا الوسط مرتعا لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين، فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الرقمي[2]، ولذا كان الدليل الرقمي هو الدليل الأفضل لإثبات هذا النوع من الجرائم، لأنه من طبيعة الوسط الذي ارتكبت فيه، ومن هنا بدت أهمية هذا النوع من الأدلة، ذلك أن الدليل الرقمي كدليل إثبات لا ينحصر مجاله فقط على جرائم المعلوماتية التي من ضمنها جرائم التوقيع الإلكتروني، إنما يصلح في ذات الوقت لإثبات الجرائم التقليدية، مثلما يعتبر الدليل الأفضل لإثبات الجرائم المعلوماتية، ويميز الفقه في هذا الشأن بين نوعين من الجرائم[3]:

---

[1]–ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005، ص 9، ص 10

[2]–ياسر الكومي، مرجع سابق، ص266

[3]–ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سبق ذكره، 2237

1. الجرائم المرتكبة بواسطة الآلة:

وهذا النوع من الجرائم يستخدم فيه الحاسب الآلي والأنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل إستخدامه في الغش أو الاحتيال أو غسل الأموال أو لتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة، وبكلمة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة رقمية، فبرغم عدم إتصال هذه الجريمة بالنظام المعلوماتي فإن الدليل الرقمي يصلح كدليل لإثباتها.

2. جرائم الأنترنت والآلة الرقمية:

وهذا النوع من الجرائم يكون محله جهاز الحاسب الآلي أو الآلة بصفة عامة، بحيث يكون الإعتداء واقعا إما على الكيان المادي للآلة، وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول، وإما يكون الإعتداء واقعا على الكيان المعنوي للحاسب أو الآلة أو على قاعدة البيانات أو المعلومات التي قد تكون على شبكة المعلومات العالمية، مثال جرائم تزوير التوقيع الإلكتروني أو جريمة التوصل أو الدخول غير المصرح به لنظام المعالجة الآلية للمعطيات أو انتهاك الملكية الفكرية، أو جرائم القرصنة أو غيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بجرائم المعلوماتية والتي يكون الدليل الرقمي هو الدليل الأفضل لإثباتها إن وجد.[1]

ولا يقتصر إثبات جرائم التوقيع الإلكتروني على الدليل الرقمي فقط رغم صلتها به، فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف أو غيرها[2]، ولا يوجد أي تلازم حتمي بين الدليل الرقمي واثبات جرائم التوقيع الإلكتروني، فإذا كانت غاية الدليل عموما هي إثبات الجريمة ونسبتها إلى مرتكبيها، فإن هذا الدليل لا يكون قطعيا إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها، إذ مع ذلك تصح تسميته كدليل.

---

[1]–راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الأنترنت، الفترة: 2–4/يونيو 2008، منشور على الأنترنت، ص5 وما بعدها، على الموقع: http: //www.f-law.net تاريخ الزيارة 2019/8/22.

[2]–اثبت الواقع العملي الحديث حاجة بعض الأدلة التقليدية إلى تطوير يتناسب مع الطبيعة الخاصة لهذه الجرائم، فالخبرة مثلا تصلح لإثبات الجريمة المعلوماتية إلا أنها تحتاج إلى أن يكون الخبير متمتعا بمستوى عال من العلم والمهارة الفنية في مجال إثبات هذه الطائفة من الجرائم.

وتبدو أهمية هذا النوع من الأدلة بالنسبة لجرائم التوقيع الإلكتروني لصعوبة إثبات وقوعها عادة مع ملاحظة أنه قد يكون الدليل الرقمي متضمنا إثبات الجريمة ومرتكبها معا، فجسم جرائم التوقيع الإلكتروني عادة هو الدليل الرقمي ذاته وقد يكون هذا الجسم "الدليل الرقمي" متضمنا ما يفيد نسبة الجريمة لشخص ما، كما لو أرسل شخص لآخر رسالة عبر البريد الإلكتروني تتضمن فيروسات تؤدي إلى إتلاف منظومة إنشاء التوقيع الإلكتروني الخاصة بذلك الشخص، فإن هذه الرسالة بذاتها تعد دليلا على وقوع الجريمة، وفي الوقت نفسه ستعد دليلا على نسبة ارتكابها لشخص معين وهو المرسل إذا تضمنت بيانات تدل على شخصيته.[1]

ثالثا: ضبط الدليل الرقمي الناشئ عن جرائم الاعتداء على التوقيع الإلكتروني

يعد ضبط الدليل الرقمي النتيجة النهائية التي تنتهي إليها إجراءات التفتيش، وفي هذه الحالة يلزم اتخاذ إجراءات تقنية محددة، فلا تصلح الإجراءات المادية المعروفة للقيام بضبط الأدلة، كما هو الشأن في العالم المادي[2]، باستثناء عملية الفصل الضرورية بين الحاسب الآلي وبين كل شخص ليس له علاقة بالقائمين على الدعوى الجنائية، وذلك خشية قيام المتهم أو من له علاقة أو ملحة ما بتدمير الأدلة وإزالتها من الحاسب.[3]

---

[1]–ياسر الكومي، مرجع سابق، ص267، ص268.

[2]–حسن إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه، دار النهضة العربية، ص 173 وما بعدها.

[3]–حدد المشرع الأمريكي في المرشد الفيدرالي، اساليب الضبط المختلفة وفقا لطبيعة كل مخالفة والقانون الصادر بشأنها فيجوز وفقا للقانون الأمريكي مصادرة القطع الصلبة (الحاسب الآلي ومكوناته المادية) حال وجود عدوان على التوقيع الإلكتروني عبر الأنترنت، ابوبكريونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، دار الفكر العربي، مصر 2005، ص219.

– من التطبيقات التشريعية التي تجيز ضبط الأدلة الرقمية قانون الإجراءات الجنائية اليوناني، حيث تعطى المادة 251 منه سلطة التحقيق إمكانية القيام باي شيء يكون ضروريا لجمع وحماية الدليل، ويفسر الفقه اليوناني عبارة (اي شيء) تفسيرا موسعا بحيث تشمل ضبط البيانات المخزنة او المعالجة إلكترونيا، ولذلك فان ضبط البيانات المخزنة في ذاكرة الحاسب الالي لا يثير مشكلة في اليونان اذ يجوز للمحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن ان تكون مقبولة كدليل أمام المحكمة، ياسر الكومي، مرجع سابق، ص269.

و تعتبر مصادرة أجهزة الحاسب الألي أهم وسائل الضبط في جرائم الاعتداء على التوقيع الإلكتروني، إلا أن هذا الإجراء قد لا يكون ذا إمكانية دائمة في اتخاذه كما لو كان الضبط يتم عن بعد في حالة اتخاذ إجراءات ثنائية عن بعد، ولذلك اتجه المشرع المقارن إلى الاعتراف بوجود أساليب أخرى تصلح لكي يتم الضبط بمقتضاها، مثل النسخ (Copy) في حالة عدم وجود إمكانية لضبط القطع الصلبة التي تخزن عليها المستندات المقلدة، فيتم مثلا نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، وهنا نجد أسلوب النسخ يصلح تماما أن ينتج عنه دليل رقمي مقبول أمام القضاء.[1]

وإلى جانب النسخ يوجد أيضا أسلوب تجميد التعامل مع الحاسب الآلي أو احد القطاعات المكونة له، التي تم إستخدامها في ارتكاب الجريمة، حيث تحتوي على ما يفيد من الأدلة على ارتكابها. ومثل هذا الإجراء، يصلح أن يتخذ في مواجهة الحاسبات الخادمة التي تحتوي على مواقع القرصنة، وكذلك يصلح أسلوب التجميد إذا كان القرص الصلب يحتوي على ملفات مشفرة، ويحتاج بالتالي إلى فك شفرتها لكي يمكن التعرف على محتواها والدليل المستمد منها.[2]

وهناك مجموعة من الخطوات العملية التي ينبغي القيام بها عند جمع الأدلة الرقمية وهي[3]:

- **التعرف على الدليل:** وهي الخطوة الأولى في عملية جمع الأدلة الرقمية، حيث يتعرف خبير الأدلة الجنائية على الدليل، ومكان وكيفية تخزينه، ويجب عليه تحديد نوع المعلومات المخزنة، وطريقة تخزينها حتى يستطيع اختيار التقنية المناسبة لاستخلاصها.
- **الاحتفاظ بالدليل:** وفي هذه الخطوة يتم الاحتفاظ بالدليل الرقمي مع محاولة عدم حدوث أي تغيير على البيانات الموجودة. خشية ان يؤثر على مشروعية الدليل. وفي بعض الحالات لا يمكن منع حدوث تغيير ولو بشكل بسيط على بيانات الدليل الموجود بها

[1]–عمر ابوبكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، مرجع سابق، ص21 وما بعدها.

[2]–احمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الاثبات الجنائي، دراسة مقارنة، دار النهضة العربية، مصر، 2015، ص180.

[3]– ياسر الكومي، مرجع سابق، ص270

- **تحليل الدليل:** يتم في هذه المرحلة استخلاص البيانات وتفسيرها بطريقة مفهومة لأغلب الأشخاص عن طريق استخدام مجموعة من التقنيات المعقدة.
- **تقديم الدليل:** وتعتبر آخر الخطوات اللازمة لإدانة المتهم، حيث تقدم الأدلة إلى المحكمة متضمنة طريقة التقديم، ومؤهلات الخبير، وطريقة جمع وتحليل الأدلة، ومدى اقتناع المحكمة بالنتيجة التي إنتهى إليها الخبير، وإصدار الحكم، بإدانة المتهم أو براءته.

رابعا: شروط الدليل الإلكتروني المتحصل من التفتيش الرقمي

الدليل المتحصل من تفتيش نظام الحاسب الآلي والأنترنت لا يكون مشروعا، ويعتبر باطلا إذا تم الحصول عليه بغير الشروط التالية:

1. الشرط الأول: مشروعية الدليل الإلكتروني

يجب أن يثبت لدى المحكمة أن الدليل الذي يحتج به لإثبات جريمة من جرائم الإعتداء على التوقيع الإلكتروني مشروعا، أي أن تكون إجراءات الحصول على الأدلة الجنائية ضمن الإطار العام الذي حدده الدستور، مما يفرض على المشرع عند وضع قواعد الإجراءات الجزائية الالتزام بها وعدم الخروج عنها، وإلا فان الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلا بطلانا مطلقا لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها.

وفي هذا السياق نص الدستور الجزائري، في المادة (46) منه على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون.[1]

- سرية المراسلات والإتصالات الخاصة بكل إشكالها مضمونة
- لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم.
- حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه."

[1]–القانون 01/16 المؤرخ في 06 مارس2016، (ج.ر) عدد (14) لـ07 مارس 2016 المتضمن تعديل الدستور.

- ونصت المادة (47) من الدستور أيضا على انه: "تضمن الدولة عدم انتهاك حرمة المسكن".
- فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه.
- ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة."

ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن جرائم الإعتداء على التوقيع الإلكتروني، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضبطية القضائية، كالتحريض على الغش أو تزوير التوقيع الإلكتروني أو التجسس المعلوماتي، أو زراعة فيروسات والإستخدام غير المصرح به للحاسب الآلي، أو التصنت، أو المراقبة عن بعد.[1]

وتعد من الطرق غير المشروعة أيضا إستخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية. وفي هذا الإطار صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28 على إتفاقية خاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الإتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة، ومدة حفظها محددة زمنيا، وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها، وحق الشخص المعني في التعرف والاطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها.[2]

---

[1]–جميل عبد الباقي الصغير، أدلة الاثبات الجنائي والتكنولوجيا الحديثة، أجهزة الرادار، الحاسبات الالية، البصمة الوراثية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص111.

[2]–في إطار مشروعية الأدلة الإلكترونية، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب في جرائم الحاسب الآلي والأنترنت، كأن يستخدم أعضاء الضبطية القضائية طرقا معلوماتية في أعمال التصنت على المحادثات الهاتفية.

– ويشير رأي فقهي فرنسي إلى قبول القضاء استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم شريطة أن يتم الحصول على الأدلة الجنائية، ومن بينها الأدلة المتحصلة من الحاسب الآلي والأنترنت، بطريقة شرعية ونزيهة، ونفس الشيء نجده في سويسرا وبلجيكا. هلالي عبد اللاه احمد، حجية المخرجات الكمبيوترية في الاثبات الجنائي، ط1، دار النهضة العربية، مصر، 1997، ص14، ص22.

2. الشرط الثاني: حجية الدليل الإلكتروني (مبدأ يقينية الدليل الإلكتروني)

يشترط في الأدلة المتحصل عليها من الحاسب الآلي وشبكة الأنترنت أن تكون غير قابلة للشك ومن شأن هذه الأدلة اقناع القاضي إلى حد الجزم واليقين، وبالتالي الحكم بالإدانة[1]، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية، والمصغرات الفيلمية، وغيرها من الإشكال الإلكترونية التي تتوافر سواء عن طريق الوصول المباشر، أو كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسب الآلي على الشاشة الخاصة به أو على الطرفيات[2]، وبالنتيجة يستطيع القاضي تحديد القوة الاستدلالية للأدلة، انطلاقا مما يكونه في ذهنه من تصورات واحتمالات، ونسبة أي من جرائم الإعتداء على منظومة التوقيع الإلكتروني إلى شخص معين من عدمه.

3. الشرط الثالث: إمكانية مناقشة الأدلة الإلكترونية

أي أن تكون الأدلة المتحصلة من جرائم الحاسب الآلي والأنترنت محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، سواء كانت هذه الأدلة مطبوعة أم بيانات معروضة على شاشة الحاسب الآلي، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية.[3]

وتنطبق هذه الأحكام على كل الأدلة يتم الحصول عليها من خلال بيئة تكنولوجيا المعلومات، وأيضا بالنسبة لشهود جرائم الإعتداء على التوقيع الإلكتروني أثناء المحاكمة، الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، ومثول خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم، أمام المحكمة، لمناقشة تقاريرهم التي خلصوا اليها وصولا للحقيقة.

الفرع الثالث: الشهادة الإلكترونية والخبرة في مجال الجرائم الواقعة على التوقيع الإلكتروني

لا تختلف الشهادة في مجال الجرائم المعلوماتية من حيث ماهيتها عنها الجرائم التقليدية، إلا أنها تكتسي أهمية بالغة في مجال الإثبات الجنائي عل غرار وسائل الإثبات الأخرى كالمعاينة

---

[1]– بن فردية محمد، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، المجلة الأكاديمية للبحث القانوني، العدد 01، ص281، 2014.

[2]–احمد يوسف الطحطاوي، مرجع سابق، ص160.

[3]– نفس المرجع، ص157.

والتفتيش والخبرة، وعيه سيتم تناول مدلول الشهادة الإلكترونية والشاهد المعلوماتي في مجال جرائم التوقيع الإلكتروني، ثم نتعرض إلى الخبرة التقنية ودورها في إثبات هذه الجرائم.

أولا: الشهادة الإلكترونية والشاهد المعلوماتي في مجال جرائم الاعتداء على التوقيع الإلكتروني

1. مدلول الشهادة الإلكترونية في مجال جرائم الاعتداء على التوقيع الإلكتروني:

يمكن تعريف الشهادة بصفة عامة بأنها: "الأقوال التي يدلي غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها"[1]. أما في مجال الجرائم الإلكترونية فيقصد بالشهادة الإلكترونية: "ذلك الشخص المتخصص في مجال المعلوماتية، والذي يستطيع وبطلب من الجهات المختصة، الولوج إلى نظام المعالجة الآلية للمعطيات بهدف الحصول على الأدلة الرقمية".[2]

وتخضع مخرجات الحاسب الآلي لقواعد الشهادة السماعية في جرائم الاعتداء على التوقيع الإلكتروني، ومن التطبيقات على ذلك ما أُثير في الفقه الأمريكي حول إمكانية تطبيق قواعد السماع على مخرجات الحاسب الآلي الواردة في المادة (6)/803، حيث انتهت محكمة Blackburn إلى أن مخرجات الحاسب الإلكتروني لا تصلح لتطبيق قواعد السماع، واعتبرت المحكمة المستند الإلكتروني الناتج عن الحاسب الإلكتروني في تلك الحالة غير معترف به وفقا لتلك المادة[3]. غير أن محكمة استئنافBlackburn خالفت ذلك النهج واعتبرت أن مخرجات طابعة الحاسب الآلي يعتمد عليها بشكل كاف، ويمكن قبولها وفقا لإستثناء السماع في المادة (24)/806 من قانون الإثبات الفيدرالي.

ومؤدى ذلك إستثناء سجلات الكمبيوتر المخزنة التي تحتوي على بيانات سماعية أو بصرية من قاعدة السماع، وذلك متى قدمت لإثبات جريمة إعتداء على التوقيع الإلكتروني، غير أنه وحتى

---

[1]–علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012، ص61.

[2]–عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، من 12 إلى 14 نوفمبر 2007، الرياض، السعودية، ص21.

[3]–Fed, r. evidence 803 (6) (stating that business records must be "made…by or transmitted by, a person").

تقبل المحكمة في تلك الحالة المستند الإلكتروني كدليل إثبات، يجب استيفاء شرطي المشروعية والثقة عند التحقق من بيانات المستند الإلكتروني.[1]

2. مدلول الشاهد المعلوماتي في جرائم الإعتداء على التوقيع الإلكتروني:

تعد شهادة الشهود في الجرائم الواقعة على التوقيع الإلكتروني من الأدلة الهامة التي يمكن تقديمها للمحكمة، بالنظر للطبيعة الخاصة لهذه الجرائم المستحدثة وهي بهذا الشكل تمثل العامل الحاسم في الاثبات الجنائي، ويعرف الشاهد في جرائم الإعتداء على التوقيع الإلكتروني بأنه: " ذلك الشخص الفني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات أساسية وجوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية للمعطيات أو للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة تتعلق بالجريمة داخله، ويطلق على هذا الشاهد اسم الشاهد المعلوماتي نسبة للجريمة المعلوماتية، وذلك تمييزا له عن الشاهد التقليدي".[2]

ويشمل بهذا المفهوم الشاهد المعلوماتي في جرائم الإعتداء على التوقيع الإلكتروني عدة اقسام أهمها:

- **القائم على تشغيل الحاسب الآلي:** وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز وإستخدام لوحة المفاتيح في إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد إعداد البرامج، ودراية كافية بآلية إنشاء التوقيع الإلكتروني .
- **المبرمجون:** وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين: **الأولى:** هم مخططو برامج التطبيقات – **والثانية:** هم مخططو برامج النظم.[3]

---

[1]–ايمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق، ص314.

[2]–عبد الفتاح بيومي حجازي، الجوانب الاجرائية لاعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، مصر، ط1، 2009، ص ص612 –613

[3]–يتولى الموظفين المكلفين باعداد برامج التطبيقات الحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما المكلفين باعداد برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنهم يقومون بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي تعديلات في

- **المحللون:** والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام، أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات.
- **مهندسو الصيانة والاتصالات:** وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.
- **مديرو النظم:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

وبالرجوع إلى نص المادة (05) الفقرة الأخيرة من القانون رقم: 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها، فقد يطلب هذا الشخص على سبيل مساعدة السلطات القضائية في جوانب تقنية لحل لغز الجريمة، كما قد يستعين به الخبير في انجاز الخبرة الرقمية بموافقة سلطات التحقيق، كما يمكن أيضا أن يحمل صفة الشاهد المعلوماتي في جريمة وقعت في المؤسسة التي يعمل بها. ومثال ذلك طلب الجهات القضائية من مهندس في الإعلام الآلي تخصص برمجة شهادته للكشف عن ملابسات الجريمة.

كما جاءت المادة (10) من القانون نفسه لتحدد إلتزامات مقدمي الخدمات والتي من بينها مساعدة السلطات القضائية المكلفة بالتحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات وكذلك حفظ المعطيات المتعلقة بحركة السير[1]، والأمر نفسه بالنسبة للمادة (12)، حينما نصت على الالتزامات الخاصة لمقدمي خدمة الأنترنت مثل: حفظ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، وكذا المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم للإتصال،

إضافات لهذه البرامج، انظر هلالي عبد اللاه، التزام الشاهد بالاعلام في الجرائم المعلوماتية، دار النهضة العربية، 1997، ص33 وما بعدها.

[1]–المادتان (11/10) من القانون رقم: 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وعناوين المواقع المطلع عليها ... الخ[1]. ففي كل هذه الحالات يمكن للجهات القضائية الاستعانة بهؤلاء الأشخاص حسب مقتضيات التحقيق، سواء كانوا أشخاصا طبيعيين أو معنويين بصفتهم كشهود معلوماتيين.

3. التزامات الشاهد المعلوماتي في جرائم الاعتداء على التوقيع الإلكتروني:

إن طبيعة التحقيق في الجرائم الواقعة على التوقيع الإلكتروني توجب على الشاهد المعلوماتي الإدلاء إلى القضاء بكل ما يحوزه من معلومات جوهرية مثل: شفرات الدخول للنظام المعلوماتي لاستخراج الأدلة الرقمية بما فيها بيانات إنشاء التوقيع الإلكتروني والآلية المستعملة في إنشاءه والتحقق منه ومفاتيح التشفير الخاصة والعمومية والبيانات المتعلقة بشهادة التصديق الإلكتروني[2]

---

[1]– المادة (12) من القانون رقم: 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]–اختلف الفقه المقارن بين مؤيد ومعارض لفكرة قيام الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات، وفي هذا الصدد برز اتجاهين رئيسيين:

الاتجاه الأول: يرى انصار هذا التجاه أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة، أن يقوم بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ففي إتفاقية التربس تنص المادة 39 من القسم السابع على أن البيانات المحتفظ بها لدى الغير والمقدمة لجهات حكومية تتمتع بالسرية، ولا يحق لأي شخص طبيعي أو معنوي أن يفصح عن محتوى تلك البيانات، ومن ثم، فإن لهم الحق بموجب تلك المادة في الامتناع عن الإدلاء بالشهادة بشأن بيانات المستند الإلكتروني حتى ولو كانت محلا للاعتداء.– ففي لوكسمبورج، الشاهد ليس مجبرا على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة، وبالتالي من الصعب إجباره على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه في ذاكرة الحاسب الآلي، وان كان يستطيع الوصول إليها نظرا لمعرفته بكلمات المرور السرية، أما إذا تعاون الشاهد على هذا النحو فإن دوره يكون اقرب إلى الخبرة منه إلى الشهادة، وفي ألمانيا، تذهب غالبية الفقه إلى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب الآلي، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وفي تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة.

وفي فرنسا توجد بعض الفئات الممنوعة بنص القانون من الإفصاح عن بعض البيانات التي تكون بحوزتها مثل المحامين والأطباء متى تعلقت أسرار مهنتهم ومن ثم فمتى كان تحت يد أيا من هؤلاء مستندا يحمل توقيعا مزورا متعلقا بسر من أسرار مهنته أو كان محلا للتلاعب، فلا يجوز إلزامه بتقديمه أو الشهادة بشأنه.

الاتجاه الثاني: تبنى هذا الاتجاه إلزامية طبع ملفات البيانات من قبل الشاهد، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ففي فرنسا يرى جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفا

وقد وضع المشرع الجزائري أمام الشاهد بصفة عامة كل الوسائل التي تمكنه من الإدلاء بشهادته دون زيادة أو نقصان وتحت طائلة العقوبات في حالة عدم الحضور أو رفضه للشهادة بعد تصريحه بمعرفة الجاني[1]. غير أن التنظيم القانوني للقواعد الإجرائية في الدعاوى المعتمدة على أدلة رقمية والتي تتصل أساسا بالعالم الافتراضي يجب إعادة توصيفها قانونا، بل وتنظيمها، بشكل لا يضع الشاهد موضع المسائلة في حالة إخلاله بالسر المهني بما لا يحرم القضاء فرصة الإفادة من شهادة الشاهد في الكشف عن الجريمة الإلكترونية، خاصة في ظل صعوبة إستخلاص الأدلة الرقمية في هذا النوع من الجرائم[2].

ولا ينشأ التزام الشاهد بالإعلام في جرائم الإعتداء على التوقيع الإلكتروني، إلا إذا توافرت ثلاثة شروط:

- **الشرط الأول:** أن تكون جريمة من جرائم الإعتداء على التوقيع الإلكتروني قد وقعت بالفعل سواء كانت جناية أو جنحة، إذ لا يصح هذا الالتزام، ضبط جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، كما أنه لا يكفي، مجرد وقوع جريمة معلوماتية للقول بقيام هذا الالتزام، لابد أن تكون مما يعتبرها القانون جناية أو جنحة. [3]

بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج، ما عدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بأداء الشهادة، وفي هولندا يتيح قانون الحاسب الآلي لسلطات التحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة للاختراق والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، أو حل رموز البيانات المشفرة. وقد تجاوزت المادة 18 من إتفاقية بودابست عام 2001 بشأن جرائم الحاسب ذلك المدى عندما ألزمت الغير ليس فقط بتقديم ما يحوزه من معلومات، وإنما أيضا بالتحفظ والإفصاح عن بيانات المستندات الإلكترونية التي يعتقد أنها محلا للتلاعب أو المحو، والتي من شأنها الكشف عن الجريمة وتحديد هوية مرتكبيها، راجع ايمن رمضان محمد احمد، مرجع سابق، ص319-321.

[1]-حيث تنص المادة (98) من (ق.إ.ج.ج) على: "كل شخص بعد تصريحه علانية بأنه يعرف مرتكبي جناية أو جنحة يرفض الإجابة على الأسئلة التي توجه إليه في هذا الشأن بمعرفة قاضي التحقيق يجوز إحالته إلى المحكمة المختصة والحكم عليه بالحبس من شهر إلى سنة وبغرامة من 1.000 إلى 10.000 دينار أو بإحدى هاتين العقوبتين".

[2]-يزيد بوحليط، مرجع سابق، ص 347

[3]-عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص 623.

- الشرط الثاني: أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة، وهو شرط هام للالتزام بالإعلام في الجرائم المعلوماتية ويتمثل مضمون هذه المعلومات الجوهرية في ثلاثة عناصر هي: طبع ملفات البيانات، والإفصاح عن كلمات السر، والكشف عن مفاتيح الشفرات. [1]
- الشرط الثالث: أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية، فلا يكفي التزام الشاهد بالإعلام في جرائم الاعتداء على التوقيع الإلكتروني أن نكون بصدد جريمة وقعت بالفعل، وأن يكون الشاهد على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة، بل ينبغي إلى جانب ذلك أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية. [2]

ثانيا: الخبرة التقنية في مجال جرائم الاعتداء على التوقيع الإلكتروني

تعتبر الخبرة التقنية في مجال المساعدة القضائية أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنولوجيا المعلومات والأنترنت، ونظرا للطبيعة الخاصة للجرائم الواقعة على التوقيع الإلكتروني، من حيث طابعها الفني المتعلق بأساليب ارتكابها وسهولة إخفاء أو محو الدليل، بات من الضرورة استعانة القاضي وأجهزة البحث والتحري بخبير متخصص في المعلوماتية لاستخلاص الدليل الإلكتروني.

وتعرف الخبرة أنها: " الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقييم الأدلة، دون المسائل القانونية التي يحتاج تقديرها إلى معرفة فنية ودراية علمية لا تتوفر لدي عضو السلطة القضائية المختص بحكم عمله وثقافته".[3]

وقد أجاز المشرع الجزائري لجهات التحقيق وللمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، حيث تنص المادة (143) من (ق.ا.ج.ج) على: "لجهات التحقيق أو الحكم

---

[1]–هلالي عبد الاله جلال، تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي، دار النهضة العربية، مصر1997، ص67–68.

[2]–ايمن رمضان محمد، مرجع سابق، ص323.

[3]–شيماء عبد الغني عطاالله، مرجع سابق، ص217.

عندما تعرض لها مسالة ذات طابع فني ان تأمر بندب خبير اما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو الخصوم..."[1]، في حين حدد المشرع الهدف من إجراء الخبرة بموجب نص المادة (125) من قانون الإجراءات المدنية والإدارية رقم: 08/09 المؤرخ في 2008/02/25 التي تنص على:

"تهدف الخبرة إلى توضيح واقعة مادية تقنية أو علمية محضة للقاضي"[2]، كما تجدر الإشارة إلى انه ليس هناك اختلاف بين الخبرة القضائية عموما والخبرة التقنية من حيث القواعد القانونية المنظمة لها، إلا فيما يخص الجوانب الفنية التي تحكم عمل الخبير التقني، ورغم هذا هناك بعض التشريعات ومنها التشريع البلجيكي الذي نظم الخبرة التقنية في مجال الجرائم الإلكترونية بموجب قواعد خاصة.[3]

1. أساليب عمل الخبير التقني:

إن الوصول إلى دليل مادي في جرائم الإعتداء على التوقيع الإلكتروني، يستدعي إستخدم الخبير الأساليب العلمية التي يقوم عليها تخصصه تتلخص في أسلوبان: [4]

---

[1]–المواد (143–156) من (ق.ا.ج.ج).

[2]–تهدف الخبرة التقنية في الجرائم الإلكترونية إلى:

- الكشف عن الدليل الرقمي.
- إجراء الاختبارات التكنولوجية والعلمية على الدليل الرقمي للتأكد من أصالته وصلاحيته ومصدره لتقديمه كدليل لأجهزة إنفاذ القانون.
- اصلاح الدليل واعادة تجميعه من المكونات المادية للحاسوب (Hard Drive).
- عمل نسخ اصلية عن الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.
- جمع الاثار المعلوماتية الرقمية (Cyber Trial Digital) التي قد تكون تبدلت خلال الشبكة المعلوماتية.
- استخدام الخوارزميات (Algorithmes) للتأكد من ان الدليل لم يتم العبث به او تعديله، راجع، خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص 302–303.

[3]–حيث تنص المادة (88) من القانون البلجيكي الصادر في: 2000/11/23 على: " يجوز لقاضي التحقيق وللشرطة القضائية ان يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، او الدخول للبيانات المخزونة او المعالجة او المنقولة بواسطته"، راجع، علي عدنان الفيل، المرجع السابق، ص 30.

[4]–احمد عصام عجيلة، مرجع سابق، ص448.

- **الأول:** يقوم الخبير بعملية تحليل تقني للمواقع الإلكترونية التي كان الإعتداء على التوقيع الإلكتروني محلا لها، والتي سبق وأن قام بتحديدها وحصرها، وصولا لكيفية إعدادها ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها وكيفية التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الأنترنت IP الذي ينسب إلى جهاز الحاسب الآلي والحصول على رقمه وتحديد موقعه لمعرفة الجاني.
- **الثاني:** الانتقال إلى الجهة التي رخصت بإصدار التوقيع الإلكتروني للإطلاع على آلية إنشاء التوقيع الإلكتروني الموصوف والتحقق منه قبل إصدار التوقيع الإلكتروني[1]، والوقوف على مدى التطابق الفني بين التوقيع الإلكتروني المستخدم في ارتكاب الجريمة والتوقيع الإلكتروني الصحيح، والكيفية الفنية التي تم من خلالها الاعتداء عليه والحاسب الإلكتروني والوسائط الفنية المستخدمة في ذلك.

2. **موقف المشرع الجزائري:**

أدرك المشرع الجزائري خصوصية الجريمة الإلكترونية وصعوبة التحقيق فيها، لذا حاول وضع نصوص قانونية تسهل وضع ترتيبات لإجراء الخبرة الرقمية وذلك على عدة مستويات:

- **على مستوى تعيين الخبراء:**

كما رأينا سلفا، نلاحظ أن المشرع الجزائري ترك المجال مفتوحا أمام جهات التحقيق والقضاة حول إمكانية الاستعانة بالخبير الاستشاري من خارج الجدول القضائي نظرا لخصوصية الجريمة الإلكترونية ولصعوبة التحقيق فيها، ولإدراكه أهمية التطور التكنولوجي السريع في مجال تكنولوجيات الإعلام والاتصال، ناهيك على إمكانية عدم توفر كفاءات وخبرات عالية ضمن الخبراء المقيدين في الجداول، حيث تنص المادة (144) من (ق.إ.ج.ج) على: " يختار الخبراء من الجدول الذي تعده المجالس القضائية... ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول". ويستوي أن يكون هذا الخبير شخصا طبيعيا أو معنويا، والعبرة بتوافر المعرفة العلمية والخبرة اللازمتين في مجال تكنولوجيا المعلومات التي تتطور بصورة مذهلة.

[1]–انظر المادة (10) وما بعدها من القانون 15–04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

وفي السياق نفسه، أجاز المشرع لجهات التحقيق أثناء تفتيش المنظومة المعلوماتية الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، وهذا بموجب المادة(05) من القانون رقم: 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها التي تنص على: "... يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

حيث لم يحدد المشرع طبيعة هذا الشخص فقد يكون شخصا طبيعيا أو معنويا، كما قد يكون خبيرا أو شخصا عاديا، ولكنه يملك مهارات وقدرات عالية في مجال من مجالات تكنولوجيا الإعلام والإتصال. في هذا الشأن ونظرا للطبيعة الخاصة للجرائم الإلكترونية، وفي إطار الإتفاق مع الجهات القضائية المختصة، يمكن الاستعانة بالقراصنة الذين انهوا عقوبتهم أو تمت تبرئه ساحتهم، قصد الكشف عن الجريمة الإلكترونية ومرتكبيها، نظرا للمهارات والخبرات الاستثنائية التي يمتلكونها في مجال تقنية المعلومات وشبكة الأنترنت.[1]

- **على مستوى إنشاء الهيئات:**

نص المشرع الجزائري على إنشاء هيئات بكوادر مؤهلة تقوم بإجراء الخبرة الرقمية سواء بمناسبة إجراء تحقيق أو المساعدة على إجرائه وذلك كما يلي:

- إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي[2]، حيث تم تنظيم المصالح والأقسام والمخابر لذات المعهد بموجب قرار وزاري مشترك تضمن 05 مخابر جهوية، يحتوي كل

---

[1]– خالد محمد المهيري، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، دبي، الإمارات العربية المتحدة، معهد القانون الدولي، ص489

[2]–المرسوم الرئاسي رقم: 04–432المؤرخ في: 29/12/2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، حيث نصت المادة(05) منه على: "يتولى المعهد المهام الآتية: ... إعداد تقارير الخبرة بناء على طلب من السلطات المختصة المؤهلة قانونا – القيام بأعمال التكوين وتجديد المعارف وتحسين المستوى والتكوين ما بعد التدرج في ميداني علم التحقيق الجنائي والإجرام..."، (ج.ر) رقم: 84 المؤرخة في: 29/12/2004، ص 25.

مخبر على مصالح تقنية تضم بدورها 06 مخابر من بينها مخبر الأدلة المعلوماتية وجرائم الكمبيوتر إضافة إلى مخبر استغلال الهواتف المحمولة. [1]

- إنشاء قيادة الدرك الوطني للمركز الوطني لمكافحة الجريمة المعلوماتية الموجود "ببئر مراد رايس" بالجزائر العاصمة، مهمته تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها، وكذا تأمين الأنظمة المعلوماتية.
- إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام[2]، وهي مؤسسة عمومية ذات طابع إداري تشكل أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يقدم خدمات أساسية في مجال خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية.

[1]–القرار الوزاري المشترك المؤرخ في: 2007/04/14، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، (ج.ر) رقم: 36 المؤرخة في: 03 يونيو 2007، ص 14–18.

[2]–المرسوم الرئاسي رقم: 183–04 المؤرخ في: 26 جوان 2004 يتضمن أحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج.ر) رقم: 41 المؤرخة في: 2004/06/27، ص18.

الفصل الثاني

إجراءات المحاكمة في الجرائم الواقعة على التوقيع الإلكتروني

تمهيد:

لا يتوقف الأمر عند حد الكشف عن الجرائم الواقعة ضد التوقيع الإلكتروني وشهادة التصديق الإلكتروني والقبض على الجناة، إذ من الضروري تتبع الدعوى العمومية بمحاكمتهم عن تلك الجرائم وصولا لإنزال العقاب عليهم. وفي ظل الإستخدام المتزايد لتقنية التوقيع الإلكتروني في مجالات متعددة، لم تعد الجرائم الواقعة على هذه التقنية محصورة في حدود دولة بعينها، بل تخطى مداها إلى خارج الدولة، مما أثار إشكالية إنعقاد الاختصاص بنظر تلك الجرائم لأكثر من دولة من بين الدول التي ارتكب في إقليمها أي إعتداء إجرامي يقع على التوقيع الإلكتروني، ومدى إعمال قواعد التنازع الايجابي بين قوانين تلك الدول من جهة أولى، ومن جهة ثانية ظهرت الحاجة إلى تعاون دولي في مجال إثبات هذه الجرائم والحيلولة دون إفلات المجرم من العقاب في حالة ما إذا كان القانون الداخلي للدولة المتواجد على إقليمها المتهم لا يسمح لتلك الدولة بمحاكمته عن جريمته. في ضوء ما تقدم قسمت دراسة هذا الفصل إلى مبحثين على النحو التالي:

- **المبحث الأول:** الاختصاص القضائي في الجرائم الواقعة على التوقيع الإلكتروني
- **المبحث الثاني:** التعاون الدولي في مجال إثبات الجرائم الواقعة على التوقيع الإلكتروني

المبحث الأول:

الاختصاص القضائي في الجرائم الواقعة على التوقيع الإلكتروني:

الاختصاص القضائي هو صلاحية القاضي العادي لمباشرة ولايته القضائية في نطاق معين، ومن هنا يجب التمييز بين ولاية القضاء والاختصاص، فالأولى تضفي على القاضي الصلاحية المجردة لمباشرة جميع إجراءات الخصومة المدنية والجنائية، أما الثانية تقصر هذه الصلاحية على نوع معين من الإجراءات وفي حدود معينة[1]، فلا يكفي لكي يستجمع الحكم سلامته القانونية أن يكون صادرا من محكمة قضائية مشكلة تشكيلا قانونيا، إنما يلزم فوق ذلك أن يكون صادرا من محكمة لها الاختصاص في إصداره[2].

ولذلك يعتبر الاختصاص القضائي من أهم المواضيع التي يجب تحديدها في التصدي لأي جريمة كانت تقليدية أو مستحدثة، وهو ما سيتم التطرق له في هذا المبحث الذي قسم إلى مطلبين، تناول المطلب الأول: إختصاص القضاء الجنائي الوطني، أما المطلب الثاني، فتعرض إلى مبدأ العالمية في الاختصاص الوطني.

المطلب الأول:

إختصاص القضاء الجنائي الوطني

تعد الدعوى الجزائية الوسيلة التي من خلالها يستطيع المجتمع محاسبة مرتكبي الجرائم التي من شأنها أن تهز إستقراره وتعرض مصالحه للخطر، ويختص بنظر هذه الدعوى الجزائية القضاء الجنائي وفقا لقيود وضوابط يلتزم بها ويخضع لها نظرا لارتباط قواعد الاختصاص بحقوق وحريات الأفراد، ذلك أن التقيد بضوابط الاختصاص يعبر عن شرعية ممارسة السلطة فعدم التقيد بها يعني ممارسة الإجراء خارج نطاق القانون ومخالفة لحقوق وحريات الأفراد، وتجاوزا لحقوق المتهم

[1]–أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الصفحة الثامنة، دار النهضة العربية، القاهرة، 2012، ص704.

[2]–محمد زكي أبو عامر، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 1994، ص735.

والضمانات الواجب توافرها له، لأنه من متطلبات المحاكمة العادلة أن يمثل المتهم أمام محكمة مختصة تناسب جسامة جريمته أو مكانها أو شخصه.

ومن خلال استعراض أحكام القانون نجد أن الاختصاص القضائي في المواد الجنائية ثلاثة أنواع: إختصاص مكاني، اختصاص نوعي واختصاص شخصي.

لذلك سيتم تقسيم هذا المطلب إلى ثلاثة فروع، حيث يتناول الفرع الأول الاختصاص المكاني، فيما يتطرق الفرع الثاني للاختصاص النوعي ويتم التعرف في الفرع الثالث على الاختصاص الشخصي.

الفرع الأول: الاختصاص المكاني

إن المقصود بالقيد المكاني هو تقيد المحكمة بالاختصاص المكاني وهو عدم جواز نظر المحكمة في الجرائم التي وقعت في خارج المكان الذي حدد فيه اختصاصها[1] وحسب المادة 40 من قانون الإجراءات الجزائية فإنه يتحدد الاختصاص المحلي بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المستثنية في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر وهذه الضوابط التي حددها القانون لاختصاص قاضي التحقيق محليا هي ذاتها التي حددها كذلك القانون بالنسبة لمحكمة الجنح والمخالفات في نص المادة 329 من قانون الإجراءات الجزائية الجزائري.[2]

وهذه الضوابط الثلاثة المعتمدة من قبل المشرع لتحديد الاختصاص محليا أو إقليميا تعتمد عليها أغلب التشريعات العربية والغربية.

---

[1]–عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون المحاكمات الجزائية، الجزء الثاني، الطبعة الثانية، مطبعة المعارف، بغداد 1974، ص88.

[2]–نص المادة 329 ق إ ج ج« تختص محليا بال بنظر في الجنح، محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.....»

ونظرا لأهمية الضوابط المتقدمة في تحديد الاختصاص المكاني نتولى توضيح ذلك كالآتي:

أولا: مكان وقوع الجريمة

إن مكان ارتكاب الجريمة له أهمية كبيرة في تحديد المحكمة المختصة في نظر الدعوى سواء في مرحلة التحقيق أو المحاكمة، لأنه فيه إختل الأمن واضطربت المراكز القانونية المستقرة وتم الإعتداء على الحقوق التي يحميها القانون ولو أن المشرع قدر أن من الملائم في السياسة التشريعية أن تحدد محكمة واحدة تنظر الجريمة لأختار المحكمة التي ارتكبت فيها، لأن مكان ارتكاب الجريمة يحقق العدالة بصورة أفضل ويحقق أهداف العقوبة في تحقيق الردع وإعادة الأمن إلى نصابه بالإضافة إلى ذلك فإن مكان ارتكاب الجريمة يسهل عمل المحكمة الجزائية وضبط أدوات الجريمة والوصول إلى الأدلة والقبض على المتهم وإنجاز كافة إجراءات الدعوى الجزائية[1] وفي تحديد المحكمة المختصة في نظر الدعوى الجزائية إذا تحققت جميع عناصر الركن المادي للجريمة في منطقة واحدة وينعقد الاختصاص للمحكمة التي وقعت ضمن دائرتها، وهذا هو حال جل الجرائم الكلاسيكية، ولكن يثور الإشكال في الجرائم المستحدثة فإن تحديد مكان هذه الجرائم ليس بهذه السهولة خاصة إذا وقعت في أكثر من مكان واحد، كما لو وقعت على حدود مكانين أو وقع السلوك الإجرامي في مكان معين وتحققت النتيجة في مكان آخر فإن المحكمتين يختصان معا في الجريمة، وإذا تحققت بعض الحلاقات السببية في مكان ثالث كانت هذه المحكمة مختصة أيضا وفي الفقه ظهرت بصدد تحديد مكان الجريمة ثلاث نظريات، الأولى تعتمد المحل الذي يقع فيه النشاط ألجرمي لا الآثار التي ينتجها فعل الجريمة. والثانية تأخذ بنظر الاعتبار في تحديد مكان الجريمة بالآثار التي يخلفها النشاط الجرمي وتعول على مكان حصول الضرر (النتيجة الإجرامية) لأن هذا الأمر هو الذي قصد الجاني إحداثه وهو الذي يؤثر في المشاعر تأثيرا يستوجب الردع.

أما النظرية الثالثة تتضمن بأن الجريمة تعد قد ارتكبت في المكان الذي قام الجاني فيه بعمله التنفيذي المخالف للقانون، كما أنها تعد ارتكبت في المكان الذي حدثت فيه النتيجة لهذا الفعل أو الذي كان ينتظر أن تحدث فيه وهي بذلك تجمع بين النظريتين السالفتين في رأي واحد[2] ويمكن القول أن مبدأ الإقليمية يطبق على الجرائم التي ترتكب داخل إقليم الدولة مهما كانت طبيعتها أو وصفها فهو

[1]–محمود نجيب حسين، شرح قانون الإجراءات الجنائية، الطبعة الثانية، القاهرة، 1982، ص389.

[2]–كمال أنور محمد، تطبيق العقوبات من حيث المكان، القاهرة، 1965، ص90.

يتمتع بقدر كبير من الأخلاق والعموم[1] ووفقا لرأي السائد في الفقه والقضاء الجنائي العربي والأجنبي، فإنه لا يشترط أن ترتكب الجريمة بكاملها داخل إقليم الدولة حتى يسري قانونها، إذ يكفي أن يتحقق أحد العناصر المكونة لها داخل هذا الإقليم، وبالتحديد يكفي أن يتحقق جزء من ماديات في النشاط أو النتيجة أو حتى التسلسل السببي الذي يرتبط فيما بينهما[2] وهذا يتماشى مع سيادة الدولة، وقد كان سائدا بصفة مطلقة في المجتمعات البدائية التي كانت الدول منغلقة على نفسها انغلاقا يتسم بعداء كل منها اتجاه الأخرى، وهو يفسر ظاهرة كثرة الحروب والإعتداءات في هذه المرحلة. وإن كان مبدأ الإقليمية هو الأصل في بسط القانون على أراضي الدولة لحماية مصالحها وحماية مواطنيها، فإن هذا الاختصاص المكاني المحدد بأقاليم جغرافية محددة داخل الدولة الواحدة قد يتنوع ليشمل مناطق أخرى في جرائم معينة حددها نص القانون صراحة وهو ما يعرف بالاختصاص الإقليمي الموسع في المادة الجزائية[3] إن البداية الحقيقية لظهور فكرة الأقطاب القضائية المتخصصة كانت في صورة اختصاص إقليمي موسع في المادة الجزائية، ظهرت رسميا في 2004 مع صدور القانون رقم 141/04المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155/66 المؤرخ في 8 نوفمبر سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، عندما تناول في المواد 37، 40، 329 إمكانية تمديد الاختصاص الإقليمي لكل من وكيل الجمهورية، قاضي التحقيق والمحكمة عندما يتعلق الأمر بالبحث والتحري في جرائم معينة على سبيل الحصر، وهذا يخص بعض المحاكم تتحد عن طريق التنظيم.[4]

---

[1]–نص المادة الثالثة من قانون العقوبات الجزائري «يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية»

[2]–عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان وفقا لمعطيات التكنولوجيا المعاصرة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، سنة 2006، ص15.

[3]–نظم القانون الجزائري موضوع الاختصاص الإقليمي للجهات القضائية ذات الاختصاص الموسع في المادة الجزائية أو المدنية بنصوص متعددة، لاسيما القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية وقانون الإجراءات المدنية والإدارية الصادر بموجب القانون رقم 09/08 بالإضافة إلى بعض النصوص الخاصة على غرار قانون مكافحة الفساد 2006.

[4]–انظر المرسوم التنفيذي رقم 348/06 مؤرخ في 5 أكتوبر سنة 2006 المتضمن تمديد الاختصاص المحلي لبغض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة رسمية عدد 63، ص29.

وقد بدأت الأقطاب القضائية المتخصصة في المادة الجزائية العمل بالفعل في سنة 2008، حيث تم فعلا إعطاء إشارة الانطلاق الرسمي للأقطاب الجزائية المتخصصة في كل من الجزائر العاصمة يوم26 فيفري 2008، وقسنطينة يوم 3 مارس 2008، ووهران يوم5مارس 2008 أما تدشين مقر القطب الجزائي المتخصص لمحكمة ورقلة وإعطاء إشارة الانطلاق الرسمي لنشاط هذا القطب فقد كانت يوم 19 مارس 2008 بإشراف من وزير العدل وحافظ الأختام السيد الطيب بلعيز هذا في المادة الجزائية[1] والجرائم التي حددها القانون والتي يجوز تمديد الاختصاص الإقليمي فيها لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة هي جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة لآلية المعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[2]

ولقد أحسن المشرع بتوسع الاختصاص الإقليمي في هذه الجرائم الخطيرة خاصة تلك المتعلقة بأنظمة المعالجة الآلية للمعطيات وغيرها وتوجهه نحو التخصص القضائي من خلال إنشاء أقطاب قضائية تتضمن قضاة متخصصين على مستوى النيابة والتحقيق والمحاكمة تستأثر بالاختصاص في تلك الجرائم، ذلك أن هذه الجرائم تتطلب من أجل تعقب مرتكبيها وإثبات الأفعال المحرمة وإسنادها إليهم، الكثير من الوسائل البشرية واللوجيستية والتحكم في التكنولوجيا الحديثة من أجل إدارة بحث وتحريات فعالة، هذا من جهة، وتنطوي على مخاطر كبيرة وآثار بالغة على الحقوق والحريات من جهة أخرى، الأمر الذي لا يمكن توفير هذه الوسائل في كل المحاكم، مما حذا بالسلطات إلى الاهتداء إلى فكرة تجميع هذه الإمكانيات في محاكم محددة على شاكلة الأقطاب المتخصصة، وفي هذا الصدد قال الأستاذ عبد السلام ذيب: " وإن إنشاء هذه الأقطاب، يفرضه منطق تجميع الوسائل البشرية والمادية في عدد محدد من الجهات القضائية بسب حجم وتعقيد المنازعات الذي يتطلب تخصصا دقيقا ومتزايدا باستمرار ".[3]

---

[1]–محمد بكرار شوش، الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، العدد الرابع عشر، جانفي 2016، ص307.

[2]–أنظر المادة 37–40–329 من قانون الإجراءات الجزائية.

[3]–محمد بكرار شوش، المرجع السابق، ص314.

ثانيا: محل إقامة المتهم أو مكان القبض عليه.

حسب المادة 40 من قانون الإجراءات الجزائية الجزائري فإن المحكمة وفقا للمادة 329 من نص القانون يتحدد الاختصاص الإقليمي أو المحلي بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقتراف الجريمة أو بمحل القبض على أحد هؤلاء حتى ولو كان القبض قد حصل لسبب آخر، وتظهر أهمية انعقاد الاختصاص لمحكمة محل إقامة المتهم عندما لا يعرف مكان ارتكاب الجريمة بصورة محددة ومكان الإقامة هو المسكن المعتاد وقت ارتكاب الجريمة لا وقت المحاكمة، وقد عرفته محكمة النقض المصرية بالقول (يقصد بلفظ المسكن في معنى قانون الإجراءات الجنائية، أخذ من مجموع نصوصه، كل مكان يتخذه الشخص مسكنا لنفسه على وجه التوقيت والدوام، بحيث يكون حرما آمنا لا يباح لغيره دخوله إلا بإذنه)[1] وترتيبا على ما تقدم يتضح أن محل الإقامة هو المكان الذي يمكن أن تتحصل منه على المعلومات المتعلقة بشخص المتهم وعلاقاته العائلية والاجتماعية بوجه عام كما يمكن التعرف على سوابقه الإجرامية.

وبالنسبة لمكان القبض على المتهم راعت التشريعات جعل الاختصاص المكاني لمحكمة مكان القبض على المتهم في حالة لا يوجد له محل إقامة معروف(مجهول الإقامة) أو مكان وقوع الجريمة غير معين، كما تراعي سلطات التحقيق هذا الضابط في الجرائم البسيطة التي تكون الإجراءات التي ستنفذ بشأنها تتطلب مصاريف كثيرة فيفضل محاكمة المتهم بمكان القبض عليه بدلا من نقله إلى مكان وقوع الجريمة أو محكمة مكان الإقامة.[2]

وبهذا يكون المشرع الجزائري أشرك ثلاث محاكم وجعل كل منها صاحبة الاختصاص في نظر الدعوة الجزائية وهي: المحكمة التي ترتكب الجريمة في نطاقها الإقليمي أو المحكمة التي يقيم المتهم في دائرتها أو المحكمة التي يقبض على المتهم في نطاقها.

---

[1]–محمود نجيب حسين، مرجع سابق، ص393.

[2]–صالح عبد الزهرة الحسون، قواعد الاختصاص في التحقيق الابتدائي في القانون العراقي، مجلة القضاء، ع1، س42، 1987، ص192.

الفرع الثاني: الاختصاص النوعي

إن معنى الاختصاص النوعي إذا حاولنا تحديده فيمكن القول بأنه سلطة جهة قضائية معينة للفصل دون سواها في دعاوي معينة، أي يتم تحديد الاختصاص النوعي بالنظر إلى موضوع الدعوى وطبيعة النزاع، المبدأ العام أن قواعد الاختصاص النوعي متعلقة بنظام العام، أي لا يجوز الاتفاق على مخالفتها، ويشرحها القاضي من تلقاء نفسه وفي أي مرحلة من مراحل الدعوى.

لقد أخذ المشرع بمعيار الخطورة في تقسيم الجرائم إلى جنايات وجنح ومخالفات، بحيث لا يتغير نوع الجريمة إذا أصدرت المحكمة حكما بعقوبات تطبق أصلا على جريمة أخرى بسبب توافر ظرف مخفف أو مشددا للعقوبة طبقا للمادتين 27و28 من قانون العقوبات.

وتبعا بهذا التقسيم، فإن الجهات القضائية الجزائية تنظر في الدعوى العمومية تختلف باختلاف نوع الجريمة وفئة الأشخاص المتابعين أمامه، فهناك قواعد عامة مشتركة تحكم إجراءات الفصل في الدعوى العمومية أمام مختلف هذه الجهات القضائية.

أولا: محكمة الجنح والمخالفات:

تختص هذه المحكمة بنظر الدعاوى العمومية المرفوعة أمامها في مواد الجنح والمخالفات وتعتبر جنحة كل جريمة يعاقب عليها القانون بالحبس تتراوح بين شهرين إلى 5 سنوات أو بغرامة تزيد عن 20.000 دج. أما المخالفة فهي كل جريمة يعاقب عليها القانون بالحبس لمدة أقل من شهرين أو بغرامة تتراوح ما بين 2000دج و20.000 دج. [1]

ثانيا: محكمة الجنايات

تختص محكمة الجنايات بنظر الجرائم التي تحمل وصف جنايات والجنح والمخالفات المرتبطة بها والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار من غرفة الاتهام باعتبارها درجة ثانية في التحقيق. [2]ولمحكمة الجنايات كامل الولاية في نظر الدعاوى العمومية والحكم على المتهمين

[1]–حسب المادة 328 من قانون الإجراءات الجزائية.

[2]–حسب المادة 240 من إجراءات جزائية.

البالغين، كما ينعقد اختصاص المحكمة في الحكم على الأحداث البالغين من العمر 16 سنة كاملة والمحالين إليها بقرار من غرفة الاتهام بتهمة ارتكابهم جرائم موصوفة بأفعال إرهابية أو تخريبية. [1]

وليس للمحكمة أن تقرر عد اختصاصها بالنسبة للاتهامات التي تضمنها قرار غرفة الاتهام، أما إذا كان الاتهام غير وارد في قرار الإحالة فلا تنظر فيه المحكمة أصلا. [2]

ويتضمن جهاز القضاء الجنائي العادي إضافة إلى محكمة الجنح والمخالفات ومحكمة الجنايات، الغرفة الجزائية لدى المجلس القضائي والتي تتشكل لدى كل مجلس قضائي تستأنف أمامها الأحكام الضرورية الصادرة في الجنح والمخالفات[3]وكذا المحكمة العليا حيث تشكل هذه الأخيرة في المواد الجزائية من غرفتين هما الغرفة الجنائية وغرفة الجنح والمخالفات، حيث تختص الغرفة الجنائية بالنظر في الطعن بالنقض في قرارات غرفة الاتهام باستثناء تلك القرارات الغير قابلة للطعن فيها[4]، وفي الأحكام التي تصدرها محكمة الجنايات سواء بالبراءة أو الإدانة.

وتختص غرفة الجنح والمخالفات بالفصل في الطعون بالنقض في القرارات التي تصدرها الغرفة الجزائية لدى المجلس القضائي عند نظرها الاستئناف المرفوعة في الأحكام في مواد الجنح والمخالفات. [5]

الفرع الثالث: لاختصاص الشخصي:

الأصل في المسائل الجنائية أن لكل دولة الحق في أن تختص بمحاكمة كل شخص يرتكب الجريمة في إقليمها أمام محاكمها المختصة ولكن لاعتبارات معينة قد يضع المشرع فيها شخصيا ويعفي بعض الأشخاص من الخضوع للقضاء الجنائي وهذا القيد قد يكون راجع لقواعد في القانون

---

[1]–حسب المادة 249من قانون إجراءات جزائية.

[2]–حسب المادة: 251 من قانون الإجراءات الجزائية.

[3]–أنظر المواد 429–432–433من قانون الإجراءات الجزائية.

[4]–القرارات الغير قابل للطعن بالنقض هي تلك المتعلقة بالحبس المؤقت والرقابة القضائية فهي نهائية غير قابلة للطعن فيها.

[5]–حسب المادة 445 من قانون الإجراءات الجزائية.

الداخلي تمنع خضوع بعض الأشخاص للمحاكمة أمام المحاكم الجنائية العادية وهذا القيد على اختصاص المحكمة يعود إلى سن المتهم أو وظيفته.

وعليه نجد أن الفئات التي تحاكم أمام المحاكم المتخصصة مثل الأحداث أو العسكريين أو القضاة أو الوزراء أو رؤساء الدول يخضعون للقانون الجنائي للدولة التي ارتكبت الجريمة في إقليمها لكن لا يمثلون أمام المحاكم العادية بل يمثلون أمام محاكم مخصصة لمحاكمتهم.

وقد يرد القيد الشخصي بموجب قواعد القانون الدولي العام أو الاتفاقيات الدولية فيخرج بموجبه بعض الأشخاص من نطاق المحاكم المختصة في الإقليم كرؤساء الدول الأجنبية ورؤساء الهيئات الدبلوماسية وغيرهم، وهؤلاء نطاق تطبيق القانون الجنائي من حيث المكان يعتمد استثنائهم من الخضوع للقانون الجنائي والمحاكمة أمام محاكم الدول التي ارتكبت الجريمة على إقليمها والخضوع تحت طائلة قانون ومحاكم دولهم.

والمشرع الجزائري لم يخرج عن هذه القواعد فحدد اختصاص المحكمة على أساس مواصفات معينة تتميز بها فئة المتهمين عن الفئات الأخرى فمثلا يختص قضاة الأحداث بمحاكمة المتهمين الذين لم يكملوا سن الرشد الجنائي وهو 18 سنة. [1] وتختص المحاكم العسكرية بمحاكمة المتهمين العسكريين المنصوص عليها في المادة 03 من قانون القضاء العسكري الذين ارتكبوا جرائم القانون العام أو الجرائم العسكرية البحتة.

إذن لا اختلاف في قواعد الاختصاص القضائي الجنائي بين الجرائم الكلاسيكي والجرائم المعلوماتية والتي من بينها تلك الجرائم الواقعة على التوقيع الإلكتروني مجموعة حروف أو أرقام أو رموز أو إشارات أو غيرها وقع على محرر إلكتروني فيمنع بطابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره، إلا أن ما قام به المشرع الجزائري من حيث توسع الاختصاص المحلي أو الإقليمي كما سبق بيانه وذلك لتوفير الإمكانات المادية والبشرية في بعض المحاكم لمواجهة الخطورة لمجموعة من الجرائم محددة حصرا من قبل المشرع والتي من بينها تلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1]–حسب المواد 446–447 و 451 من قانون الإجراءات الجزائية.

المطلب الثاني:

الاختصاص الجنائي العالمي في محاكمة الجرائم الواقعة على التوقيع الإلكتروني

إن تطبيق القانون الجنائي في الجرائم المستحدثة وفي طليعتها الجرائم المعلوماتية والتي يعتبر الاعتداء على منظومة التوقيع الإلكتروني من ضمنها أوجد إشكالا في تحديد القضاء المختص في معاينتها ومتابعتها والتحقيق فيها ومعاقبة مرتكبيها، مما دفع دول العالم لإيجاد صيغة جديدة تختلف عن المبادئ المطبقة في تحديد الاختصاص القضائي والقانون الواجب التطبيق من حيث المكان، لذلك اتجهت التشريعات الجنائية الدولية التي تنص على مبدأ آخر يمكن الاعتماد عليه كمعيار للاختصاص القضائي للدولة.

وعليه سيتم التطرق في هذا المطلب إلى مبدأ العالمية في ثلاثة فروع. حيث يتناول الفرع الأول مفهوم مبدأ العالمية، والفرع الثاني شروط تطبيق مبدأ العالمية، أما الفرع الثالث والأخير فيناول موقف المشرع الجزائري من مبدأ العالمية.

الفرع الأول: مفهوم مبدأ العالمية

الأصل في تطبيق التشريع العقابي إقليمية النص الجنائي، يجب تطبيق هذا الأخير على كافة الجرائم المرتكبة على إقليم الدول بصرف النظر عن جنسية الجاني أو المجني عليه حيث يستوي أن يكون وطنيا أم أجنبيا، وبصرف النظر أيضا عن المصلحة التي أهدرتها الجريمة، ولو كانت تخص دولة أخرى كما لو مست الجريمة تزييف العملة الخاصة بها، لكن لم يعد هذا المبدأ كافيا حيث ظهر مبدأ آخر فرضته جرائم ودواعي مستجدة ألا وهو مبدأ العالمية، فما هو هذا المبدأ؟

أولا: تعريف مبدأ العالمية

لقد حاول العديد من فقهاء القانون الجنائي الدولي والقانون الدولي الجنائي وضع تعريف للاختصاص الجنائي العالمي نذكر منهم:

الدكتور طارق سرور: الذي عرفه على أنه:" صلاحية تقررت للقضاء الوطني في ملاحقة ومحاكمة وعقاب مرتكبي أنواع معينة من الجرائم التي يحددها التشريع الوطني دون النظر لمكان ارتكابها ودون اشتراط توافر ارتباط معين يجمع بين الدول وبين مرتكبيها أو ضحاياها، وأيا كانت

جنسية مرتكبيها أو ضحاياها، فيصبح تحديد نطاق إقليم الدولة أو تحديد مكان وقوع الجريمة أو النظر إلى جنسية مرتكبيها أو جنسية ضحاياها غير ذي جدوى". [1]

أما الدكتور محمد منصور الصاوي يعرفه على أنه:" حق كل دولة في مطاردة وعقاب كل من يدان بجريمة دولية، بصرف النظر عن جنسيته، أو مكان ارتكابه لها، باعتباره نظاما أو فكرة– تلازم الجريمة ذات الطبيعة الدولية، مستهدفا ملاحقة وعقاب مرتكب تلك الجريمة في أية دولة وإعطاء الصلاحية لقضاء أي دولة للعقاب على الجريمة الدولية يصرف النظر عن جنسية مرتكبها أو مكان وقوعها". [2]

ويأخذ على التعريف الأخير مأخذين بارزين أولها أن التعريف ذكر كلمة مدان والإدانة لا تكون إلا بعد المحاكمة وصدور الحكم الذي يقررها، وثانيها أن هذا التعريف قد أغفل جنسية المجني عليه أو ضحايا الجريمة الدولية في عدم الاعتداد بها لتحديد الاختصاص الجنائي العالمي للدولة.

إذن يقصد بهذا المبدأ أن العبرة في تحديد الاختصاص التشريعي القضائي لدولة ما بمكان إلقاء القبض على المتهم، فهذا المكان هو الذي يقول عليه كتحديد المحكمة المختصة والقانون الواجب التطبيق، وذلك دون اعتبار لمكان ارتكاب الجريمة أو جنسية الجاني أو المجني عليه أو المصالح التي مستها الجريمة بالإعتداء. [3]

فمكان القبض على المتهم هو أساس تحديد الاختصاص القضائي، ومن الواضح أن هذا النوع من الاختصاص يفرض وجود نوع من التضامن بين الدول المختلفة، بحيث تخول بعضه ليحل مكان

---

[1]–طارق سرور، الاختصاص الجنائي العالمي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2006، ص26.

[2]–الصاوي محمد منصور، أحكام القانون الدولي المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دار المطبوعات الجامعية(ب–ط)، الإسكندرية، (ب–ت–ن)، ص20.

[3]–أحسن بوسقيفة، الوجيز في القانون الجزائي العام، دار هومة للنشر والتوزيع، الطبعة الرابعة عشر، سنة 2014، ص112.

البعض في المحاكمة وتوقيع العقاب، ولكن الأمر هذا لا يتعلق بإنابة دولية لغيرها في الاختصاص وإنما نحن بصدد اختصاص أصيل، تمارسه الدولة. [1]

ثانيا: تقييم مبدأ العالمية

لقد واجه مبدأ العالمية عدة انتقادات، باعتبار قيام دولة ما بالقبض على المتهم يشكل عبئا ثقيلا على العدالة فيها، خاصة أن الجريمة لم تقع على أرضها، ولا يوجد عنصر من عناصر التماس التي تبرر إختصاصها كالسيادة أو المصلحة المحمية أو جنسية الجاني أو المجني عليه، بالتالي فإن الدول المختلفة لا ترحب كثيرا بهذا النوع من الاختصاص.[2]

كما أنه من الصعوبة قبول اختصاص بجريمة لا صلة للدولة بها إلا إذا تم إلغاء القبض على الجاني داخل الدولة.[3]إضافة إلى إثارة هذا الاختصاص العديد من الصعوبات بين الدول (التي ارتكبت على إقليمها الجريمة) ودولة المصدر(أي الدولة التي ينتمي إليها الجاني أو المجني عليه) والدولة التي تم فيها إلقاء القبض على الجاني نزاعات ومشاكل. [4]

وهذا المبدأ يتلاءم كثير وطبيعة الجريمة المعلوماتية رغم ما يطرحه من نزاع حاد بين التشريعات الجنائية في الدول، وعليه فإنه يمكننا القول–بأن أهمية هذا المبدأ ومدى ملائمته للجريمة المعلوماتية مستمدة من خطورتها من جهة، ومن طبيعتها من جهة أخرى– كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة وفي فترات زمنية قصيرة جدا وهذا المبدأ–أي العالمية– يبقى عاجزا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي جاد وسريع، وكذا وجوب إعداد تشريعات وطنية لتجريم الظاهرة

[1]–عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 2006، ص204.

[2]–المرجع نفسه، ص206.

[3]–المرجع نفسه، ص207.

[4]–عمر عبيد محمد الغول، نفس المرجع، نفس الصفحة.

ومنها إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاة الجنسية أو مكان وقوع الفعل الإجرامي. [1]

الفرع الثاني: شروط تطبيق مبدأ العالمية

إن الفقه والتشريع وضع شروط، عند تطبيق مبدأ العالمية والتي يجب توافرها لتطبيقه ضمن الأنظمة القانونية للدول من أجل تفعيله وللإلمام بتلك الشروط يجب تعريف كل من الجريمة الدولية (أولا)، ثم الجريمة العالمية (ثانيا).

أولا: تعريف الجريمة الدولية

يعرف محمد محي الدين عوض الجرائم الدولية بأنها: " الجرائم التي ينص عليها القانون الدولي باعتبارها جريمة ذات عنصر دولي واقعة ضد النظام العام، وتعرض السلم والأمن والحقوق الأساسية للمجتمع الإنساني للخطر.[2]

وتتصف الجريمة الدولية بأنها ذاتية، والمقصود بذلك أنها تقتصر في العدوان على المصالح التي تهم المجتمع الدولي بأسره وهذه المصالح تتعلق بالركائز الأساسية، التي يترتب على المساس بها زعزعة الأمن والاستقرار في المجتمع الدولي، لذلك تخرج من نطاق الجريمة الدولية تلك التي لا تحدث هذا الأثر. [3]

ثانيا: تعريف الجريمة المعلوماتية

الجريمة العالمية مصدرها القانون الوطني والذي يعاقب على ما يقع من جرائم من داخل الدولة، لأنها تنطوي على تصرفات مناخية للأخلاق والتي تشكل عدوانا على القيم، بالإضافة إلى الصور الإجرامية التي يعاقب عليها قانون العقوبات كجرائم المخدرات وتزييف العملة...إلخ.

---

[1]–لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، المجلد الثاني، العدد الثاني، 2009، ص–ص152–167.

[2]–محمد محي الدين عوض، دراسات في القانون الدولي الجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2005، ص472.

[3]–فتوح عبد الله الشاذلي، القانون الدولي الجنائي، الكتاب الأول، أوليات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، دار المطبوعات الجامعية، الإسكندرية، 2001، ص214.

وهذا المبدأ يرجع إليه في تسمية تلك الجرائم العالمية يضاف إليه اعتبار آخر وهو مزاولة النشاط الإجرامي عبر الدول والحدود، نتيجة للمد المذهل في وسائل الإتصالات والمواصلات. [1]

إذن الجريمة المعلوماتية تنطوي تحت مفهوم الجريمة العالمية لأنها تعد جريمة عابرة للحدود الإقليمية للدولة وبالتالي يجب على الدولة التي تلقي القبض على الجاني محاكمته حتى ولو لم يكن إقليمها مسرحا للجريمة ولم يكن الفاعل أو الضحية حاملا لجنسيتها ولو لم تكن مصالحها المحمية قد هدرت من جراء وقوع تلك الجريمة وذلك حتى لا تشكل تلك الدولة مكانا آمنا للجاني وأن تكون فعالة في تحقيق المكافحة الدولية للجريمة مهما كان فاعلها: وضحيتها ومكانها في هذا العالم.

ومن خلال هذا التقديم يمكن وضع شروط لتطبيق مبدأ العالمية من قبل القضاء الجنائي الوطني:

- أن تكون الجريمة ذات طبيعة عالمية.
- أن يتم القبض على المتهم من طرف السلطات المختصة أو يتم تسليمه إليها عن طريق إجراءات تسليم المجرمين.

وتجدر الإشارة إلى أن هناك فرق بين مبدأ العالمية ومبدأ الاختصاص القضائي العالمي فالأول مجاله جرائم منصوص عليها في القانون الداخلي للدولة. [2] أما الثاني فمجاله جرائم دولية[3] منصوص عليها في إتفاقيات دولية، فإتفاقيات جنيف الأربعة لسنة 1949 م أخذت بمبدأ الاختصاص العالمي بالنسبة للجرائم الدولية فيها، ونصت على أن تحاكم كل دولة متعاقدة كل من يرتكب إحدى هذه الجرائم دون النظر إلى جنسيته، أو تقوم بتسليمه إلى الدولة التي تطلبه

---

[1]–طارق فوزي التقي، الجوانب الإجرائية في الجرائم المعلوماتية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة منوفية، مصدر سنة 2011، ص 250.

[2]–مثلا حدد المشرع الجزائري مجموعة من الجرائم الخطيرة والتي خصها بإجراءات متابعة خاصة نظرا لأنها جرائم عابرة للحدود الدولية كتلك المذكورة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

[3]–حصرت المادة 5 من النظام الأساسي للمحكمة الجنائية الدولية، الجرائم الدولية في جريمة إبادة الجنس البشري، جرائم الحرب الأساسية وجريمة العدوان.

لاختصاصها بمحاكمته.[1] هذا وساير الاجتهاد القضائي الدولي من خلال قرار المحكمة الجنائية الدولية المؤقتة ليوغسلافيا (سابقا) الاتجاه القائل أن الجرائم الأكثر خطورة هي تلك الجرائم التي تدخل في اختصاص المتابعة الجنائية العالمية، ففي قضية «تاديك» اعتبرت المحكمة في قرارها المؤرخ في 2 أكتوبر 1995 م أن الجرائم المتابع بها «تاديك» هي جرائم ذات طبيعة عالمية وأن ممارسة مبدأ الاختصاص موجه ضد الجرائم الدولية. [2]

إذن كل الجرائم التي تتجاوز حدود الدولة وتتصف بالخطورة على غرار جرائم المخدرات والإرهاب والجريمة المنظمة والجرائم المعلوماتية هي جرائم ذات طبيعة عالمية يمكن إخضاعها لمبدأ العالمية في المحاكمة من قبل القضاء النظامي الوطني للدولة، ذلك أن الاختصاص القضائي العالمي الدولي لا يختص بها لأنها ليست من الجرائم الدولية التي حددتها المواثيق الدولية حصرا.

الفرع الثالث: موقف المشرع الجزائري من مبدأ العالمية

الملاحظ أن أغلب التشريعات الوضعية ومنها المشرع الجزائر لم ينص على هذا مبدأ بالرغم من أهميته خصوصا في مجال الجريمة المعلوماتية وترى وجوب النص عليه عند إعداد قانون خاص بمعالجة الجريمة المعلوماتية وجرائم الكمبيوتر والأنترنت وهذا على الرغم من أن الإتفاقيات الدولية تركز بل وتعول عليه كثيرا في هذا المجال خصوصا إتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية وكذا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية 2003 في المادة 26[3]، كما أن الفقه يرى وجوب الأخذ به على غرار جريمة القرصنة كونها تستهدف أمن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة المعلوماتية مما يهدد الاقتصاد العالمي الذي يشهد وتيرة متصاعدة خصوصا في المجال المالي والبنكي وعليه أصبح

[1]–فتوح عبد الله الشاذلي، القانون الجنائي، مرجع سابق ص–ص226–227.

[2]–T , I, P ,Y, chambre d'appel , affaire AADIC .arrét2 Octobre1995, p62.

[3]–نصت المادة 26 من القانون المذكور أعلاه «تسري أحكام هذا القانون على أي نوع من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كليا أو جزئيا خارج إقليم الدولة متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عنها.»

من الضروري الأخذ بهذا المبدأ ومعاقبة الجاني في أي إقليم يتم القبض عليه فيه دون مراعاة لجنسية الجاني أو مكان ارتكاب الجريمة، لارتكابه جريمة عالمية. [1]

ويعتبر حاليا التعاقد عبر الأنترنت من أهم مظاهر الثورة التكنولوجية وكان الاستعمال الواسع للبطاقات البلاستيكية وخاصة بطاقات الدفع والسحب والتي تعتمد جميعها على التوقيع الإلكتروني، كل هذه الأهمية لهذا الأخير بحياة الفرد ومؤسسات الدولة يحتاج إضافة إلى الحماية الفنية والقانونية إلى اعتماد الاعتداءات الواقعة عليه ضمن مجال الحماية الجزائية العالمية التي تخضع لاختصاص القضاء الوطني من خلال تطبيق مبدأ العالمية.

[1]–لموسخ محمد، مرجع سابق، ص–ص 151–167.

المبحث الثاني:

التعاون الدولي في مجال إثبات الجرائم الواقعة على التوقيع الإلكتروني

إذا كان خطر جرائم الإعتداء على التوقيع الإلكتروني يتمثل في طبيعتها اللامادية وفي مجالها اللامحدود، إضافة إلى أنها جرائم ترتكب ضد الأشخاص والأموال وضد الهيئات الحكومية وإقتصادات الدول، فإن الخطر الأهم هو غياب التجاوب المطلوب من الدول مع المواثيق الدولية ذات الصلة بالإجرام المعلوماتي، فلا تكفي المكافحة التي تقوم بها كل دولة على حدة، لأنها ستتسم بالمحدودية وستكون قاصرة على التصدي والمواجهة لهذا النوع من الجرائم، لذلك يكون من الأفضل التعاون بين الدول والتنسيق فيما بينها لاتخاذ موقف موحد تكون نتائجه أكثر إيجابية وفاعلية.

وعليه لم تتوقف السياسة الجنائية الإجرائية للمشرع الجزائري في مجال إثبات الجرائم الإلكترونية داخل الوطن باستحداث إجراءات بحث وتحري تواكب التطور السريع لهذا النوع من الإجرام، وكذا تمديد الاختصاص للسلطات المكلفة بالتحريات والتحقيق، وما تضمنته مواد القانون رقم: 04/09، إنما امتدت خارج الوطن لتشمل التعاون الدولي وطلبات المساعدة القضائية تجاوبا مع التوصيات الدولية ذات العلاقة بمكافحة الجريمة المعلوماتية.

انطلاقا من كل ذلك، سيتم التعرف على الإتفاقيات الدولية ذات الصلة بالتعاون الدولي في مجال إثبات الجرائم الواقعة على التوقيع الإلكتروني في المطلب الأول، ثم يتم التطرق إلى صور المساعدة القضائية الدولية المتبادلة في المطلب الثاني.

المطلب الأول:

الإتفاقيات الدولية المتعلقة بمكافحة جرائم الإعتداء على التوقيع الإلكتروني

نظرا لما قد تشكله جرائم التوقيع الإلكتروني باعتبارها أحدث أنواع الإعتداءات التي تطال المنظومات المعلوماتية، وما يتفرع عنها من إشكاليات قانونية واقتصادية واجتماعية وأمنية معقدة، اتجاه المجتمع الدولي إلى اتخاذ مجموعة من التدابير على الصعيدين الدولي والإقليمي، يتمثل أهمها في الإتفاقيات والمعاهدات الدولية، وهي الصورة الأكثر تعبيرا عن التعاون الدولي في مجال مكافحة

هذا النوع من الجرائم والتي تنعكس سلبا على الأنشطة والمجالات التي تمارس عبر الوسائط الإلكترونية.[1]

على ضوء ذلك سيتم إستعراض أبرز الإسهامات الدولية والإقليمية للحد من إنتشار الجرائم الماسة بالتوقيع الإلكتروني بدءا بالإتفاقية الدولية لمكافحة الجريمة المعلوماتية بودابست2001 في الفرع الأول، ثم قانون الأونسيترال النموذجي في الفرع الثاني، ويتناول الفرع الثالث التوجيه الأوروبي لسنة 1995، وفي الفرع الرابع يتم التطرق إلى توصيات الجمعية الدولية لقانون العقوبات.

الفرع الأول: الإتفاقية الدولية لمكافحة الجريمة المعلوماتية بودابست 2001

في 23 نوفمبر 2001 وفي مدينة بودابست عاصمة المجر قامت 26 دولة بالتوقيع على تلك الإتفاقية فيما بينها لمكافحة الجريمة المعلوماتية تتويجا لجهود اللجان القانونية والفنية الدولية وكذا المعاهدات الأوربية بشأن حماية البيانات الشخصية.

كما تأثرت بمعاهدة التعاون الدولي في مكافحة الجريمة المعلوماتية الصادرة عن الأمم المتحدة ومنظمة التعاون الاقتصادي والتنميةOECDودول الاتحاد الأوربي ومجموعةG8 وكذلك التوصية الأوربية رقم 10/85 والتوصية رقم2/88 والتوصية رقم 9/89 والتوصية رقم13/95.[2]

وقد إحتوت هذه الإتفاقية على أربعة فصول، حيث تناولت تعريف معطيات الكمبيوتر ومزودي الخدمة (المادة الأولى من الإتفاقية)، ثم تقسيم الجرائم الإلكترونية بداية من أمن المعلومات كصورة أولى وتشمل جريمة الدخول غير القانوني (م/2 من الإتفاقية) والاعتراض غير القانوني (م/3) والتدخل في المعطيات(م/4) والتدخل في نظم الحاسوب (م/5) وإساءة إستخدام الأجهزة (م6)

وضمت الصورة الثانية الجرائم المرتبطة بالكمبيوتر، كجريمة التزوير عن طريق الحاسوب (م/7) والاحتيال بواسطة الكمبيوتر (م/8)، والصورة الثالثة تتعلق بالاستغلال الجنسي للأطفال عبر الانترنيت (م/9).

---

[1]–عبد العزيز البواري، السياسة الجنائية المعاصرة في حماية التجارة الإلكترونية، رسالة ماجستير، جامعة نايف للعلوم الامنية، الرياض 2011، ص129.

[2]–ايمن عبد الله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض 2015، ص149.

أما الصورة الأخيرة فتتعلق بجرائم الإعتداء على الحقوق الفكرية وحقوق المؤلف (م/10)، كما أبـرزت الإتفاقيـة أحكـام المسـاهمة الجنائيـة والشـروع ومسـؤولية الأشـخاص المعنويـة وكـذا معـايير العقاب.[1]

أما عن نصوص المسائل الإجرائية الخاصة بجرائم الكمبيوتر والانترنيت ذات العلاقة بالتجارة الإلكترونيـة فجـاءت أحكـام الإتفاقيـة بقواعـد عامـة وتوجيهـات عريضـة تتطلـب تحديـدا منضـبطا مـن المؤسسات التشريعية لدى وضع القوانين الوطنية كون هذه الجرائم تنطوي على خصوصية في ميدان الإثبات والتحري والضبط والتفتيش والمقاضاة والاختصاص ضمانا لانسجام الحلول الإجرائية، هذا من جهـة، ومـن جهـة أخرى تمثل أحكـام الإتفاقيـة الأداة التشـريعية الرئيسـية التـي سـتحكم مسـائل التعـاون الدولي في أنشطة المكافحة، متمثلة في القواعد المتعلقة بتسليم المجرمين والإنابات القضائية ومسائل الضبط والتفتيش وتحرير الأدلة خارج الحدود.[2]

الفرع الثاني: قانون الأونسيترال النموذجي

أنشأت الجمعية العامة للأمم المتحدة هيئة فرعية تحت مسمى: " لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، في عام 1966 مهمتها تعزيز التنسيق بين القوانين الوطنية المختلفة وخلق قواعد عصرية بشأن المعاملات التجارية من خلال الإتفاقيات والقوانين منها على الخصوص قانون الأونسيترال النموذجي للتجارة الإلكترونية الذي إعتمد عام 1996، ويهدف إلى تسيير إستخدام الوسائل الحديثة للإتصالات وتخزين المعلومات في الأنشطة التجارية الدولية.[3]

كما إعتمدت سنة 2001 قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، ويدخل كل ذلك في إطار مكافحة الجرائم الواقعة على التوقيع الإلكتروني في ضوء الطابع الدولي والمتنامي لها.

---

[1]–م.م لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد للنشر والتوزيع، عمان 2015، ص89.

[2]–نصر شومان، التكنولوجيا الجرمية الحديثة واهميتها في الاثبات الجنائي، بدون دار نشر، ص302.

[3]–انظر موقع شبكة قوانين الشرق EastLawsعلى شبكة الانترنيت: Site.eastlaws.com/news.

أولا: قانون الأونسيترال النموذجي الموحد للتوقيعات الإلكترونية:

إعتمد هذا النص في 5 جويلية 2001 ومجاله الإستخدامات المختلفة للتوقيع الإلكتروني، بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة، والحداثة والتكنولوجيا.

ثانيا: قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996

يشتمل هذا القانون على سبعة عشر مادة تناولت كافة الجوانب القانونية لمختلف المعاملات التجارية عبر شبكة الأنترنت ويضم جزأين: الجزء الأول خاص بتطبيقات التجارة الإلكترونية بشكل عام وإستخدامات التوقيع الإلكتروني بشكل خاص، والجزء الثاني يتناول جوانب محددة للتجارة الإلكترونية، وأرفق هذا القانون النموذجي بدليل تشريعي يهدف إلى مساعدة المشرعين الوطنيين على وضع تشريعات خاصة تنظم التجارة الإلكترونية وبالأخص ذات الطبيعة الدولية، والتي تأخذ في العموم شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية.[1]

الفرع الثالث: التوجيه الأوربي لسنة 1995

أصدر المجلس الأوربي التوجيه رقم (95) لسنة 1995، متضمنا سلسلة من الأدلة التوجيهية المعتمدة على إتفاقية الاتحاد الأوربي لسنة 1981 الخاصة بحماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية[2]، وهي عبارة عن توصيات موجهة إلى حكومات الدول الأعضاء تتعلق على الخصوص بحماية قواعد المعلومات المعالجة إلكترونيا الخاصة بخدمات الإتصال، والبيانات المتعلقة بالقطاع المصرفي، وكل ما له علاقة بمكافحة الجرائم الماسة بالتجارة الإلكترونية والتي من بينها الإعتداءات التي تطال آلية التوقيع والتصديق الإلكترونين.

---

[1]–لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار هومة، الجزائر 2012، ص33.

[2]–في عام 1981 وضع الاتحاد الاوربي إتفاقية حماية الافراد من مخاطر المعالجة الالية للبيانات الشخصية (Convention for the protection of individualswithregard to automaticprocessing of personal data)وقد وقعت على هذه الإتفاقية 31 دولة صادق منها 21 دولة بتاريخ 25 جانفي 2012 صادقت باقي الدول الموقعة على الإتفاقية وانضمت اليها ثمانية دول أخرى ليصبح عدد اعضاؤها 39 دولة موقعة ومصدقة على الإتفاقية.

وحث الاتحاد الأوربي في هذا المجال الدول الأعضاء في المجلس على تحديث القوانين الجنائية الوطنية بما يتلاءم مع التنامي المتزايد لهذه الجرائم، من خلال إصداره لدليلين إرشاديين سنة 1995 و1997.

أولا: الدليل الإرشادي لسنة 1995

وهو عبارة عن دليل حماية البيانات، اهتم بمسألة توجيه القوانين الوطنية لتنظيم معالجة البيانات الشخصية بالشكلين الإلكتروني واليدوي، ويتضمن حماية فاعلة ضد إستخدام البيانات الشخصية الحساسة، كالبيانات المتعلقة بالأمور المالية للأشخاص، وتلتزم الجهات التجارية والحكومية لدى إستخدامها هذه البيانات بالتقيد بقواعد الإستخدام، وبما قرره الدليل للشخص من حقوق عليها، مما يضفي فعالية تطبيق قواعد الحماية، وهو ما أدى بالاتحاد الأوربي إلى فرض وجود هيئة رقابية تكفل تنفيذ هذا القانون تعرف في بعض الدول بالمفوض أو المراقب أو مسجل البيانات.[1]

ويفرض الدليل على الدول الأعضاء التزامات بشأن نقل بيانات المواطنين الأوربيين إلى خارج الحدود أو معالجتها بأنظمة معلومات خارجها، وضرورة توفير حماية الخصوصية المعلوماتية.

ثانيا: الدليل الإرشادي للاتصالات لسنة 1997

أسس هذا الدليل من اجل توفير حماية خاصة تغطى الهاتف والتلفزيون الرقمي وشبكات الهاتف الخلوية ومختلف الأنشطة المتصلة بالأنترنت وغيرها من نظم الاتصالات وألزم الدول الأعضاء بضرورة سن تشريعات في هذا المجال في مهلة أقصاها عام 2000.

و بالرجوع لهذين الدليلين نجدهما يقرران عدة قواعد ومبادئ رئيسية لحماية بيانات التجارة الإلكترونية على الخصوص من أي اعتداء محتمل تتمثل في ما يلي: [2]

- الحق في معرفة مكان استخدام معالجة البيانات.
- الحق في الوصول إلى هذه البيانات وتصحيحها.
- الحق في الدفاع والحماية من أنشطة المعالجة غير القانونية.

---

[1]–شريف يوسف خاطر، مرجع سابق، ص19

[2]–شريف يوسف خاطر، المرجع السابق، ص18

- الحق في الحصول على إذن لاستخدام البيانات في بعض الظروف والأغراض، كالتسوق المجاني عبر مواقع التجارة الإلكترونية.
- تعديل القوانين الإجرائية بما يمكن سلطات التحقيق اصدار أمرا للغير بأن يقدم المستندات الإلكترونية المخزنة في الحاسب متى كانت تفيد في كشف الحقيقة في جريمة من جرائم التجارة الإلكترونية.
- تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية والاعتراف بها بين الدول المختلفة، ووجوب تطبيق النصوص الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

وقد كان للمجلس الأوربي الدور البارز في الإشراف على إتفاقية بودابست الموقعة في 23 نوفمبر 2001 والتي سبق التعرض اليها، حيث تم الإتفاق على ضرورة تحديث القانون الجنائي بان يحافظ على مواكبته للتطورات التكنولوجية والتي تقدم فرصا واسعة لإساءة إستخدام إمكانيات الفضاء المعلوماتي وأن يعمل على ردع هذه الأفعال الإجرامية.[1]

وفي عام 2000 أصدرت المفوضية الأوربية نموذجا جديدا لدليل معالجة البيانات الشخصية وحماية الخصوصية في قطاع الإتصالات الإلكترونية، استكمالا لحزمة الجهود الرامية إلى حماية سوق الإتصالات بما فيها بيانات ومعلومات التجارة الإلكترونية وكذا المستهلك الإلكتروني.[2]

تضمنت النصوص الجديدة حماية البيانات المنقولة عبر الأنترنت ومنع السلوكيات الإتصالية الضارة في السوق التجاري الإلكتروني مثل(SPAM)[3]، وحماية مستخدمي الهواتف الخلوية وتوسيع نطاق حماية الخصوصية والسيطرة على كافة انواع البيانات المعالجة.

---

[1]–زيد حمزة مقدم، وسائل وضمانات التوقيع الإلكتروني، مجلة جامعة بحري للآداب والعلوم الانسانية، جمهورية ايران، 2004، ص185

[2]–شريف يوسف خاطر، مرجع سابق، ص20

[3]–(SPAM) (رسائل البريد الإلكتروني الموجهة دون رغبة الملتقى وبإعداد كبير وعلى نحو دوري احيانا). انظر شريف يوسف خاطر، مرجع سابق، ص20

الفرع الرابع: توصيات الجمعية الدولية لقانون العقوبات

تبنى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات –المنعقد بريو ديجانيرو بالبرازيل في الفترة ما بين الرابع والتاسع سبتمبر 1994 بشأن جرائم الكمبيوتر– مقررات وتوصيات تناولت في البداية الشق الموضوعي لهذه الجرائم، حيث أوصى المؤتمر بان تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي: [1]

- الاحتيال أو الغش المرتبط بالكمبيوتر.
- التزوير المعلوماتي.
- الإتلاف المعلوماتي.
- الدخول غير المصرح به إلى نظام معالجة إلكترونية وكذا الاعتراض غير المصرح به عن طريق وسائل فنية توجه لنظام كمبيوتر.

كما تبنى المؤتمر تدابير إجرائية تطبق على جرائم التجارة الإلكترونية منها:

- أن تمكن سلطات التحقيق والتحري بصلاحيات قسرية كافية دون الإضرار بحقوق الإنسان وحرمة الحياة الخاصة.
- أن يتم تحديد السلطات التي تقوم بإجراءات التفتيش والضبط لشبكات الحاسب والسماح لها باعتراض الإتصالات داخل نظام الحاسب أو بينه وبين نظم حواسيب أخرى مع إستخدام الأدلة المتحصل عليها في كامل إجراءات المحاكمة.

كما يجب أن يحدد بوضوح:

- السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات.
- واجبات التعاون الفعال من جانب المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيا المعلومات.
- إدخال التغيرات التشريعية الضرورية في مجال قبول ومصداقية الأدلة الرقمية.

[1]–منتدى د. شيماء عطا الله على الشبكة الأنترنت: www.Shaimaaatalla.com/vb

المطلب الثاني:

المساعدة القضائية الدولية في مجال إثبات الجرائم الواقعة على التوقيع الإلكتروني

أدى الطابع العالمي للجريمة المعلوماتية ومنها الجرائم الواقعة على التوقيع الإلكتروني إلى امتداد أثرها لأكثر من دولة، وعليه يستلزم ملاحقة مرتكبي هذه الجرائم القيام بإجراءات خارج الدولة محل ارتكاب الجريمة أو جزء منها، وقد وضعت إتفاقية بودابست جملة من المبادئ الخاصة يتجه تفعيلها إذا اتخذت الجريمة شكلها الدولي، وهي تتمثل في جملة الوسائل التي قسمتها الإتفاقية إلى وسائل وقتية سيتم تناولها بالدراسة في الفرع الأول وأخرى إستقرائية وتقنية[1]يتم التطرق إليها في الفرع الثاني، ثم التعرض إلى آليتي الانابة القضائية وتبادل المعلومات في الفرع الثالث، ويتم التعرف في الفرع الرابع على نظام تسليم المجرمين كآلية لمكافحة الجرائم الواقعة على التوقيع الإلكتروني.

الفرع الأول: الطرق الوقتية

تحتوي على وسيلتين هما الحفظ السريع المعطيات الإلكترونية المخزنة والكشف السريع عن المعطيات المحفوظة:

أولا: الحفظ السريع لبيانات التوقيع الإلكتروني المخزنة

يحق لأي دولة بموجب هذا الإجراء المطالبة بحفظ البيانات المخزنة في أجهزة الحاسب الآلي الموجودة في أراضي الدولة المطلوب إليها على وجه السرعة، ويتميزهذا الإجراء بطابعه الاستعجالي إذ المهم أن لا تندثر المعطيات المعنية، بالنظر إلى إمكانية تلاعب الجناة بالبيانات وإتلافها في ظرف وجيز.[2]

ويرمي الإجراء كذلك إلى حفظ المعطيات التي سبق خزنها، ذلك أن التخزين لا يدوم لفترة طويلة، أما الحفظ فيحفظ لها وجودها وأمنها لفترة معينة قبل إثارة التتبع وتقديم الطلبات، فالمقصود

---

[1]– منية الزغلامي، الإثبات في جرائم الاتصالاتبحث منشور على موقع: https: //www.mohamah.net/law تاريخ الاطلاع: 2019/07/21 الساعة: 22.24 .

[2]–موسى مسعود ارحومة، الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، اكاديمية الدراسات العليا، يومي: 28 و29 اكتوبر 2009، طرابلس، ليبيا، ص3.

بهذا الإجراء المحافظة على وجود هذه المعطيات تحت يد حافظها الذي يكون عادة مزود الخدمة أو أي طرف ثالث إلى أن يتم استعمالها في الأبحاث الجزائية اللاحقة.[1]

وقد حددت إتفاقية بودابست الفترة اللازمة للتحفظ على البيانات عندما نصت المادة (29) على انه يجب على كل دولة التأكد من أن البيانات المحفوظة ستحجز لمدة 60 يوما على الأقل، وإذا تبين لسلطات الدولة المطلوب إليها أن حفظ البيانات قد يتخذ إجراءات من شأنها تهديد السرية أو عرقلة التحقيق الذي تجريه الدولة الطالبة، فعليها أن تبلغها بذلك، على وجه السرعة، ومن ميزات هذا الإجراء انه سريع ويكفل حماية سرية البيانات التي تهم الشخص المعني.[2]

ويتقيد اللجوء إلى هذا الإجراء بشرط هام نصت عليه المادة (31) من اتفاقية بودابست وهو وجود سبب للاعتقاد بان البيانات ذات الصلة بالتوقيع الإلكتروني قد تتعرض للفقد أو التعديل، حتى تلتزم الدولة بحفظ تلك البيانات أو الإفصاح عنها.

ويجب أن يستعرض طلب الحفظ السريع ولو بإيجاز طبيعة الجريمة وبعض الحيثيات المتصلة بها، وطبيعة المعطيات المخزنة ومدى ارتباطها بالجريمة، وجميع البيانات المتوفرة، والتعريف بحافظ البيانات ومكان الأنظمة المعلوماتية وبيان نجاعة إجراء الحفظ. ويجب على الطالب أن يُعرب عن رغبته في التقدم بطلب تعاون في تاريخ لاحق بغرض التفتيش والحجز أو الكشف عن البيانات[3].

ولا تشترط الاتفاقية في مثل هذه الصورة، كقاعدة عامة، لزوم أن تكون الأفعال محل عقاب في البلدين للاستجابة للطلب، لأن شرط ازدواجية التجريم من شأنه أن يعلق إجراء الحفظ، ويرى رجال القانون بصفة عامة أن اللجوء إلى هذا الشرط يتوقف على مدى عمق تدخل هذا الإجراء في خصوصية الفرد مثل التفتيش أو الحجز والالتقاط البيني، ويبقى حق الرفض قائما إذا كان الطلب فيه مساسا بسيادة الدول أو بنظامها العام أو بجميع المصالح الأساسية.

---

[1]–منية الزغلامي، الاثبات في جرائم الاتصالات، مرجع سابق.

[2]–YANN PADOVA un aperçu de la lutte contre la cyber criminalité en France, Revue de science criminelle et droit pénal compare, 3 février 2002,p227.

[3]–منية الزغلامي، الإثبات في جرائم الاتصالات، مرجع سابق.

ويشترط أن تبقى المعطيات إذا تم حفظها مدة ستين (60) يوما على الأقل، وعلى الطالب أن يُحرر طلبه الأساسي في التفتيش أو الحجز، وإذا تقدم بطلب تبقى البيانات محفوظة إلى تاريخ الإنجاز.

ثانيا: الكشف السريع عن المعطيات المحفوظة

بناء على الطلب المقدم من سلطات التحقيق في الدولة المعنية بالنشاط الاجرامي، تقوم الدولة المطلوب إليها الإفصاح السريع عن البيانات المارة المحفوظة حفظ بيانات المستند الإلكتروني المارة لتعقبها، وصولا إلى مصدر النشاط والكشف عن هوية المجرم أو الحصول على الأدلة.[1]

وقد تواجه طالب الحفظ السريع للمعطيات إشكالية رفض الطلب لتعلقه بسيادة الدولة وأمنها ونظامها العام، وهو ما يدعوه إلى تبرير الإجراء عبر الاتصال بمختلف المتدخلين ومزودي الخدمات الموجودين في مختلف أنحاء العالم والذين تنتقل المعلومة بينهم، لطلب الكشف عن جملة البيانات التي لها علاقة بالنشاط، لتحديد مكان وصول المعلومة وغيرها من الآثار، حتى يتمكن الطالب من إعادة عرض الطلب أمام هياكل الدولة المعنية، وبذلك يضمن طالب الحفظ قبول طلبه من قبل الدولة المطلوب منها الإفصاح عن بيانات التوقيع الإلكتروني.

وقد حددت المادة (30) من اتفاقية بودابست الأحوال التي يجوز فيها التحفظ على المساعدة بهذا الإجراء حيث نصت على انه لا يحق لسلطات التحقيق في الدولة المطلوب منها، رفض الإفصاح عن البيانات المارة إلا للأسباب نفسها المتعلقة بطلب حفظ البيانات المخزنة في جهاز الحاسوب، ولسلطات الدولة المطلوب منها أن الإفصاح عن بيانات المستند الإلكتروني ان تتحفظ على الإفصاح،

---

[1]–حيث نصت المادة (29) من إتفاقية بودابست على ان: " في حال التحقيق في جريمة جنائية ارتكبت من خلال نظام كمبيوتر، تكون هنالك حاجة إلى بيانات الحركة لتعقب مصدر الاتصال كنقطة انطلاق من أجل جمع أدلة إضافية أو كجزء من الأدلة على الجريمة. لكن بيانات الحركة معرضة للزوال، مما يدعو إلى الأمر بالتعجيل بحفظها. ونتيجة لذلك، قد يكون من الضروري الكشف السريع عنها بغية تحديد طريق الاتصال من أجل جمع المزيد من الأدلة قبل حذفها أو بغية التعرف على المشتبه به. لذلك، قد يكون الإجراء العادي لجمع بيانات الكمبيوتر والكشف عنها غير كاف. فضلا عن ذلك، يعتبر جمع هذه البيانات من حيث المبدأ أقل تطفلا، حيث أنه لا يكشف عن محتوى الاتصال الذي يعتبر أكثر حساسية". راجع التقرير التفسيري لإتفاقية الجريمة الإلكترونية على الموقع الإلكتروني: https: //rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174

إذا تبين لها أن اتخاذ الإجراء من شأنه تهديد السرية أو عرقلة التحقيق الذي تجريه الدولة التي قدمت الطلب، كما ألزمت المادة تلك السلطات ضرورة إبلاغ سلطات التحقيق في الدولة الطالبة بذلك على وجه السرعة، والعلة من ذلك بطبيعة الحال إتاحة الفرصة للدولة الطالبة اتخاذ تدابير أخرى توصلا لأدلة في حق مرتكبي أي جريمة تتعلق بالإعتداء على التوقيع الإلكتروني.[1]

الفرع الثاني: الطرق الاستقرائية والتقنية

أولا: النفاذ إلى المعطيات المخزنة إلكترونيا داخل وخارج الدولة

تسمح إتفاقية بودابست في إطار المساعدة المتبادلة بين الدول بأن يطلب إنهاء إحدى الأعمال الاستقرائية المتعلقة بالتفتيش أو الحجز، أو الكشف عن هذه المعطيات بما في ذلك تلك التي سبق حفظها، على أن تجد هذه المطالب الاستجابة الكافية، وأن تُنفذ في أقرب الآجال خاصة بالنسبة إلى البيانات التي يُخشى إتلافها أو فسخها، مع احترام المتطلبات الواردة بالإتفاقية وضوابط القوانين الداخلية.[2]

كما يمكن النفاذ من خارج الحدود إلى البيانات المخزنة على شرط أن تكون البيانات مفتوحة للعموم، أو أن يتحصل الطالب على موافقة المعنى بالأمر، فالسماح بالنفاذ مباشرة من خارج الحدود مشروط بأن يكون الطرف مؤهلا قانونا في الكشف عن هذه البيانات.

---

[1]–وفي السياق ذاته نصت المادة (30) من إتفاقية بودابست على ان: "وضع التعريف قائمة مستفيضة لفئات بيانات الحركة التي تخضع معالجتها لنظام خاص في هذه الإتفاقية: منشأ الاتصال، وجهته، طريقه، وقته (توقيت غرينتش)، تاريخه، حجمه، مدته ونوع الخدمة التي ينطوي عليها. ولن تكون جميع هذه الفئات متاحة دائما من الناحية الفنية أو قد لا يتمكن مقدم الخدمة من إنتاجها، أو لن تكون ضرورية لإجراء تحقيق جنائي معين. ويشير مصطلح "المنشأ" إلى رقم الهاتف أو عنوان بروتوكول الأنترنت(IP) أو ما شابه ذلك من هوية هيئة الاتصالات التي يزودها مقدم الخدمة بخدماته. ويقصد بمصطلح "الوجهة" العنوان المماثل لهيئة الاتصالات التي تنقل إليها الاتصالات .وتشير عبارة "نوع الخدمة التي ينطوي عليها" إلى نوع الخدمة التي يتم استخدامها داخل الشبكة، مثل نقل الملفات، أو البريد الإلكتروني أو الرسائل الفورية". راجع التقرير التفسيري لإتفاقية الجريمة الإلكترونية على الموقع الإلكتروني المشار اليه سابقا.

[2]–منية الزغلامي، مرجع سابق.

ثانيا: الجمع الحيني لبيانات التوقيع الإلكتروني المتصلة بالنشاط

إن المعطيات المتصلة بالنشاط هي المعطيات التي لها علاقة بمصدر البيانات ومكان وصولها وساعة إرسالها، وغيرها من الإرشادات التي تفيد في التعرف على الجاني.

ومن المفروض أن تقع الاستجابة لطلب جمع هذه البيانات دون أي شرط، كما يجب أن تكون الأفعال محل البحث الجنائي مخالفة للنظام العام في كلا البلدين، كما يجب مراعاة الأحكام الواردة بالإتفاقية والقوانين الداخلية للدول.

وفي الكثير من الحالات، يتعذر على سلطات التحقيق في جرائم الإعتداء على التوقيع الإلكتروني تعقب اتصال ما، وصولا إلى مصدره عبر متابعة سجلات عمليات البث السابقة، إذ لا يستبعد إقدام مورد الخدمات على محو البيانات المارة الأساسية تلقائيا ضمن سلسلة البث قبل التمكن من حفظها.

وبالتالي، لا بد أن يتمتع المحققون التابعون لكل دولة بالقدرة على الحصول على البيانات المارة في الوقت الحقيقي فيما يتعلق بالاتصالات المارة عبر أحد أجهزة الحاسوب لدى الدول الأخرى.

لذلك، فقد ألزمت المادة (33) من اتفاقية بودابست كل دولة بجمع البيانات المارة في الوقت الحقيقي لصالح دولة أخرى، على أن يجري هذا التعاون بموجب المعاهدات والاتفاقات والقوانين المرعية[1]. باعتبار أن جمع البيانات المارة في الوقت الحقيقي يشكل الوسيلة الوحيدة لتحديد هوية المجرم، ونظرا لطبيعة هذا الإجراء الذي يقل في مساسه بالخصوصية عن غيره، حثت الإتفاقية الدول على تقديم أوسع مساعدة ممكنة حتى في غياب الجريمة المزدوجة.

وتعتبر تلك الصورة احد أهم سبل تبادل الإنابة القضائية الدولية وذلك للفصل في مسالة معروضة على السلطة القضائية في الدولة الطالبة عندما يتعذر عليها القيام بها بنفسها.[2]وفي هذا الصدد حرصت إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والتي تم التوقيع عليها

[1]–Tyner Russell, The Importance of International Cooperation in Preventing Cybercrime, Conférence régional sur La Cybercriminalité Casablanca, Royaume du Maroc 19-20 juin.

[2]–Cristina Schulman Le rôle de la collaboration entre les secteurs public et privé dans la lutte contre la cybercriminalité Conférence régionale 1 sur La Cybercriminalité Casablanca, Royaume du Maroc 19-20 juin, 2007, p 129.

في مدينة باليرمو عام 2000، على حث الدول إلى تطوير المساعدة القضائية في مجال التحقيقات الجنائية خاصة ما تعلق منها بالجرائم المعلوماتية، ودعوة جميع الدول إلى عقد إتفاقيات أخرى بهدف تعزيز هذا التعاون.[1]

ثالثا: إحداث شبكة إتصالات دولية مشتركة

يعتبر هذا التنظيم من أهم ما جاءت به إتفاقية بودابست في اتجاه ضمان نجاعة إجراءات المتابعة الجزائية في محيطها الإلكتروني، ويتمثل أساسا في إحداث شبكة إتصالات معلوماتية بين الدول الأعضاء بهدف ضمان الإتصال السريع وتبادل الإثبات وحصرها في أوقات قياسية، باستعمال طرق فنية توازي الخطر المعلوماتي، ويجب أن تكون شبكة الإتصالات هذه متوفرة باستمرار لفائدة الدول المتعاقدة، التي تلتزم بإنشاء نقطة إتصال إلكترونية تبقى مفتوحة على كامل الأيام والساعات لتقدم المساعدة الفورية، ويجب أن تجهز هذه النقطة بالوسائل الفنية المتطورة والأساليب التكنولوجية العالية وأن يتم تزويدها بالكفاءات المختصة في الميدان.

ويعود لكل دولة بيان مكان ترابط هذه الشبكة والأغلب أن يسند الاختصاص إلى الهيئة المركزية المختصة في إجراءات التعاون الدولي، أو إلى المكاتب المركزية للإنتربول Bureau central) (de l'Interpol، أو إلى وزارة الداخلية في إطار البحث عن الجريمة، أو إلى أي هيكل آخر تتوفر فيه الشروط المطلوبة سواء كان إداريا أو قضائيا.

وتؤكد الإتفاقية على ضرورة الاستعانة بوسائل الإتصال الحديثة، بما في ذلك البريد الإلكتروني والفاكس والهاتف، كما أرشدت إلى التعويل على منظومات التشفير لضمان السرية خاصة بالنسبة إلى الجرائم الخطيرة.

غير أنه بالنسبة إلى بقية وسائل الإتصالات مثل الهاتف والهاتف الجوال والفاكس والتلكس وغيرها، فإنه لم تصدر في شأنها إتفاقات دولية وبقي اعتمادها في الإثبات من اختصاص التشريعات الوطنية، على الرغم مما وصلته هذه الوسائل من تطور، إذ هي الآن وسائل رقمية، تعتمد في تنقلها

[1]–إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (إتفاقية باليرمو)، إعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون، المؤرخ في 15نوفمبر2000.

على الأقمار الصناعية والشبكات العالمية وتحقق بالتالي السرعة نفسها التي تحققها الأنترنت كما تختزل الحدود وتتجاوزها وهو ما يجعلها تمثل الخطر ذاته.[1]

[1]–جاء في التقرير التفسيري لإتفاقية الجريمة الإلكترونية النص على احداث شبكة على مدار الساعة و7 أيام في الأسبوع (المادة35):

– المادة (297): " كما سبق مناقشة ذلك، تتطلب المكافحة الفعالة للجرائم التي ترتكب عن طريق استخدام أنظمة الكمبيوتر والجمع الفعال للأدلة في شكل إلكتروني استجابة سريعة للغاية. فضلا عن ذلك، يمكن، من خلال نقرات قليلة على لوحة المفاتيح، اتخاذ إجراء في منطقة من العالم تترتب عنه فورا آثار عدة على بُعد آلاف الكيلومترات والعديد من المناطق الزمنية. لهذا السبب، يتطلب التعاون القائم بين الشرطة وآليات المساعدة المتبأدلة وجود قنوات تكميلية للتصدي لتحديات عصر الكمبيوتر بشكل فعال. وتستند القناة المنشأة في هذه المادة إلى الخبرة المكتسبة من شبكة تعمل بالفعل تحت رعاية مجموعة الدول الثمانية. وبموجب هذه المادة، يقع على كل طرف التزام بتعيين نقطة اتصال متاحة 24 ساعة في اليوم و7 أيام في الأسبوع لضمان تقديم المساعدة الفورية في التحقيقات والإجراءات في نطاق هذا الفصل، خاصة كما هو محدد بموجب المادة 35(الفقرة 1، البندين "أ" – "ج"). وتم الإتفاق على أن إنشاء هذه الشبكة يعتبر من بين أهم الوسائل المنصوص عليها في هذه الإتفاقية لضمان قدرة الأطراف على الاستجابة بفعالية لتحديات إنفاذ القانون التي تطرحها الجرائم المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر".

– المادة (299): يتعين على كل نقطة اتصال على مدار الساعة وطوال أيام الأسبوع يعينها الطرف أن تقوم إما بتيسير أو الاضطلاع مباشرة بتقديم المشورة التقنية وحفظ البيانات وجمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه بهم، من بين أمور أخرى. ويقصد بمصطلح "المعلومات القانونية" في الفقرة 1 تقديم المشورة لطرف آخر يطلب التعاون بأي شروط قانونية مسبقة مطلوبة لتوفير التعاون غير الرسمي أو الرسمي.

المادة 300: يتم تعكل طرف بحرية تحديد المكان الذي تستقر فيه نقطة الاتصال داخل بنية إن فإذ القانون. وقد ترغب بعض الأطراف في جعل مقر نقطة الاتصال 7/24 داخل سلطتها المركزية للمساعدة المتبادلة، وقد يعتبر البعض الآخر أن أفضل مكان لإيواء نقطة الاتصال هو وحدة الشرطة المتخصصة في مكافحة الجريمة المرتبكة عبر الكمبيوتر – أو الجرائم ذات الصلة بالكمبيوتر، ومع ذلك، قد تكون هنالك خيارات أخرى ملائمة لطرف معين، بالنظر إلى هيكله الحكومي ونظامها القانوني .وحيث يتعين على نقطة الاتصال 7/24 تقديم المشورة الفنية لوقف هجوم أو تتبعه، علاوة على واجبات التعاون الدولي من قبيل تحديد مكان المشتبه بهم، فلا يمكن تلخيص الحلول في إجابة واحدة صحيحة، علما أنه من المتوقع أن تتطور بنية الشبكة مع مرور الوقت. وينبغي عند تعيين نقطة الاتصال الوطنية، إيلاء الاعتبار الواجب للحاجة إلى التواصل مع نقاط الاتصال في لغات أخرى .

المادة (301): " تنص الفقرة 2 على أن من بين المهام الحاسمة التي يتعين أن تضطلع بها نقطة الاتصال 7/24 ثمة القدرة على تيسير التنفيذ السريع لتلك المهام التي لا تضطلع بها مباشرة بنفسها. على سبيل المثال، إذا كانت نقطة الاتصال 7/24 للطرف جزءا من وحدة الشرطة، وجب أن تكون لديها القدرة على التعجيل بالتنسيق مع العناصر

الفرع الثالث: الانابة القضائية وتبادل المعلومات

أولا: الإنابة القضائية

ويقصد بها: " طلب من السلطة القضائية المنيبة إلى السلطات المناوبة قضائية كانت أم دبلوماسية أساسه التعاون في اتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة من الخارج وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة أو المحتمل إثارتها في المستقبل أمام القاضي المنيب ليس مقدوره القيام به في نطاق دائرة اختصاصه"[1]

وتدخل الإنابة القضائية ضمن الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية

وتهدف الإنابة القضائية إلى نقل الإجراءات في المسائل الجنائية، لمواجهة ما تشهده الظواهر الإجرامية من تطور، وتذليل العقبات التي تعرض سير الإجراءات الجنائية المتعلقة بقضايا ممتدة خارج الوطنية، والإنابة القضائية تجد أساسها في القوانين الوطنية، وفي الإتفاقيات الدولية وفق مبدأ المعاملة بالمثل.

الأخرى ذات الصلة داخل الحكومة، من قبيل السلطة المركزية لتسليم المجرمين أو المساعدة المتبادلة، بغية تمكين اتخاذ الإجراءات المناسبة في أي ساعة من النهار أو الليل. وبالإضافة إلى ذلك، تقتضي الفقرة 2 أن يكون لدى كل نقطة اتصال 7/24 لدى طرف القدرة على إجراء اتصالات عاجلة بأعضاء آخرين في الشبكة".

المادة (302): " تقتضي الفقرة 3 أن تتوفر كل نقطة اتصال في الشبكة على المعدات المناسبة، حيث تعتبر أجهزة الهاتف والفاكس والكمبيوتر الحديثة ضرورية لاشتغال الشبكة بشكل سلس، كما ستكون هنالك حاجة إلى إدراج إشكال أخرى من معدات الاتصال والتحليل كجزء من النظام متقدم التكنولوجيا. وتقتضي الفقرة 3 أيضا بأن يكون الموظفون المشاركون في فريق الطرف المعني بالشبكة مدربين بالشكل اللازم في مجال الجريمة المرتكبة على الكمبيوتر والجريمة ذات الصلة بالكمبيوتر وطرق التصدي لها بفعالية".

[1]–عكاشة محمد عبد العالي، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار المطبوعات الجماعية، الإسكندرية، 1994، ص7.

وقد اهتم المشرع الجزائري بموضوع الإنابات القضائية الدولية، من خلال النص عليها في قانون الإجراءات الجزائية حيث نصت المادة (721) على أنه: "في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في المادة 703، وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري، وكل ذلك بشرط المعاملة بالمثل".

وتنص المادة (103) انه: " يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل الذي يتحقق من سلامة الطلب ويعطيه خط السير الذي يتطلبه القانون".

ويجري تنفيذ الانابات القضائية الدولية وفق المواد 721-725 من (ق.ا.ج.ج)، كما يلاحظ أن القانون لم يتناول الإنابات القضائية الصادرة من القضاء الجزائري والموجهة إلى الخارج[1].

ثانيا: تبادل المعلومات في جرائم الإعتداء على التوقيع الإلكتروني

تعطي الدول أهمية قصوى لتبادل المعلومات بوصفها الوسيلة الأكثر نجاعة في مكافحة الجريمة عموما والجريمة المعلوماتية خصوصا، لما توفره المعلومات الدقيقة والموثوقة من دعم للأجهزة القضائية والأمنية في كافة المجالات، لاسيما ما تعلق منها بمتابعة نشاط المنظمات الإجرامية. وقد حرصت المادة (26) من إتفاقية بودابست على التأكيد على واجب الدولة التي تمتلك معلومات هامة في مساعدة دولة أخرى أثناء التحقيقات أو تداول الدعوى الجنائية في الحالات التي لا تدرك فيها سلطات التحقيق في الدولة التي تجري التحقيقات أو الملاحقة وجود هذه المعلومات، دون حاجة لتقديم طلب بالمساعدة المتبادلة في تلك الحالة.[2]

وتتعدد صور تبادل المعلومات بين الدول، من بينها ما يتعلق بالسوابق القضائية للجناة، حيث تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها، وتداول الصحيفة الجنائية في

[1]– نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الثاني، الطبعة الثانية، دار هومة، الجزائر، 2016، ص555.

[2]–Cristina Schulman Le rôle de la collaboration entre les secteurs public et privé dans la lutte contre cybercriminalité Conférence régionale 1 sur La Cybercriminalité Casablanca, Royaume du Maro19-20 juin, 2007p129

مراحله الأولى، إلا أن الدول تقوم بإعدادها بالنسبة لرعايا الدولة التي ترتبط بها إتفاقيات تبادل معلومات.[1]

غير أن هناك حالات أخرى يلزم فيها تقديم طلب للدولة الأخرى لمدها بالمعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم.

وفي هذا السياق أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين[2]، بتطوير التبادل المنهجي للمعلومات بوصفه عنصرا رئيسيا من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وضرورة إنشاء قاعدة معلومات لإعلام الدول الأطراف بالمؤشرات العالمية للإجرام.

الفرع الرابع: نظام تسليم المجرمين كآلية لمكافحة جرائم التوقيع الإلكتروني

يعد موضوع تسليم المجرمين من أبرز إشكال المساعدة القانونية المتبادلة في المسائل الجنائية، ذلك لأنه يتعلق بالأشخاص المطلوب تسليمهم لتوجيه الاتهام إليهم، أو لمحاكمتهم، أو لتنفيذ العقوبة عليهم، لذا حرصت أغلب الاتفاقيات الدولية على إلزام الدول بالمساعدة المتبادلة في المسائل الجنائية بوجه عام، وفي مجال تسليم المجرمين بوجه خاص، وقامت أغلب الدول بإبرام اتفاقيات ثنائية لترسيخ آليات التعاون القضائي الدولي في إطار المبادئ المستقرة في القانون الدولي (مبدأ المعاملة بالمثل).

---

[1]–MERLE (Roger) et vitu (André), Traite de droit criminel, Droit pénal spécial par vitu, Cujas, Paris, 4éme ed., 1981p.239.

[2]–انعقد المؤتمر في كاراكاس بفنزويلا سنة 1980 تحت شعار: " الوقاية من الجريمة ونوعية الحياة"، وتم عرض أول دراسة استقصائية مفصلة اعدتها الامم المتحدة في مجال الجريمة عبر مختلف انحاء العالم، استنادا إلى معلومات واردة من 65 دولة عضوا، واظهرت الدراسة ان غالبية الدول المتقدمة منها والنامية تواجه تصاعدا في العنف والاجرام، وان الاجرام يتخذ إشكالا وابعادا جديدة وان التدابير التقليدية لمنع الجريمة ومكافحتها ليست قادرة على معالجة الوضع، راجع مضمون هذا المؤتمر على الموقع:

https: //portal.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html

تاريخ الاطلاع: 2019/08/31 على الساعة: 21: 05.

ويعرف الدكتور جميل عبد الباقي نظام تسليم المجرمين بانه:" إجراء تتخلى الدولة بموجبه عن فرد موجود لديها لسلطات دولة أخرى– تطالب بتسليمه اليها– بغرض محاكمته عن جريمة ارتكبها، أو لتنفيذ حكم صادر ضده بعقوبة جنائية".[1]

ويتمثل تسليم المجرمين في الجرائم الواقعة على التوقيع الإلكتروني، أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود مثل الاعتداءات الاجرامية التي تطال آليتي التوقيع والتصديق الإلكترونيين، عليها أن تقوم بمحاكمته، إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه إلى دولة أخرى تختص بمحاكمته.[2]

وقد أكد البند (17) من المادة 16 من إتفاقية باليرمو للجريمة المنظمة عبر الوطنية على أهمية تسليم المجرمين في الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات، حيث نصت على انه يتعين على الدول الأطراف على الدول الأطراف ان تسعى إلى إبرام اتفاقات لتنفيذ تسليم المجرمين كما نص البندين (2) و(4) من ذات المادة على انه إذا كان طلب التسليم يتضمن عدة جرائم خطيرة منفصلة، وبعض منها ليس مشمولا بهذه المادة، جاز للدولة الطرف التي تلقت الطلب ان تطبق هذه المادة أيضا فيما يتعلق بالجرائم الأخيرة وجاز لها أن تعتبر هذه الإتفاقية هي الأساس القانوني للتسليم فيما يتعلق بأي جرم تنطبق عليه هذه المادة.

وبالتالي فانه كلما انطبقت شروط اعتبار الجرائم الواقعة على التوقيع الإلكتروني من الجرائم المنظمة العابرة للحدود، فان التسليم في تلك الحالة يخضع لنصوص المواد (16) و(17) من إتفاقية باليرمو.[3]

وتتنوع أنظمة تسليم المجرمين من دولة إلى أخرى بحسب السلطة المصدرة للطلب في الدولة، الا أن هناك ثلاث أنظمة متبعة هي:

---

[1]–جميل عبد الباقي، الجوانب الاجرائية لجرائم الأنترنت، مرجع سابق، ص27، ص91.

[2]–محمد زكي ابو عامر، قانون العقوبات، القسم العام دار المطبوعات الجامعية، الاسكندرية، مصر، 1986، ص109.

[3]–Convention Des Nations Unies contre La Criminalité Transnationale Organisée et Protocole S'y Rapportant 2004 Article 16/17,
https: //www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-f.pdf

1. التسليم القضائي:

تسليم المجرمين وفق هذا النظام يكون من اختصاص السلطة القضائية عن طريق إصدار قرار التسليم وفق منهجين تأخذ بهما الدولة أثناء تنفيذ هذا القرار، الأول أن تكون المحكمة هي الجهة الوحيدة المختصة بإصدار قرار التسليم للدولة، والثاني يتمثل في إعطاء النائب العام في الدولة المطلوب منها التسليم سلطة الفصل في إصدار القرار النهائي من عدمه.[1]

2. التسليم الإداري:

يكون التسليم في هذا النظام عملا من أعمال السلطة التنفيذية، فطلب الاسترداد يتلقاه وزير العدل ويتم الرد عليه عبر إجراءات إدارية ودبلوماسية تنتهي بقرار من رئيس الدولة أو الحكومة بالقبول أو الرفض، ويمتاز هذا النظام بالسرعة والبساطة، إلا أن من عيوبه عدم توفير الضمانات الكافية للشخص المطلوب استرداده للدفاع عن حقوقه.

3. التسليم المختلط:

يجمع هذا الأسلوب بين النظامين القضائي والإداري، حيث يوازي بين المصلحتين المتعارضتين، مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه بتوفير الضمانات القانونية للدفاع.[2]

وفي هذا الصدد اقر المشرع الجزائري بوجوب إبرام معاهدات في مجال تسليم المجرمين، من خلال النصوص المنظمة لهذا النظام في قانون الإجراءات الجزائية سيما المادة (694) منه، وقد تم عقد إتفاقيات ثنائية مع الكثير من الدول منها فرنسا وبريطانيا.[3]

---

[1]–ياسر محمد الكومي، مرجع سابق، ص445

[2]– هشام رستم، الجرائم المعلوماتية، مرجع سابق، ص439، ص440

[3]–إتفاقية تسليم المجرمين بين مملكة بريطانيا والجزائر المصادق عليها بموجب المرسوم الرئاسي رقم: 06–264 المؤرخ في 2006/12/11 ج.ر العدد 81 المؤرخ في 2006/12/13، إتفاقية تسليم المجرمين بين فرنسا والجزائر المصادق عليها بموجب المرسوم الرئاسي رقم: 194/65 المؤرخ في 1988/06/09

وقد منح الدستور الجزائري للإتفاقيات الدولية المصادق عليها من طرف الجزائر مكانة تسمو على القانون الداخلي من حيث التطبيق طبقا للمادة (150) منه وهو ما كرسته المادة (694) من قانون الإجراءات الجزائية.

خاتمة

تناولت هذه الدراسة البحث في الجوانب الموضوعية والإجرائية، التي أقرها المشرع الجزائري في إطار مكافحة الجرائم الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني، باستعمال تكنولوجيات الإعلام والإتصال الحديثة، التي وفرت سهولة اتصال الحاسوب أو الهاتف النقال بشبكة الأنترنت، ومن خلال ذلك سهولة التلاعب في بيانات التوقيع الإلكتروني، وتطبيقاته المختلفة في مجالات الحكومة الإلكترونية والتجارة الإلكترونية والمعاملات المصرفية ووسائل الدفع الإلكتروني...الخ. مما نتج عنه تعدد إشكال الجرائم التي تقع إعتداءا على اليتي التوقيع والتصديق الإلكترونيين، التي تستوجب الدراسة الدقيقة للبنيان القانوني لها، حيث تناولت الدراسة أركانها إضافة إلى توضيح إشكالية مدى اعتبار بيانات التوقيع الإلكتروني موضوعا لنصوص جرائم الأموال، حيث خلص البحث إلى إضفاء المشرع الحماية الجزائية على قواعد البيانات باعتبارها قيما مالية مستحدثة، وهذا بموجب الأمر رقم: 05/03 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة.

أما على صعيد التجريم والعقاب، قام المشرع الجزائري بخطوات هامة في هذا المجال تمثلت في النص على الجرائم الواقعة على التوقيع الإلكتروني وشهادة التصديق الإلكتروني على سبيل الحصر، بموجب القانون رقم: 04/15 المؤرخ في: 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، مثل جرائم التلاعب في بيانات التوقيع الإلكتروني عن طريق حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الإلكتروني موصوف خاصة بالغير، وكذا الجرائم الماسة ببيانات شهادة التصديق الإلكتروني، وجرائم مؤدي خدمات التصديق الإلكتروني، وجرائم الشخص المعنوي.

وتطرقت الدراسة قبل ذلك إلى جرائم الإعتداء على التوقيع الإلكتروني في إطار القواعد العامة لقانون العقوبات، والتي تدخل ضمن جرائم الأموال وجرائم التزوير، وكذا الجرائم الواردة في القانون 15/04المعدل لقانون العقوبات، المؤرخ في: 10 نوفمبر 2004، في القسم السابع مكرر بعنوان: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، من المواد (394 مكرر إلى 394 مكرر 7) مثل: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات وغيرها.

كما إتجه المشرع إلى تجريم بعض إشكال الإعتداءات الواقعة على التوقيع الإلكتروني بموجب بعض القوانين الخاصة، كالقانون رقم: 03/15 المؤرخ في: 2015/02/01 المتعلق بعصرنة العدالة، والقانون رقم: 04/18 المؤرخ في 2018/05/10، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، والقانون رقم: 05/18 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية، والقانون رقم: 07/18 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ويلاحظ عدم نص المشرع على بعض الجرائم الماسة بالمعطيات الخاصة بالتوقيع الإلكتروني رغم أهميتها، مثل: جريمة التزوير المعلوماتي، وجرائم إفساد النظام المعلوماتي، في مجال التوقيع والتصديق الإلكتروني، وعليه يجب على المشرع تدارك هذا الفراغ التشريعي من خلال تعديل النصوص التقليدية، أو استحداث نصوص أخرى جديدة تتلاءم وطبيعة هذه الجرائم.

وبإعتبار الجرائم الماسة بالتوقيع والتصديق الإلكترونيين، جرائم عابرة الحدود يتطلب مكافحتها تظافر جهود الدول، قام المشرع الجزائري بالتصديق على نصوص الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، إضافة إلى إبرام إتفاقيات ثنائية بخصوص التعاون القضائي والمساعدة القضائية الدولية، والتي تعتبر خطوات هامة على صعيد المكافحة الدولية لهذه الجرائم.

أما فيما يتعلق بالجانب الإجرائي، فقد تطرقت الدراسة إلى بعض الإجراءات التقليدية كإجراء المعاينة والخبرة ومدى انطباق هذه الإجراءات على الجرائم الواقعة على التوقيع الإلكتروني، وتمت الإشارة إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم: 22/06 المؤرخ في 2006/12/20 المعدل والمتمم، بالنظر إلى قصور النصوص التقليدية للإثبات في مجال الجرائم المعلوماتية، أين استحدثت أساليب خاصة للبحث والتحري عن بعض الجرائم على سبيل الحصر، ومنها الجرائم الإلكترونية، مثل: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب، وذلك بموجب المواد من (65 مكرر 5 – 65 مكرر 18).

كما تمت الإشارة أيضا إلى السياسة الجزائية الوقائية في مواجهة مثل هذه الجرائم، والتي تبناها المشرع الجزائري من خلال القانون رقم: 04/09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أين نص على جملة من الإجراءات الخاصة، مثل: تفتيش

المنظومة المعلوماتية داخل الإقليم الوطني أو خارجه، وجز المعطيات المعلوماتية والتعاون القضائي والمساعدة الدولية المتبادلة.

بناء على ما سبق ذكره، خلصنا في دراستنا هذه إلى ما يأتي:

1. تقتضي الحماية الجزائية للتوقيع والتصديق الإلكترونين الوقوف على التدابير التقنية التي يجب الاعتماد عليها لتوفير حماية وقائية من مخاطر الاعتداء على هذه الالية، اذ يعتبر منع وقوع الجريمة في هذا المجال اكثر فاعلية من إدانة الجاني.
2. تعتبر الية التشفير أحد أهم وسائل الحماية التقنية التي تحقق الحجية المطلوبة في التوقيع والتصديق الإلكترونيين، ونسبة التوقيع إلى صاحبه، وصدوره عن ارادة صحيحة منه، وأن أي تزوير يطاله هو بمثابة تزوير محرر رسمي، تنطبق عليه اركان جرائم التزوير في المحررات الرسمية.
3. تتكامل الحماية الوقائية للتوقيع الإلكتروني مع الحماية الجزائية المقررة له، ويظهر ذلك من خلال تنظيم التزامات قانونية على عاتق الأطراف ذات الصلة بالتوقيع والتصديق الإلكترونيين، سواء تعلق الأمر بطرفي المعاملة، أو بالجهات التي تلعب دورا في إنشائه وإدارته، فبقدر التزام كل طرف من الأطراف المتعاملة بقدر ما تتضاءل المخاطر الناجمة عن التوقيع الإلكتروني، ومن هنا برزت أهمية فرض التزامات على جميع جهات العمل لتنفيذ تدابير تأمين المعلومات لحماية بياناتها الخاصة والإفصاح عن أي خرق قد يحدث لنظم التأمين.
4. إن المصالح محل الحماية الجزائية في التوقيع والتصديق الإلكترونيين متعددة، لا تقتصر فقط على المعاملات الحكومية كقطاع العدالة والجماعات المحلية، وإنما تمتد أيضا إلى حماية المستهلك في مجالات التجارة الإلكترونية والمعاملات المصرفية، وحرية تداول السلع والخدمات عبر الأنترنت، وتتمثل المصالح المحمية في شرعية تداول البيانات، وسرية البيانات وخصوصيتها، ومبادئ الملائمة وعدم التمييز تجاه التوقيع الإلكتروني.
5. تعددت أنماط تجريم الإعتداءات الواقعة على آلية التوقيع والتصديق الإلكترونيين وفقا للمصلحة محل الإعتداء، فقد يرتبط السلوك المادي لجرائم الإعتداء على التوقيع الإلكتروني بتداول بيانات التوقيع الإلكتروني، كما هو الحال بالنسبة لجريمة التعامل غير المشروع في نشاط التصديق أو انتهاك سرية وخصوصية البيانات، كما انه من المتصور أن يكون محل الجريمة هو المساس

بحجية التوقيع الإلكتروني في الإثبات كما هو الحال في الجرائم الماسة بنظام المعالجة الالية للمعطيات، وجرائم تزوير التوقيع الإلكتروني أو إتلافه، لذلك كان ضروريا النص على تجريم تلك الإعتداءات بالنظر إلى تطبيقاته المختلفة.

6. نص المشرع على إجراءات وقائية بموجب القانون 04/09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الهدف منها تفادي أي إعتداء إجرامي محتمل تمثلت في مراقبة الإتصالات الإلكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات والتعاون القضائي والمساعدة الدولية المتبادلة وفق شروط معينة.
7. لم يجرم المشرع الجزائري صراحة جريمة تزوير التوقيع الإلكتروني واكتفى بنصوص المادة (394 مكرر) من قانون العقوبات في جزئه المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات والمتمثلة في جريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات عن طريق (أفعال: الإدخال والمحور والتعديل).
8. رغم خلو القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين من نصوص إجرائية تنظم أدلة الإثبات الجنائي في الجرائم الواقعة على التوقيع الإلكتروني الا انه يلاحظ ملائمة النصوص التقليدية في (ق.إ.ج.ج) وكذا النصوص الواردة في القانون 04/09 السالف ذكره (مواجهة هذا النوع من الجرائم)، مع زيادة تأهيل الشرطة المتخصصة في الجرائم المعلوماتية على الأساليب التقنية المستحدثة والمستخدمة في ارتكاب جرائم الإعتداء على التوقيع والتصديق الإلكترونيين وتعزيز التعاون الدولي والمساعدة القضائية في هذا المجال.

التوصيات:

في ضوء نتائج الدراسة سالفة الذكر، خلص البحث إلى التوصيات الآتية:

- **أولا:** مراجعة التشريع الجزائري فيما يتعلق بتجريم الأفعال الماسة بالمصالح المحمية في الجرائم الواقعة على التوقيع والتصديق الإلكترونيين، وضرورة النص على تجريم تزوير التوقيع الإلكتروني، وتجريم صنع أو حيازة أو الحصول على برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني أو شهادة تصديق إلكتروني، وتغليظ عقوبة الغرامة، لما لهذه الجرائم من آثار اقتصادية وخيمة.

- **ثانيا:** تعزيز الإجراءات الوقائية سواء داخل الدولة عن طريق التعاون الدولي لمكافحة الجرائم الواقعة على التوقيع الإلكتروني.
- **ثالثا:** ضرورة تأهيل أجهزة الأمن المتخصصة في الجرائم المعلوماتية، وتدريبهم على كيفية اعتراض محتوى بيانات التوقيع الإلكتروني وشهادة التصديق الإلكتروني.
- **رابعا:** التجسيد الميداني لمشروع التخصص للمحاكم المنوط بها النظر في الجرائم الواقعة على التوقيع الإلكتروني، وتأهيل القضاة من الناحية التقنية وكيفية التعامل مع الدليل الإلكتروني وفحصه أثناء المحاكمة، تحقيقا لمبدأ المحاكمة العادلة.
- **خامسا:** ضرورة التعاون الدولي، وتفعيل المساعدة القضائية الدولية، عن طريق إبرام الإتفاقيات الثنائية والانضمام إلى المعاهدات والإتفاقيات في مجال مكافحة الإجرام المعلوماتي

قائمة المصادر والمراجع

أولا: المراجع باللغة العربية

1) المراجع العامة:

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة 2016/2015، دار هومة، الجزائر 2016.
2. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للنشر والتوزيع، الطبعة الرابعة عشر، سنة 2014.
3. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2012.
4. الصاوي محمد منصور، أحكام القانون الدولي المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دار المطبوعات الجامعية(ب–ط)، الإسكندرية، (ب–ت–ن).
5. طارق سرور، الاختصاص الجنائي العالمي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2006.
6. عبد الأمير العكيلي، أصول الإجراءات الجنائية في قانون المحاكمات الجزائية، الجزء الثاني، الطبعة الثانية، مطبعة المعارف، بغداد 1974.
7. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، الطبعة الثالثة، دار هومة، الجزائر 2012.
8. عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام)، ديوان المطبوعات الجامعية، الجزائر 2009.
9. عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأول "الجريمة"، ديوان المطبوعات الجامعية، الجزائر 2009.
10. عكاشة محمد عبد العالي، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار المطبوعات الجامعية، الإسكندرية، 1994.
11. علي عبد القادر القهوجي، قانون العقوبات القسم الخاص، منشورات الحلبي الحقوقية، بيروت، 2002
12. عمر سالم، الوجيز في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2011–2012.

13.حسن علي الذنون، ومحمد سعد الرحو، الوجيز في النظرية العامة للالتزام- مصادر الالتزام- الجزء الأول، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن، 2000.

14.حمدي باشا عمر، القضاء المدني، ط4، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009.

15.فتوح عبد الله الشاذلي، القانون الدولي الجنائي، الكتاب الأول، أوليات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، دار المطبوعات الجامعية، الإسكندرية، 2001.

16.فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، 2012.

17.كمال أنور محمد، تطبيق العقوبات من حيث المكان، القاهرة، 1965.

18.مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الأول، مكتبة رجال القضاء، الطبعة الثانية، 2005.

19.محمد صبري السعدي، الواضح في شرح القانون المدني الجزائري، النظرية العامة للالتزامات، مصادر الالتزام، الجزء الأول، الطبعة الأولى، دار الهدى للنشر والتوزيع، الجزائر، 2007 – 2008.

20.محمد صبري السعدي، الواضح في شرح القانون المدني، الطبعة الرابعة، دار الهدى، الجزائر، 2009

21.محمد زكي أبو عامر، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 1994.

22.محمد زكي أبو عامر، قانون العقوبات، القسم الخاص، دار الجامعة الجديدة للنشر، الإسكندرية 2015.

23.محمد زكي أبو عامر، قانون العقوبات، القسم العام دار المطبوعات الجامعية، الإسكندرية، مصر، 1986.

24.محمد محي الدين عوض، دراسات في القانون الدولي الجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2005.

25.محمود نجيب حسين، شرح قانون الإجراءات الجنائية، الطبعة الثانية، القاهرة، 1982.

26.مصطفى محمد الدغيدي، التحريات والإثبات الجنائي، مطابع جامعة المينا، مصر، 2002.

27.منذر الفضل، النظرية العامة للالتزاماتّ، الجزء الأول، دار الثقافة، عمان، الأردن، 1996.

28.نبيل إبراهيم سعد، النظرية العامة للالتزام، مصادر الالتزام، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009.

29.نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر، 2012.

30.نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الثاني، الطبعة الثانية، دار هومة، الجزائر، 2016.

2) المراجع المتخصصة

1. إبراهيم حامد مرسي، سلطات مأمور الضبط القضائي، دراسة مقارنة، الطبعة الثانية، 1997.
2. أبوبكر يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي، دار الفكر العربي، مصر 2005.
3. أحمد حسام طه، الجرائم الناشئة عن إستخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي) دراسة مقارنة، دار النهضة العربية، 2000.
4. احمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، دار النهضة العربية، مصر، 2015.
5. أسامة احمد المناعسة، جلال مهد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان 2014.
6. أيمن رمضان محمد احمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، مصر 2011.
7. أيمن سعد، التوقيع الإلكتروني، دار النهضة العربية، القاهرة 2013.
8. أيمن عبد الله فكري، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض 2015.
9. بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر 2007.
10. ثروت عبد الحميد، التوقيع الإلكتروني ماهيته، مخاطره، مدى حجيته في الإثبات، الإسكندرية، دار الجامعة الجديدة، ط1، 2007.

11. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
12. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001.
13. جميل عبد الباقي الصغير، جرائم الأنترنت، الأحكام الموضوعية والجوانب الإجرائية، طبعة نادي القضاة، 2010.
14. حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.
15. خالد محمد المهيري، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، دبي، الإمارات العربية المتحدة، معهد القانون الدولي.
16. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دراسة مقارنة، دار الكتب القانونية، مصر، 2011.
17. سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، مصر 20060.
18. سليم سعداوي، عقود التجارة الإلكترونية، دار الخلدونية، الجزائر 2008.
19. شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظامين اللاتيني والانجلو أمريكي، مصر 2013.
20. ضياء مصطفى عثمان، السرقة الإلكترونية دراسة فقهية، الطبعة الأولى، دار النفائس، الأردن 2011.
21. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.
22. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر 2007.
23. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول، دار الكتب القانونية، مصر 2007.
24. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، مصر، 2005.

25. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، مصر، ط1، 2009.
26. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، ط1، دار النهضة العربية، القاهرة، مصر، 2003.
27. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، نظام التجارة الإلكترونية وحمايتها مدنيا، مصر، 2005.
28. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
29. عبد الفتاح بيومي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الكتب القانونية، مصر 2007.
30. عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة 2002.
31. عبد الفتاح ييرمي حجازي، الحكومة الإلكترونية، الكتاب الثاني، دار الكتب القانونية، مصر 2007.
32. عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية 1999، ص52.
33. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف، المصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت 2007.
34. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012.
35. عمر محمد يونس، الإتفاقية الأوربية حول الجريمة الافتراضية، دار النهضة العربية، القاهرة 2007، ص 85.
36. غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية، الجزائر، 2015.

37. فؤاد حسن العزيزي، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، مصر، 2015.
38. لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار هومة، الجزائر 2012.
39. م.م.لينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد للنشر والتوزيع، عمان 2015.
40. محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر 2007.
41. محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2011.
42. محمد حسين منصور، الإثبات الإلكتروني، دار الفكر الجامعي، الاسكندرية، 2006.
43. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، مصر 2014.
44. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2000.
45. ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005.
46. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.
47. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب الوطنية، 2006.
48. نبيلة هبة هروال، الجوانب الإجرامية لجرائم الأنترنت، دار الفكر الجامعي، الإسكندرية 2007.
49. نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، مصر، 2013.
50. نجوى أبو هيبة، التوقيع الإلكتروني تعريفه ومدى حجيته في الإثبات، دار النهضة العربية، القاهرة 2004.
51. نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الثاني، الطبعة الثانية، دار هومة، الجزائر، 2016.

52. نصر شومان، التكنولوجيا الإجرامية الحديثة وأهميتها في الإثبات الجنائي، الطبعة الأولى، بدون دار وبلد النشر، 2011.
53. نصر شومان، التكنولوجيا الجرمية الحديثة، وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة في الكتاب، طرابلس، لبنان، ط1، 2011.
54. نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية، بيروت 2006.
55. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2010.
56. لينا إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة (دراسة مقارنة)، دار الراية للنشر والتوزيع، ط1، الأردن عمان،
57. هشام محمد فريد رستم، الجوانب الإجرائية للجريمة المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، آسيوط 1994.
58. هلالي عبد الإله أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، مصر، 1997.
59. هلالي عبد الإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية في ضوء إتفاقية بودابست، دار النهضة العربية، الطبعة الأولى، 2003.
60. هلالي عبد الإله احمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة 1997.
61. هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، مصر، 1997.
62. ياسر محمد الكومي محمود أبو وحطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف الإسكندرية 2014.
63. يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، الجزائر 2016.

3) الرسائل العلمية:

أ. اطروحات الدكتوراه:

1. إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وصوره وتطبيقاته، أطرحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009.
2. براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، جامعة بسكرة 2015.
3. براهيمي جمال، التحقيق في الجرائم الإلكترونية، أطروحة دكتوراه، جامعة مولود معمري تيزي وزو، كلية الحقوق، 2018.
4. بن قارة مصطفى عائشة، الحماية الجنائية للحكومة الإلكترونية، أطروحة دكتوراه، جامعة أبوبكر بلقايد، تلمسان، 2018.
5. حسن إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه، دار النهضة العربية، 2006.
6. حسن إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه، كلية الحقوق، عين شمس، القاهرة.
7. حفصي عباس، جرائم التزوير الإلكترونية، أطروحة دكتوراه، جامعة وهران، 2015 .
8. صالح شنين، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، جامعة أبو بكر بلقايد، كلية الحقوق، تلمسان، 2013،
9. طارق فوزي التقي، الجوانب الإجرائية في الجرائم المعلوماتية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة منوفية، مصدر سنة 2011.
10. عمر عبيد محمد الغول، نطاق تطبيق القانون الجنائي من حيث المكان، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2006.
11. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004.
12. نبيلة هروال، جرائم الأنترنت، أطروحة دكتوراه، جامعة أبي بكر بلقايد، تلمسان، 2014.

4) الابحاث والمقالات:

1. بلحسين حمزة، الحماية القانونية والفنية للتوقيع الإلكتروني، مجلة العلوم القانونية والإدارية، العدد (11)، جامعة جيلالي اليابس، سيدي بلعباس، 2015.
2. بن فردية محمد، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، المجلة الأكاديمية للبحث القانوني، العدد01.
3. زهدور كوثر، حجية التوقيع الإلكتروني في الإثبات والمسؤولية المدنية المتولدة عنه في التشريع الجزائري، مجلة الدفاع، العدد (02).
4. زهيرة كيسي، النظام القانوني لجهات التوثيق (التصديق الإلكتروني)، مجلة دفاتر السياسة والقانون، المركز الجامعي بتمنراست، الجزائر، العدد (07)، جوان 2012.
5. زيد حمزة مقدم، وسائل وضمانات التوقيع الإلكتروني، مجلة جامعة بحري للآداب والعلوم الإنسانية، جمهورية إيران، 2004.
6. سوزان عدنان، انتهاك الحياة الخاصة عبر الأنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد29–العدد الثالث–2013.
7. صالح عبد الزهرة الحسون، قواعد الاختصاص في التحقيق الابتدائي في القانون العراقي، مجلة القضاء، العدد الأول، 1987.
8. عبد الجبار الحنيص، الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27، العدد الأول، 2011.
9. لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، المجلد الثاني، العدد الثاني، 2009.
10. محمد أمين الخرشة، نائف عبد الجليل الحمايدة، الحماية الجنائية للتوقيع الإلكتروني في التشريعيين الاماراتي والبحريني " دراسة مقارنة "، مجلة جامعة الأزهر غزة، سلسلة العلوم الإنسانية، المجلد 16، العدد الأول، 2014.
11. محمد بكرار شاوش، الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، العدد الرابع عشر، جانفي 2016.

5) الملتقيات:

1. جوناثان ج. روش. الأطر التشريعية والقانونية لمكافحة الجرائم الإلكترونية، إستراتيجية قضائية لتطبيق قانون التوقيع الإلكتروني، مؤتمر التواقيع الإلكترونية، القاهرة، مصر، الفترة ما بين 8 و9 مارس2006.
2. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الأنترنت، الفترة: 2-4/يونيو 2008، منشور على الأنترنت، على الموقع: http: //www.f-law.net
3. عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، من 12 إلى 14 نوفمبر 2007، الرياض، السعودية.
4. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للمعاملات الإلكترونية، دبي، 2004.
5. محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر "القانون والكمبيوتر والأنترنت، جامعة الإمارات العربية المتحدة، العين في الفترة ما بين 1 و3 ماي 2000.
6. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، بحث منشور ضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية"، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من: 10 إلى 12 ماي لسنة 2004، المجلد الخامس.
7. مؤتمر تأمين المعلومات والدليل الرقمي وكيفية إثباته في الجرائم الإلكترونية، مصر في الفترة ما بين: 10 و16 ديسمبر 2010، المركز القومي للبحوث الاجتماعية، مصر.
8. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، يومي: 28 و29 أكتوبر 2009، طرابلس، ليبيا.

9. محمد حاتم البيات، مؤتمر المعاملات التجارة الالكترونيةالحكومية،المسؤولية المدنية عن الخطأ في المعاملات التي تتم عن طريق الوسائط الالكترونية، كلية القانون، جامعة قطر.

6) النصوص الرسمية:

أ. الدساتير

1- القانون رقم: 01/16 المؤرخ في: 06 مارس2016، (ج.ر) عدد (14) المؤرخة في: 07 مارس2016 المتضمن تعديل الدستور.

ب. الإتفاقيات

1- إتفاقية تسليم المجرمين بين فرنسا والجزائر المصادق عليها بموجب المرسوم الرئاسيرقم: 194/65 المؤرخ في 1988/06/09.

2- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (إتفاقية باليرمو)، إعتمدتوعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون، المؤرخ في 15نوفمبر2000.

3- إتفاقية تسليم المجرمين بين مملكة بريطانيا والجزائر المصادق عليها بموجب المرسوم الرئاسي رقم: 06-264 المؤرخ في 2006/12/11 ج.ر العدد 81 المؤرخ في 2006/12/13.

4- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 2010/12/21، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم: 14-252 المؤرخ في: 2014/09/08، (ج.ر) رقم: 57 المؤرخة في: 2014/09/28.

ج. القوانين والأوامر:

- **القوانين:**

1- القانون رقم: 15/04 المؤرخ في: 2004/11/10 يعدل ويتمم الأمر رقم: 156/66 المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات، (ج.ر) رقم: 71 المؤرخة في: 2004/11/10.

2- القانون رقم: 14/04 المؤرخ في: 2004/11/10، المعدل والمتمم لقانون الإجراءات الجزائية (ج.ر) رقم: 71 المؤرخة في: 2004/11/10.

3- القانون 10/05 المؤرخ في 2005/06/20 يعدل ويتمم الأمر رقم: 58/75 المؤرخ في 1975/09/26 المؤرخ في: 1975/09/26 والمتضمن القانون المدني المعدل والمتمم، (ج.ر) رقم: 44 المؤرخة في: 2005/06/26.

4- القانون 22/06 المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 155/66 المؤرخ في 1966/06/08، والمتضمن قانون الإجراءات الجزائية (ج.ر) رقم 84 المؤرخة في 2006/12/24.

5- القانون رقم: 23/06 المؤرخ في: 2006/12/20 يعدل ويتمم الأمر رقم: 156/66 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم: 84 المؤرخة في: 2006/12/24.

6- القانون رقم: 01/09 المؤرخ في: 2009/02/25، يعدل ويتمم الأمر رقم: 156/66 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم: 15 المؤرخة في: 2009/03/08.

7- القانون 04/09 المؤرخ في 2009/08/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها (ج.ر) رقم 47 المؤرخة في: 2009/08/16.

8- القانون رقم: 03/15 المؤرخ في: 2015/02/01، يتعلق بعصرنة العدالة (ج.ر) العدد (06) المؤرخة في: 10 فيفري 2015

9- القانون رقم: 04/15 المؤرخ في: 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (ج.ر) رقم: 06 المؤرخة في: 02/10/ 2015.

10- القانون 18/ 04 المؤرخ في 10ماي2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، (ج.ر) عدد: 27 المؤرخة في 13ماي2018.

11- القانون رقم: 05/18 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية، (ج.ر) العدد: 28 المؤرخة في 2018/05/16.

12- القانون رقم: 07/18 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، (ج.ر) العدد: 34 المؤرخة في 2/06/16

❖ **الأوامر:**

1- الأمر 155/66 المؤرخ في 08 يونيو عام 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.
2- الأمر 156/66 المؤرخ في 08 يونيو عام 1966 المتضمن قانون العقوبات، المعدل والمتمم.
3- الأمر رقم: 58/75 المؤرخ في: 26 سبتمبر 1975 يتضمن القانون المدني المعدل والمتمم.
4- الأمر رقم: 59/75 المؤرخ في: 26 سبتمبر 1975 والمتضمن القانون التجاري، المعدل والمتمم.
5- الأمر رقم: 05/03 المؤرخ في: 2003/06/19 يتعلق بحقوق المؤلف والحقوق المجاورة، (ج.ر) رقم: 44، المؤرخة في: 2003/06/23.

د. النصوص التنظيمية:

❖ **المراسيم الرئاسية:**

1- الموسوم رقم19-172 على "تمارس المديرية التقنية مهامها المرتبطة بالشرطة القضائية وفقا لأحكام التشريع المعمول به، لا سيما المر 66-155 المؤرخ في 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.
2- المرسوم الرئاسي رقم 183/04المؤرخ في 8 جمادى الأولى عام 1425 هـ الموافق 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج.ر) العدد رقم: (41) المؤرخة في: 27 جوان 2004.
3- المرسوم الرئاسي رقم: 04/183 المؤرخ في: 26 جوان 2004 يتضمن أحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج.ر) رقم: 41 المؤرخة في: 2004/06/27.
4- المرسوم الرئاسي رقم: 432/04المؤرخ في: 2004/12/29 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، (ج.ر) رقم: 84 المؤرخة في: 2004/12/29.
5- المرسوم الرئاسي رقم 183/14 المؤرخ في 11 جوان 2014، يتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الاستعلام والأمن ومهامها وتنظيمها (ج.ر) عدد: (32) المؤرخة في: 12 جوان 2014.

6- المرسوم الرئاسي رقم 172/19 المؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر العدد37 بتاريخ 09 يونيو 2019.

❖ **المراسيم التنفيذية:**

1. المرسوم التنفيذي رقم 348/06 مؤرخ في 5 أكتوبر سنة 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، (ج.ر) عدد (63).
2. المرسوم التنفيذي162/07 مؤرخ في 30ماي2007، يعدل ويتمم المرسوم التنفيذي رقم123/01المؤرخ في09 ماي 2001 والمتعلق بنظام الاستغلال المطلق على كل نوع من أنواع الشبكات بما فيها السلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، (ج.ر) عدد (37) .

❖ **القرارات الوزارية:**

1- القرار الوزاري المشترك المؤرخ في: 2007/04/14، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، (ج.ر) رقم: (36) المؤرخة في: 03 يونيو 2007.

أ. النصوص القانونية الاجنبية:

1- القانون الفرنسي رقم: 17 المؤرخ في: 6 جانفي 1978 بشأن الاطلاع على البطاقات ذات البيانات الشخصية.

2- القانون رقم 1336/92 الصادر في 16 ديسمبر 1992 بشأن إصدار قانون العقوبات الفرنسي الجديد.

3- مشروع قانون التجارة والمعاملات الإلكترونية المصري، مركز المعلومات ودعم اتخاذ القرار، رئاسة مجلس الوزراء، القاهرة 2000.

4- قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 2 لسنة 2002، حكومة دبي، الجريدة الرسمية العدد 277، فيفري 2002.

5- قانون التوقيع الإلكتروني المصري رقم 15 لعام 2004، الجريدة الرسمية العدد 17 تابع (3) الصادر في 2004/04/22.

6- القانون المصري بشأن التوقيع الإلكتروني لسنة 2004 .

7- التشريع المصري رقم: 15 لسنة 2004

8- قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 01 لسنة 2006.

9- قانون المعاملات الإلكترونية العماني رقم 2008/69، الصادر في 18/مايو/2008.

10- قانون تقنية المعلومات الإماراتي رقم 05 لسنة 2012 .

7- مواقع الأنترنت:

- باللغة الأجنبية

1- http://www.arablaw.org/donload/ec_tunisia.do
2- http://w.w.w.droitentreprise.com
3- http://www.javelinstartegy.com
4- http://www.courdecassation.fr/uriprudence2/chambre_criminelle-578/dite_societe_28730.html
5- http://ar.wikipedia.org
6- http://law.justia.com/cases/federal/districtcourts/fsupp2/120/1194/2499659/
7- http://portal.moi.gov.qa/unccpcjdoha/arabic/previous_congresses.html
8- http://ppgn.mdn.dz/prep.php
9- http://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174
10- http://www.mohamah.net/law
11- http://www.unodc.org/documents/treaties/untoc/publications/toc%20convention/tocebook
12- http://www.droit.d2.com/forum/threads
13- http://www.finances.gouv.fr
14- http://www.minichaoui.com
15- http://www.radioalgerie.dz/news/ar
16- http://www.shaimaaatalla.com/vb
17- http://www.signelec.com-le
18- https://www.arpce.dz/ar/obs/prest/?c=voip
19- الموقع الرسمي للشرطة الجزائرية بتاريخ 2019/06/02 http.//www.dgsn.dz/
20- موقع سلطة الضبط للبريد والواصلات السلكية واللاسلكية /ar/gd/cewww.arpt.dz
21- موقع شبكة قوانين الشرق eastlaws على شبكة الانترنيت: site.eastlaws.com/news
22- موقع وكالة الانباء الجزائرية على الأنترنت: www.aps.dz/ar

ثانيا: المراجع باللغة الاجنبية:

1. الكتب:

1- B.bouloc , droit penalegeneral ; 22 edition , dalloz , 2010,2011.
2- Bainbridge (david) , hacking, the access of computer systems ,the legal implications , wiley, 1989.
3- Carbonnier, droit civil, presses universitaires de france, paris, 1973, t3, les biens.
4- W. Jeandidier, Les trucage et usages frauduleux de cartes magnétiques , Cahiers de droit de l'entreprise, 1986.
5- Merle (roger) et vitu (andré), traite de droit criminel, droit pénal spécial par vitu, cujas, paris, 4éme ed, 1981.
6- Planiol (m) et ripert (g) , traité pratique de droit civil français , librairie générale de droit et de jurisprudence, paris,t3,les biens,no50.
7- Soussi roubi , carte de crédit , le guide juridique dalloz.

2. المقالات:

1- Yann padova, un aperçu de la lutte contre la cyber criminalité en France, revue de science criminelle et droit pénal compare, 3 février 2002.
2- Alain Ben soussan et Yves le roux, cryptologie et signature électronique, aspects juridiques, E, Hermes, 1999.

3. الرسائل الجامعية:

1- Sophie Bardou, Les Traitements de donnees biometriques en entreprise, thése pour le doctorat en droit,faculte de droit, universite monpellier 1, novembre, 2010.
2- Abbas YoussefJaber, Les contrats conclus par voie electronique : étude comparée, these pour le doctorat en droit privé, ecole doctorale droit er science politique, universite monpellier 1, juin, 2012.

4. الملتقيات:

1- Cristina schulman, le rôle de la collaboration entre les secteurs public et privé dans la lutte contre la cybercriminalité, conférence régionale 1 sur la cybercriminalité casablanca, royaume du maroc 19-20 juin, 2007.
2- Jean – françoishenrotte, l' importance de la collaboration internationale et l'expérience belgedans l'échange d'informations policières et de coopération judiciaireprojet sur la modemisation des ministères publics "conférence régionale sur la cybercriminalité casablanca , royaume du maroc 19-20 juin , 2007.

3- Tynerrussell, the importance of international cooperation in preventingcybercrime, conférence régional sur la cybercriminalité casablanca, royaume du maroc 19-20 juin.
4- Rapport du coseil d'etat français, intrnet et les reseaux numerique, les documentation français, 1988.

5. النصوص القانونية:

1- Code de procèdurepenal français.
2- Code penalefrançais .
3- Electronic signatures law 106(5), report to the governor and legislatureon new Yorkstate's, electronic signatures and records act.
4- La loi no2000-2230du 13 mars 2000.j.o 14 mars.
5- u.s. Codetitle18.crimes and criminalprocedure.parti.crimes.
6- United state code.sec.2511. - public law 106/229- june 30. 2000 article no 101/d.

فهرس الموضوعات

الفصل الثاني:

صور الجرائم الواقعة على التوقيع الالكتروني

الباب الثاني:

الجوانب الإجرائية للحماية الجزائية للتوقيع والتصديق الإلكترونيين

الفصل الأول:

إجراءات التحقيق في الجرائم الواقعة على التوقيع الإلكتروني

الفصل الثاني

إجراءات المحاكمة في الجرائم الواقعة على التوقيع الإلكتروني