جامعة عمار ثليجي الأغواط

كلية الحقوق و العلوم السياسية

قسم الحقوق –قانون عام-

العنوان

الجرائم المرتبطة بقانون التوقيع والتصديق الإلكتروني

مذكرة في إطار مقتضيات نيل شهادة الماستر في القانون الجنائي و العلوم الجنائية

من إعداد الطلبة :

غويني عائشة

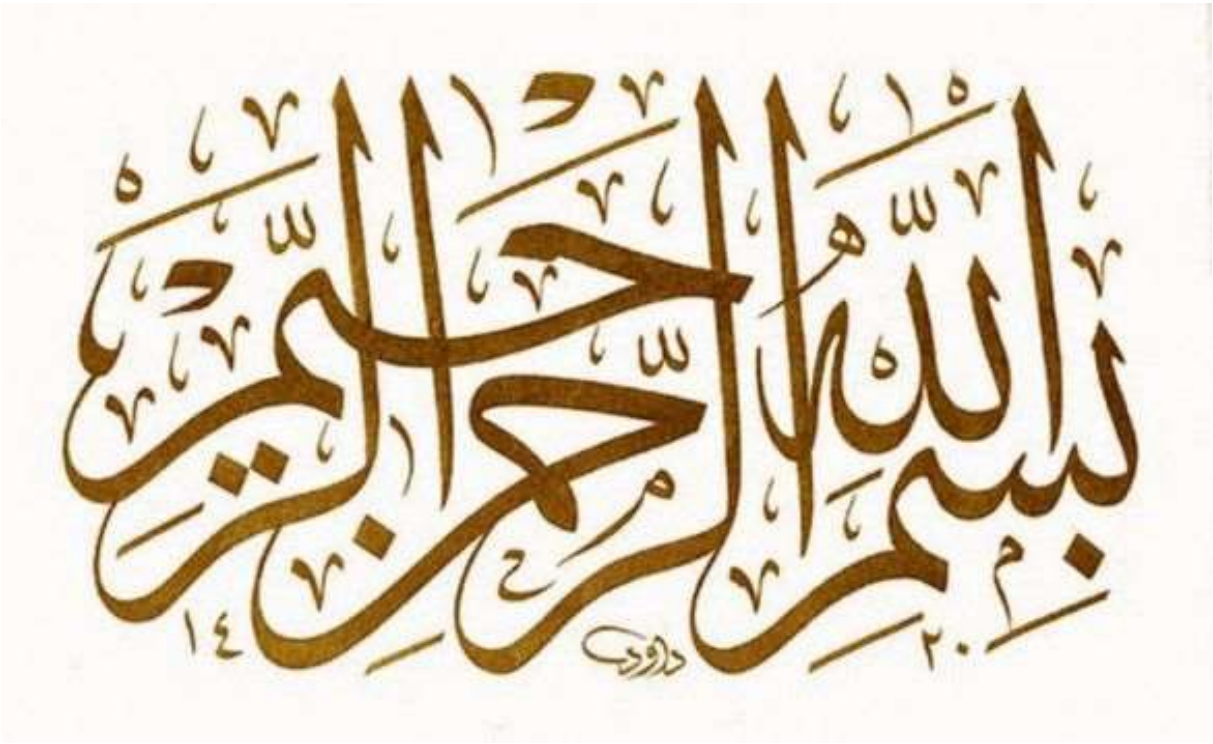
بلمشري نبيلة

الأستاذ المشرف

د. سي ناصر محمد

الأستاذ	الرتبة	الصفة
سعودي علي	دكتور	رئيسا
د. سي ناصر محمد	دكتور	مشرفا ومقررا
بن حليمة بومدين	دكتور	ممتحنا

السنة الجامعية 2026/2025


بسم الله الرحمن الرحيم

شكر وعرفان

الحمد لله و كفى و الصلاة على الحبيب المصطفى و اهله ومن

وفى أما بعد الحمد لله الذي وفقنا لتثمين هذه الخطوة في

مسيرتنا الدراسية بمذكرتنا هذه ثمرة الجهد و النجاح بفضل الله

تعالى مهداة الى ، إلى أستاذي المشرف

الدكتور سي ناصر محمد

كما نتقدم بالشكر والعرفان لجميع القائممين على قسم

الحقوق في جامعة عمار ثليجي

إهداء

بسم الله ذي الشأن العظيم السلطان الذي تقدست له الأسماء وكان لي العون والرجاء.

بسم من يطيب باسمه الاهداء وقرة عيني ونور صدري سيدنا "محمد" عليه أزكى السلام.

إهداء خاص إلى' أمي' البطلة، السند، إلى من كانت لي أما حانية وأبا حازما يحميني، ومنارة تضيء عتمة الطريق بعد أن غاب السند... إلى من عاشت لتراني أكبر، وتحملت ثقل الحياة وحدها ليبقى رأسي مرفوعا

إلى غالية الغاليات، التي لم تسمح لليتم أن يكسرنا، في غياب أبي رحمه الله فكانت الأمان في الخوف، إلى التي لو بقي لساني ينطق الدهر كله لما اوفيتها حقها حفظك الله لي يا أعظم ملكة 👸 أمي الغالية. 👸

إلى روح والدي الحبيب (رحمه الله) إلى من رحل عن دنيانا وبقي حيا في تفاصيلي، أهدي إليك هذا العمل تخليدا لذكراك العطرة أسأل لله أن يتقبله ويجعله نورا لروحك الطاهرة.

إلى من أبصرت عينيا على وجودهم إلى ترعرعت وأحببتهم بكل جوارحي إخوتي أخواتي (عيسى، عبد القادر، سعد، زكريا، صليحة، فاطمة، خولة، خديجة، هند) الذين شجعوني نحو تحقيق هدفي عن إنجاز عملي هذا، وإلى جميع الزملاء وإلى أعز وأغلا الأصدقاء وإلى كل من ساعدوني في إنجاز هذه مذكرة والي كل من نسيهم قلمي و لم ينساهم قلبي .

عائشة غويني

اهداء

وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ التوبة: 105

الحمد لله الذي بنعمته تتم الصالحات، والحمد لله الذي وفقني لإتمام هذا المشوار العلمي، فله الحمد أولًا وآخرًا، ظاهرًا وباطنًا

اهدى ثمرة جهدي وتخرجي الي أمي الحبيبة، رمز الحنان والتضحية والعطاء، التي كانت سندا لي في كل حياتي ودعواتها ترافقني في كل خطوة، وسهرت من أجل راحتي ونجاحي، فأدامها الله تاجًا فوق رأسي وحفظها الله لنا

وإلى أبي الغالي، سندي وفخري، و مصدر قوة لي فجزاه الله عني خير الجزاء وأدامه نعمة في حياتي.

وإلى أختي وأخي العزيزين وضلعي ثابت الذي لا يمل ، (فتيحة، عبد مالك) الذين شاركوني لحظات الفرح والتعب، وكانوا خير معين وسند، أقدم لكم خالص المحبة والامتنان.

وإلى أخي الغالي رحمه الله رحمة واسعة وأسكنه فسيح جناته، أهدي هذا الإنجاز إلى روحه الطاهرة، وأسأل الله أن يجعل قبره روضة من رياض الجنة، وأن يجمعني به في الفردوس الأعلى.

سيبقى ذكرك حيًا في قلبي.

والى صديقتي المقربة (نور الهدى) التي كانت بمثابة الاخت وصديقة شكرا لأنك كنتي معي في اوقات الفرح وحزن كنتِ خير رفيقة في هذه الرحلة

وفي الختام، أحمد الله تعالى على هذه النعمة العظيمة، وأسأله أن يجعل هذا النجاح بدايةً لمزيد من التوفيق والعطاء، وأن يبارك في أهلي وأحبتي، وأن يرزقني الإخلاص في العلم والعمل

نبيلة بلمشري

مقدمة

مقدمة :

شهد العالم خلال العقود الأخيرة ثورة تكنولوجية ومعلوماتية غير مسبوقة، انعكست آثارها على مختلف مجالات الحياة، لاسيما في مجال المعاملات القانونية والتجارية والإدارية التي انتقلت تدريجيًا من الشكل التقليدي إلى الشكل الإلكتروني. وقد أدى هذا التحول الرقمي إلى ظهور وسائل حديثة لإثبات التصرفات القانونية، من أبرزها التوقيع الإلكتروني والتصديق الإلكتروني اللذان أصبحا يشكلان ركيزة أساسية لضمان الثقة والأمان في البيئة الرقمية.

غير أن التطور المتسارع في استخدام الوسائط الإلكترونية لم يقتصر على الجوانب الإيجابية فحسب، بل صاحبه ظهور أنماط جديدة من الجرائم استهدفت الأنظمة المعلوماتية والمعاملات الإلكترونية، ومن بينها الجرائم المرتبطة بالتوقيع والتصديق الإلكتروني. وتتمثل هذه الجرائم في مختلف الأفعال غير المشروعة التي تستهدف التوقيعات الإلكترونية أو بيانات التصديق الإلكتروني، كالدخول غير المشروع إلى الأنظمة المعلوماتية، والاستيلاء على بيانات التوقيع الإلكتروني بطرق احتيالية، وتزوير التوقيعات الإلكترونية، وانتحال الهوية الرقمية، وغيرها من الأفعال التي من شأنها المساس بأمن المعلومات والثقة في المعاملات الإلكترونية.

ونظرًا لخطورة هذه الجرائم وما قد يترتب عنها من أضرار تمس الأفراد والمؤسسات والاقتصاد الوطني، سارعت مختلف التشريعات إلى وضع منظومة قانونية متكاملة تهدف إلى تنظيم استعمال التوقيع والتصديق الإلكترونيين، وتجريم الأفعال الماسة بهما، مع تقرير عقوبات تتناسب مع طبيعتها وخطورتها. ويأتي ذلك في إطار تعزيز الحماية القانونية للمعاملات الإلكترونية وضمان استقرارها وتشجيع الأفراد والمؤسسات على استخدامها بثقة وأمان.

وانطلاقًا مما سبق، يثير هذا الموضوع إشكالية رئيسية مفادها:

فيما تتمثل أهم الجرائم الواقعة على التوقيع والتصديق الإلكتروني من خلال القانون رقم 15/04؟

ويكتسي موضوع الجرائم المرتبطة بقانون التوقيع والتصديق الإلكتروني أهمية بالغة باعتباره من المواضيع الحديثة التي فرضها التطور التكنولوجي، حيث أصبح التوقيع الإلكتروني أداة

أساسية في إبرام العقود وإثبات التصرفات القانونية إلكترونيًا، الأمر الذي يستوجب توفير حماية جنائية فعالة ضد مختلف الاعتداءات التي قد تستهدفه.

وتتجلى أهمية دراسة هذا الموضوع في عدة اعتبارات، من بينها:

- إبراز الطبيعة القانونية للجرائم المرتبطة بالتوقيع والتصديق الإلكتروني وبيان خصائصها.
- التعرف على أهم صور الاعتداءات الواقعة على أنظمة التوقيع والتصديق الإلكتروني.
- دراسة الأركان القانونية للجرائم المرتبطة بالتوقيع الإلكتروني.
- الوقوف على العقوبات المقررة لهذه الجرائم ومدى فعاليتها في تحقيق الردع والحماية الجنائية.
- إبراز دور التشريعات الحديثة في توفير الأمن القانوني للمعاملات الإلكترونية.

وقد جاء اختيارنا لهذا الموضوع لعدة أسباب موضوعية وذاتية، من أهمها:

- حداثة الموضوع وأهميته المتزايدة في ظل الانتشار الواسع للتعاملات الإلكترونية.
- تزايد الجرائم المعلوماتية المرتبطة بالتوقيع والتصديق الإلكتروني وما تثيره من إشكالات قانونية.
- الرغبة في التعرف على آليات الحماية الجنائية المقررة للتوقيع الإلكتروني.
- المساهمة في إثراء الدراسات القانونية المتعلقة بالمعاملات الإلكترونية والجرائم المعلوماتية.

وقد واجهتنا أثناء إعداد هذا الموضوع بعض الصعوبات، من أبرزها:

- حداثة الموضوع وقلة الدراسات المتخصصة فيه مقارنة بالموضوعات القانونية التقليدية.
- تشتت النصوص القانونية المنظمة للجرائم المعلوماتية والتوقيع الإلكتروني.
- محدودية الاجتهادات القضائية المنشورة المتعلقة بالجرائم الواقعة على التوقيع والتصديق الإلكتروني.

وللإجابة عن الإشكالية تم الاعتماد على:

- المنهج الوصفي، من خلال التعريف بالتوقيع والتصديق الإلكتروني وبيان الجرائم المرتبطة بهما.
- المنهج التحليلي، من خلال تحليل النصوص القانونية المنظمة لهذه الجرائم والعقوبات المقررة لها.
- المنهج المقارن، عند الاقتضاء، من خلال الاستعانة ببعض التشريعات المقارنة لإبراز أوجه الاتفاق والاختلاف في مجال الحماية الجنائية للتوقيع الإلكتروني.

وللإجابة عن الإشكالية المطروحة والإحاطة بمختلف جوانب الموضوع، تم تقسيم الدراسة إلى فصلين رئيسيين:

الفصل الأول: الجرائم المرتبطة بالتوقيع الإلكتروني، وتم تخصيصه لدراسة الجرائم الواقعة على التوقيع الإلكتروني والعقوبات المقررة لها، حيث تم تقسيمه إلى مبحثين؛ تناولنا في المبحث الأول الجرائم الواقعة على التوقيع الإلكتروني، من خلال التطرق إلى جريمة الدخول غير المشروع إلى أنظمة أو قواعد بيانات التوقيع الإلكتروني، وجريمة الحصول على التوقيع الإلكتروني بطرق احتيالية، وجريمة التزوير المعلوماتي في التوقيع الإلكتروني وأركانها. أما المبحث الثاني فخصص لدراسة العقوبات المقررة لجرائم التوقيع الإلكتروني، من خلال بيان العقوبات الأصلية والعقوبات التكميلية.

أما الفصل الثاني: الجرائم المرتبطة بالتصديق الإلكتروني، فقد تم تخصيصه لدراسة الجرائم الواقعة على التصديق الإلكتروني والعقوبات المقررة لها، حيث تناولنا في المبحث الأول الجرائم الواقعة على التصديق الإلكتروني، من خلال دراسة جريمة إصدار شهادة تصديق إلكتروني دون ترخيص، وجريمة إنشاء أو نشر شهادة تصديق إلكتروني لغرض احتيالي. أما المبحث الثاني فقد خصص لدراسة العقوبات المقررة لجرائم التصديق الإلكتروني، من خلال

بيان العقوبات الأصلية المنصوص عليها في القانون رقم 15-04، والعقوبات التكميلية والتدابير الوقائية المقررة لمواجهة هذه الجرائم.

.

الفصل الأول:
الجرائم المرتبطة بقانون التوقيع

. تمهيد :

شهد العالم خلال العقود الأخيرة تطورًا هائلًا في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى انتقال العديد من المعاملات والتصرفات القانونية من البيئة التقليدية إلى البيئة الإلكترونية. وقد أصبح التوقيع الإلكتروني من أهم الوسائل المعتمدة لإثبات الهوية والتعبير عن الإرادة في المعاملات الرقمية، لما يوفره من سرعة وفعالية وأمان في إنجاز مختلف العمليات التجارية والإدارية والمالية.

غير أن الانتشار الواسع لاستخدام التوقيع الإلكتروني صاحبه ظهور العديد من المخاطر والاعتداءات الإلكترونية التي تستهدف سلامته ومصداقيته، وذلك من خلال اختراق الأنظمة المعلوماتية، والاستيلاء على بيانات التوقيع الإلكتروني، أو تزويرها واستعمالها بطرق احتيالية. وقد شكلت هذه الأفعال تهديدًا حقيقيًا لأمن المعاملات الإلكترونية وللثقة التي تقوم عليها البيئة الرقمية، مما استوجب تدخل المشرعين لوضع قواعد قانونية وتجريم مختلف الأفعال الماسة بالتوقيع الإلكتروني، مع تقرير عقوبات تتناسب مع خطورتها.

وانطلاقًا من ذلك، سيتم في هذا الفصل دراسة الجرائم الواقعة على التوقيع الإلكتروني من خلال بيان أهم صورها وأركانها القانونية، ثم التطرق إلى العقوبات المقررة لها، قصد إبراز مدى فعالية الحماية الجنائية التي أقرها المشرع لمواجهة الاعتداءات التي تمس التوقيع الإلكتروني وتعزيز الثقة في المعاملات الإلكترونية.

المبحث الاول: الجرائم الواقعة علي التوقيع الإلكتروني

سنتناول في هذا المبحث جريمة الدخول غير المشروع إلى الأنظمة أو قواعد البيانات المتعلقة بالتوقيع الإلكتروني في المطلب الأول، ثم نتطرق إلى جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية في المطلب الثاني.

المطلب الأول: جريمة الدخول غير مشروع الي انظمة او قواعد بايانات توقيع الإلكتروني

يمكن تعريف هذه الجريمة بأنها كل فعل أو نشاط يقوم به الجاني في نظام الحاسوب من شأنه الدخول أو الإزالة أو التعديل في المعطيات المتعلقة بنظام الحاسوب[1]، هذا من جهة، ومن جهة أخرى يطلق على هذه الجريمة بالقرصنة المعلوماتية لأن هدف الجاني فيها هو تحقيق النظام المعلوماتي لنتائج ومعطيات غير تلك التي كان يجب أن يحققها.[2]

وقد عرف المشرع الجزائري جريمة الاعتداء على سلامة المعطيات من خلال نص المادة 394 مكرر 1 من قانون العقوبات: "كل من أدخل بطريق الغش المعطيات في نظام المعالجة الآلية أو أزال أو عدل عن طريق الغش المعطيات التي يتضمنها[3]."

كما أن الاعتداء على قواعد بيانات التوقيع الإلكتروني قد يؤدي إلى انتحال الهوية الرقمية للأشخاص، أو تزوير التوقيعات الإلكترونية، أو استعمالها في إبرام تصرفات قانونية غير مشروعة، وهو ما يترتب عليه أضرار جسيمة تمس الأفراد والمؤسسات على حد سواء. فالتوقيع الإلكتروني يعد وسيلة حديثة لإثبات الهوية والتعبير عن الإرادة في البيئة الرقمية، وبالتالي فإن أي مساس بسلامته أو بسلامة المعطيات المرتبطة به يشكل تهديداً مباشراً لأمن المعاملات الإلكترونية.

---

[1] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، طبعة 02، سنة 2010، ص.119

[2] دردور نسيم، الج ارئم المعلوماتية على ضوء القانون الج ازئري والمقارن، مذكرة ماجستير، قانون جنائي، جامعة منتوري 2 قسنطينة، 2012، ص .25

[3] قانون العقوبات الصادر بموجب الأمر رقم 66 – 156، المؤرخ في 18 صفر عام 1386، الموافق لـ 08 يونيو 1966، الذي يتضمن قانون العقوبات، الجريدة الرسمية، العدد 49، 1966، المعدل والمتمم بالقانون 06-24، المؤرخ في 2024/04/28، الجريدة الرسمية العدد 30، سنة 2024، ص .22

كما أن حماية المعطيات أصبحت ضرورة ملحة في العصر الرقمي، خاصة مع اعتماد الإدارات والمؤسسات الاقتصادية والبنكية على نظم المعالجة الآلية للبيانات والتوقيع الإلكتروني في تسيير مختلف نشاطاتها. لذلك حرص المشرع الجزائري، على غرار مختلف التشريعات المقارنة، على تجريم كل أشكال الاعتداء على المعطيات الإلكترونية وأنظمة التوقيع الإلكتروني، سواء تعلق الأمر بإدخال بيانات مزيفة، أو حذف بيانات صحيحة، أو تعديلها بطريقة غير مشروعة، أو الدخول غير المصرح به إلى قواعد البيانات الإلكترونية، وذلك بهدف ضمان سلامة وأمن الأنظمة المعلوماتية، وتعزيز الثقة في البيئة الرقمية، وحماية الحقوق والمصالح المرتبطة بالتعامل الإلكتروني.

وتظهر خطورة الاعتداء على سلامة المعطيات في كون الجاني يستطيع تغيير الحقيقة الإلكترونية دون ترك آثار مادية ظاهرة، الأمر الذي يجعل اكتشاف الجريمة وإثباتها أكثر تعقيداً مقارنة بالجرائم التقليدية. فالمجرم المعلوماتي يعتمد غالباً على مهارات تقنية متقدمة تمكّنه من اختراق الأنظمة أو التعديل في البيانات أو حذفها بطرق احتيالية، وهو ما يهدد الثقة في التعاملات الإلكترونية والأنظمة الرقمية.[1]

الفرع الأول : خصائص جريمة الدخول غير المشروع إلى أنظمة أو قواعد بيانات التوقيع الإلكتروني تُعد جريمة الدخول غير المشروع إلى أنظمة أو قواعد بيانات التوقيع الإلكتروني من الجرائم المعلوماتية المستحدثة التي ظهرت نتيجة التطور التكنولوجي والاعتماد المتزايد على الأنظمة الرقمية في مختلف المعاملات الإدارية والمالية والتجارية. وتمتاز هذه الجريمة بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، وتبرز خطورتها على أمن المعلومات والثقة في البيئة الإلكترونية[2].

1- جريمة ذات طبيعة تقنية ومعلوماتية

تتميز هذه الجريمة بأنها تعتمد أساساً على الوسائل الإلكترونية والتقنيات الحديثة، حيث يتم ارتكابها عن طريق الحاسوب أو شبكة الإنترنت أو أي وسيلة رقمية أخرى. فالجاني لا

[1] خثير مسعود، مرجع سابق، ص .120

[2] محمد صبحي نجم، *جرائم الكمبيوتر والإنترنت*، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص. 188-190.

يحتاج إلى استخدام القوة المادية أو الوسائل التقليدية، بل يعتمد على مهارات تقنية وبرمجيات متطورة تمكّنه من اختراق الأنظمة المعلوماتية أو تجاوز وسائل الحماية الأمنية للوصول إلى قواعد بيانات التوقيع الإلكتروني.

كما أن ارتكاب هذه الجريمة يتطلب في الغالب معرفة تقنية بمجال البرمجة والشبكات وأنظمة الحماية الإلكترونية، وهو ما يجعلها جريمة ترتبط بالتطور العلمي والتكنولوجي المستمر.

-2جريمة تمس بسرية وسلامة المعطيات الإلكترونية : إن الهدف الأساسي من أنظمة التوقيع الإلكتروني هو ضمان الثقة والأمان في المعاملات الإلكترونية، لذلك فإن أي دخول غير مشروع إلى هذه الأنظمة يشكل اعتداءً مباشراً على سرية البيانات وسلامتها. فقد يقوم الجاني بالاطلاع على معلومات سرية، أو تعديلها، أو حذفها، أو استغلالها لأغراض غير مشروعة[1].

وتكمن خطورة ذلك في أن التوقيع الإلكتروني يرتبط بالهوية الرقمية للأشخاص والمؤسسات، وبالتالي فإن المساس به قد يؤدي إلى تزوير الوثائق الإلكترونية أو انتحال الشخصية أو إبرام معاملات غير قانونية باسم الغير.

-3جريمة خفية وصعبة الاكتشاف : من أهم خصائص هذه الجريمة أنها ترتكب في بيئة افتراضية غير ملموسة، وغالباً لا تترك آثاراً مادية واضحة مثل الجرائم التقليدية. فالجاني يستطيع التسلل إلى النظام والدخول إلى قواعد البيانات دون أن يثير الانتباه، وقد يستخدم وسائل لإخفاء هويته أو حذف الآثار الرقمية التي تدل على نشاطه الإجرامي.

كما أن اكتشاف الجريمة يحتاج إلى خبرة تقنية متخصصة في مجال الأدلة الرقمية والتحقيق المعلوماتي، وهو ما يزيد من صعوبة إثباتها أمام الجهات القضائية.

4- جريمة سريعة التنفيذ : تتميز هذه الجريمة بسرعة ارتكابها، إذ يمكن للمجرم الإلكتروني خلال دقائق معدودة اختراق النظام المعلوماتي والوصول إلى البيانات أو نسخها أو التعديل

[1] خثير مسعود، مرجع سابق، ص .121

فيها. وقد يتم تنفيذ الجريمة عن بعد دون الحاجة إلى التواجد في مكان وجود النظام المستهدف.

وتزداد خطورة هذه السرعة مع التطور الكبير في وسائل الاتصال الحديثة، حيث أصبح بالإمكان تنفيذ الهجمات الإلكترونية في وقت قصير جداً وبأقل جهد ممكن[1].

الفرع الثاني : أركان جريمة الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات:

أولا : الركن المادي يُعد الركن المادي العنصر الأساسي الذي تقوم عليه جريمة الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات،[2] إذ يتمثل في النشاط الإجرامي الذي يأتيه الجاني بالمخالفة للقانون، ويهدف من خلاله إلى الولوج إلى النظام المعلوماتي أو البقاء فيه دون وجه حق أو دون ترخيص من الجهة المالكة أو المشرفة على النظام.

ويتكون الركن المادي لهذه الجريمة من سلوك إجرامي يتمثل أساساً في فعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات أو إلى جزء منه، سواء تعلق الأمر بحاسوب منفرد، أو شبكة معلوماتية، أو قاعدة بيانات، أو نظام خاص بالتوقيع الإلكتروني والمعاملات الرقمية. كما قد يتحقق الركن المادي كذلك من خلال البقاء داخل النظام بعد الدخول إليه بطريقة مشروعة ثم الاستمرار في استعماله دون إذن أو بعد انتهاء الصلاحية الممنوحة للمستخدم.

ويقصد بالدخول غير المشروع كل ولوج أو اتصال يتم إلى النظام المعلوماتي دون ترخيص مسبق من صاحبه أو المسؤول عنه، أو بالمخالفة للشروط والقيود المحددة للاستعمال. ويستوي في ذلك أن يكون الدخول عن طريق اختراق وسائل الحماية التقنية، أو باستعمال كلمات مرور مسروقة، أو عبر وسائل احتيالية وتقنيات إلكترونية مختلفة تمكن الجاني من تجاوز الحواجز الأمنية المفروضة على النظام.

---

[1] خثير مسعود، مرجع سابق، ص .121

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

ولا يشترط لتحقق الجريمة أن يؤدي الدخول غير المشروع إلى إتلاف البيانات أو سرقتها أو تعديلها، بل يكفي مجرد الدخول أو البقاء غير المصرح به داخل النظام المعلوماتي لقيام الركن المادي، لأن المشرع يهدف أساساً إلى حماية حرمة الأنظمة المعلوماتية وضمان أمنها وسلامتها من أي اعتداء خارجي.

كما قد يتحقق الركن المادي للجريمة في عدة صور، من بينها:

- الدخول إلى الحاسوب أو الشبكة المعلوماتية دون إذن .
- الولوج إلى قواعد بيانات التوقيع الإلكتروني والاطلاع على محتوياتها .
- تجاوز الصلاحيات الممنوحة للمستخدم الشرعي .
- البقاء داخل النظام بعد انتهاء الترخيص أو بعد سحبه .
- استعمال برامج الاختراق أو وسائل تقنية لفك كلمات المرور أو تجاوز أنظمة الحماية.

ثانيا : الركن المعنوي لجريمة الدخول غير المصرح به إلى نظم معلومات التوقيع الإلكتروني تُعد جريمة الدخول غير المصرح به إلى نظم معلومات التوقيع الإلكتروني من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام،[1] والذي يقوم على عنصرين أساسيين هما العلم والإرادة. ويقصد بذلك أن يكون الجاني عالماً بأنه يقوم بالدخول إلى نظام معلوماتي محمي دون ترخيص أو إذن قانوني، وأن تتجه إرادته الحرة إلى ارتكاب هذا الفعل مع علمه بعدم مشروعيته.

ويتمثل عنصر العلم في إدراك الجاني لطبيعة النظام المعلوماتي الذي يقوم باختراقه أو الدخول إليه، ومعرفته المسبقة بأنه غير مخول قانوناً للولوج إلى هذا النظام أو البقاء فيه. كما يشمل العلم إدراك الجاني بأن النظام المستهدف يتعلق بمعطيات أو بيانات إلكترونية محمية، خاصة إذا تعلق الأمر بأنظمة التوقيع الإلكتروني التي تتضمن معلومات ذات طابع سري أو مهني أو مالي.

[1] صالح شنين، المرجع السابق، ص 165.

أما عنصر الإرادة فيتحقق من خلال اتجاه إرادة الجاني إلى تنفيذ فعل الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، أي أن يكون قد أقدم على الفعل بمحض إرادته دون إكراه أو خطأ غير مقصود. فالمجرم المعلوماتي غالباً ما يستعمل وسائل تقنية وبرامج خاصة تساعده على تجاوز أنظمة الحماية والدخول إلى قواعد البيانات الإلكترونية، وهو ما يدل على توافر النية الإجرامية لديه[1].

ولا يشترط في هذه الجريمة توافر قصد جنائي خاص، كنية الإضرار بالنظام أو سرقة البيانات أو تحقيق منفعة مادية، وذلك لأنها من جرائم الخطر التي يكتفي فيها المشرع بمجرد تحقق السلوك الإجرامي المتمثل في الدخول غير المشروع. فالمشرع يعاقب على مجرد تعريض النظام المعلوماتي للخطر، حتى ولو لم يترتب عن ذلك أي ضرر فعلي أو نتيجة مادية ملموسة.

وعليه، فإن جريمة الدخول غير المشروع إلى نظم معلومات التوقيع الإلكتروني تقوم بمجرد تحقق الفعل المادي المقترن بالقصد الجنائي العام، دون اشتراط تحقق نتيجة معينة، كإتلاف البيانات أو تعديلها أو استعمالها. ويعود ذلك إلى رغبة المشرع في توفير حماية استباقية للأنظمة المعلوماتية والمعطيات الإلكترونية، نظراً لما تتميز به من حساسية وأهمية في العصر الرقمي.

كما تظهر خطورة الركن المعنوي في هذه الجريمة من خلال اعتماد الجاني على التخطيط والإعداد المسبق، حيث يقوم في كثير من الأحيان بدراسة النظام المستهدف ومحاولة اكتشاف الثغرات الأمنية الموجودة فيه قبل تنفيذ عملية الاختراق. وقد يستخدم أسماء وهمية أو وسائل تقنية لإخفاء هويته الحقيقية، الأمر الذي يعكس توافر النية الإجرامية بشكل واضح.

وتزداد أهمية القصد الجنائي عندما يكون محل الاعتداء هو نظم التوقيع الإلكتروني، لأن هذه الأنظمة ترتبط بإثبات الهوية الرقمية للأشخاص والمؤسسات، وتستخدم في توثيق العقود

[1] صالح شنين، المرجع السابق، ص 13.

والمعاملات الإلكترونية. وبالتالي فإن أي دخول غير مشروع إليها قد يؤدي إلى المساس بمصداقية التوقيع الإلكتروني وتهديد الثقة في المعاملات الرقمية[1].

كما أن إثبات الركن المعنوي في الجرائم المعلوماتية يعد من المسائل المعقدة، نظراً للطابع التقني لهذه الجرائم وصعوبة الكشف عن نية الجاني. لذلك تعتمد جهات التحقيق غالباً على القرائن والأدلة الرقمية، مثل طريقة الدخول إلى النظام، واستعمال برامج الاختراق، ومحاولات إخفاء الهوية أو حذف الآثار الإلكترونية، لاستخلاص توافر القصد الجنائي لدى الفاعل.

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

أما القانون الأمريكي فقد تطلب فقط أن يكون الدخول دون تصريح، وتطلب القانون الإنجليزي أن يكون الدخول للنظام على نحو غير مصرح به مع العلم بذاك. في حين لم يتطلب المشرع المصري في القانون رقم 15 لسنة 2004 قصدا في جريمة الدخول غير المشروع داخل النظام المعلوماتي للتوقيع الإلكتروني، ومن ثم فإن القواعد العامة بشأن القصد الجنائي تسرب على هذه الجريمة[2].

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

---

[1] حسن بن سعد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدارسات والبحوث، سلطنة عمان، 2006، ص18

[2] عبد الفتاح بيومي حجازي، *النظام القانوني لحماية الحكومة الإلكترونية والتوقيع الإلكتروني في المعاملات الإلكترونية*، دار الفكر الجامعي، الإسكندرية، 2007، ص. 356.

المطلب الثاني: الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية بعد الوقوف على جريمة الدخول غير المشروع إلى قواعد البيانات المتعلقة بالتوقيع الإلكتروني، تظهر جريمة أخرى لا تقل خطورة عن سابقتها، تتمثل في الحصول على التوقيع الإلكتروني بطرق ووسائل احتيالية. وتعد هذه الجريمة من أبرز الجرائم المعلوماتية التي تستهدف أمن المعاملات الإلكترونية والثقة الرقمية، لما لها من آثار سلبية خطيرة على الأفراد والمؤسسات والاقتصاد بصفة عامة.

ويُقصد بالحصول على التوقيع الإلكتروني بالوسائل الاحتيالية قيام الجاني باستعمال أساليب غير مشروعة أو تقنيات احتيالية بهدف الاستيلاء على بيانات التوقيع الإلكتروني الخاصة بالغير أو استعمالها دون إذن صاحبها الشرعي. وقد يتم ذلك من خلال اختراق الأنظمة المعلوماتية، أو انتحال الهوية الرقمية، أو استعمال برامج خبيثة، أو الاعتماد على وسائل الخداع الإلكتروني للإيقاع بالضحية والحصول على معلوماته السرية[1].

ويعد الاحتيال في مجال نظم معلومات التوقيع الإلكتروني من أخطر الجرائم التي يمكن أن تقع على هذا النوع من التوقيعات، نظراً للتطور المذهل في مجال المعاملات الإلكترونية واعتماد المؤسسات والأفراد على التوقيع الإلكتروني في توثيق العقود والتصرفات القانونية والتجارية والمالية. كما أن تخزين بيانات التوقيع الإلكتروني داخل حواسيب آلية مرتبطة بشبكة الإنترنت جعلها عرضة لمحاولات الاختراق والسرقة والاستغلال غير المشروع.

وتكمن خطورة هذه الجريمة في أن الجاني يستطيع استعمال التوقيع الإلكتروني المستولى عليه في إبرام معاملات مزورة أو تحويل أموال أو إصدار أوامر إلكترونية باسم الضحية، مما يؤدي إلى خسائر اقتصادية ومالية كبيرة، إضافة إلى الإضرار بسمعة الأشخاص أو المؤسسات المستهدفة. كما أن هذا النوع من الجرائم يهدد الثقة في البيئة الرقمية ويؤثر سلباً على انتشار التجارة الإلكترونية والخدمات الإلكترونية الحديثة.

[1] حسن بن سعد بن سيف الغافري مرجع سابق ص19

الفرع الأول : الإحتيال الإلكتروني نصت المادة 372 من قانون العقوبات الجنائية المتعلقة بالنصب والاحتيال التقليدي عندما يتم استعمال الوسائل الإلكترونية لخداع الضحية والاستيلاء على أموالها أو بياناتها، كما نصت المذكرة التفسيرية للاتفاقية الأوروبية لمكافحة جرائم المعلومات الموقعة في بودابست عام 2001 في المادة (8) (ف ب) على أن: «على أن التلاعب في المكونات المادية للحاسب والتلاعبات المعلوماتية الاحتيالية تكون مجرّمة إذا سببت ضرراً اقتصادياً أو مادياً للغير، أو أن يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، ومصطلح الضرر يشمل النقود والأشياء غير المادية[1].

وعرف مكتب التحقيقات الفيدرالي الأمريكي الاحتيال عبر الإنترنت بأنه: «أي مخطط احتيالي عبر الإنترنت يلعب دوراً هاماً في عرض السلع أو الخدمات غير الموجودة أصلاً أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة العنكبوتية». أما وزارة العدل الأمريكية فعرفته بأنه: «شكل من أشكال التخطيط الاحتيالي الذي يستخدم خدمات ومحتويات الإنترنت مثل الدردشة والبريد الإلكتروني والمواقع الإلكترونية من أجل خداع الضحايا وتحقيق مكاسب غير مشروعة.»

ويُعد الاحتيال الإلكتروني من أخطر الجرائم المعلوماتية الحديثة وأكثرها انتشاراً في العصر الرقمي، وذلك بسبب التطور الكبير الذي شهدته وسائل الاتصال والتكنولوجيا الحديثة، واعتماد الأفراد والمؤسسات على الإنترنت في مختلف المعاملات اليومية، سواء التجارية أو البنكية أو الإدارية. وقد ساهم هذا التطور في ظهور أنماط جديدة من الجرائم التي تعتمد على استغلال الوسائل الإلكترونية للإيقاع بالضحايا وتحقيق منافع غير قانونية.

ثانيا : الركن المادي يتمثل الركن المادي لجريمة الاحتيال الإلكتروني في التلاعب في معلومات وبيانات لها قيمة مالية بطرق احتيالية، قد لا تكون محصورة تماشيا مع طبيعة

[1] حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، ، 2013 ، ص.13

الاحتيال المعلوماتي، فالجريمة المعلوماتية بصفة عامة جريمة متطورة ومتجددة لارتباطها بتكنولوجيا المعلومات[1].

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

الفرع الثاني : تسليم معلومات التوقيع الإلكتروني تتمثل النتيجة الجرمية في جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية في تمكن الجاني من الحصول على معلومات أو بيانات التوقيع الإلكتروني الخاصة بالمجني عليه نتيجة استعمال وسائل التدليس والخداع. وتكتسي هذه النتيجة أهمية خاصة في البيئة الرقمية، لأن التوقيع الإلكتروني يرتبط بهوية صاحبه ويمنحه القدرة على إبرام التصرفات القانونية وإثباتها إلكترونيًا، مما يجعل الاستيلاء على بياناته وسيلة خطيرة للمساس بحقوق الأفراد والمؤسسات.

وفي مجال المعلومات الإلكترونية، يثور التساؤل حول مفهوم التسليم باعتباره أحد العناصر الأساسية في جرائم الاحتيال، ذلك أن البيانات والمعلومات لا تنتقل بالطريقة التقليدية التي تنتقل بها الأشياء المادية. فالحاسب الآلي أو الأنظمة المعلوماتية لا تقوم بعملية التسليم بالمفهوم المادي المعروف، وإنما يتم نقل البيانات أو تمكين الجاني من الوصول إليها إلكترونيًا عبر وسائل تقنية متعددة. لذلك لم يعد مفهوم التسليم مقتصرًا على المناولة المادية للشيء محل الجريمة، بل أصبح يشمل كل تصرف إرادي يؤدي إلى تمكين الجاني من السيطرة على المعلومات أو البيانات محل الحماية القانونية.

ومن ثم فإن جوهر التسليم في الجرائم المعلوماتية لا يتمثل في الانتقال المادي للمعلومة، وإنما في الإرادة المعيبة للمجني عليه التي تدفعه إلى الكشف عن بياناته أو تمكين الجاني من الوصول إليها نتيجة تعرضه للخداع أو التدليس. فقد يقوم الضحية، بناءً على رسائل

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

إلكترونية مزورة أو مواقع إلكترونية وهمية أو اتصالات احتيالية، بإدخال بيانات التوقيع الإلكتروني الخاصة به أو مفاتيح التشفير السرية أو كلمات المرور في نظام يسيطر عليه الجاني، معتقدًا أنه يتعامل مع جهة مشروعة. وفي هذه الحالة يتحقق التسليم رغم عدم وجود أي انتقال مادي ملموس للبيانات[1].

1- **القصد الجنائي العام** يُعد القصد الجنائي العام الركن المعنوي الأساسي في جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، ويقوم على توافر عنصري العلم والإرادة. فلا يكفي لقيام المسؤولية الجزائية مجرد ارتكاب السلوك المادي المتمثل في الاستيلاء على بيانات أو وسائل إنشاء التوقيع الإلكتروني، بل يجب أن يكون الجاني مدركًا لطبيعة فعله ومريدًا لارتكابه عن وعي واختيار.

ويقصد بعنصر العلم أن يكون الجاني على دراية بأن بيانات التوقيع الإلكتروني أو مفاتيح التشفير أو وسائل إنشاء التوقيع التي يسعى إلى الحصول عليها ليست مملوكة له، وإنما تعود إلى شخص آخر يتمتع بحق مشروع في حيازتها واستعمالها. كما يجب أن يعلم أن الوسائل التي يستعملها للحصول على تلك البيانات هي وسائل غير مشروعة ومخالفة للقانون، وأن من شأنها المساس بحقوق الغير أو تهديد أمن المعاملات الإلكترونية. ويتحقق هذا العلم سواء تعلق الأمر بالحصول على التوقيع الإلكتروني مباشرة أو بالحصول على البيانات السرية المرتبطة به والتي تمكن من استعماله أو انتحال شخصية صاحبه.

أما عنصر الإرادة فيتمثل في اتجاه إرادة الجاني الحرة إلى ارتكاب الفعل الإجرامي وتحقيق النتيجة المترتبة عليه، وذلك من خلال استخدام وسائل الخداع أو التدليس أو التحايل الإلكتروني بقصد الحصول على بيانات التوقيع الإلكتروني أو السيطرة عليها. ويقتضي ذلك أن يكون الجاني قد أقدم على فعله بإرادة واعية ومدركة، لا نتيجة خطأ أو إهمال أو جهل بحقيقة الوقائع.

[1] حسام محمد نبيل الشنراقي، المرجع السابق، ص 185

المبحث الثاني: العقوبات المقررة لجرائم التوقيع الإلكتروني

إن الاعتداء على التوقيع الإلكتروني لا يمس شخصًا معينًا فحسب، بل يهدد الثقة العامة في المعاملات الإلكترونية ويزعزع استقرار التجارة الإلكترونية والخدمات الرقمية. لذلك اتجهت التشريعات الحديثة إلى إقرار نظام عقابي متكامل يجمع بين العقوبات الأصلية والعقوبات التكميلية من أجل تحقيق الردع العام والخاص وضمان أمن البيئة الرقمية. وقد تفاوتت هذه التشريعات في تقدير العقوبات المقررة تبعًا لخطورة الأفعال المرتكبة والنتائج المترتبة عنها، إلا أنها اتفقت جميعًا على ضرورة توفير حماية جنائية فعالة للتوقيع الإلكتروني.

وعليه، سنتناول في هذا المبحث العقوبات المقررة لجرائم التوقيع الإلكتروني، وذلك من خلال دراسة العقوبات الأصلية المقررة لجرائم التوقيع الإلكتروني في المطلب الأول، ثم التطرق إلى العقوبات التكميلية المقررة لجرائم التوقيع الإلكتروني في المطلب الثاني.

المطلب الأول: العقوبات الأصلية المقررة لجرائم التوقيع الإلكتروني تتمثل العقوبات الأصلية في الجزاءات الأساسية التي يقررها المشرع لمواجهة الجرائم الواقعة على التوقيع الإلكتروني، وتشمل أساسًا العقوبات السالبة للحرية والعقوبات المالية[1].

الفرع الأول: العقوبات السالبة للحرية تعد العقوبات السالبة للحرية من أهم الوسائل التي يعتمد عليها المشرع في مكافحة الجرائم المعلوماتية بصفة عامة والجرائم الواقعة على التوقيع الإلكتروني بصفة خاصة، وذلك لما لها من أثر ردعي يحد من ارتكاب هذه الجرائم.

وقد أخذ المشرع المصري بهذا الاتجاه من خلال قانون التوقيع الإلكتروني رقم 15 لسنة 2004، حيث عاقب كل من حصل بغير حق على توقيع إلكتروني أو وسيط إلكتروني أو محرر إلكتروني بعقوبة الحبس، وهو ما يعكس إدراك المشرع لخطورة هذه الأفعال التي تمس سلامة المعاملات الإلكترونية.

[1] حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدارسات والبحوث، سلطنة عمان، 2006، ص18

كما اتجه المشرع السعودي إلى تشديد العقوبة، فنص في نظام التعاملات الإلكترونية لسنة 1428هـ على إمكانية الحكم بالسجن لمدة تصل إلى خمس سنوات لكل من يرتكب إحدى الجرائم المتعلقة بالتوقيع الإلكتروني. ويظهر من خلال هذا النص أن المشرع السعودي يولي أهمية كبيرة لحماية الثقة في التعاملات الإلكترونية باعتبارها ركيزة أساسية للاقتصاد الرقمي.

أما في التشريع الفرنسي، فقد جرم الدخول أو البقاء غير المشروع داخل أنظمة المعالجة الآلية للبيانات المرتبطة بالتوقيع الإلكتروني، ورتب على ذلك عقوبات سالبة للحرية تتدرج حسب جسامة الفعل والنتائج المترتبة عنه. فإذا اقتصر الفعل على مجرد الدخول غير المشروع قامت الجريمة البسيطة، أما إذا نتج عنه تعديل أو حذف أو إتلاف للبيانات فإن العقوبة تصبح أكثر تشددًا.

ويلاحظ أن أغلب التشريعات المقارنة تعتمد مبدأ التدرج في العقوبة، بحيث تتناسب مدة الحبس أو السجن مع حجم الضرر الناتج عن الجريمة ومدى تأثيرها على أمن المعلومات والمعاملات الإلكترونية[1].

الفرع الثاني: العقوبات المالية (الغرامة) تعتبر الغرامة من أكثر العقوبات استخدامًا في مجال الجرائم الإلكترونية، ويرجع ذلك إلى الطبيعة الاقتصادية لهذه الجرائم وما تحققه من مكاسب غير مشروعة للجاني.

وقد نص المشرع المصري على غرامة تتراوح بين عشرة آلاف ومائة ألف جنيه مصري بالنسبة لجريمة الحصول غير المشروع على التوقيع الإلكتروني. وتهدف هذه الغرامة إلى حرمان الجاني من الفائدة الاقتصادية المتحصلة من الجريمة وتحقيق الردع المالي.

أما النظام السعودي فقد جاء أكثر صرامة، إذ أجاز الحكم بغرامة تصل إلى خمسة ملايين ريال سعودي، وهو مبلغ يعكس حجم الخطر الذي يمكن أن تشكله جرائم التوقيع الإلكتروني على الاقتصاد الوطني وأمن المعاملات الإلكترونية.

[1] محمد الأمين البشري، الحماية الجنائية للتوقيع الإلكتروني في التشريعات المقارنة، دار الجامعة الجديدة، الإسكندرية، 2018، ص 214.

كما نص القانون العربي النموذجي الموحد لمكافحة جرائم إساءة استعمال أنظمة تقنية المعلومات على عقوبة الغرامة بالنسبة للأفعال المتمثلة في الاختراق غير المشروع لأنظمة المعالجة الآلية للبيانات، تاركًا تحديد قيمتها للتشريعات الوطنية.

وتتميز الغرامة بأنها تحقق عدة أهداف في آن واحد، فهي تمثل وسيلة عقابية وردعية، كما أنها تعوض الدولة عن الجهود المبذولة في مكافحة هذه الجرائم، فضلًا عن كونها تتناسب مع الطبيعة المالية للعديد من الجرائم الإلكترونية.

الفرع الثالث: الجمع بين الحبس والغرامة لم تكتف بعض التشريعات بتقرير عقوبة الحبس أو الغرامة منفردة، وإنما أجازت الجمع بينهما عندما تكون الجريمة ذات خطورة كبيرة أو عندما يترتب عنها ضرر جسيم[1] .

ففي النظام السعودي يمكن للمحكمة أن تحكم بالسجن والغرامة معًا، وهو ما يمنح القاضي سلطة تقديرية واسعة لتفريد العقاب وفق ظروف كل قضية. كما أن الجمع بين العقوبتين يحقق فعالية أكبر في مكافحة جرائم التوقيع الإلكتروني، لأن الجاني يتعرض في هذه الحالة لعقوبة تمس حريته الشخصية وأخرى تمس ذمته المالية.

ومن ثم فإن الجمع بين العقوبتين يعد من أبرز مظاهر السياسة الجنائية الحديثة الرامية إلى تشديد الحماية الجنائية المقررة للتوقيع الإلكتروني.

المطلب الثاني: العقوبات التكميلية المقررة لجرائم التوقيع الإلكتروني إلى جانب العقوبات الأصلية، قررت التشريعات الحديثة مجموعة من العقوبات التكميلية التي تهدف إلى إزالة آثار الجريمة ومنع الجاني من تكرارها، وهي عقوبات لا تستقل بذاتها وإنما تضاف إلى العقوبات الأصلية.

الفرع الأول: مصادرة الأجهزة والوسائل المستعملة في الجريمة تعد المصادرة من أهم العقوبات التكميلية في مجال الجرائم المعلوماتية، إذ تستهدف الأدوات والوسائل التي استخدمت في ارتكاب الجريمة.

[1] حسين بن سعيد بن سيف الغافري مرجع سابق ص19

وقد نص النظام السعودي صراحة على جواز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستعملة في الجرائم المتعلقة بالتوقيع الإلكتروني. ويشمل ذلك الحواسيب والخوادم والبرمجيات ووسائط التخزين التي استخدمت في تنفيذ الفعل الإجرامي[1].

وتكمن أهمية المصادرة في حرمان الجاني من الوسائل التي مكنته من ارتكاب الجريمة، وبالتالي الحد من احتمال عودته إلى النشاط الإجرامي مستقبلاً.

الفرع الثاني: إتلاف أو حذف البيانات غير المشروعة قد تقتضي حماية التوقيع الإلكتروني إزالة الآثار الناتجة عن الجريمة، خاصة إذا ترتب عنها إنشاء بيانات مزورة أو تعديل بيانات صحيحة أو الاستيلاء على معلومات سرية.

ولهذا تلجأ المحاكم في العديد من الأنظمة القانونية إلى الأمر بحذف البيانات غير المشروعة أو إتلاف البرامج المستخدمة في الجريمة. ويهدف هذا الإجراء إلى إعادة الوضع إلى ما كان عليه قبل ارتكاب الجريمة وضمان عدم استمرار الضرر الناتج عنها.

كما يشكل حذف البيانات المزورة وسيلة فعالة للحفاظ على مصداقية المحررات الإلكترونية ومنع تداولها بين الأشخاص أو المؤسسات.

الفرع الثالث: إغلاق المواقع والأنظمة المعلوماتية قد ترتكب بعض الجرائم من خلال مواقع إلكترونية أو منصات رقمية خصصت أساسًا لممارسة أنشطة غير مشروعة مرتبطة بالتوقيع الإلكتروني.

وفي هذه الحالة يمكن للمحكمة أن تأمر بإغلاق الموقع أو النظام المعلوماتي الذي استعمل في ارتكاب الجريمة، سواء بصورة مؤقتة أو نهائية بحسب خطورة الفعل المرتكب.

وتبرز أهمية هذا الإجراء في منع استمرار النشاط الإجرامي وقطع الوسيلة التي يستغلها الجناة للاعتداء على التوقيعات الإلكترونية أو تزويرها أو الاستيلاء عليها[2].

---

[1] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، 2004، ص 325

[2] عبد الفتاح بيومي حجازي مرجع سابق ص326

الفرع الرابع: نشر الحكم والحرمان من بعض الحقوق تأخذ العقوبات التكميلية أحيانًا شكل نشر الحكم القضائي في وسائل الإعلام أو المواقع الإلكترونية المختصة، وذلك بهدف تحقيق الردع العام وتحذير الجمهور من خطورة هذه الجرائم.

كما قد يتم الحكم بحرمان الجاني من ممارسة بعض الأنشطة المهنية أو التقنية إذا ثبت استغلاله لوظيفته أو مهنته في ارتكاب الجريمة، وهو ما يعزز الثقة في المعاملات الإلكترونية ويحمي المتعاملين من إساءة استعمال الخبرات التقنية.

خلاصة الفصل

يتضح من خلال هذا الفصل أن التوقيع الإلكتروني أصبح من أهم الوسائل القانونية والتقنية المعتمدة في إبرام المعاملات الإلكترونية وإثباتها، الأمر الذي جعله محلاً للعديد من الاعتداءات الإجرامية المستحدثة الناتجة عن التطور المتسارع لتكنولوجيا المعلومات والاتصالات. وقد تناول الفصل أهم الجرائم الواقعة على التوقيع الإلكتروني، وعلى رأسها جريمة الدخول غير المشروع إلى الأنظمة وقواعد البيانات المرتبطة بالتوقيع الإلكتروني، وجريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، مع بيان خصائص هذه الجرائم وأركانها المادية والمعنوية وصورها المختلفة.

كما تبين أن هذه الجرائم تتميز بطابعها التقني وخطورتها البالغة على أمن المعلومات والثقة في البيئة الرقمية، لما قد يترتب عليها من تزوير للمحررات الإلكترونية، وانتحال للهوية الرقمية، والإضرار بالمصالح المالية والقانونية للأفراد والمؤسسات. ومن أجل التصدي لهذه الأفعال، أقرت التشريعات الحديثة مجموعة من العقوبات الأصلية والتكميلية التي تستهدف تحقيق الردع وحماية المعاملات الإلكترونية من مختلف أشكال الاعتداء.

وعليه، فإن فعالية الحماية الجنائية للتوقيع الإلكتروني لا تتوقف عند تجريم الأفعال الماسة به فحسب، وإنما تقتضي كذلك تطوير الآليات القانونية والتقنية الكفيلة بالكشف عن هذه الجرائم وإثباتها، وتعزيز التعاون الوطني والدولي في مكافحتها، بما يضمن ترسيخ الثقة في المعاملات الإلكترونية وتحقيق الأمن القانوني في البيئة الرقمية.

الفصل الثاني:
الجرائم المرتبطة بالتصديق الإلكتروني

تمهيد :

يشهد العالم المعاصر تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصال، وهو ما انعكس بشكل مباشر على طبيعة المعاملات القانونية والتجارية والإدارية، التي أصبحت تعتمد بشكل متزايد على الوسائط الإلكترونية، وفي مقدمتها التوقيع والتصديق الإلكترونيين باعتبارهما أداتين محوريتين لإثبات الهوية الرقمية وضمان حجية التصرفات الإلكترونية.

غير أن هذا التطور التقني، ورغم ما يوفره من سرعة وفعالية، قد أفرز في المقابل مخاطر جديدة تمس أمن المعلومات وسلامة البيانات، الأمر الذي أدى إلى ظهور صور مستحدثة من الجرائم المعلوماتية، تتعلق أساسًا بالاعتداء على التوقيع والتصديق الإلكترونيين. وتتمثل هذه الاعتداءات في الدخول غير المشروع إلى الأنظمة وقواعد البيانات، والحصول على معطيات التوقيع أو شهادات التصديق بطرق احتيالية، إضافة إلى التزوير المعلوماتي واستغلال البيانات في أنشطة غير مشروعة تمس الثقة في البيئة الرقمية.

وأمام خطورة هذه الأفعال وانعكاساتها على استقرار المعاملات الإلكترونية، تدخل المشرع الجزائري من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، إلى جانب أحكام قانون العقوبات، من أجل وضع إطار قانوني يجرّم هذه السلوكيات ويحدد العقوبات المناسبة لها، فضلًا عن إقرار مجموعة من التدابير الوقائية والتقنية، وفي مقدمتها نظام التشفير، وتنظيم عمل مؤدي خدمات التصديق الإلكتروني، بما يضمن حماية الثقة الرقمية وتعزيز الأمن القانوني في البيئة الإلكترونية.

المبحث الاول: الجرائم الواقعة علي التصديق الإلكتروني:

سنتناول في هذا المبحث جريمة إصدار شهادة تصديق إلكتروني دون ترخيص في المطلب الأول، ثم نتطرق إلى جريمة إفشاء أو نشر شهادة تصديق إلكتروني لغرض احتيالي في التشريع الجزائري في المطلب الثاني.

المطلب الأول: جريمة اصدار شهادة تصديق الإلكتروني دون ترخيص

يتضح من نص المادة 72 المنوه عنها أعلاه أن المشرع الجزائري اشترط لقيام جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص توافر ركنين، ركن مادي وركن معنوي. ويتمثل الركن المادي في مزاولة نشاط التصديق الإلكتروني دون الحصول على ترخيص مسبق من السلطة الاقتصادية المختصة، باعتبارها الجهة المخولة قانونًا بمنح التراخيص لكل من يرغب في ممارسة نشاط التصديق الإلكتروني في الجزائر. ويتحقق هذا الركن بمجرد قيام الشخص الطبيعي أو المعنوي بإصدار شهادات التصديق الإلكتروني أو تقديم خدمات التوثيق الرقمي للغير دون استيفاء الإجراءات القانونية والتنظيمية المطلوبة.

و طبقا لنص المادة 1072 من القانون رقم 04/15[1] المتعلق بالتوقيع والتصديق الإلكترونيين، فإن جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص تعد من الجرائم التي تهدف إلى حماية الأمن القانوني والتقني للمعاملات الإلكترونية، وذلك بالنظر إلى الأهمية الكبيرة التي يحتلها التصديق الإلكتروني في إثبات الهوية الرقمية وضمان سلامة الوثائق والتصرفات المبرمة عبر الوسائط الإلكترونية، فالمشرع الجزائري اعتبر نشاط التصديق الإلكتروني نشاطًا حساسًا لا يجوز ممارسته إلا في إطار قانوني منظم وتحت رقابة السلطات المختصة، لما يترتب عنه من آثار قانونية وتقنية تمس الثقة العامة في البيئة الرقمية.

ويهدف المشرع من اشتراط الترخيص المسبق إلى ضمان الثقة والأمان في المعاملات الإلكترونية، خاصة وأن شهادة التصديق الإلكتروني تعد وسيلة أساسية للتحقق من هوية

[1] القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 10 فبراير 2015، المادة 02

المتعاملين وصحة التوقيع الإلكتروني المستعمل في مختلف المعاملات الرقمية. لذلك فإن ممارسة هذا النشاط دون رقابة أو ترخيص من شأنه أن يعرض أمن المعاملات الإلكترونية للخطر، ويفتح المجال أمام عمليات التزوير أو انتحال الهوية أو المساس بسرية البيانات الإلكترونية.

الفرع الأول: الركن المادي

يعرف الركن المادي للجريمة بصفة عامة على أنه المظهر الخارجي لنشاط الجاني، والذي يتمثل في السلوك الإجرامي الذي يجعله القانون مناطًا ومحلاً للعقاب،[1] لأن التشريع الجزائي لا يعاقب على مجرد النوايا أو الأفكار، وإنما يشترط صدور فعل مادي ملموس يترتب عليه الاعتداء على المصلحة المحمية قانونًا. ويختلف هذا النشاط من جريمة إلى أخرى بحسب طبيعتها وظروفها والأهداف التي يسعى المشرع إلى حمايتها.

ويتكون الركن المادي للجريمة من ثلاثة عناصر أساسية تتمثل في: السلوك الإجرامي، والنتيجة الإجرامية، ثم العلاقة السببية التي تربط بين السلوك والنتيجة. فالسلوك الإجرامي هو النشاط الذي يصدر عن الجاني سواء كان فعلًا إيجابيًا أو امتناعًا، أما النتيجة فهي الأثر المترتب عن هذا السلوك، في حين تتمثل العلاقة السببية في الرابطة التي تثبت أن النتيجة كانت بسبب السلوك المرتكب.

وبالرجوع إلى الجريمة محل الدراسة، وهي جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص، نجد أنها من جرائم الخطر وليست من جرائم الضرر، أي أن المشرع لا يشترط لقيامها تحقق ضرر فعلي أو وقوع اعتداء حقيقي على أحد الأشخاص أو الأنظمة المعلوماتية، وإنما يكفي مجرد ارتكاب السلوك المجرم قانونًا حتى تقوم الجريمة. ويعود ذلك إلى أن الخطر الذي قد ينجم عن ممارسة نشاط التصديق الإلكتروني دون ترخيص يعتبر في حد ذاته مساسًا بالثقة والأمن الواجب توافرهما في البيئة الرقمية.

ويتمثل السلوك الإجرامي في هذه الجريمة في مباشرة نشاط إصدار شهادات التصديق الإلكتروني أو تقديم خدمات التوثيق الرقمي دون الحصول على الترخيص المسبق من

[1] الشباس ي إبراهيم: الوجيز في شرح قانون العقوبات الجزائر - القسم العام، د.ط، دار الكتاب اللبناني، بيروت، لبنان، 11 ي د.ت،ص.6

السلطة المختصة. ويتحقق هذا السلوك بمجرد ممارسة النشاط بصورة فعلية، سواء تم ذلك بصفة دائمة أو مؤقتة، وسواء ترتب عنه استعمال فعلي للشهادات الإلكترونية أم لا. فالعبرة هنا بقيام الشخص بمزاولة نشاط محظور قانونًا خارج الإطار التنظيمي الذي حدده المشرع[1].

كما أن المشرع من خلال تجريم هذا الفعل يسعى إلى حماية الثقة العامة في المعاملات الإلكترونية وضمان سلامة التوقيع والتصديق الإلكترونيين، لما لهما من دور أساسي في إثبات المعاملات والعقود الإلكترونية. فالسماح لأي جهة بممارسة نشاط التصديق دون رقابة أو ترخيص قد يؤدي إلى انتشار شهادات غير موثوقة، الأمر الذي يهدد أمن المعلومات ويعرض المتعاملين لخطر التزوير والاحتيال وانتحال الهوية الرقمية.

ومن ثم، فإن الركن المادي في هذه الجريمة يتحقق بمجرد مزاولة النشاط المحظور دون الحاجة إلى إثبات وقوع نتيجة ضارة، وهو ما يبرز الطبيعة الوقائية لهذا التجريم، حيث يهدف المشرع إلى منع الخطر قبل وقوع الضرر الفعلي وحماية النظام العام الرقمي من أي تهديد محتمل.

و عليه يمكن القول أن هذه الجريمة تقع جراء مخالفة الجاني لأحكام نص المادة 33 من القانون رقم 15/04 المتعلق بالتوقيع والتصديق الإلكترونيين ".[2]

الفرع الثاني: الركن المعنوي الركن المعنوي هو عبارة عن نية داخلية يضمرها الجاني في نفسه، ويتخذ صورتين أساسيتين: إما صورة الخطأ العمدي أي القصد الجنائي، وإما صورة الخطأ غير العمدي أي الإهمال أو عدم الاحتياط. ويعتبر الركن المعنوي عنصرًا أساسيًا في قيام المسؤولية الجزائية، لأنه يعبر عن الصلة النفسية بين الجاني والفعل المرتكب، فلا يكفي لقيام الجريمة مجرد تحقق الركن المادي، بل يجب أن تتجه إرادة الجاني إلى ارتكاب السلوك المجرم مع علمه بعدم مشروعيته[3].

---

[1] سليمان عبد الله شرح قانون العقوبات الجزائري القسم العام، ج 1، د.ط ديوان المطبوعات الجامعية بن عكنون 144 الجزائر، 1995م، ص144

[2] تنص المادة 33 على يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني".

[3] سليمان عبد الله شرح قانون العقوبات الجزائري - القسم العام المرجع السابق، ص 84.

ويعد القصد الجنائي أخطر صور الركن المعنوي، ذلك أن إرادة الجاني تنصرف إلى ارتكاب الفعل المجرم وإلى النتيجة التي يعاقب عليها القانون، ويتكون القصد الجنائي من عنصرين أساسيين هما: العلم والإرادة. فالعلم يقصد به إدراك الجاني لجميع العناصر القانونية المكونة للجريمة، أما الإرادة فتتمثل في اتجاه إرادته الحرة إلى ارتكاب الفعل المجرم رغم علمه بمخالفته للقانون[1].

وصورة الركن المعنوي في جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص تتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، أي انصراف علم الجاني إلى أن نشاط إصدار شهادات التصديق الإلكتروني يخضع لترخيص مسبق من السلطة المختصة وفق ما يقرره القانون، ومع ذلك يتعمد ممارسة هذا النشاط دون الحصول على الترخيص اللازم. كما تتجه إرادته إلى مباشرة هذا السلوك الإجرامي وقبول ما قد يترتب عنه من آثار ومخاطر تمس بأمن المعاملات الإلكترونية والثقة الرقمية.

ويتحقق عنصر العلم متى كان الجاني على دراية بالنظام القانوني المنظم لنشاط التصديق الإلكتروني، وبأن مزاولة هذا النشاط دون ترخيص يشكل مخالفة صريحة لأحكام القانون. ولا يشترط أن يكون الجاني متخصصًا في المجال القانوني، بل يكفي أن يكون عالمًا بضرورة الترخيص بحكم طبيعة النشاط الذي يمارسه، خاصة وأن نشاط التصديق الإلكتروني يعد من الأنشطة التقنية المنظمة التي تتطلب إجراءات قانونية وإدارية دقيقة.

أما عنصر الإرادة فيتحقق عندما تتجه إرادة الجاني بحرية واختيار إلى إصدار شهادات التصديق الإلكتروني أو تقديم خدمات التوثيق الرقمي دون احترام الإجراءات القانونية المفروضة. وبالتالي فإن الجريمة تقوم بمجرد تعمد ممارسة النشاط المحظور، حتى ولو لم يقصد الجاني إلحاق ضرر معين بالغير أو تحقيق منفعة غير مشروعة، لأن المشرع اكتفى بتوافر القصد العام دون اشتراط قصد خاص.

وتبرز أهمية الركن المعنوي في هذه الجريمة في كونه يكشف عن خطورة السلوك الإجرامي، إذ إن تعمد مزاولة نشاط حساس كالتصديق الإلكتروني خارج الرقابة القانونية

[1] المرجع نفسه، ص86

من شأنه أن يهدد أمن المعلومات وسلامة المعاملات الإلكترونية، ويؤدي إلى فقدان الثقة في الوسائل الرقمية الحديثة. ولهذا حرص المشرع الجزائري على تجريم هذا الفعل حماية للنظام العام الرقمي وضمانًا لاستقرار المعاملات الإلكترونية داخل المجتمع.

المطلب الثاني : جريمة إفشاء أو نشر شهادة تصديق إلكتروني لغرض احتيالي في التشريع الجزائري

طبقا لنص المادة 1072 من القانون رقم 15/04 المتعلق بالتوقيع والتصديق الإلكترونيين، فإن جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص تعد من الجرائم العمدية لتوافر أركانها، وقد رتب المشرع الجزائري على هذه الجريمة عقوبات،

أركان جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص: يتضح من نص المادة 72 المنوه عنها أعلاه أن المشرع الجزائري اشترط لقيام جريمة إصدار شهادة تصديق إلكتروني بدون ترخيص توافر ركنين ركن مادي ويتمثل في مزاولة نشاط التصديق الإلكتروني دون الحصول على ترخيص من السلطة الاقتصادية باعتبارها مانحة الترخيص لكل من يريد ممارسة نشاط التصديق الإلكتروني في الجزائر، وهذا تطبيقا لنص المادتين 30 و 33 من القانون رقم 15/04 (الفرع الأول وركن ثاني وهو الركن المعنوي والمتمثل في القصد الجنائي العام (الفرع الثاني)

لم ينص المشرع الجزائري صراحة ضمن أحكام القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على جريمة إفشاء أو نشر شهادة تصديق إلكتروني لغرض احتيالي[1]، غير أن ذلك لا يمنع من تطبيق القواعد العامة الواردة في قانون العقوبات الجزائري، خاصة تلك المتعلقة بجرائم الاحتيال والإفشاء غير المشروع للبيانات واستعمال الوسائل الإلكترونية للإضرار بالغير. ويستفاد من أحكام هذا القانون أن شهادة التصديق الإلكتروني تعد محررًا إلكترونيًا رسميًا يتضمن بيانات ومعلومات ذات طابع تقني وقانوني تخص مؤدي خدمات التصديق الإلكتروني وصاحب الشهادة، الأمر الذي يقتضي توفير الحماية القانونية لها من أي استعمال غير مشروع.

[1] القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين – وزارة التجارة الجزائرية

ويقصد بجريمة إفشاء أو نشر شهادة التصديق الإلكتروني لغرض احتيالي قيام الجاني بالكشف عن بيانات شهادة التصديق الإلكتروني أو تداولها أو نشرها للغير دون وجه حق، بقصد استعمالها في عمليات احتيالية أو في انتحال الهوية الرقمية أو الإضرار بصاحب الشهادة أو بالمعاملات الإلكترونية المرتبطة بها. وقد يتم هذا السلوك من طرف مؤدي خدمات التصديق الإلكتروني بحكم اطلاعه على البيانات السرية المتعلقة بالشهادات الإلكترونية، كما قد يرتكب من طرف صاحب الشهادة نفسه أو من قبل أي شخص تمكن بطريقة مشروعة أو غير مشروعة من الوصول إلى تلك البيانات.

ولا يكفي لقيام هذه الجريمة مجرد نشر أو إفشاء البيانات الإلكترونية، بل يجب أن يكون هذا الفعل قد تم بقصد احتيالي أو ترتب عنه استعمال غير مشروع للشهادة الإلكترونية. فالجاني قد يستعمل الشهادة المنشورة في إبرام معاملات إلكترونية وهمية، أو انتحال شخصية صاحب الشهادة، أو الوصول غير المشروع إلى الأنظمة المعلوماتية، أو خداع الغير للحصول على منافع مالية أو معلومات سرية[1].

كما يمكن أن يتحقق هذا الفعل من خلال نشر الشهادة الإلكترونية أو بياناتها عبر الوسائط الرقمية المختلفة، كالبريد الإلكتروني أو المواقع الإلكترونية أو تطبيقات التواصل الإلكتروني، بما يؤدي إلى تعريض أمن المعاملات الإلكترونية للخطر والمساس بسرية البيانات والثقة الرقمية. ويزداد خطر هذا السلوك عندما يصدر عن مؤدي خدمات التصديق الإلكتروني باعتباره شخصًا مؤتمنًا على إدارة وحماية بيانات التصديق الإلكتروني، إذ إن إخلاله بالتزام السرية والثقة يهدد سلامة النظام الإلكتروني بأكمله.

وبتطبيق القواعد العامة لقانون العقوبات، يمكن تكييف هذا الفعل ضمن جرائم الاحتيال الإلكتروني أو إساءة استعمال المعطيات الإلكترونية أو إفشاء السر المهني بحسب طبيعة الفعل والنتائج المترتبة عنه. كما أن القصد الجنائي في هذه الجريمة يتمثل في علم الجاني

[1] رمزي بن الصديق، تزوير المحررات الالكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد 7 ، العدد 2، 2018، ص 207

بعدم مشروعية نشر أو إفشاء شهادة التصديق الإلكتروني، مع اتجاه إرادته إلى استعمالها أو تمكين الغير من استعمالها لتحقيق غرض احتيالي أو غير مشروع.

وقد حرص المشرع الجزائري من خلال تجريم الأفعال المرتبطة بالمساس بأمن المعاملات الإلكترونية إلى توفير الحماية القانونية للثقة الرقمية، وضمان سرية وأمن شهادات التصديق الإلكتروني باعتبارها وسيلة أساسية لإثبات الهوية الإلكترونية وصحة المعاملات المبرمة عبر الوسائط الرقمية.

الفرع الأول: الركن المادي يعرف الركن المادي للجريمة بصفة عامة على أنه عبارة عن المظهر الخارجي لنشاط الجاني، والذي يتمثل في السلوك الإجرامي الذي يجعله القانون مناطا ومحلا للعقاب، لأن التشريع العقابي لا يعاقب على النوايا والأفكار، بل على وجود نشاط مادي معين، ويختلف هذا النشاط من جريمة إلى أخرى حسب طبيعتها ونوعها وظروفها. [1]

ويتكون الركن المادي للجريمة من عناصر ثلاث هي: السلوك الإجرامي والنتيجة التي تحققت، والعلاقة السببية التي تربط بين السلوك و النتيجة.

وبالرجوع إلى الجريمة محل الدراسة فإننا نجد أنها جرائم خطر، وليست جرائم ضرر، وبالتالي يكفي لقيامها توفر السلوك الإجرامي دون الحاجة إلى تحقق أو عدم تحقق نتيجة معينة ، ويعرف السلوك أو الفعل الإجرامي على أنه ذلك السلوك المادي الصادر عن إنسان، والذي يتعارض مع القانون[2].

إذن فالسلوك الإجرامي في هذه الجريمة محل الدراسة يتمثل في قيام الجاني انتحال صفة مؤدي خدمات التصديق الإلكتروني ، فيقوم بإصدار شهادة تصديق إلكتروني دون الحصول على ترخيص من السلطة الاقتصادية مانحة الترخيص بموجب القانون.

---

[1] لشباسي إبراهيم: الوجيز في شرح قانون العقوبات الجزائر - القسم العام،- د.ط، دار الكتاب اللبناني، بيروت، لبنان، 11 ي د.ت،ص.6.

[2] سليمان عبد الله: شرح قانون العقوبات الجزائري القسم العام، ج 1، د.ط ديوان المطبوعات الجامعية بن عكنون 144 الجزائر، 1995م، ص83

و عليه يمكن القول أن هذه الجريمة تقع جراء مخالفة الجاني لأحكام نص المادة 33 من القانون رقم 15/04 المتعلق بالتوقيع والتصديق الإلكترونيين[1]."

الفرع الثاني: الركن المعنوي الركن المعنوي هو عبارة عن نية داخلية يضمرها الجاني في نفسه، ويتخذ صورتين أساسيتين إما صورة الخطأ العمدي أي القصد الجنائي، وإما صورة الخطأ غير العمدي أي الإهمال أو عدم الاحتياط.

ويعد القصد الجنائي أخطر صورتي الركن المعنوي للجريمة، ذلك أن إرادة الجاني تنصرف إلى ارتكاب الفعل الذي يأتيه وإلى النتيجة المقصودة بالعقاب، ويتكون من عنصرين اثنين هما: اتجاه ارادة الجاني نخو ارتكاب الجريمة والعلم بتوافر أركان الجريمة كما يتطلبها القانون[2].

وصورة الركن المعنوي في هذه الجريمة هو القصد الجنائي العام بعنصريه العلم والإرادة، أي انصراف علم الجاني بأن سلوكه المتمثل في إصدار الشهادة مخالف لنص القانون الذي يلزمه بالحصول على ترخيص من السلطة المختصة، ومع ذلك تتجه إرادته إلى هذا السلوك الإجرامي، ويقبل النتائج المترتبة عليه[3].

[1] تنص المادة 33 على يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني".

[2] سليمان عبد الله المرجع السابق، ص 84.

[3] المرجع نفسه، ص 86، 88.

المبحث الثاني: العقوبات المقررة لجرائم الصديق الإلكتروني

سوف نتطرق في هذا المبحث إلى كيفية الحماية من الجرائم المتعلقة بالتزوير الالكتروني حيث خصصنا مطلبين في المطلب الأول تناولنا العقوبات المطبقة على الجرائم وفي المطلب الثاني أساليب وآليات الحماية من جريمة التوقيع الالكتروني.

المطلب الأول: العقوبات المطبقة على الجرائم الواقعة على التصديق الإلكتروني :تم تقسيم العقوبات المقررة لجرائم التصديق الإلكتروني إلى ثلاثة أصناف رئيسية، تم تناولها في فروع متتالية، بالنظر إلى اختلاف طبيعة الأفعال المجرّمة ومدى خطورتها على منظومة الثقة الرقمية.

ففي الفرع الأول تم التطرق إلى عقوبة جريمة الدخول غير المصرح به إلى قاعدة بيانات تتعلق بالتصديق الإلكتروني، وفي الفرع الثاني إلى عقوبة جريمة الحصول على شهادة التصديق الإلكتروني بطرق احتيالية، وفي الفرع الثالث إلى عقوبة جريمة التزوير المعلوماتي في مجال التصديق الإلكتروني، باعتبارها من أخطر صور الاعتداء على البنية الرقمية الموثقة للمعاملات الإلكترونية.

الفرع الأول: عقوبة جريمة الدخول غير المصرح به إلى قاعدة بيانات تتعلق بالتصديق الإلكتروني

تختلف العقوبات المقررة لجريمة الدخول غير المشروع إلى قاعدة بيانات التصديق الإلكتروني من تشريع إلى آخر، تبعًا لمدى خطورة الفعل والضرر المحتمل الذي قد يمس أنظمة التصديق الإلكتروني أو البيانات الشخصية للمستفيدين منها[1] .

وفي إطار حماية البنية الرقمية للتصديق الإلكتروني، حرص المشرع الجزائري على تجريم كل صور الاعتداء على أنظمة المعالجة الآلية للمعطيات، وذلك بموجب المواد 394 مكرر وما بعدها من قانون العقوبات، والتي تعاقب كل من يدخل أو يبقى عمداً وبدون وجه حق داخل نظام معلوماتي محمي أو قاعدة بيانات إلكترونية.

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

وتتجلى خطورة هذا الفعل بشكل أكبر عندما يتعلق الأمر ببيانات التصديق الإلكتروني، باعتبارها مرتبطة مباشرة بإصدار الشهادات الإلكترونية والتحقق من هوية الأطراف. فمجرد الولوج غير المشروع قد يؤدي إلى الاطلاع على بيانات حساسة أو تعديلها أو حذفها أو حتى استغلالها في عمليات انتحال هوية رقمية أو تزوير شهادات تصديق إلكتروني.

وتزداد العقوبة تشديدًا كلما ترتب عن هذا الدخول غير المشروع إتلاف البيانات أو تعطيل النظام أو المساس بسرية المعطيات، وهو ما يعكس حرص المشرع على حماية الثقة في البنية التحتية الرقمية التي يقوم عليها نظام التصديق الإلكتروني.

الفرع الثاني: عقوبة جريمة الحصول على شهادة التصديق الإلكتروني بطرق احتيالية

تُعد شهادة التصديق الإلكتروني إحدى الركائز الأساسية في منظومة الثقة الرقمية، إذ تُستخدم لإثبات هوية الأشخاص والمؤسسات في المعاملات الإلكترونية. ولهذا السبب، أولى المشرع الجزائري أهمية خاصة لحمايتها من أي استغلال غير مشروع[1].

وقد نص القانون رقم 15-04[2] المؤرخ في 01 فبراير 2015 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين على مجموعة من الأحكام الجزائية التي تهدف إلى حماية خدمات التصديق الإلكتروني، ومن بينها تجريم الحصول على شهادة التصديق الإلكتروني أو معطياتها بطرق احتيالية أو غير مشروعة.

وتقوم هذه الجريمة عندما يستعمل الجاني وسائل التدليس أو الخداع أو أي أساليب تقنية غير مشروعة للحصول على شهادة التصديق الإلكتروني، سواء بهدف انتحال هوية الغير أو استعمالها في إبرام تصرفات قانونية أو تجارية غير مشروعة.

ويترتب على ذلك الإضرار المباشر بالثقة في نظام التصديق الإلكتروني، إضافة إلى إمكانية إلحاق خسائر مادية ومعنوية بالأشخاص أو المؤسسات المتضررة، خاصة إذا استُعملت هذه الشهادات في عمليات مالية أو تعاقدية إلكترونية.

---

[1] حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2013 ، ص.137.

[2]، القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 10 فبراير 2015، المادة 02.

الفرع الثالث: عقوبة جريمة التزوير المعلوماتي في مجال التصديق الإلكتروني

تُعد جريمة التزوير المعلوماتي في مجال التصديق الإلكتروني من أخطر الجرائم التي تمس النظام الرقمي للمعاملات الإلكترونية، نظراً لدور شهادة التصديق الإلكتروني في إضفاء الحجية القانونية على المحررات الإلكترونية والتحقق من هوية الأطراف[1] .

وقد كرس المشرع الجزائري الحماية القانونية لهذه الشهادات من خلال القانون رقم 15-04، لاسيما المادة 04 منه التي تنص على أن شهادة التصديق الإلكتروني الموصوف تتمتع بنفس الحجية القانونية للمحررات الرسمية أو التوقيع التقليدي متى استوفت الشروط القانونية المحددة.

وبالتالي، فإن أي عبث أو تزوير أو تعديل في بيانات التصديق الإلكتروني أو في الشهادات الصادرة يعد اعتداءً مباشراً على وسيلة إثبات قانونية معترف بها، ويشكل جريمة معلوماتية تستوجب العقاب.

أولاً: العقوبات الأصلية

تختلف العقوبات بحسب طبيعة الفعل المرتكب ودرجة جسامته، حيث يعاقب الشخص الطبيعي بالحبس والغرامة في حالة الدخول غير المشروع أو التلاعب أو التزوير في بيانات التصديق الإلكتروني أو شهاداته.

وتشتد العقوبة إذا ترتب عن الفعل استعمال شهادة مزورة أو انتحال هوية رقمية أو إلحاق ضرر جسيم بالغير، خاصة إذا استُعملت هذه الوسائل في معاملات مالية أو تجارية إلكترونية. [2]

أما بالنسبة للشخص المعنوي، فقد أقر المشرع الجزائري مسؤوليته الجزائية متى ارتكبت الجريمة لحسابه أو باسمه، حيث تطبق عليه غرامة مالية قد تصل إلى خمسة (05) مرات

[1] فضيلة عائلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري مقال منشور ضمن أعمال المؤتمر الدولي الرابع عشر 24-25 مارس 2017 منشور عبر الموقع www.jilrc.com : ص 129

[2] القانون رقم 15-04 مرجع سابق

الحد الأقصى للغرامة المقررة للشخص الطبيعي، وذلك وفقًا لأحكام قانون العقوبات، دون الإخلال بالعقوبات الأخرى الممكن تطبيقها.

ثانياً: العقوبات التكميلية إلى جانب العقوبات الأصلية، أجاز المشرع توقيع عقوبات تكميلية تهدف إلى الحد من خطورة الجريمة ومنع تكرارها، مثل مصادرة الأجهزة والوسائل المعلوماتية المستعملة في ارتكاب الجريمة، أو إغلاق الأنظمة والمواقع الإلكترونية التي استُخدمت في تنفيذ الأفعال الإجرامية.

كما يمكن أن تشمل هذه التدابير تعطيل الحسابات أو حذف البيانات المزورة وإزالة آثار الجريمة، بما يضمن إعادة الوضع إلى ما كان عليه قبل وقوع الاعتداء، ويحافظ على سلامة منظومة التصديق الإلكتروني.

وتبرز أهمية هذه العقوبات التكميلية في كونها لا تقتصر على الردع فقط، بل تهدف أيضًا إلى تعزيز الأمن الرقمي وحماية الثقة في خدمات التصديق الإلكتروني باعتبارها أحد أهم دعائم المعاملات الإلكترونية الحديثة.

المطلب الثاني: التدابير الوقائية لحماية التصديق الإلكتروني تعد مسألة الأمن المعلوماتي من أهم الضمانات والتحديات التي تواجهها وسائل الدفع الالكتروني، لأن غياب الأمن المعلوماتي يعتبر من معوقات اعتماد التجارة الالكترونية على الرغم من المزايا التي توفرها. ويقصد بالأمن المعلوماتي حماية جميع المعلومات التي يتم التعامل معها والمعالجة من منظمة وغرفة تشغيل أجهزة، ووسائط التخزين من السرقة والتزوير والتلف والضياع والاختراق.[1]

فلا يكفي الاعتراف بحجية التوقيع الالكتروني في الإثبات، دون العمل على إيجاد الآليات الكفيلة التي تبعث الثقة والاطمئنان لدى المتعاملين به، وتحقيق الحماية الضرورية للتوقيع الالكتروني من أي تحايل أو اختراق، ما جعل المشرع يقر عملية التشفير كإجراء الكتروني

[1] الحميد محمد دباس ، حماية أنظمة المعلومات، الأردن، دار الحامد للنشر والتوزيع، 2017، ص37، نقلا عن وفاء صد ارتي، آليات الحماية القانونية للتوقيع الالكتروني في التشريع الجزائري ،جامعة تبسة، مقال في مجلة العلوم القانونية والسياسة ، العدد01، 2020، ص595.

تقني لحماية البيانات الالكترونية، إضافة إلى تنظيم مهام جهة التوثيق الالكتروني وتحديد مسؤولياتها قصد تحقيق الأمان القانوني للمتعاملين في المجال الالكتروني.

الفرع الأول: نظام التشفير بعد نظام التشفير أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكات المفتوحة من أي تعديل أو تغير غير مرغوب فيه، ولذلك تأتي تقنيات التشفير في مقدمة الوسائل في مجال توفير الأمن وسرية المعلومات والمعاملات والصفقات المتبادلة.

أولا: المقصود بالتشفير يعرف التشفير بأنه كل العمليات التي تؤدي بفضل بروتوكولات سرية إلى تحويل معلومات أو إشارات مفهومة (مقروءة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية، ويعرف أيضا بأنه: آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس أو يمكن إرجاعها إلى حالتها الأصلي[1].

أما بالنسبة للتعريف التشريعي للتشفير ، فلم يتطرق المشرع الجزائري من القانون 18-05 المتعلق بالتجارة الالكترونية القانون رقم 05 / 18 المؤرخ في 10 ماي 2018 (2018) إلى تعريف التشفير، واكتفى بتعريف مفتاح التشفير الخاص ومفتاح التشفير العمومي في القانون 15-04 للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، نصت على ذلك المادة 02 في فقرتها الثامنة بقولها: مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي".

ويعرف التشفير بأنه كل الأعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة باستخدام وسائل مادية أو معالجة آلية إلى معلومات أو إشارات غامضة للغير أو إلى إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض .

[1] وسيم شفيق الحجار، الإثبات الالكتروني لبنان منشورات الحلبي الحقوقية، 2002، ص 198 ، نقلا عن وفاء

ثانيا : ضوابط وطرق التشفير لقد أقر المشرع الجزائري بضرورة تشفير البيانات والمعلومات حفاظا على سرية البيانات والمعلومات، وواضع ضوابط لذلك، كما حدد طرق التشفير وسنوضحها في الآتي:

أ- ضوابط التشفير نص المشرع الجزائري على ضرورة التشفير، كما نص على العمل من أجل الحفاظ على سرية البيانات والمعلومات المشفرة وتتمثل هذه الضوابط في:

-1مشروعية تشفير البيانات والمعلومات والتي يتم تبادلها عن طريق الوسائط الالكترونية، إذ أقر المشرع الجزائري من خلال القانون 15-04 نصوصا تتناول نظام التشفير، وعرف التشفير الخاص والعام، وأجاز استخدامه في المراسلات الالكترونية والتعاملات التجارية الالكترونية، كما أكد على حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها من كل اعتداء سواء تم ذلك باستخدام عناصر التشفير الخاصة بالتوقيع من غير طرفي العلاقة، أو بسبب استخدام التشفير في ارتكاب جرائم احتيالية.

2 - الحق في الحفاظ على سرية البيانات والمعلومات المشفرة اعتبر المشرع الجزائري من خلال القانون 15-04 (42) و 11/1 المواد الاعتداء على البيانات المرسلة بين طرفي العقد عبر الوسائط الالكترونية هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بين طرفي العلاقة، وبالتالي وجب ضمان سرية البيانات المستخدمة لإنشاء التوقيع الالكتروني بكل الوسائل التقنية المتوفرة .

الفرع الثاني : دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع الالكتروني اختلف الفقه والقانون في الاصطلاح الذي يطلق على الجهة المختصة بإصدار شهادات التصديق الالكتروني، حيث يستخدم جانب من الفقه اصطلاح سلطة الإشهار، ويطلق عليها جانب من الفقه مصطلح مقدم خدمات التصديق، أما قانون الأمم المتحدة النموذجي بشأن التوقيعات الالكترونية لسنة 2001، فاستخدم مصطلح مقدم خدمات التصديق. وعرفه في المادة 02 من بأنه شخص بصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية. أما التوجه الأوروبي فعرف مقدم الخدمات بأنه كل

شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الالكتروني، ويتولى خدمات أخرى مرتبطة بالتوقيع الالكتروني[1].

أما المشرع الجزائري فقد استمد مصطلح وتعريف مقدم خدمات التوثيق من نصوص قانون اليونسترال بشأن التوقيعات الالكترونية وأحكام التوجيه الأوروبي عند تعريفه بأنه: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة، ويقدم خدمات أخرى في مجال التصديق الالكتروني (المادة 02/11 من القانون 15/04) ويكمن الهدف الأساسي من إنشاء جهات مختصة في إصدار شهادات التصديق الالكتروني في تسهيل مراقبة التعاملات الالكترونية، إضافة إلى ضمان الأمن القانوني وحماية التعاملات الالكترونية.

وخاصة التوقيع الالكتروني من الأخطار التي قد تواجهه بسبب طبيعة هذه المعاملات التي تتم عبر وسائط الكترونية ومجلس عقد افتراضي. [2]

ولعل من أهم الضمانات القانونية للحماية والمحافظة على سلامة التوقيع الالكتروني هو إصدار شهادة التصديق الالكتروني، والتحقق من هوية الشخص الموقع، إضافة إلى إثبات مضمون البيانات الالكترونية وإصدار مفاتيح التشفير ، تحاول إنجازها فيما يلي:

أ - **إصدار شهادة التصديق الالكتروني** ميز المشرع الجزائري بين الشهادة الالكترونية البسيطة والشهادة الالكتروني الموصوفة ، كما سبقت الإشارة، فالشهادة الالكترونية البسيطة تتطلب إجراءات ترتبط بمعطيات ومعلومات تتعلق بالتحقق من توقيع شخص معين وتأكيد هوية هذا الشخص المادة 03 مكرر من المرسوم التنفيذي 07/162 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001 . (2007).

أما شهادة التصديق الالكترونية الموصوفة، فإنها ترتبط بإصدار الشهادة التوعية وفق شروط حددها المشرع من بينها أن تتضمن على الخصوص التوقيع الالكتروني الموصوف المادة 7 فقرة 2 من القانون 04 / 15 المتضمن تحديد القواعد العامة للتوقيع مادة 2/11 من القانون 15/04 المحدد للقواعد الخاصة بالتوقيع والتصديق الالكترونيين.

---

[1] - فواز المطالقة محمد، الوجيز في عقود التجارة الإلكترونية (الإصدار 2)، الأردن: دار الثقافة للنشر والتوزيع، 2008،

[2] محمد عقوني. الآلات التقنية والقانونية لحماية التوقيع الالكتروني. مجلة المفكر (18) ، ،2019ص.304

وكل من الشهادتين تفي بوجوب ارتباط التوقيع الالكتروني بشهادة الكترونية والتي تصدر حصريا من جهة تصديق الكتروني معتمدة، ومن ثم فلابد من توافر شهادة التصديق الالكتروني لكل بكون التوقيع الالكتروني موصوفا..

ب التحقق من هوية الشخص الموقع: يتمثل الدور الرئيسي لجهات التصديق الالكتروني في تمكين المرسل إليه من التأكد من هوية المرسل وصلاحية توقيعه، حيث تقوم بإصدار شهادة تصديق الكترونيين تفيد التصديق على التوقيع الالكتروني في تعاقد معين، كما تفيد أيضا في صحة التوقيع ونسبته إلى من صدر عنه الشخص الموقع ، وقد نص المشرع الجزائري من خلال المادة 44 من القانون 15-04 على أنه يجب على مؤدي خدمات التصديق الالكتروني وقبل منح شهادة التصديق الالكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، ويمنح مؤدي خدمات التصديق الالكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته وعند الاقتضاء التحقق من صفاته الخاصة. أما في حالة الأشخاص المعنوية فإن مؤدي خدمات التصديق الالكتروني يحتفظ بسجل بدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل.

خلاصة الفصل:

من خلال دراسة الجرائم الواقعة على التوقيع والتصديق الإلكترونيين في التشريع الجزائري، يتضح أن المشرع أولى أهمية كبيرة لحماية الثقة والأمن في البيئة الرقمية، باعتبار التوقيع والتصديق الإلكترونيين من الركائز الأساسية للمعاملات الإلكترونية الحديثة.

وقد تجلت هذه الحماية من خلال تجريم مجموعة من الأفعال التي تمس سلامة التوقيع والتصديق الإلكترونيين، كإصدار شهادات التصديق الإلكتروني دون ترخيص، والدخول غير المشروع إلى قواعد البيانات المتعلقة بالتوقيع الإلكتروني، والحصول على بيانات التوقيع بطرق احتيالية، والتزوير المعلوماتي للمعطيات الإلكترونية.

كما تبين أن المشرع لم يقتصر على تقرير العقوبات الجزائية المتمثلة في الحبس والغرامات المالية والعقوبات التكميلية، بل اعتمد كذلك جملة من التدابير الوقائية الرامية إلى تعزيز أمن المعاملات الإلكترونية، وفي مقدمتها نظام التشفير ودور جهات التصديق الإلكتروني في التحقق من هوية المتعاملين وإصدار شهادات التصديق وضمان سلامة البيانات الإلكترونية.

وعليه، فإن فعالية الحماية القانونية للتوقيع والتصديق الإلكترونيين لا تتحقق بالعقوبات الجزائية وحدها، وإنما تتطلب تكاملاً بين الآليات القانونية والتقنية والتنظيمية، بما يضمن تعزيز الثقة في المعاملات الإلكترونية وحماية الحقوق والمصالح المرتبطة بالاقتصاد الرقمي، ويساهم في تطوير بيئة إلكترونية آمنة ومستقرة قادرة على مواكبة التطورات التكنولوجية الحديثة.

خاتمة

خاتمة

وفي ختام دراستنا لموضوع الجرائم المرتبطة بالتوقيع والتصديق الإلكتروني، يتضح أن التطور التكنولوجي الذي شهده العالم قد أفرز وسائل حديثة لإثبات المعاملات الإلكترونية وتوثيقها، غير أن هذا التطور صاحبه ظهور أنماط جديدة من الجرائم المعلوماتية التي تستهدف سلامة هذه الوسائل ومصداقيتها. وقد تبيّن من خلال البحث أن التوقيع الإلكتروني والتصديق الإلكتروني يشكلان ركيزة أساسية لضمان الثقة في البيئة الرقمية، إلا أنهما يظلان عرضة لاعتداءات متعددة مثل الدخول غير المشروع إلى الأنظمة، والاستيلاء على بيانات التوقيع بطرق احتيالية، والتزوير المعلوماتي، إضافة إلى الجرائم المرتبطة بإصدار أو استعمال شهادات التصديق الإلكتروني بطرق غير مشروعة.

كما خلصت الدراسة إلى أن هذه الجرائم تتسم بطابع تقني معقد يجعل اكتشافها وإثباتها أكثر صعوبة مقارنة بالجرائم التقليدية، الأمر الذي دفع المشرعين إلى تبني نصوص قانونية خاصة تهدف إلى تجريم مختلف صور الاعتداء على الأنظمة المعلوماتية، وتقرير عقوبات أصلية وتكميلية من شأنها تحقيق الردع وحماية المعاملات الإلكترونية.

ومع ذلك، فإن فعالية الحماية الجنائية للتوقيع والتصديق الإلكتروني تبقى مرتبطة بمدى مواكبة التشريعات للتطور التكنولوجي المستمر، وتعزيز آليات الرقابة والكشف والتحقيق في الجرائم المعلوماتية، إضافة إلى ضرورة تعزيز التعاون الدولي لمواجهة الطبيعة العابرة للحدود لهذا النوع من الجرائم.

وبناءً على ما سبق، يمكن القول إن تحقيق أمن المعاملات الإلكترونية وضمان الثقة في التوقيع والتصديق الإلكتروني يتطلب تضافر الجهود القانونية والتقنية والمؤسساتية، بما يضمن بيئة رقمية آمنة وموثوقة تخدم تطور الاقتصاد الرقمي والمعاملات الحديثة.

قائمة المصادر والمراجع

اولا المصادر :

1. [1]قانون رقم 09_01، مؤرخ في 25 فبراير سنة 2009، يعدل و يتمم الأمر رقم 66_156 المؤرخ في 8 يونيو 1966، والمتضمن قانون العقوبات الجريدة الرسمية عدد 30
2. دردور نسيم، الج ارئم المعلوماتية على ضوء القانون الج ازئري والمقارن، مذكرة ماجستير، قانون جنائي، جامعة منتوري 2 قسنطينة، ،2012 ص .25
3. قانون العقوبات الصادر بموجب الأمر رقم 66 – ،156 المؤرخ في 18 صفر عام ،1386 الموافق لـ 08 يونيو ،1966 الذي يتضمن قانون العقوبات، الجريدة الرسمية، العدد ،49 ،1966 المعدل والمتمم بالقانون ،06-24 المؤرخ في ،28/04/2024 الجريدة الرسمية العدد ،30 سنة ،2024
4. محمد صبحي نجم، جرائم الكمبيوتر والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص. 188-190.
5. صالح شنين، الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، رسالة دكتوراه، جامعة تلمسان، ،2013
6. حسن بن سعد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدارسات والبحوث، سلطنة عمان، ،2006
7. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية والتوقيع الإلكتروني في المعاملات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2007،
8. القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 10 فبراير 2015، المادة4
9. تنص المادة 33 على يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني."

10. القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين وزارة التجارة الجزائرية
11. ، القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 10 فبراير 2015، المادة 02

ثانيا المراجع :

1. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، طبعة 02، سنة 2010،
2. حسين بن سعيد بن سيف الغافري، الجرائم الواقعة على التجارة الإلكترونية، موقع المنشاوي للدارسات والبحوث، سلطنة عمان، 2006،
3. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، 2004، ،
4. محمد الأمين البشري، الحماية الجنائية للتوقيع الإلكتروني في التشريعات المقارنة، دار الجامعة الجديدة، الإسكندرية، 2018،
5. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، ، 2013 ،
6. الشباس ي إبراهيم: الوجيز في شرح قانون العقوبات الجزائر - القسم العام،- د.ط، دار الكتاب اللبناني، بيروت، لبنان، 11 ي د.ت،
7. سليمان عبد الله شرح قانون العقوبات الجزائري القسم العام، ج 1، د.ط ديوان المطبوعات الجامعية بن عكنون 144 الجزائر، 1995م
8. رمزي بن الصديق، تزوير المحررات الالكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المجلد 7 ، العدد 2، 2018،

9. لشباسي إبراهيم: الوجيز في شرح قانون العقوبات الجزائر - القسم العام،- د.ط، دار الكتاب اللبناني، بيروت، لبنان، 11 ي د.ت،
10. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقع الإلكتروني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2013 ،
11. فضيلة عائلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري مقال منشور ضمن أعمال المؤتمر الدولي الرابع عشر 24-25 مارس 2017 منشور عبر الموقع :com.jilrc.www
12. الحميد محمد دباس ، حماية أنظمة المعلومات، الأردن، دار الحامد للنشر والتوزيع، 2017، ص37، نقلا عن وفاء صد ارتي، آليات الحماية القانونية للتوقيع الالكتروني في التشريع الجزائري ،جامعة تبسة، مقال في مجلة العلوم القانونية والسياسة ، العدد01، 2020،
13. وسيم شفيق الحجار، الإثبات الالكتروني لبنان منشورات الحلبي الحقوقية، 2002، ص 198 ، نقلا عن وفاء
14. فواز المطالقة محمد، الوجيز في عقود التجارة الإلكترونية (الإصدار 2)، الأردن: دار الثقافة للنشر والتوزيع، 2008،
15. محمد عقوني. الآلات التقنية والقانونية لحماية التوقيع الالكتروني. مجلة المفكر (18) ، 2019،

فهرس

ملص دراسة

ملخص الدراسة

تناولت هذه الدراسة موضوع الجرائم المرتبطة بقانون التوقيع والتصديق الإلكتروني في التشريع الجزائري، وذلك في ظل التطور التكنولوجي المتسارع الذي فرض تحول المعاملات القانونية والتجارية من الشكل التقليدي إلى الشكل الإلكتروني. وقد هدفت الدراسة إلى التعرف على أهم الجرائم الواقعة على التوقيع والتصديق الإلكترونيين، وتحليل أركانها القانونية، وبيان العقوبات المقررة لها، مع استعراض آليات الحماية الجنائية والوقائية المتبعة لمواجهة هذه الجرائم.

وقد خلصت الدراسة إلى أن التوقيع والتصديق الإلكترونيين يشكلان ركيزة أساسية لضمان الثقة والأمان في البيئة الرقمية، غير أنهما يظلان عرضة لاعتداءات متعددة أبرزها: جريمة الدخول غير المشروع إلى أنظمة وقواعد بيانات التوقيع الإلكتروني، وجريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، وجريمة إصدار شهادة تصديق إلكتروني دون ترخيص، إضافة إلى جريمة التزوير المعلوماتي في مجال التصديق الإلكتروني. كما تبين أن المشرع الجزائري اعتمد نظاماً عقابياً يجمع بين العقوبات الأصلية المتمثلة في الحبس والغرامة، والعقوبات التكميلية كالمصادرة وإغلاق المواقع، إلى جانب تدابير وقائية كالتشفير وتنظيم جهات التصديق الإلكتروني، غير أن فعالية هذه الحماية تظل مرهونة بمواكبة التشريعات للتطور التكنولوجي وتعزيز آليات الكشف والتحقيق والتعاون الدولي.

الكلمات المفتاحية :التوقيع الإلكتروني، التصديق الإلكتروني، الجرائم المعلوماتية، الدخول غير المشروع، الاحتيال الإلكتروني، شهادة التصديق، الحماية الجنائية، التشريع الجزائري.

Summary of the Study

This study examines **crimes related to the law on electronic signature and electronic certification** in Algerian legislation, in light of the rapid technological development that has transformed legal and commercial transactions from traditional to electronic forms. The study aimed to identify the most significant offenses against electronic signatures and certification, analyze their legal elements, outline the prescribed penalties, and review the criminal and preventive protection mechanisms employed to combat these crimes.

The study concluded that electronic signatures and certification constitute a fundamental pillar for ensuring trust and security in the digital environment. However, they remain vulnerable to various attacks, most notably: the crime of unauthorized access to electronic signature systems and databases, the crime of obtaining electronic signatures through fraudulent means, the crime of issuing an electronic certification certificate without a license, and the crime of information forgery in the field of electronic certification. The study also revealed that the Algerian legislator has adopted a punitive system combining primary penalties (imprisonment and fines) with complementary penalties (confiscation and website closure), alongside preventive measures such as encryption and the regulation of certification service providers. Nevertheless, the effectiveness of this protection remains contingent upon keeping legislation aligned with technological developments, enhancing detection and investigation mechanisms, and strengthening international cooperation.

Keywords: Electronic Signature, Electronic Certification, Cybercrimes, Unauthorized Access, Electronic Fraud, Certification Certificate, Criminal Protection, Algerian Legislation.