جامعة زيان عاشور -الجلفة-
Zian Achour University of Djelfa
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

قسم الحقوق

# جرائم الإعتداء على التوقيع الإلكتروني

مذكرة ضمن متطلبات
نيل شهادة الماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية

إعداد الطالب :
- بروان خالد
-

إشراف الأستاذ:
-د. خلدون عيشة

لجنة المناقشة

| | |
|---|---|
| -د/أ. بن مسعود احمد | رئيسا |
| -د/أ. خلدون عيشة | مقررا |
| -د/أ. بيدي امال | ممتحنا |

الموسم الجامعي 2020/2019

2020/M071P/M1539034765/


بسم الله الرحمن الرحيم

# تشكر

**بسم الله الرحمان الرحيم**

الحمد لله الذي أنار بنوره السموات والأرض، و وفقني لإتمام هذه الرسالة والصلاة والسلام على سيد المرسلين محمد وعلى اله وصحبه ومن سار على دربه إلى يوم الدين.

أما بعد فهذا مقام لا بد فيه من أن يعترف بالفضل لأهله وتقديم الشكر لهم امتثالا لقوله تعالى: **« ومن شكر فإنما يشكر لنفسه »** سورة النمل الآية 40.

ولذلك فأنني أتقدم بخالص الشكر والتقدير والاحترام للأستاذة الفاضلة المشرفة الدكتورة " خلدون عيشة ".التي تابعت عملي هذا وأعطتني الثقة الكافية لذلك .

كما أتقدم بخالص الشكر والتقدير والاحترام لأعضاء لجنة المناقشة على قبولهم مناقشة هذه المذكرة.

كما أتوجه بالشكر إلى كافة أساتذة كلية القانون والعلوم السياسية

بجامعة زيان عاشور بالجلفة ، والشكر موصول إلى كل زملاء الدراسة.

**وشكرا**

# إهـــداء

**بسم الله الرحمان الرحيم**

الهي لا يطيب الليل إلا بشكرك، ولا يطيب النهار إلا بطاعتك ولا تطيب الدنيا إلا بذكرك، ولا تطيب الآخرة إلا بعفوك إلى معنى الحب والحنان والأنس والأمان إلى بسمة الحياة وسر الوجود إلى من كان دعاؤها سر نجاحي، إلى أغلى الحبايب

" **أمي.....أمي** "

إلى تاج راسي وقرة عيني، إلى صاحب الفضل الجزيل والدعم المتواصل إلى من خطى لي المبادئ والأخلاق على صفحة بيضاء إلى روح أبي الطاهرة جعل قبره روضة من رياض الجنة

**"أبي العزيز"**

إلى من نشأت وترعرعت بينهم **إخوتي وأخواتي** سندي في الحياة .

إلى جميع الأصدقاء والأهل والأحباب

إلى من هم في قلبي ولم يكتبهم قلمي

إلى كل من وسعتهم ذاكرتي ولم تحملهم مذكرتي

إلى كل من يساهم في نشر رسالة العلم والدين

إلى كل هؤلاء اهدي ثمرة جهدي .

**بروان خالد**

# مقدمة

**مقدمة:**

مهدت الثورة الصناعية التي تفجرت في منتصف القرن التاسع عشر، لبزوغ ثورة جديدة هي ثورة المعلومات، التي تقترن دائما بفكرة الحاسوب التي بدأها Charles Badbage الذي يعتبر أول من فكر في الحاسوب الرقمي من خلال سعيه الدؤوب لمكننة بعض العمليات الحسابية حيث اكتشف آلة الفروق ثم الآلة التحليلية، وفي سنة 1943 قام جون فان نيومن J. W. Neumann عالم الرياضيات الأمريكي بوضع أسس الحاسوب كما هو معروف الآن، والذي يتكون من خمسة مكونات أهمها اثنتان هما وحدة المعالجة المركزية التي يتم بواسطتها تنفيذ سلسلة العمليات الحسابية والمنطقية المطلوب تنفيذها، والذاكرة التي يتم فيها حفظ نتيجة كل عملية حيث يتم تنفيذ العملية طبقا لمجموعة من التعليمات أو البرامج المخزنة في الذاكرة، فولد الحاسوب كجهاز رئيسي في الإعلام الآلي والمعلوميات، وبفضل الحاسوب يعيش العالم الآن عصر المعلومات الذي يتسم بالتطور السريع لتكنولوجيا الحاسبات، فقد أخذت المعلومات الآن، في التزايد والتفاعل مع التقدم العلمي والتطور التكنولوجي، كل دقيقة، بل كل ثانية، وبات تدفق المعلومات أساسا للرقي الحضاري للدول وبسبب تزايد المعلومات وكثرتها بدأت الدول تهتم بأساليب جمع هذه المعلومات وتبويبها وتصنيفها وتحليلها بغية الإستفادة منها، في الوقت الذي تطورت فيه المستحدثات التكنولوجية، والتي استهدفت التحكم في هذه المعلومات وتخزينها واسترجاعها، وهو ما يعرف بتكنولوجيا المعلومات وباتت وفرة المعلومات معيار الجدوى جهود التنمية وزيادة الإنتاج ورسم السياسات واتخاذ أنجع القرارات للنهوض باقتصاد الأمم، ولا غرو، فإن ما أنتجه العقل البشري في الخمسين سنة الماضية يعادل ما أنتجه العقل البشري في خمسة قرون سابقة ولابد أن السنوات العشر الأخيرة قد حققت أكثر مما تحقق في الخمسين سنة السابقة عليها، وباستخدام تكنولوجيا المعلوميات وبرامج الحاسبات يمكن أن يتحقق في عام واحد مثلما حققته البشرية في كل تاريخها الطويل من معلومات.

ولقد اتسعت في الآونة الأخيرة دائرة استخدام الشبكات الإلكترونية للمعلومات ، كوسيلة اتصال دولية في شتى مجالات الحياة ، لتحقيق ما تصبو إليه الإنسانية من السرعة في إنجاز المشاريع ، اختصار الوقت و المسافات و حتى الجهد البدني و الذهني.

و أضحت هذه الشبكات تحوي معلومات غير محصورة في مجال محدد، بل تتعلق بكافة ميادين الحياة الاجتماعية، الاقتصادية، العلمية و غيرها.

إلا أن الاستخدام المتزايد لهذه الأنظمة الالكترونية أدى إلى الكثير من المخاطر و أفرز أنواعا من الجرائم ، أصبح يعرف بالجرائم الالكترونية.

و تنوعت هذه الجرائم الالكترونية من تزوير سرقة معلومات و أموال – اختراق لنظم – جرائم ماسة بالأخلاق و الآداب العامة.... ، و ذلك عن طريق الدخول غير المشروع إلى جهاز حاسب آلي أو نظام معلوماتي أو شبكة معلوماتية ، بغرض تدمير ، تغيير أو إعادة نشر بيانات أو معلومات سرية أو شخصية ، إتلاف مستندات أو موقع أو نظام الكتروني و ما شابه ، ناهيك عما تسببه من خلافات بين الأفراد بسبب التشهير أو إشاعة الأخبار الكاذبة ، التهديد، الابتزاز لشخص طبيعي أو معنوي.

## 1) الإشكالية :

أسفر التطور الهائل في المجال المعلوماتي على ميلاد عقود إلكترونية ليس هذا فحسب وإنما صاحبته جملة من التحديثات والتي مست كل مجالات الحياة، ومن بينالأشياء الجديدة التي جاء بها التقدم التكنولوجي نجد ما يسمى بالتوقيع الالكتروني، مصطلح جديد في الساحة الاقتصادية والتجارية خاصة.

يحظى التوقيع الالكتروني بأهمية واسعة النطاق بالنظر إلى شموليته حيث أصبح استعماله في مختلف مجالات الحياة ليس هذا فحسب وإنما حتى في أبسط المعاملات، لذلك فقد ساهم إلى حد كبير في التقليص من عدة أمور خاصة في الحياة التجارية لاسيما مع انتشار عدة مواقع تقوم بعرض سلع وخدمات عبر الشبكة يتم شراءها عن طريق بطاقات

ممضية الكترونيا، لكن تقابل هذه الأهمية التي أحالنا إليها التوقيع الالكتروني، الوجه المظلم الذي يتمثل في الجريمة. كل هذه العوامل كانت سببا في طرح مشكلة دراستنا متمثلة في التساؤل التالي:

- **فيما تتمثل أهم جرائم الاعتداء على التوقيع الالكتروني، وما هي العقوبات التي سطرها القانون الجزائري في حق هذه الجرائم ؟**

2) **المنهج المتبع:**

قد تطلب منا هذا البحث إعتماد المنهج الوصفي التحليلي .فالمنهج الوصفي يظهر من خلال قيامنا بوصف ظاهرة الجريمة الالكترونية المتمثلة في التوقيع الالكتروني وتحديد بعض المفاهيم التي تقوم عليها، وكذا قيامنا بوصف المفاهيم الخاصة بالإجراءات المستعملة في استخلاص الدليل والصعوبات التي تواجهها

3) **أسباب اختيار الموضوع** : هناك أسباب ذاتية وأخرى موضوعية

- **الأسباب الذاتية**
- الميول الشخصي لهذا النوع من البحوث
- تطابق عنوان الموضوع مع تخصص دراستنا
- محاولة إثراء مكتبة كليتنا بهذا النوع من البحوث قصد أن يكون مرجعا للطلبة في المستقبل

- **الأسباب الموضوعية**

- تمحورت حول الحداثة القانونية والتشريعية للحماية الجنائية للتوقيع والتصديق الإلكترونيين، مما يدفع نحو البحث في مدى انسجام النصوص القانونية لهذه المنظومة مع المستجدات الراهنة في مجال المعاملات الإلكترونية خاصة في ظل أهمية التوقيع الإلكتروني، وأهمية المصادقة على هذا التوقيع بما يضفي عليه حجية في الإثبات،

فضلا عن وسائل الحماية الجنائية المعتمدة من قبل المشرع لمواجهة جرائم الاعتداء على التوقيع الإلكتروني.

**4) أهمية البحث:**

يعد موضوع البحث من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي وهو من الموضوعات التي لا تزال بكرا ولم تنل حظها من البحث ، وإذا كانت الجرائم الالكترونية تعد من الأنماط الإجرامية التي فجرتها حديثا ثورة تقنية المعلومات والإتصالات عن بعد، حيث تعتبر من المستجدات التي لم تكن معروفة للقانون الجزائي سواء الموضوعي أو الإجرائي، فمن دون شك أن أي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي في إطار عملية البحث والتجريب سوف يخلق إشكالات إجرائية للأجهزة المكلفة بهذه العملية، ينبغي أن تأتي الدراسات القانونية عليها بالشرح والتحليل.

**5) أهداف الدراسة :**

- ينبع الهدف من هذه الدراسة في وضع الخطوط العريضة للتعرف على الآثار السلبية للجريمة الالكترونية وسبل مكافحتها ، و ذلك أن جدة وحداثة الجرائم الالكترونية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها، إذ لاشك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

- محاولة الوقوف على ماهية التوقيع الالكتروني من خلال تحديد صورة و الشروط التي يطلبها لإضفاء الحجية عليه.

**6) صعوبات الدراسة:**

تكمن اكبر صعوبة التي واجهتنا لدراسة هذا الموضوع هو الوباء الذي اجتاح كامل العالم المتمثل في وباء كورونا المستجد كوفيد 19 الذي فرض على العالم حضر تجول وحجر صحي مما أدى إلى غلق جميع الإدارات والمؤسسات التربوية منها الجامعات والمكتبات مما طرأ لنا صعوبة في اقتناء المراجع .

**7) الدراسات السابقة:**

**7-1) الدراسة الأولى:**

- دراسة صالح شنين تحت عنوان : «الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة» وهو بحث مقدم للحصول على الدكتوراه بجامعة تلمسان، تطرق لأهمية الحماية الجنائية للمعاملات الإلكترونية من خلال تعداد جرائم الاعتداء على التوقيع والتصديق الإلكترونيين ووسائل حمايتهما جنائيا في ظل التشريعات الأجنبية والوطنية.

**7-2) الدراسة الثانية:**

- دراسة حنان براهمي تحت عنوان : «جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية» وهي أطروحة مقدمة لنيل الدكتوراه بجامعة بسكرة، عالجت إشكالية تتعلق بجريمة التزوير الإلكتروني من منطلق ما إذا كان تغيير الحقيقة في المعلومات المعالجة أليا تزويرا في إطار المعاملات الإدارية، متخذة المقارنة والاستدلال والتحليل مناهج لمعالجة هذا الإشكال.

**7-3) الدراسة الثالثة:**

- دراسة عزيزة لرقط تحت عنوان : « الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري » ، وهي ورقة بحثية منشورة على شكل مقال في مجلة الاجتهاد للدراسات القانونية والاقتصادية بالمركز الجامعي تمنراست العدد 11، جانفي 2017)، عالجت إشكالية تمحورت حول معرفة أوجه الحماية الجنائية التي قررها المشرع الجزائري للتوقيع والتصديق الإلكترونيين، وخرجت بالنتيجة التي مفادها عدم كفاية القانون رقم (15-04) في تناول جميع أوجه الاعتداء على التوقيع والتصديق الإلكترونيين.

**8) تقسيمات البحث:**

لقد قمنا بتقسيم الدراسة إلى فصلين ، حيث عنونا الفصل الأول بـ : الإطار المفاهيمي للتوقيع الالكتروني ،حيث قسمناه إلى مبحثين جاء الأول ماهية التوقيع الالكتروني فيما عنونا الثاني المبحث الثاني حجية وشروط التوقيع الالكتروني ، أما الفصل الثاني عنوناه بـ الجرائم الواقعة على التوقيع الالكتروني وكيفية الحماية منها ، حيث قسمناه بدوره إلى مبحثين المبحث الأول المبحث الأول الجرائم الواقعة على التوقيع الالكتروني والمبحث الثاني المبحث الثاني كيفية الحماية من الجرائم الواقعة على التوقيع الالكتروني ، واختتمنا دراستنا بخاتمة خلصنا فيها إلى أهم نتائج الدراسة.

# الفصل الأول

# الإطار المفاهيمي للتوقيع الإلكتروني

**تمهيد :**

لقد أصبح التوقيع الإلكتروني مع ظهور الوثائق الإلكترونية، يلعب دورا محوريا في إثبات حجية هذه الوثائق وإضفاء الحماية القانونية لها، وحتى يؤدي هذا التوقيع وظائف التوقيع التقليدي، سعت التشريعات الوطنية والدولية إلى تبيان مفهومه، أشكاله، وشروطه، ولدراسة موضوع التوقيع الالكتروني سوف نتطرق في هذا الفصل إلى الإطار المفاهيمي للتوقيع الالكتروني حيث قسمناه إلى مبحثين يتمثلان في :

- **المبحث الأول: ماهية التوقيع الإلكتروني**
- **المبحث الثاني: حجية وشروط التوقيع الالكتروني**

## المبحث الأول: ماهية التوقيع الإلكتروني

يحتل التوقيع التقليدي أهمية كبيرة في توفير عنصر الثقة في المعاملات والمحررات الورقية، ولكن بالنظر إلى إفرازات الثورة التكنولوجية التي اجتاحت العالم خاصة بظهور شبكة الإنترنت، ثم الإعلان عن ميلاد نوع جديد من التوقيع أطلق عليه التوقيع الإلكتروني يتماشى مع هذا النوع من المحرر الإكتروني سيما في العقود المبرمة عن بعد، ونظرا إلى كثرة استعمال هذه التوقيعات الحديثة جاءت الضرورة إلى تأطيرها ووضع قواعد خاصة بها بالتالي سنتناول في هذا المبحث مفهوم التوقيع الإلكتروني.

### المطلب الأول: مفهوم التوقيع الالكتروني

تعددت التعريفات التي منحت للتوقيع الإلكتروني بتعدد الجهات التي عرفته، وهذا ما سنتناوله في الفرع الحالي من خلال تعريف التوقيع الإلكتروني وفقا للفقه القانوني، فتعريفه في ظل التشريعات الدولية، وصولا إلى تعريفه وفق التشريع الجزائري.

#### الفرع الأول : تعريف التوقيع الالكتروني

**أولا: تعريف التوقيع الإلكتروني في الفقه القانوني**

لم يثر تعريف التوقيع الإلكتروني جدلا كبيرا من ناحية الفقه، إذ كانت معظم التعريفات الفقهية التي قيلت في شأنه تدور حول فكرة إظهار شكل التوقيع وبيان خصائصه، وعلى الرغم من إجماع الفقهاء على هذه الفكرة إلا أنهم لم يتفقوا على تعريف واحد، وذلك تبعا للزاوية التي ينظر إليها كل فقيه[1] .

فقد عرف التوقيع الإلكتروني على أنه "إتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معينة معروفة مقدما، فيكون مجموع هذه الإجراءات هو البديل للتوقيع التقليدي[2].

---

[1]- محمد محمد السادات، **حجية المحررات الموقعة إلكترونية في الإثبات دراسة مقارنة**، دار الجامعة الجديدة، مصر القاهرة، 2011، ص 43. نقلا عن ياسمينة كواشي، الحماية الجنائية للتوقيع والتصديق الالكترونيين في ظل القانون، مذكرة ماستر، جامعة العربي بن مهيدي قسم الحقوق، 2017، 07.

[2]- محمد المرسي الزهرة، **عناصر الدليل الكتابي التقليدي**، شون ناشر، 2001، ص 92

كما عرف على أنه ما يوضع على محرر إلكتروني (شريحة إلكترونية) ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متميز ومنفرد يسمح بتحديد الشخص الموقع ويميزه عن غيره [1] .

وعرف هذا النوع من التوقيعات بأنه الطريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الأنترنيت [2].

وعرف بأنه "عبارة عن إجراء يقوم به المرسل بحيث يتم ربط هويته بالوثيقة الموقع عليها، وبحيث يمكن المستلم الوثيقة التحقق من صحة التوقيع....[3]

وقد عرفه جانب آخر من الفقه على أنه "مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته [4]

من خلال ما سبق ذكره حول توجهات الفقه القانوني في تعريف التوقيع الإلكتروني، نستخلص أنها ركزت من جهة على الكيفية التي ينشأ من خلالها من حيث هو مجموعة من الرموز أو الإجراءات (آلية إنشاء التوقيع الإلكتروني)، ومن جهة ثانية على وظائفه ومميزاته من حيث إفادته في إثبات وحجية استعماله وإسناده لشخص معين، وموافقة هذا الأخير من خلال توقيعه على ما يتضمنه السند أو الوثيقة التي تحمل هذا التوقيع.

**ثانيا: تعريف التوقيع الالكتروني في التشريع الجزائري**

استخدم المشرع الجزائري مصطلح التوقيع الالكتروني لأول مرة بموجب نص المادة 2/372 من القانون المدني المعدل سنة 2005 والتي تنص على أنه: ".. ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكررا" (المدني).

---

[1]- أمير فرج يوسف، **التوقيع الإلكتروني**، دار المطبوعات الجامعية، مصر، الإسكندرية، 2008.

[2]- **نفس المرجع**، ص17.

[3]- **نفس المرجع**، ص18.

[4]- لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، دار الثقافة، الأردن، 2009، ص 120.

ولم يضع المشرع الجزائري تعريفا للتوقيع الالكتروني، بل اعترف بحجية هذا الأخير رابطا بذلك هذه الأخيرة بتوفر نفس الشروط المتطلبة في الكتابة العادية، ليتدخل بعد ذلك بموجب المرسوم التنفيذي 07-162 (المرسوم التنفيذي رقم 162-07) ليميز بين التوقيع الالكتروني العادي والتوقيع الالكتروني المؤمن وذلك بموجب المادة 3 مكرر[1]. وهذا بقولها إن: ".. التوقيع الالكتروني المؤمن هو توقيع الكتروني يفي بالمتطلبات الآتية: يكون خاصا بالموقع، يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحضرية يضمن مع الفعل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه".

وبصدور القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق لـ 01 فبراير سنة 2015م الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين (القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق ل 01 فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين 6، 2015)، تم وضع تعريف للتوقيع الالكتروني وذلك من خلال نص المادة 1/2 وذلك بقولها: "التوقيع الالكتروني بيانات في شكل الكتروني، مرفقة ومرتبطة منطقيا بيانات الكترونية أخرى، تستعمل كوسيلة توثيق القانون 04/15)".

ولم يحدد المشرع الجزائري صورا للتوقيع الالكتروني، بل اكتفى بأن يكون التوقيع في شكل الكتروني فقط أيا كان هذا الشكل، وقد أحسن فعلا كونه فتح المجال أمام الاعتراف بجميع صور التواقيع الالكترونية التي تتمتع بالثقة الكافية وتحقيق وظائف التوقيع هذا من جهة، ومن جهة ثانية هناك نظام مزدوج للتوقيع الالكتروني، العادي والموصوف، هذا الأخير الذي يتمتع بكافة المزايا التي تتمتع بها التوقيع التقليدي ( المادة 8 من القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني)، أما التوقيع الالكتروني فيشبه تعريف التوجيه الأوروبي بشأن التوقيعات الالكتروني [2].

---

[1]- المادة 03 مكرر من المرسوم التنفيذي 162/07 المؤرخ في 30 ماي 2007 ،المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001-30 ماي، 2007 ، المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية )العدد 37.

[2]- رشيدة بوكر، **التوقيع الالكتروني في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر العدد الرابع، ديسمبر 2016،ص67 ، نقلا عن وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري ،جامعة تبسة، مقال في مجلة العلوم القانونية والسياسية ، العدد01، 2020، ص584.

**الفرع الثاني: آلية إنشاء التوقيع الإلكتروني**

حرص المشرع الجزائري على ضمان سلامة التوقيع الإلكتروني وصحته لينتج آثاره القانونية مثل التوقيع التقليدي، وهذا من خلال التحديد الواضح والدقيق لآلية إنشاء التوقيع الإلكتروني التي تتضمن مجموعة من الإجراءات تعبر عن الظروف التي تضمن سلامة التوقيع الإلكتروني وحفظه، كما تعبر عن موثوقية ارتباط معطيات هذا التوقيع بصاحبه، مما يكسبه حجية قانونية في الإثبات على غرار التوقيع الكتابي.

ويتعين أن يستجيب التوقيع الإلكتروني المعطيات إنشائه، ونصت على تلك المعطيات المادة (03) مكرر، الفقرة (04) من المرسوم (07-162) لسنة 2007[1] حيث عرفتها بأنها: «العناصر الخاصة بالموقع مثل الأساليب التقنية التي يستخدمها الموقع نفسه لإنشاء التوقيع». .

ولقد فصل القانون رقم (15-04) لسنة 2015[2] في آلية إنشاء التوقيع الإلكتروني من خلال تعريفه لكل من آلية وبيانات إنشاء التوقيع الإلكتروني في الفصل الثاني (تعريفات لاسيما المادة (02) منه، إذ عزفت الفقرة (03) من هذه المادة بيانات إنشاء التوقيع الإلكتروني على أنها: «بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع». .

وعزفت الفقرة (04) من المادة نفسها آلية إنشاء التوقيع الإلكتروني بكونها: «جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني».

وللتفصيل أكثر في إجراءات إنشاء التوقيع الإلكتروني وآليات ووسائل التحقق منه، أفرد القانون رقم ( 04 - 15 ) لسنة 2015 فصلا كاملا منه بهذا الصدد، حدد من خلاله متطلبات إنشاء التوقيع الإلكتروني بصفة مؤمنة، ومن ثم تحديد متطلبات الآلية الموثوقة للتحقق من التوقيع الإلكتروني.

---

[1]- المرسوم التنفيذي رقم 07-162 المؤرخ في 30-05-2007 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 الصادر في 09-05-2001.

[2]- القانون رقم 15-04 المؤرخ في 01-02-2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06.

**أولا- متطلبات آلية إنشاء التوقيع الإلكتروني:**

ركزت المادة 10 من القانون رقم (15-04) لسنة 2015 على ضرورة أن تكون آلية إنشاء التوقيع الإلكتروني مؤمنة، حيث جاء فيها: «يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة»..

ووضع المشرع الجزائري مجموعة من المتطلبات التي تضمن لآلية إنشاء التوقيع الإلكتروني أن تكون مؤمنة، تم تحديدها بنص المادة (11) من هذا القانون، والتي جاء فيها أن: «الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني تتوفر فيها المتطلبات الآتية:

1-يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج، وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد

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

2- يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع.

من خلال هذه المتطلبات التي وضعها المشرع الجزائري، تستخلص اشتراطه سرية بيانات إنشاء التوقيع الإلكتروني، وهو ما يمكن أن يشكل ضمانة لحفظها من أخطار التحريف أو التزوير أو استعمالها من قبل شخص آخر غير صاحب التوقيع.

وفي هذا الصدد يبدو أن المشرع استنبط هذه المتطلبات من التشريع الفرنسي الذي اشترط بدوره سرية معطيات إنشاء التوقيع الإلكتروني بنص المادة (3-1) من المرسوم رقم (2001-272) المؤرخ في2001/03/30[1].

**ثانيا- متطلبات آلية التحقق من التوقيع الإلكتروني:**

على غرار تأكيد المشرع الجزائري على ضرورة توفير المتطلبات والشروط التي تجعل من آلية إنشاء التوقيع الإلكتروني آلية مؤمنة، اشترط في الوقت نفسه متطلبات للتحقق من التوقيع الإلكتروني لضمان موثوقيته.

حيث نصت المادة 12 من القانون رقم (15-04) لسنة 2015 على أنه: «يجب أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة».

ولخصت المادة 13 من القانون نفسه المتطلبات الكفيلة بتحقيق هذه الموثوقية، حين نصت على أن: الآلية الموثوقة للتحقق من التوقيع الإلكتروني هي آلية تتوفر فيها المتطلبات الآتية:

1-أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الإلكتروني

2-أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة، وأن تكون نتيجة هذا التحقق معروض عرضا صحيحا.

3-أن يكون مضمون البيانات الموقعة إذا اقتضى الأمر محددا بصفة مؤكدة عند التحقق من التوقيع الإلكتروني

4-أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الإلكتروني المطلوبة عند التحق من التوقيع الإلكتروني.

5-أن يتم عرض نتيجة التحقق وهوية الموقع بطريقة واضحة وصريحة.

ولقد أسند المشرع الجزائري إجراءات التأكد من تطبيق الآلية المؤمنة لإنشاء التوقيع الإلكتروني، والآلية المؤمنة للتحقق منه مع المتطلبات التي جاءت في المادتين (11-13)

[1]- نقلا عن ياسمينة كواشي، مرجع سابق، ص10.

المذكورتين سابقا إلى هيئة وطنية مكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه.

بعد تعريف التوقيع الإلكتروني في الفقه القانوني والتشريعات الدولية والإقليمية وكذلك في التشريع الجزائري، يبدو أنه يأخذ أشكالا وصورا متعددة أفرزتها ثورة المعلومات وتكنولوجيا الاتصال في إطار التوجه نحو الاستجابة المستمرة للتطورات الحاصلة في ميدان التجارة والمعاملات الإلكترونية.

**المطلب الثاني : خصائص التوقيع الإلكتروني.**

بالنظر إلى الطبيعة الخاصة للتوقيع الإلكتروني جعل منه مفهوما يتمتع بخصائص نذكر من بينها :

**1 -الشكل الإلكتروني للتوقيع:**

تشكل هذه الخاصية نقطة اختلاف مهمة بين التوقيع التقليدي والإلكتروني، حيث أن التوقيع الإلكتروني يعتمد بالأساس على دعامة إلكترونية ذات قدرات كهرومغناطسية أو لاسلكية[1] أو ضوئية في تبادل وتخزين المعلومات[2] والتي تمس مجالات الحياة أكثر بكثير من التي يشملها التوقيع اليدوي الذي يعتمد على دعامة ورقية يكتبها الموقع يدويا .

**2 -نشأة ووجود التوقيع في بيئة إلكترونية:**

حيث يعتمد التوقيع الإلكتروني في نشأته على وجود مجموعة متكاملة من الأجهزة أهمها جهاز الحاسوب الذي يعتبر همزة وصل بين إنشاء التوقيع وضمان استمراريته في إطار الشبكة[3] ، ضف إلى ذلك السرعة والسرية التي يوفرها التوقيع الالكتروني في المعاملات.

---

[1]- سادات محمد محمد، **خصوصية التوقيع الإلكتروني**، دار الفكر والقانون، مصر، 2011 ،ص. 103.

[2]- نقلا عن ياسمينة كواشي ، **مرجع سابق**، ص15.

[3]- ديلمي جمال، **الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر**، مذكرة لنيل شهادة الماجستير في القانون الخاص، فرع قانون العقود، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2017 ،ص 11

**ثالثا: أنواع التوقيع الإلكتروني.**

يختلف التوقيع الإلكتروني حسب الوسيلة التي استخدمت لإنشائه، كما تختلف كل صورة أو كل نوع عن الآخر حسب الوظيفة التي يؤديها كل صنف من التوقيعات الإلكترونية وتتمثل هذه الأنواع في النقاط التالية :

**1) التوقيع الرقمي:**

يعد هذا النوع من التوقيعات الإلكترونية عبارة عن أرقام مطبوعة لمحتوى الرسالة الإلكترونية مشكلا في النهاية توقيعا إلكترونيا، كما يتميز باستخدام مفتاح للتشفير يمكنه من تحويل الأرقام والرموز التي تكون التوقيع إلى معادلات ورموز غير واضحة ولا مقروءة إلا من طرف أصحاب الشأن في العلاقة القانونية [1] ، تستعمل هذه الصورة على وجه الخصوص في المعاملات البنكية ومعاملات الشركات [2].

**2) التوقيع بالقلم الإلكتروني:**

يقوم الموقع في هذه الصورة بوضع توقيعه باستخدام قلم ضوئي خاص يكتب على شاشة جهاز الحاسوب المزود ببرنامج يلتقط التوقيع ويتحقق من صحته استنادا إلى حركة القلم والأشكال التي يرسمها ثم يتم نقله (التوقيع الإلكتروني) إلى جهاز الماسح الضوئي ( Scanner) ليتم نقل الصورة إلى المحرر المراد توقيعه إلكترونيا [3] ، تتميز هذه الصورة بالمرونة إلا أنه أكثر عرضة للتزوير على أساس أن أصحاب الخبرة من مجرمي المعلوماتية

[1]- نصر محمد محمد، **الدليل الإلكتروني وحجيته أمام القضاء**، دار الكتب العلمية، لبنان، 2013 ،ص. 74

[2]- ديلمي جمال،**مرجع سابق**، ص19.

[3]- نصر محمد محمد، **مرجع سابق**، ص69-70، كواشي نقلا عن كشابية زهرة، صايفي غانية، تزوير التوقيع الالكتروني، مذكرة ماستر في القانون، جامعة مولود معمري تيزي وزو ، 2017، ،ص11.

بإمكانهم بسهولة اختراق التوقيع لذا فيرى الفقه أن هذه الصورة لا تحقق الأمن الكافي للتوقيع [1].

**3-التوقيع البيومتري:**

يعتمد هذا النوع على الحواس الذاتية للموقع مثل بصمة الأصبع، حدقة العين، نبرة الصوت... وتتم العملية بأخذ مسحة عن البصمة أو حدقة العين وتخزينها في جهاز الحاسب الآلي وتشفيرها أي حمايتها من الإعتداء من قبل الغير، وبالرغم من تكلفة هذه التقنية الباهظة إلا أنها لا توفر الحماية المطلوبة للتوقيع الإلكتروني [2]إذ أن هذه الحواس قابلة لتغيير بفعل الحوادث فمثلا بصمة الأصبع قد تختفي كليا بفعل حريق قد يتعرض له الموقع.

**4-التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السري:**

تعتمد هذه الصورة امتلاك الموقع لجهاز حاسوب متصل بشبكة الأنترنت ولكن الشيء الجيد فيها هو أنها لا تتطلب توفر الخبرة للحصول على هذا النوع من التوقيعات .تجدر الإشارة إلى أن هذا التوقيع شائع جدا خاصة في المعاملات البنكية، يكون مرفوقا برقم سري يشمل أرقام، حروف، رموز بحوزة العملاء تمكنهم من سحب وإيداع النقود وتسديد ثمن السلع والخدمات[3] ، يقوم الموقع بإدخال رقم سري خاص به في فتحة جهاز الصراف الآلي، فإذا كان الرقم السري صحيحا تظهر بيانات في شاشة الجهاز توجه الموقع إلى تحديد مبلغ السلعة أو الخدمة وهكذا [4].

---

[1]- ديلمي جمال،**مرجع سابق**، ص20.

[2]- لملوم كريم، **الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية**، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، 2011/02/14 ،ص-126. . 125.ص

[3]- لالوش راضية، **أمن التوقيع الإلكتروني**، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012/09/23 ،ص. 40 وما يليها

[4]-نصر محمد محمد، **مرجع سابق**، ص83.

**ثالثا: صور التوقيع الإلكتروني.**

يختلف التوقيع الإلكتروني حسب الوسيلة التي استخدمت لإنشائه، كما تختلف كل صورة أو كل نوع عن الآخر حسب الوظيفة التي يؤديها كل صنف من التوقيعات الإلكترونية وتتمثل هذه الأنواع في النقاط التالية :

**3) التوقيع الرقمي:**

يعد هذا النوع من التوقيعات الإلكترونية عبارة عن أرقام مطبوعة لمحتوى الرسالة الإلكترونية مشكلا في النهاية توقيعا إلكترونيا، كما يتميز باستخدام مفتاح للتشفير يمكنه من تحويل الأرقام والرموز التي تكون التوقيع إلى معادلات ورموز غير واضحة ولا مقروءة إلا من طرف أصحاب الشأن في العلاقة القانونية [1] ، تستعمل هذه الصورة على وجه الخصوص في المعاملات البنكية ومعاملات الشركات [2].

**4) التوقيع بالقلم الإلكتروني:**

يقوم الموقع في هذه الصورة بوضع توقيعه باستخدام قلم ضوئي خاص يكتب على شاشة جهاز الحاسوب المزود ببرنامج يلتقط التوقيع ويتحقق من صحته استنادا إلى حركة القلم والأشكال التي يرسمها ثم يتم نقله (التوقيع الإلكتروني) إلى جهاز الماسح الضوئي ( Scanner) ليتم نقل الصورة إلى المحرر المراد توقيعه إلكترونيا [3] ، تتميز هذه الصورة بالمرونة إلا أنه أكثر عرضة للتزوير على أساس أن أصحاب الخبرة من مجرمي المعلوماتية بإمكانهم بسهولة اختراق التوقيع لذا فيرى الفقه أن هذه الصورة لا تحقق الأمن الكافي للتوقيع [4].

---

[1]- نصر محمد محمد، **الدليل الإلكتروني وحجيته أمام القضاء**، دار الكتب العلمية، لبنان، 2013 ،ص. 74

[2]- ديلمي جمال،**مرجع سابق**، ص19.

[3]- نصر محمد محمد، مرجع سابق، ص69-70.

[4]- ديلمي جمال،**مرجع سابق**، ص20.

**5-التوقيع البيومتري:**

يعتمد هذا النوع على الحواس الذاتية للموقع مثل بصمة الأصبع، حدقة العين، نبرة الصوت... وتتم العملية بأخذ مسحة عن البصمة أو حدقة العين وتخزينها في جهاز الحاسب الآلي وتشفيرها أي حمايتها من الإعتداء من قبل الغير، وبالرغم من تكلفة هذه التقنية الباهظة إلا أنها لا توفر الحماية المطلوبة للتوقيع الإلكتروني [1]إذ أن هذه الحواس قابلة لتغيير بفعل الحوادث فمثلا بصمة الأصبع قد تختفي كليا بفعل حريق قد يتعرض له الموقع.

**6-التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السري:**

تعتمد هذه الصورة امتلاك الموقع لجهاز حاسوب متصل بشبكة الأنترنت ولكن الشيء الجيد فيها هو أنها لا تتطلب توفر الخبرة للحصول على هذا النوع من التوقيعات .تجدر الإشارة إلى أن هذا التوقيع شائع جدا خاصة في المعاملات البنكية، يكون مرفوقا برقم سري يشمل أرقام، حروف، رموز بحوزة العملاء تمكنهم من سحب وإيداع النقود وتسديد ثمن السلع والخدمات[2] ، يقوم الموقع بإدخال رقم سري خاص به في فتحة جهاز الصراف الآلي، فإذا كان الرقم السري صحيحا تظهر بيانات في شاشة الجهاز توجه الموقع إلى تحديد مبلغ السلعة أو الخدمة وهكذا [3].

[1]- لملوم كريم ، **مرجع سابق** ،ص125-126.

[2]- لالوش راضية، **مرجع سابق**،ص43.

[3]- نصر محمد محمد، **مرجع سابق**، ص83.

## المبحث الثاني: حجية وشروط التوقيع الالكتروني

سوف نتطرق في هذا المبحث إلى عنصرين مهمين هما حجية التوقيع الالكتروني في الإثبات ( المطلب الأول ) ، و شروط التوقيع الالكتروني ( المطلب الثاني ).

### المطلب الأول : حجية التوقيع الإلكتروني في الإثبات

اعترفت الدول بحجية التوقيع الإلكتروني من خلال تعديل منظوماتها القانونية سواء على الصعيد الدولي (أولا) أو على الصعيد الداخلي (ثانيا)

#### أولا: حجية التوقيع الإلكتروني في التشريعات الدولية.

بلورت لجنة الأونسيترال مفاهيم التجارة الإلكترونية الصادر في 1996 الذي يعتبر أول قانون يضع اللبنة الأولى للتجارة في العالم الافتراضي بواسطة تكنولوجيات وتقنيات مختلفة عن التجارة التقليدية[1] ، إلا أن هذا القانون وضع الخطوط العريضة فقط ذلك ما استدعى صدور قانون خاص بالتوقيعات الإلكترونية والذي اعتمدت عليه الدول المختلفة في سن قوانين ذات صلة بالتجارة الإلكترونية والتوقيع الإلكتروني خاصة، وباعتبار أن مختلف التشريعات الغربية اعتمدت قانون الأونسيترال فإن قواعدها لا تختلف كثيرا عن قواعد هذا القانون لذلك أخذنا بعض النماذج فقط ويظهر ذلك في القوانين التالية:

##### 1 -قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية ( Uncitral)

جاء في نص المادة 06 من قانون Uncitral النموذجي بشأن التوقيعات الإلكترونية ما يلي: «حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفي بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني يعول عليه بالقدر المناسب للغرض الذي انشئت أو أبلغت من أجله رسالة بيانات في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة»،

[1]- ياسمينة كواشي ، **مرجع سابق**، ص16.

وقد جاء معناها ما ورد في المادة الثامنة من قانون الأنسيترال بشأن التجارة الإلكترونية لاسيما الفقرة (أ) منها [1].

يفهم من خلال قراءة هذا النص [2] أن التوثيق هو شرط لا غنى عنه في إنشاء الإلتزامات عندما يتطلب أو يشترط القانون وجود توقيع على محرر ما يمكن التعويل عليه بقدر يتماشى مع الغرض الذي أنشئت من أجله رسالة البيانات[3].

**2-توجيهات الاتحاد الأوروبي:**

كان القانون النموذجي للتجارة الإلكترونية الصادر عن لجنة الأمم المتحدة سنة 1996 مصدرا اعتمد عليه المشرع الأوروبي في مسألة التوقيع الإلكتروني[4]، وقد قامت لجنة الإتحاد الأوروبي في 07 أكتوبر 1997 بإصدار بيانا أعلنت فيه عن رغبتها في إعداد مشروع متعلق بالتوقيع الإلكتروني وعمليات التشفير وقد كان الهدف الأساسي من وراء ذلك هو توفير الثقة في المعاملات الإلكترونية، لكن قبل هذه المرحلة قامت لجنة الإتحاد الأوروبي بإضفاء نفس القيمة الثبوتية للتوقيع الإلكتروني وقد سوت بذلك بينه وبين التوقيع التقليدي وذلك في التوجيه الذي يحمل رقم 93-1999 لكن لابد أن يكون هذا التوقيع موثوقا، طبقت اللجنة في ذلك نص المادة (06) لأمن لجنة الأونسيترال بشأن التوقيع الإلكتروني [5].

---

[1]- أنظر المادة الثامنة فقرة (أ) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية: «عندما يشترط القانون تقديم المعلومات أو الاحتفاظ بها في شكلها الأصلي، تستوفي رسالة البيانات هذا الشرط إذا( أ) وجد ما يعول عليه لتأكيد سلامة المعلومات منذ الوقت الذي أنشئت فيه للمرة الأولى في شكلها النهائي، بوصفها رسالة بيانات أو غير ذلك...

[2]- أنظر المادة 06 من قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني 2001.

[3]- لالوش راضية، المرجع السابق، ص. 77.

[4]-ثروت عبد الحميد، **التوقيع الإلكتروني (ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيتها في الإثبات)**، دار الجامعة الجديدة، مصر، 2007 ،ص. 157.

[5]- -لملوم كريم، **مرجع سابق**، ص83.

**ثانيا: حجية التوقيع الإلكتروني في الإثبات في التشريعات الداخلية.**

انتقل مفهوم التجارة الإلكترونية بصفة عامة والتوقيع الإلكتروني بصفة خاصة إلى الدول العربية التي نجحت فيها هذه الطريقة الحديثة في الإثبات باعتبار أنها منحت هذا الأخير الحجية في الإثبات مثله مثل التوقيع اليدوي ونذكر من بينها الدول البارزة التي نجحت فيها الطريقة وأين عرفت تطورا مهما. :

1. في قانون دبي.
2. في قانون تونس .
3. في القانون الجزائري.

**1. في قانون دبي.**

قامت إمارة دبي بخطوات واسعة في مجال التجارة الإلكترونية فهي لم تتوقف أمام خلق منطقة حرة للتكنولوجيا التي سميت مدينة دبي للأنترنت والحكومة الإلكترونية بل قامت بإصدار قانون المعاملات الإلكترونية اللذان صدرا سنة 2002 [1]، ومن بين المواضيع التي تضمنها هذا القانون مسألة التوقيع الإلكتروني أين اعترف المشرع في دبي بإضفاء نفس القوة الثبوتية بين التوقيع اليدوي والإلكتروني وهذا ما يستنتج من خلال نص المادة 3/12 من القانون رقم 02 لسنة 2002 [2] وفق الشروط التي أدرجتها لجنة الأمم المتحدة بشأن التوقيعات الإلكترونية [3] ، لا سيما ما ورد في نص المادة (06) من هذا القانون والتي سبق وأن أشرنا إليها.

[1]- فيصل سعد الغريب، **التوقيع الإلكتروني وحجيته في الإثبات**، المنطقة العربية للتنمية الإدارية، الكويت، ص. 255

[2]-المادة 3/12 من قانون المعاملات الإلكترونية في إمارة دبي رقم 02 لسنة 2002

[3]- فيصل سعد الغريب، **المرجع السابق**، ص. 256.

- **في قانون تونس:**

اهتم القانون التونسي هو الآخر بالتوقيع الإلكتروني مثله مثل باقي التشريعات [1] حيث صدر قانون يحمل رقم 83-2000 يتعلق بالمبادلات التي تتم باستعمال الوثائق الإلكترونية، أول محاولة من جانب الحكومة التونسية في إعطاء قيمة لهذا النوع الجديد من المعاملات خاصة بعد النص صراحة على تسليط عقوبة عل كل متعدي على التوقيع الإلكتروني تطبيقا لنص المادة 48 من القانون المذكور أعلاه [2].

**3-في القانون الجزائري.**

حذى المشرع الجزائري حذو التشريعات الأخرى فيما يتعلق بالإعتراف بالتوقيع الإلكتروني وذلك من خلال تعديل ق.م.ج [3] ، حيث جاء في نص المادة 323 مكرر منه ما يلي: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها"، إلا أن هذا النص كان غامضا ولم يتناول أية إشارة صريحة إلى التوقيع الإلكتروني، ثم جاء نص المادة 323 مكرر 1 أين بين المشرع موقفه بصراحة، حيث أعطى للكتابة الإلكترونية نفس لقيمة القانونية التي يعطيها للكتابة الورقية[4].

من هنا بدأ المشرع الجزائري يأخذ بالشكل الإلكتروني في الإثبات حيث سوى بين الوثيقة الإلكترونية والتقليدية في الإثبات، وثاني محاولة من جانب المشرع الجزائري كانت بصدور

---

[1]- فيصل سعد الغريب، **المرجع السابق**، ص. 257، نقلا عن كشابية زهرة، صايفي غانية، مرجع سابق،ص15.

[2]-تنص المادة 48 من قانون 83-2000 على ما يلي : «يعاقب كلمن استعمل بصفة غير مشروعة عناصر لتشفير شخصية متعلقة بإمضاء الغير بالسجن لمدة تتراوح ما بين ستة أشهر وعامين وبغرامة ما بين ألف وعشرة آلاف دينار أو بإحدى هاتين العقوبتين.«

[3]-مولاي حفيظ علوي قادري، **المرجع السابق**، ص01.

[4]-قانون رقم 05-10 ، السالف الذكر

القانون رقم 15-04 أول قانون خاص بالتوقيع والتصديق الإلكترونيين ،[1] حيث نص في المادة 02 من هذا القانون على تعريف التوقيع الإلكتروني كما يلي:

"التوقيع الإلكتروني بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق»؛ وكرس المشرع عدة تقنيات لحماية هذا التوقيع الحديث بل ذهب إلى أبعد من ذلك وكرس عقوبات على الإعتداء عليه خاصة بالتزوير لكن لابد أن يستوفي هذا التوقيع الشروط الوارد ذكرها في المادة 07 من نفس القانون وهي: «التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية :

1- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة،
2- أن يرتبط بالموقع دون سواه،
3- أن يمكن من تحديد هوية الموقع،
4- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني،
5- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع،
6- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات»، هذه الشروط فرضتها كل التشريعات التي أخذت بالتوقيع الإلكتروني في الإثبات وسنتعرض لها بالتفصيل لاحقا.

[1]- تنص المادة 323 مكرر 1 من ق.م.ج على: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

**المطلب الثاني : شروط التوقيع الالكتروني**

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

حيث سنقوم باستعراض شروط التوقيع الإلكتروني في ضوء مجموعة من القوانين والتشريعات إذ اشتملت هذه الشروط على ثلاثة عناصر محورية هي:

- أن يكون التوقيع مميزا لصاحبه
- سيطرة الموقع على التوقيع
- عدم قابلية هذا التوقيع للتعديل أو التغيير.

**الفرع الأول: أن يكون التوقيع مميزا لصاحبه:**

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

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

[1]- آلاء أحمد محمد الحاج علي، **التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني**، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، فلسطين، 2013، ص 49.

[2]- محمد مأمون سليمان، **التحكيم الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2011، ص230

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

- § استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.
- § كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر[1].

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

أما تحديد شروط التوقيع الإلكتروني في التشريعات الوطنية، فهناك قوانين لعدة بلدان تصدت لهذا الموضوع.

حيث نص القانون الأردني للمعاملات الإلكترونية لسنة 2001 في المادة (31) منه على أنه: " إذا تبين نتيجة تطبيق إجراءات التوثيق المستخدمة أنها معتمدة أو مقبولة تجاريا أو متفق عليها بين الأطراف"، فيعتبر التوقيع الإلكتروني موثقا إذا اتصف بالآتي:

- § متميز بشكل فريد بارتباطه بالشخص صاحب العلاقة.
- § كان كافيا للتعريف بشخص صاحبه
- § تم إنشاؤه بوسائل خاصة بالشخص وتحت سيطرته

- ارتبط بالسجل الذي يتعلق به بصورة لا تسمح بإجراء تعديل على القيد بعد توقيعه دون إحداث تغيير في التوقيع[2].

---

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

[2]- نادية ياس البياتي، **التوقيع الإلكتروني عبر الأنترنيت ومنى حجيته في الإثبات**، ط1، دار الهداية ناشرون وموزعون الأردن، 2014، ص188.

كما جاء في قانون التوقيع الإلكتروني المصري في مادته (18) أنه: " يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية":

- § ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- § سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- § إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

وتحدد اللائحة التنفيذية لهذا القانون والضوابط الفنية اللازمة لذلك[1].

أما في المغرب، فقد نص القانون رقم (05-53) المتعلق بالتبادل الإلكتروني للمعطيات القانونية على هذا الشرط في المادة (06) حيث جاء فيها: «يجب أن يستوفي التوقيع الإلكتروني المؤمن المنصوص عليه في الفصل 3-417 من الظهير الشريف (المعتبر بمثابة قانون الالتزامات والعقوبات) الشروط الأتية:

- أن يكون خاصة بالموقع.
- أن يتم إنشاؤه بوسائل يمكن الاحتفاظ بها تحت مراقبته الخاصة بصفة حصرية
- أن يضمن وجود ارتباط بالوثيقة المتصلة به بكيفية تؤدي إلى كشف أي تغيير لاحق أدخل عليها.
- يجب أن يوضع التوقيع بواسطة آلية لإنشاء التوقيع الإلكتروني تكون صلاحيتها مثبتة بشهادة للمطابقة[2].

أما التشريع الجزائري، فقد نص القانون رقم (15-04) لسنة 2015 على هذا الشرط فضلا عن شروط أخرى بنص المادة (07) وتمثلت في:

- § أن ينشأ التوقيع الإلكتروني على أساس شهادة تصديق موثوقة.
- § أن يرتبط بالموقع دون سواه.

---

[1]- سمير عبد السميع الأردن، **العقد الإلكتروني**، منشأة المعارف، مصر، 2005، ص 187.

[2]- ظهير شريف رقم 129-07-01 الصادر في 30-11-2007 بتنفيذ القانون رقم 05-53 المتعلق بالتبادل الإلكتروني المعطيات القانونية، الجريدة الرسمية للملكة المغربية رقم 5584 الصادرة بتاريخ 06-12-2007، ص07.

- أن يكون مصمما بواسطة آلية مؤمنة أو إجراءات تقنية تمكن من التحكم والسيطرة عليه
- أن يكون مرتبطا بالمعلومات الموجودة بالمستند المعلوماتي، بحيث يمكن اكتشاف التغييرات اللاحقة بهذه المعلومات.

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

وعرفت المادة 03 مكرر من المرسوم التنفيذي رقم (07-162) لسنة 2007 الموقع على أنه: شخص طبيعي أو معنوي الذي يمثله ويضع موضع التنفيذ جهاز تنفيذ إنشاء التوقيع الإلكتروني، فالموقع هو دائما شخص طبيعي يوقع إما لمصلحته الخاصة أو لمصلحة غيره، وفي هذه الحالة نكون بصدد التمثيل، فإن الممثل الموقع يكون إما شخصا طبيعيا أو معنويا[1].

**الفرع الثاني: سيطرة الموقع على التوقيع**

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

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

---

[1]- يمينة حوحو، المرجع السابق، ص 188.

[2]- حنان براهيمي ، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه كلية الحقوق لجامعة بسكرة، 2015 ، ص 155.

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

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

بالإضافة إلى ذلك يجب على صاحب التوقيع الإلكتروني أن يمتلك البيانات الخاصة بإنشاء التوقيع الإلكتروني وأن يكون تحت سيطرته، ويجب عليه المحافظة عليه وأن يحرص على عدم وصوله إلى الغير لكي لا يتم التلاعب به والتحريف من أجل تحقيق مصداقية التوقيع الإلكتروني[1] .

كما تجدر الإشارة إلى أن القانون الفرنسي لم يتطرق إلى شروط التوقيع الإلكتروني صراحة، سوى الإشارة إلى أنه إذا كان التوقيع إلكترونيا فيتمثل في استخدام وسيلة آمنة لتحديد هوية الشخص تضمن صلته بالمستند الذي وضع توقيعه عليه، مع سلامة هذا المستد بالشروط التي يحددها مرسوم يصدر من مجلس الدولة[2] .

**الفرع الثالث: عدم قابلية التوقيع الإلكتروني للتعديل أو التغيير**

يقصد بعدم القابلية للتعديل عدم القدرة على التغيير في بيانات المحرر إلا عن طريق إتلافه أو ترك أثر مادي عليه، والحال كذلك فإنه يسهل الكشف عما حدث للمحرر من تغيير، سواء تم ذلك الكشف بمجرد نظر الشخص العادي أو بالاستعانة بأهل الخبرة[3].

---

[1]- إبراهيم إسماعيل الربيع، علاء موسي علي نالي، **التوثيق الإلكتروني قرارات التحكيم في التوقيع الإلكتروني دراسة مقارنة"**، مجلة المحقق الحلي للعلوم القانونية والسياسية، بابل، العراق، العدد رقم 01، 2012 ، ص 161، نقلا عن ياسمينة كواشي، مرجع سابق، ص21.

[2]- إبراهيم إسماعيل الربيع، علاء موسى علي نالي، **المرجع السابق**، ص 163

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

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

إذ يلزم لتحقيق الأمان والثقة في التوقيع الإلكتروني أن تتم كتابة المحرر الإلكتروني والتوقيع عليه باستخدام نظم أو وسائل من شأنها المحافظة على صحة وسلامة المحرر الإلكتروني المشتمل على التوقيع وتضمن سلامته، وتؤدي إلى كشف أي تعديل أو تغيير في بيانات المحرر الإلكتروني الذي تم التوقيع عليه إلكترونيا[1].

ونظرا لارتباط التوقيع الإلكتروني بالكتابة الإلكترونية، فهو أيضا يواجه ذات المخاطر التي تحاصر هذه الكتابة، وهي عدم الثقة والأمان الإمكانية التعديل أو التغيير، ونتيجة لهذا فقد أصبح التوقيع الإلكتروني يشترط فيه عدة مواصفات فنية وتقنية عالية، والتي تجعل من الصعب على الغير تزويره أو تعديله أو التلاعب فيه دون أن يترك أثرا يكشف به هذا التلاعب، وبذلك أصبح التوقيع الإلكتروني متفوقا على التوقيع التقليدي ذاته في هذا المجال من حيث توفير الأمن والثقة بين أطراف العقود[2].

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

[1]- أسامة بن غانم العبيدي، **أحجية التوقيع الإلكتروني في الإنبات، المجلة العربية للدراسات الأمنية والتدريب**، المجلد 28 العدد 56، جامعة نايف للعلوم الأمنية، 2012، ص166.

[2]- محمد مأمون سليمان، المرجع السابق، ص 237

**خلاصة الفصل :**

إن أكثر الوسائل شيوعاً في تأمين المدفوعات الالكترونية هي استعمال تكنولوجيا التشفير مثل الترميز والتوقيعات الالكترونية. والتوقيع الالكتروني هو سلسلة بيانات ملحقة بالرسالة الالكترونية من أجل ضمان صحتها، وتحديد التوقيع، وربط المضمون بالموقع (وتحمي بذلك المتلقي من الغش الذي يقوم به المرسل). ويوفر التوقيع الالكتروني وسائل فاعلة لضمان صحة ونزاهة أيّ مستند خلال فترة سريانه، وقد أكدت أهمية ذلك توصية لجنة الأمم المتحدة الاقتصادية لأوروبا رقم 35 المنشئة للإطار القانوني للنافذة الواحدة للتجارة الدولية.

# الفصل الثاني

# الجرائم الواقعة على التوقيع الإلكتروني وكيفية الحماية منها

**تمهيد :**

لقد فرض التطور التكنولوجيا استخدام التوقيع الالكتروني في المعاملات اليومية، هذا النوع من التوقيع جعل بعض محترفين يحاولون الانتفاع غير المشروع وذلك عن طريق ارتكاب جريمة تزوير التوقيع الإلكتروني بواسطة الحواسيب الالكترونية، فيلحقون أضرارا بالمتعاقدين، ولدراسة هذا الفصل المتمثل في الجرائم الواقعة على التوقيع الالكتروني وكيفية الحماية منها حيث قسمناه إلى مبحثين يتمثلان في :

- **المبحث الأول: الجرائم الواقعة على التوقيع الالكتروني**
- **المبحث الثاني : كيفية الحماية من الجرائم الواقعة على التوقيع الالكتروني**

## المبحث الأول: الجرائم الواقعة على التوقيع الالكتروني

التوقيع الإلكتروني وانطلاقا من أنه مجموعة من البيانات في شكل إلكتروني، فإنه توجد خطورة الاعتداء عليه بجرائم تأخذ أشكالا وصورا متعددة، ونظرا لهذه الخطورة وضعت مختلف التشريعات الدولية والوطنية وسائل حماية جنائية للتوقيع الإلكتروني، وعلى هذا الأساس .

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

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

#### أولا- الركن المادي للجريمة

يتكون الركن المادي لهذه الجريمة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح به[2]، ودائما ما يثار التساؤل بشأن هذا الفعل وكيف يمكن تحديد ما إذا كان الفعل الذي ارتكبه الجاني هو ذاته الفعل المؤثم قانونا[3].

---

[1]- حسام محمد نبيل الشنراقي، **الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني**، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013 ، ص137.

[2]- صالح شنين، **الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، رسالة دكتوراه، جامعة تلمسان، 2013، ص74.

[3]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 141.

**1- فعل الدخول:**

لم تحدد التشريعات المقارنة المقصود بالدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات ويمكن تعريفه بأنه الدخول إلى المعطيات المخزنة داخل نظام الحاسوب دون رضا المسؤول عن هذا النظام[1]"

"لقد رصد الفقه الإنجليزي مشكلةً بشأن تحديد معنى الدخول في القانون حيث تطلب هذا التحديد التمييز بين المشروعية وعدم المشروعية في فعل الدخول، حيث انتهى القانون الإنجليزي لتقرير ضرورة أن يكون الدخول غير مصرح به تطبيقا للمادة (05) من القسم (17) وكذا بين الدخول المباشر من الحاسب الذي يحوي البيانات ومنها بيانات التوقيع الإلكتروني والدخول عن بعد".[2]

وفكرة الدخول وفقا للتشريع الأمريكي تتمثل في مجرد فعل الدخول دون تطلب تحقق الضرر وعلى ذلك فإن الدخول غير المصرح به يتضمن عنصرين هامين هما: عنصر المكان، والذي يتمثل في الدخول إلى النظام أو المرور بداخله، والثاني عنصر الزمان وهو الزمان الذي يستغرقه التواجد داخل نظام المعلومات[3] .

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

وجاء في اتفاقية بودابست (المادة 02) أن: «على كل طرف تبني التدابير التشريعية وغيرها من التدابير حيثما كان ذلك لازما لاعتبار الدخول إلى كل أو جزء من نظام حاسب دون وجه حق جريمة طبقا لقانونه الداخلي إذا ما ارتكب عمدا [4].

---

[1]- ياسمينة كواشي، **مرجع سابق**، 50.

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص143

[3]- **المرجع نفسه**، ص 145

[4]- حنان براهمي، **المرجع السابق**، ص46

وقد يتطلب الطرف الموقع أن يكون الفعل المقترف قد تم بمخالفة تدابير الأمن، وذلك بنية الحصول على بيانات حاسب أو لغاية أخرى غير شريفة أو أن تكون اقترفت نظرا للصلة بنظام حاسب آخر[1] .

أما المشرع الأمريكي فقد قرر في قانون تزييف آليات الدخول والإساءة والاحتيال عبر الحاسب الآلي اعتبار كل دخول غير مصرح به المعلومات في حاسب آلي جناية، أما إذا كان الدخول قاصدا المعلومات مالية أو الثمانية أو انتهاك حرمة حاسب فدرالي فإن الجريمة تعد جنحة، وقد تم تعديل القانون الأمريكي في القسم (1030) عدة مرات وتناول تعليل 1996 الأفعال التي تعد أشكال الاختراق من خلال حاسب مستخدم في مؤسسة مالية أو حكومة أو مؤسسة اقتصادية أو الاتصالات في الولايات المتحدة أو خارجها [2].

ومن بين هذه الأشكال التوصل للدخول بشكل غير مشروع إلى حاسب حكومي، ومن ثم يكشف معلومات يفترض بقاؤها سرية سواء قام المخترق بإنشاء هذه المعلومات لمن لا يملك صلاحية استلامها أو حيازتها [3].

إذ أدان القضاء الأمريكي أحد الأشخاص بتهمة الدخول غير المشروع إلى سجلات المحاكم الاتحادية وهي تحتوي على سجلات إلكترونية خاصة، تضم أحكاما وقرارات ومستندات خاصة بدعاوى غرضت على المحكمة أو صدر فيها قرار ...، حيث أن نظام حفظ هذه المعلومات مفتوح للجمهور، إلا أن حق النسخ أو الإنزال مقيد بسداد مقابل نقدي، لكن الجاني تمكن من تسخ الملايين من الصفحات باستخدام برنامج خاص لوضع ملفات إلكترونية خفية في النظام حتى لا يتم احتساب نفقات النسخ[4].

ويلاحظ في هذا الإطار أن المشرع التونسي استعمل عبارة النفاذ عوضا عن عبارة الدخول، ليؤكد الخاصية المادية لهذه الجريمة، فعبارة الدخول قد يكون لها مدلول مادي في حين أن النفاذ له محلول الحماية، أو عن طريق إدخال برنامج فيروس أو باستخدام الرقم الكودي لشخص آخر أو تجاوز نظام الحماية إذا كان ضعيفا،،،، ويستوي أن يتم الدخول

---

[1]- حنان براهمي، **المرجع السابق** ، ص 46

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص144.

[3]- **المرجع نفسه**، ص 144

[4]- حنان براهمي، المرجع السابق، ص 48

مباشرة أو بطريق غير مباشرة كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلفونية[1].

**2- عدم التصريح بالدخول:**

نصت المادة 23 من القانون 15 لسنة 2004 على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته»[2].

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

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

ب - إذا كان دخول الفاعل لأماكن من النظام لم يصرح له بدخولها"[3].

**ثانيا- الركن المعنوي :**

إن جريمة الدخول غير المصرح به في نظم معلومات التوقيع الإلكتروني من الجرائم العمدية التي يتمثل الركن المعنوي فيها في القصد الجنائي العام بركنيه العلم والإرادة، ولا تتطلب قصدا جنائيا خاصا وذلك لكونها من جرائم الخطر التي يعاقب المشرع فيها على مجرد إتيان الفعل المجرم، وعلى ذلك يعاقب المشرع بعقوبة الجريمة التامة على إتيان الفعل المادي مع توافر القصد الجنائي دون اشتراط تحقق النتيجة المتوخاة من الجريمة "[4].

---

[1]- صالح شنين، **المرجع السابق**، ص 74

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 151.

[3]- **المرجع نفسه**، ص 151.

[4]- صالح شنين، **المرجع السابق**، ص 165.

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

**1- القصد الجنائي العام:**

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

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

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

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

**2- القصد الجنائي الخاص:**

هذا القصد لم نتطلبه التشريعات بوجه عام مثلما تمت الإشارة إلى ذلك سابقا، غير أن بعض التشريعات تطلبته بجوار القصد العام.

---

[1]- عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها الجنائية**، دار الفكر الجامعي، الإسكندرية، 2004، ص 302.

[2]- حسين بن سعيد بن سيف الغافري، **الجرائم الواقعة على التجارة الإلكترونية**، موقع المنشاوي للدراسات والبحوث، سلطنة عمان، 2006، ص18

[3]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 170

[4]- عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها الجنائية ، المرجع السابق**، ص 569.

مثلا نجد أنه في القانون النرويجي تشدد العقوبة إذا ارتكب فعل الدخول غير المصرح به بنية الحصول للفاعل أو لغيره على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الإطلاع على المعلومات التي يحوزها النظام[1].

وفي المملكة المتحدة تضمن قانون إساءة استخدام الحاسبات الآلية في المادة (02) منه تجريم الدخول غير المصرح به متى توافر للفاعل قصد خاص هو نية ارتكاب جريمة لاحقة على هذا الدخول كالسرقة أو النصب أو غيرها [2]

**المطلب الثاني: الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية**

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

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

**أولا- تعريف الاحتيال التقليدي والإلكتروني**

**1- الاحتيال التقليدي:**

يعرف الاحتيال على أنه: «الاستيلاء على مال مملوك للغير بخداعه وحمله على تسليم ذلك المال[3]»

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

---

[1]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص173

[2]- **المرجع نفسه**، ص173

[3]- حنان براهمي، **المرجع السابق**، ص 57

[4]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 182

والمشرع المصري لم يعرف الاحتيال في القانون، وإنما الذي عرفه هو الفقه حيث ذهب بعض الفقه إلى أله: «كل سلوك ينطوي على خداع المجني عليه بغرض الاستيلاء على أمواله، وهو ما سيفترض إتيان الجاني أسلوبا من أساليب الاحتيال ويعد وفقا لهذا التعريف إحدى عناصر الركن المادي لجريمة النصب»[1].

و المشرع الأردني لم يورد تعريفا للاحتيال، فعرفه الفقه على أنه «استيلاء على مال مملوك للغير باستعمال وسائل الخداع التي تؤدي إلى إيقاع المجني عليه في الغلط فيقوم بتسليم المال الذي في حيازته»؛

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

**2- الاحتيال الإلكتروني (المعلوماتي):**

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

وعرف مكتب التحقيقات الفدرالي الأمريكي الاحتيال عبر الأنترنيت بأنه: «أي مخطط احتيالي عبر الانترنيت، يلعب دورا هاما في عرض السلع أو الخدمات غير الموجودة أصلا أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة العنكبوتية»: أما وزارة العدل الأمريكية فعرفته بأنه: «شكل من التخطيط الاحتيالي الذي يستخدم محتويات الأنترنيت مثل الدردشة

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

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 186

والبريد الإلكتروني والمواقع الإلكترونية لتقديم صفقات احتيالية أو لإرسال نتائج الاحتيال إلى المؤسسات المالية»[1] .

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

**ثانيا: الركن المادي:**

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

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.

**1 - الوسائل الاحتيالية**

هناك خلاف فقهي بشان تطبيق النص التقليدي للاحتيال على الاحتيال في مجال المعلومات ومدى إمكانية تصور الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط، انطلاقا من أن السائد قانونا وفقها أن السلوك الاحتيالي ينبغي أن يقع على شخص طبيعي[4]؛

وعلى أساس هذا الخلاف الفقهي، تنوعت الوسائل الاحتيالية المستخدمة من قبل مرتكبي الجرائم المعلوماتية بتطور استخدامات الحواسيب، وتضمنت الوسائل الاحتيالية في جريمة

---

[1]- حنان براهمي، **المرجع السابق**، ص ص 57، 58

[2]- **المرجع نفسه**، ص59.

[3]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 184

[4]- حنان براهمي، **المرجع السابق**، ص58

النصب التقليدية عدة وسائل اشترط المشرع توافرها لكي يبلغ الجرم المرتكب مبلغ الاحتيال وهي:

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

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

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

**2- تسليم معلومات التوقيع الإلكتروني (النتيجة الجرمية)**

في مجال المعلومات الإلكترونية يقوم الحاسب الآلي بفعل التسليم بالمفهوم المادي للكلمة، كما أن التسليم يجب ألا ينظر إليه في الشكل المادي فقط وإنما هو عمل قانوني عنصره الجوهري إرادة المجني عليه المعيبة بالخداع وليست المناولة المادية سوى مظهره المادي أو أثره[3] .

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

**3- علاقة السببية بين طرق الاحتيال وتسليم المعلومات:**

لا يكفي لقيام جريمة الاحتيال التامة أن يصدر من الجاني فعل الاحتيال، وأن يسلم المجني عليه الشيء المملوك له إلى هذا الجاني، بل يلزم أن تتوفر صلة ما بين فعل

---

[1]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 190.

[2]- محمد هشام صالح عبد الفتاح، **المرجع السابق**، ص 19.

[3]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 184

الاحتيال وتسليم الشيء المملوك وأن يكون الثاني ثمرة أو نتيجة للأول [1]، بمعنى لابد من توافر علاقة سببية ما بين فعل الاحتيال وفعل التسليم.

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

كذلك ليتمكن من الاستيلاء على معلومات ذات قيمة مادية بدون حق، فالوسائل الاحتمالية التي قام بها الجانى تربط بينها وتسليم المعلومات (المال) الذي حصل عليه علاقة سببية، فلولا هذه الوسائل الاحتيالية لما حدث تسليم للمعلومات، ولما وقع المجني عليه سواء كان شخصا طبيعيا أو نظام معلوماتي في الغلط المفضي إلى تسليم معلومات للجاني[2]

**ثالثا - الركن المعنوي**

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

**1- القصد الجنائي العام**

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

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

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 214

**2- القصد الجنائي الخاص:**

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

أما الاحتيال على نظم معلومات التوقيع الإلكتروني فهي جريمة عمدية تتطلب توافر إرادة ارتكابها مع العلم بكون الفعل المراد ارتكابه مؤثم قانونا ومع ذلك تتجه نية الجاني لارتكابه، إذ أن الجاني يجب أن يكون عالما بان التلاعب الذي يرتكبه في النظام المعلوماتي للتوقيع الإلكتروني أو المعلومات التي يقوم بالتحايل على الحاسب الآلي بإدخالها إليه، فيجعله يستجيب لما يريده، ويسلمه المعلومات التي يرغب في الحصول عليها، هو فعل مجرم قانونا[1] .

إذا في إطار معلومات التوقيع الإلكتروني، فإنه يجب أن تتجه إرادة الجائي إلى تحقيق ربح غير مشروع له أو لغيره، وهو ما فسرئه المذكرة التفسيرية لاتفاقية بودابست الموقعة في 23-11-2001 بأن جريمة الاحتيال في مجال المعلومات تتطلب بالإضافة للقصد العام قصدا خاصا يتمثل في نية الغش أو نية الغش خاصة، أو بتعبير آخر نية غير آمنة أو غير شريفة بغرض الحصول على منفعة اقتصادية لشخص الجاني أو لغيره[2].

**المطلب الثالث: أركان جريمة التزوير المعلوماتي وتجريمها**

تقوم الجريمة سواء كانت تقليدية أو مستحدثة على مجموعة من الأركان، وترتبط بها في الوجود والعدم، هذه الأركان تلعب دور هام وفعال في تحديد الأفعال والنظر في العقوبة التي يجب تطبيقها بشأنها، وبالتالي فإن العقوبة تختلف حسب درجة جسامة الجريمة وعليه سوف

[1]- أسامة بن غانم العبيدي، **حجية التوقيع الإلكتروني في الإثبات**"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28 العدد 56 ،جامعة نايف للعلوم الأمنية، 2012 ، ص 365.

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 214

نرى الأركان الخاصة بالجريمة في (فرع أول) ثم العقوبات التي كرسها المشرع لها في القانون بهدف متابعة المجرم (فرع ثان)

**الفرع الأول أركان جريمة التزوير المعلوماتي**

تقوم الجريمة على ثلاث أركان، يترأسها الركن الشرعي الذي إن غاب لا وجود للجريمة، هذا الركن متوفر تقريبا في جميع الجرائم وبما أن المشرع الجزائري أدرج القسم الخاص بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، هذا دليل على توفر هذا الركن كما أنه دليل على وجود الجريمة خاصة إذا توافر الركنين الآخرين اللذان يتمثلان في:

**أولا: الركن المادي.**

هذا الركن في جريمة تزوير التوقيع الالكتروني يتمثل في تغيير الحقيقة الذي من شأنه أن يلحق ضرر بمصلحة الأفراد، بناءا على ذلك فإن هذا الركن يستدعي توفر مجموعة من العناصر [1] وهي :

**1-تغيير الحقيقة :**

يختلف تغيير الحقيقة في التوقيع اليدوي والتوقيع الالكتروني على اعتبار أن هذا الأخير يرد على دعامة مخزنة في نظام معلوماتي ويكون ذلك بصورتين:

- **الصورة الأولى:** عند التلاعب في المعلومات داخل جهاز الحاسوب.
- **الصورة الثانية:** إدخال معلومات خاطئة وتغيير محتوى المحرر

الهدف من الصورتين هو استعمال التوقيع (في المحرر الالكتروني) لما زور من أجله ويتم ذلك بالطرق التالية[2]:

[1]- خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات**، دار الهدى، الجزائر، 2010 ،ص. 134.

[2]- لالوش راضية، **المرجع السابق**، ص. 143.

- **الطريقة الأولى:**

تتم هذه الطريقة بإدخال معلومات بأي وسيلة كانت سواء بصفة مباشرة أو غير مباشرة كأن يقوم موظف في بنك بإدخال رصيد خيالي لعميل في نفس البنك مما ينتج عنه تحويل أموال لحساب آخر [1].

- **الطريقة الثانية:**

التلاعب بالبيانات في مرحلة المعالجة الآلية للمعلومات من خلال برنامج للتلاعب في أنظمة عملها مثلا أن يقوم موظف بنك بالتلاعب بالبرامج البنكية بتغيير بعض الأوامر التي يعمل بها البرنامج [2].

- **الطريقة الثالثة:**

تتم في مرحلة الإخراج المعلوماتي، تكون مرحلة متممة للمرحلتين السابقتين[3].

2-**الضرر:**

وهو عنصر هام لقيام جريمة التزوير يرتبط بها في الوجود والعدم والضرر المقصود هو الضرر المباشر الذي يتمثل في إهدار مصلحة يحميها القانون[4] .

---

[1]- لالوش راضية، **المرجع السابق**، ص. 144.

[2]- **المرجع نفسه**، ص. 145.

[3]- **المرجع نفسه**، ص. 146.

[4]- ساعد مريم، كراش مهدية، **جريمة التزوير في المحررات**، مذكرة لنيل شهادة الماستر في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، 2016/02/04 ،ص. ص . 17؛ 18.

3-**المحور**:

يعتبر هذا العنصر مهما كان نوعه محلا للتزوير لذلك كرس المشرع الحماية الجزائية في حالة المساس به، ويعرف المحرر على أنه مستند يتضمن حروف وعلامات تدل على معنى معين صادر عن شخص يتضمن واقعة من شأنها المساس بالمراكز القانونية [1].

بالإضافة إلى هذه العناصر يجب أن يكون تزوير التوقيع الالكتروني بإحدى الطرق المنصوص عليها في القانون.

**ثانيا: الركن المعنوي.**

يتمحور الركن المعنوي بشكل أساسي حول القصد الجنائي، وخاصة ما تكون هذه الجرائم في الغالب عمدية [2]، هذا الركن عنصر نفسي يرتبط بمدى رغبة الجاني في إحداث 1 ضرر للغير عن طريق تغيير الحقيقة في التوقيع الالكتروني بحيث إذا تخلف هذا العنصر يغيب الركن المعنوي [3].

والقصد الجنائي نوعان عام وخاص، فإذا كان القصد العام هو المذكور في الفقرة أعلاه فإن القصد الخاص يتمحور حول تزوير التوقيع واستعماله فيما زور من أجله[4] .وبالتالي لا يكف أن يكون الجاني على علم بأركان الجريمة التي هو مقدم على ارتكابها بل لابد من توافر القصد الخاص[5].

---

[1]- ساعد مريم، كراش مهدية، **مرجع سابق**، ص10.

[2]- خثير مسعود، **المرجع السابق**، ص. 138.

[3]- **المرجع نفسه**، ص. 139.

[4]- أيمن رمضان محمد محمد، **الحماية الجنائية للتوقيع الإلكتروني**، دار النهضة العربية، مصر، 2011 ، ص. 213

[5]- **المرجع نفسه**، ص. 214

## المبحث الثاني : كيفية الحماية من الجرائم الواقعة على التوقيع الالكتروني

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 التوقيع الالكتروني

تم تناول العقوبات على ثلاثة أصناف حيث سردناها في ثلاثة فروع على التوالي في الفرع الأول تطرقنا إلى عقوبة الجريمة جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني و في الفرع الثاني عقوبة جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية وأخيرا الفرع الثالث عقوبة جريمة التزوير المعلوماتي للتوقيع.

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

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

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

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

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

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

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

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

**الفرع الثاني : عقوبة جريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية**

جاء في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 بنص المادة 23 فقرة هاء على العقاب على التوصل بأي وسيلة للحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني...، بالحبس والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه،

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

[2]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 175

أو بإحدى هاتين العقوبتين، وذلك مع عدم الإخلال | بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر[1].

أما في التشريع السعودي، فقد نص على عقوبة كل الجرائم المتعلقة بالتوقيع الإلكتروني بما فيها جريمة الاحتيال في نظام المعاملات الإلكترونية لسنة 1428هـ والذي جاء فيه: «مع عدم الإخلال بأي عقوبة أشد ينص عليها نظام آخر، يعاقب كل من يرتكب أيا من الأعمال المنصوص عليها في المادة 23 [2] من هذا النظام بغرامة لا تزيد عن خمسة ملايين ريال أو بالسجن مدة لا تزيد عن خمسة سنوات أو بهما معا، ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في الجرائم المتصلة بالتوقيع الإلكتروني[3].

**الفرع الثالث :عقوبة جريمة التزوير المعلوماتي للتوقيع**

في الجرائم المعلوماتية تتفاوت العقوبة حسب درجة جسامة الجريمة والمشرع في ق.ع أورد مجموعة من العقوبات منها سالبة للحرية ومنها غرامات حسب الحالة ومنها ما هو مطبق على الشخص المعنوي والطبيعي[4] .

**أولا: العقوبات الأصلية.**

تختلف العقوبة باختلاف درجة جسامة أثرها، كما تختلف كذلك حسب الشخص مرتكبها وذلك باستقراء المواد 394 مكرر إلى 394 مكرر2 من ق.ع كما يلي:

---

[1]- حسام محمد نبيل الشنراقي، **المرجع السابق**، ص 214

[2]- نصت المادة 23 من نظام المعاملات الإلكترونية السعودي لسنة 1428هـ الفترة 5 آن من جرائم التوقيع الإلكترونية وإنشاء شهادة رقمية أو توقيع إلكتروني أو شهادة تصنيق إلكترونية لغرض احتيالي، والفقرة رقم 8 التي جاء فيها: الدخول على منظومة توقيع إلكتروني لشخص آخر دون تقويض صحيح أو نسخها أو إعادة تكوينها أو الاستيلاء عليها.

[3]- عباس حفصي، **جرائم التزوير الإلكتروني دراسة مقارنة**، رسالة دكتوراه، جامعة أحمد بن بلة، وهران 1، 2015 ص 16

[4]- فضيلة عاقلي، **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 ،تاريخ الإطلاع يوم 25 سبتمبر 2017 على الساعة 05:20 ،ص. 129

**أ-بالنسبة للشخص الطبيعي:**

عقوبة الحبس من شهرين إلى 3 سنوات وغرامة من 50.000 دج إلى 5.000.000 دج لجريمة الدخول والبقاء في منظومة معلوماتية عن طريق الغش، تختلف باختلاف الجريمة

**ب- بالنسبة للشخص المعنوي:**

العقوبة تقدر خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي تطبيقا لما ورد في المادة 394 مكرر4 من ق.ع

**ثانيا: العقوبات التكميلية.**

بالإضافة إلى العقوبات الواردة أعلاه نجد أن هناك عقوبات أخرى تكميلية وهي[1]:

**للشخص الطبيعي والمعنوي:**

تتمثل في مصادرة الأجهزة المستعملة في القيام بالجريمة، إغلاق المواقع، إغلاق مكان الاستغلال أو المحل إن وجد 1تطبيقا لما ورد في المادة 394 مكرر6 من ق.ع.

**المطلب الثاني : أساليب وآليات الحماية من جريمة التوقيع الالكتروني**

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[2].

[1]- فضيلة عاقلي، **مرجع سابق**، ص129.

[2]- الحميد محمد دباس ، **حماية أنظمة المعلومات**، الأردن، دار الحامد للنشر والتوزيع، 2017، ص37، نقلا عن وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري ،جامعة تبسة، مقال في مجلة العلوم القانونية والسياسية ، العدد01، 2020، ص595.

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 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[1] .

**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" [2].

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 تشفيير عمومي".

---

[1]- وسيم شفيق الحجار، **الإثبات الالكتروني**، لبنان، منشورات الحلبي الحقوقية، 2002، ص198 ، نقلا عن وفاء صدراتي، مرجع سابق، ص596.

[2]- سلطان عبد هللا محمود الجواري. **عقود التجارة الالكترونية**. الأردن: دار الثقافة للنشر والتوزيع، 2010، ص202.

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].

**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:

1- مشروعية 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].

2- الحق في الحفاظ على سرية البيانات والمعلومات المشفرة: اعتبر المشرع الجزائري من خلال القانون 15-04 (42 و 1/11 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 [3].

---

[1]- سمير حامد عبد العزيز الجمال، **التعاقد عبر تقنيات الاتصال الحديثة**. مصر: دار النهضة العربية، 2006، ص219.

[2]- محمد عقوني. **الآليات التقنية والقانونية لحماية التوقيع الالكتروني**. مجلة المفكر (18) ، 2019،ص304.

[3]- محمد عقوني، **مرجع سابق**، ص305.

كما أقر المشرع الجزائري نصوصا تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة وإفشائها سواء من طرف الغير، أو من طرف مؤدي خدمات التصديق الالكتروني، أو من طرف الشخص المكلف بالتدقيق.

3- اعتبار النص المشفر محررا الكترونيا حيث اعتبر المشرع الجزائري النص المشفر من المحررات الالكترونية بالرغم من أنها غير مفهومة للعامة، وبالتالي فإنه يتم تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من يخالف ما التزم به طرفا الاتفاق.

**ب. طرق التشفير:**

يمكن تصنيف طرق التشفير إلى فئتين رئيسيتين بالنظر إلى نوعية المفتاح المستخدم في التشفير:

1) **التشفير المتماثل:** يتم في هذا المستوى تشفير جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال، ويتم عن طريق الشبكات الافتراضية الخاصة، وهي شبكات جزئية من شبكة الانترنت تقوم فيه إحدى المنشآت أو المشروعات بتخصيصه لخدمتها عن طريق إحاطته بالاحتياطات التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله بشكل آمن .

يطلق على هذه الطريقة تقنية المفتاح الخصوصي، كونها تعمل بواسطة مفتاح واحد خصوصي يمتلكه كل من مرسل الرسالة ومتلقيها، وهذا ما يعاب على هذه التقنية، إذ أن استعمال هذا المفتاح من قبل شخصين مختلفين (المرسل والمرسل إليه) فد يضعف من حجية المستندات الرقمية والتوقيع الالكتروني وقوتها الثبوتية[1] .

2) **التشفير غير المتماثل:** يطلق على هذه التقنية التشفير بالمفتاح العمومي وخلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث يستعمل مفتاحين سريين مختلفين من أجل فك تشفيرها، الأول خصوصي يمتلكه مستخدم معين لمستعمل الوسائط الالكترونية ويبقيه سريا وخاصا به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منهم .

[1]- محمد عقوني، **مرجع سابق**، ص305 ،نقلا عن وفاء صدراتي، **مرجع سابق**، ص597.

**الفرع الثاني: التصديق الالكتروني**

إزاء تنامي مخاطر القرصنة الالكترونية وإساءة استخدام الغير، استوجب الأمر توفير الوسائل التي تكفل تحديد هوية المتعاقدين والتعبير عن إرادتهم على نحو صحيح ثم الاستعانة بطرف ثالث محايد موثوق به، يتمثل في جهة مختصة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الالكترونية بإصدار شهادة تسعى بشهادة التصديق الالكتروني

وبناء على ما سبق سنحاول التطرق إلى تعريف التصديق الالكتروني، ودور الجهة المختصة بإصدار شهادات التصديق في إضفاء الحماية على التوقيع الالكتروني.

**أولا: تعريف التصديق الالكتروني**

التصديق الالكتروني آلية تهدف إلى بناء الثقة في نظام الشهادات الرقمية وتشجيع المعاملات الالكترونية بإضفاء المصداقية عليها، فالتصديق بمعناه العام يعني التوثيق والاعتماد ومجاله الطبيعي هو التصرفات القانونية في شكلها التقليدي أي السندات الورقية حيث على الموظف التأكيد والتصديق على صحة ما ورد في المحرر المقدم للتصديق وصحة نسبته إلى من وقع عليه، وبالتالي فالتصديق الالكتروني يعني تدخل طرف ثالث لتأمين التبادل الالكتروني وللمعطيات في المجال الالكتروني التحقيق السلامة والثقة في المعاملات الالكترونية [1].

وبعد التصديق أو التوثيق الالكتروني وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر، حيث بنم نسبته إلى شخص معين أو جهة معينة أو طرف محايد يطلق عليه مقدم خدمات التصديق أو مورد خدمات التصديق أو جهة التوثيق.

ولم يعرف المشرع الجزائري التصديق الالكتروني ولكنه عرف شهادة التصديق الالكتروني وهذا من خلال المادة 02 من القانون 04/15 بأنها وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقيق من التوقيع الالكتروني والموقع.

[1]- غزالي نزيهة،**الآليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري**. مجلة البحوث السياسية والإدارية،2017، ص 291.

**ثانيا: 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 11/02 من القانون 04/15 ) 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.

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:

[1]- فواز المطالقة محمد، **الوجيز في عقود التجارة الالكترونية (الإصدار 2 )**، الأردن: دار الثقافة للنشر والتوزيع، 2008، ص173، نقلا عن وفاء صدراتي، **مرجع سابق**، ص598.

**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 162/07 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 11/2 من القانون 04/15 المحدد للقواعد الخاصة بالتوقيع والتصديق الالكترونيين).

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 [1].

**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

[1]- محمد عقوني، **مرجع سابق**، ص309 ،نقلا عن وفاء صدراتي، **مرجع سابق**، ص599.

للتوقيع المتعلق بشهادة التصديق الالكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الالكتروني .

**ج- إثبات مضمون التبادل الالكتروني**

تقوم الجهة المختصة بإصدار شهادات التصديق الالكتروني كذلك بالتحقق من مضمون التعامل أو التبادل الالكتروني بين الأطراف المتعاقدة، وكذلك التيقن من سلامته وجديته وبعده عن الغش والاحتيال، إضافة إلى إثبات ومضمونه، حماية للمتعاملين من أي غش قد يقعون فيه أثناء تعاملاتهم[1].

وفد نص المشرع الجزائري على أن يلغي خدمات التصديق الالكتروني الموصوفة عندما يتبين أنه قد تم منحها بناء على معلومات خاطئة أو مزورة أو إذا أصبحت المعلومات الواردة في شهادة التصديق الالكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع (المادة 45 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين).

**د- إصدار المفاتيح الالكترونية**

تقوم جهات التصديق الالكتروني بإصدار مفاتيح التشفير الالكتروني، سواء المفتاح الخاص الذي من خلال يتم تشفير المعاملة الالكترونية الذي يكون خاصا بصاحبه ولا بعلمه غيره، أهم المفتاح العام الذي يتم بواسطته فك هذه الشفرة، كما تتولى المصادقة على هوية الحائز على المفتاح العمومي وإصدار شهادات الكترونية من شأنها أن تضمن بأن المفتاح العمومي العائدة إلى الجهة الحائزة على المفتاح الخصوصي، ومن ثم استخدام المفتاح العام الفك تشفير الرسالة الأصلية والتأكد من عدم حصول أي تعديل عليها [2].

---

[1]- الدسوقي أبو الليل، **توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور**، مؤتمر الأعمال المصرفية الالكترونية. المجلد الخامس، صفحة 178 .جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون،(نقلا عن وفاء صدراتي، **مرجع سابق**، ص599).

[2]- محمد عقوني، **مرجع سابق**، ص310 .

**خلاصة الفصل :**

يشكل توفير المشرع الجزائري لوسائل الحماية الجنائية للتوقيع الإلكتروني في قانون خاص به، توجها نحو مسايرة التغيرات التي تشهدها بيئة التعاملات الإلكترونية على الصعيد الدولي والعمل على خلق بيئة إلكترونية آمنة وموثوقة، تعزيزا لاستعمال الوسائل التكنولوجية المعاصرة وتوجيهها نحو المساهمة الفعالة في ترقية التجارة الإلكترونية ومختلف الأنشطة الاقتصادية والاجتماعية بما ينعكس على مستوى التنمية المحلية.

# الخاتمة

## الخاتمة

و في ختام دراسة موضوعنا المتمحور حول جرائم الاعتداء الالكتروني الذي يكون محل التزوير الذي نظمته لجنة الأمم المتحدة من خلال ما تم عرضه توصلنا إلى أنه بالرغم من صدور قانون 04/15 المتعلقة بالتصديق والتوقيع الإلكتروني، وبالرغم من مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم الانترنت، واعتراف المشرع في القانون المدني المعدل سنة 2005 لإمكانية الإثبات بواسطة مستندات موقعة إلكترونيا، فإن المشرع لم ينص على جريمة تزوير التوقيع الإلكتروني، ولا يمكن تطبيق على جريمة تزوير التقليدي لاختلاف محل الجريمة، كما لا يمكن تطبيق النصوص جرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لاختلاف المصلحة المحمية بينها وبين جريمة تزوير التوقيع الإلكتروني، ناهيك عن حظر القياس في القانون الجنائي.

وعليه توصلنا إلى مجموعة من النتائج، هذه النتائج جاءت بالنظر إلى آثار التوقيع الإلكتروني في حياة الأفراد سواءا العملية أو الشخصية ومن بين النتائج التي توصلنا إليها:

- ظهور التوقيع الالكتروني ساهم في تقليص المعاملات التجارية خاصة عبر العالم من خلال ما يسمى بالتجارة الالكترونية، مجال جديد اكتسب مفهوم واسع وبعد عالمي وأصبح بديلا إن صح التعبير للتجارة التقليدية خاصة في الدولة أين عرفت فيها التجارة الإلكترونية انتشارا واسعا .
- أسفر التوقيع الالكتروني عن جانب مظلم ومستتر يسمى بالجريمة الالكترونية، هذا النوع الجديد من الإجرام هو الآخر انتشر في العالم بسبب الاستعمال السيء لبوادر التكنولوجيا من طرف أشخاص محترفين وذات خبرة عالية وكفاءات خارقة في مجال الإلكترونيك، هذه الجرائم لا تمس بالنفس والأموال ولكنها تتعدى حتى إلى حياة الأفراد الشخصية
- بذلت جهود كبيرة لمحاربة الجريمة الإلكترونية بكافة أشكالها، لكن لتميز هذه الجرائم وعدم تقليديتها، من الصعب الكشف عنها وتحديد الدليل المادي الذي يدين مرتكبها.

لذلك من المتوقع أن هذا النوع من الجرائم سيستمر ويطغى على ساحة الإجرام بقَدْرٍ كبير، وسيتطور مع مرور الوقت إلى ما هو أخطر وأعقد. لذا فإن وجود إستراتيجية فعالة لدى الدول تحارب هذه الجرائم هي الوسيلة الضامنة لتقليلها ومحاولة التحكم بها. ولا ننسى دور الأفراد في محاربتها عن طريق تبصيرهم بإيجابيات وسلبيات استخدام شبكة الإنترنت، وحث الشركات المتخصصة على إنتاج برامج حماية متخصصة تهدف إلى حماية البرامج الأخرى ومتصفحات الإنترنت.

- ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير والكثير من أمور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحواسيب والشبكة العنكبوتية ، مما جعل الحكومات والمجتمعات تنتبه إلى ضرورة نشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها .
- بهدف حماية التوقيع الالكتروني كرس المشرع عدة آليات لحماية التوقيع الالكتروني منها تقنية ومنها وقائية إلا أنه وبالرغم من تكريسها فإن التزوير يقع بطريقة أو بأخرى أي أن الحماية موجودة لكن غير كافية.

وفي الأخير وبعد الاستنتاجات التي استنتجناها من دراستنا لهذا البحث قمنا بطرح بعض التوصيات التي تكمن في

**الاقتراحات :**

- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الانترنت ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.
- العمل علي تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية.

- إنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.
- حث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة الجرائم المعلوماتية.

# قائمة المراجع والمصادر

**قائمة المراجع والمصادر:**

## I- المراجع باللغة العربية:

**أولا : المواد والقوانين والمراسيم**


1) المادة 1/323 قانون رقم 97 ـ 1159 المؤرخ في 19 ديسمبر 1997 المتضمن لقانون العقوبات الفرنسي.
2) المرسوم التنفيذي رقم (07-162) المؤرخ في 30-05-2007 المعدل والمتمم للمرسوم التنفيذي رقم (01-123) الصادر في 09-05-2001.
3) قانون 09-04المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها،الجريدة الرسمية العدد 47 لسنة 2009.
4) القانون رقم 15-04 المؤرخ في 01-02-2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06.
5) -المادة 3/12 من قانون المعاملات الإلكترونية في إمارة دبي رقم 02 لسنة 2002
6) تنص المادة 48 من قانون 83-2000 على ما يلي : «يعاقب كلمن استعمل بصفة غير مشروعة عناصر لتشفير شخصية متعلقة بإمضاء الغير بالسجن لمدة تتراوح ما بين ستة أشهر وعامين وبغرامة ما بين ألف وعشرة آلاف دينار أو بإحدى هاتين العقوبتين.


**ثانيا: الكتب**


1) أمير فرج يوسف، **التوقيع الإلكتروني**، دار المطبوعات الجامعية، مصر، الإسكندرية، 2008.
2) أيمن رمضان محمد محمد، **الحماية الجنائية للتوقيع الإلكتروني**، دار النهضة العربية، مصر، 2011 .
3) الدسوقي أبو الليل، **توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور**، مؤتمر الأعمال المصرفية الالكترونية. المجلد الخامس.
4) وسيم شفيق الحجار، **الإثبات الالكتروني**، لبنان، منشورات الحلبي الحقوقية، 2002

5) حسام محمد نبيل الشنراقي، ، **الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني**، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، 2013.

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

7) لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، دار الثقافة، الأردن، 2009.

8) محمد المرسي الزهرة، **عناصر الدليل الكتابي التقليدي**، شون ناشر، 2001.

9) محمد مأمون سليمان، **التحكيم الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2011.

10)محمد محمد السادات، **حجية المحررات الموقعة إلكترونية في الإثبات دراسة مقارنة**، دار الجامعة الجديدة، مصر القاهرة، 2011.

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

12)نادية ياس البياتي، **التوقيع الإلكتروني عبر الأنترنيت ومنى حجيته في الإثبات**، ط1، دار الهداية ناشرون وموزعون الأردن، 2014.

13)نصر محمد محمد، **الدليل الإلكتروني وحجيته أمام القضاء**، دار الكتب العلمية، لبنان، 2013 .

14)سادات محمد محمد، **خصوصية التوقيع الإلكتروني**، دار الفكر والقانون، مصر، 2011.

15)سلطان عبد هلا محمود الجواري. **عقود التجارة الالكترونية**. الأردن: دار الثقافة للنشر والتوزيع، 2010.

16)سمير حامد عبد العزيز الجمال، **التعاقد عبر تقنيات الاتصال الحديثة**. مصر: دار النهضة العربية، 2006.

17)سمير عبد السميع الأردن، **العقد الإلكتروني**، منشأة المعارف، مصر، 2005.

18)عابد فايد عبد الفتاح فايد، **الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقي: دراسة في الفكرة القانونية للكتابة الإلكترونية ووظائفها في القانون المدني**، دار الجامعة الجديدة، الإسكندرية، 2004.

19)عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها الجنائية**، دار الفكر الجامعي، الإسكندرية، 2004.

20)فواز المطالقة محمد، **الوجيز في عقود التجارة الالكترونية (الإصدار 2 )**، الأردن: دار الثقافة للنشر والتوزيع، 2008.

21)فيصل سعد الغريب، **التوقيع الإلكتروني وحجيته في الإثبات**، المنطقة العربية للتنمية الإدارية، الكويت

22)ثروت عبد الحميد، **التوقيع الإلكتروني (ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيتها في الإثبات)**، دار الجامعة الجديدة، مصر، 2007 .

23)خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات**، دار الهدى، الجزائر، 2010 .

**ثالثا: المذكرات والرسائل الجامعية**

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

3) ديلمي جمال، **الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر**، مذكرة لنيل شهادة الماجستير في القانون الخاص، فرع قانون العقود، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2017 .

4) حوحو يمينة، **عقد البيع الإلكتروني دراسة مقارنة** ، أطروحة دكتوراه ، جامعة ابن عكنون، الجزائر، 2012.

5) حنان براهيمي ، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه كلية الحقوق لجامعة بسكرة، 2015 .

6) ياسمينة كواشي، الحماية الجنائية للتوقيع والتصديق الالكترونيين في ظل القانون، مذكرة ماستر، جامعة العربي بن مهيدي قسم الحقوق، 2017

7) كشابية زهرة، صايفي غانية، تزوير التوقيع الالكتروني، مذكرة ماستر في القانون، جامعة مولود معمري تيزي وزو ، 2017.

8) لالوش راضية، **أمن التوقيع الإلكتروني**، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012/09/23 .

9) لملوم كريم، **الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية**، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، 2011/02/14 .

10) محمد هشام صالح عبد الفتاح، **جريمة الاحتيال دراسة مقارنة**، رسالة ماجستير، كلية الدراسات العليا لجامعة النجاح الوطنية، نابلس، فلسطين، 2008.

11) ساعد مريم، كراش مهدية، **جريمة التزوير في المحررات**، مذكرة لنيل شهادة الماستر في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، 2016/02/04 .

12) عباس حفصي، **جرائم التزوير الإلكتروني دراسة مقارنة**، رسالة دكتوراه، جامعة أحمد بن بلة، وهران 1، 2015 .

13) صالح شنين، **الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، رسالة دكتوراه، جامعة تلمسان، 2013.

**رابعا: المجلات والمقالات:**

1) أسامة بن غانم العبيدي، **أحجية التوقيع الإلكتروني في الإنبات، المجلة العربية للدراسات الأمنية والتدريب**، المجلد 28 العدد 56، جامعة نايف للعلوم الأمنية، 2012.

2) إبراهيم إسماعيل الربيع، علاه موسي علي نالي، **التوثيق الإلكتروني قرارات التحكيم في التوقيع الإلكتروني دراسة مقارنة**"، مجلة المحقق الحلي للعلوم القانونية والسياسية، بابل، العراق، العدد رقم 01، 2012 .

3) وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري ،جامعة تبسة، مقال في مجلة العلوم القانونية والسياسية ، العدد01، 2020

4) محمد عقوني. **الآليات التقنية والقانونية لحماية التوقيع الالكتروني**. مجلة المفكر (18) ، 2019.

5) فضيلة عاقلي، **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 ،تاريخ الإطلاع يوم 25 سبتمبر 2020 على الساعة 05:20 .

6) رشيدة بوكر، **التوقيع الالكتروني في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر ، العدد الرابع، ديسمبر 2016.

7) غزالي نزيهة،**الآليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري**. مجلة البحوث السياسية والإدارية،2017.

# فهرس

# المحتويات

## فهرس المحتويات