وزارة التعليم العالي والبحث العلمي
جامعة محمد البشيرالإبراهيمي برج بوعريريج
كلية الحقوق والعلوم السياسية
قسم الحقوق

# الحماية الجزائية للتوقيع الإلكتروني في ظل التشريع الوطني الجزائري

مذكرة مكملة لنيل شهادة ماسترتخصص قانون إعلام آلي وانترنيت

**إعداد الطالبين:**
تكالي عيسى
فارسي عبد الرؤوف

**أعضاء لجنة المناقشة**

| الإسم واللقب | الرتبة العلمية | المؤسسة الجامعية | الصفة |
|---|---|---|---|
| د- رفاف لخضر | أستاذ محاضر "أ" | جامعة برج بوعريريج | رئيسا |
| د- بن داود حسين | أستاذ محاضر "أ" | جامعة برج بوعريريج | مشرفا ومقررا |
| د- زاوي رفيق | أستاذ محاضر "ب" | جامعة برج بوعريريج | ممتحنا |

**إشراف الأستاذ**
د. بن داود حسين

الموسم الجامعي 2022/2021


بسم الله الرحمن الرحيم

# إهـــــــداء وتشكـــــرات

بسم الله الرحمن الرحيم

إهداء خاص.

إلى كل عائلتي الكبيرة والصغيرة واخص بالذكر الوالدين الكريمين ، الصهر الوردي ، وكل الإخوة .

إلى الكتكوتات رهودة (ريم) ، رنوة (رنيم) ، سيمونة (ياسمين)

شكر خاص وإهداء كبير إلى وصيبة التي منحتني الكثير.

إلى روح المرحومة الصهرة تغمدها الله برحمته الواسعة.

إلى أساتذتي الكرام بن داود حسين ، زاوي رفيق رفاف لخضر والى كل أستاذ باسمه الخاص دون أن ننسى أخونا الأستاذ رائد بن داود حفظه الله ورعاه

إلى كل من قدم لنا يد المساعدة والتسهيلات.

عيـــــــسى

يوم الجمعة 2022/06/03

# إهـــــــداء وتشكـــرات

بسم الله الرحمن الرحيم

إهداء خاص إلى عائلتي الكبيرة واخص

بالذكر الوالدين الكريمين وكل الإخوة .

إلى عائلتي الصغيرة خاصة زوجتي أم أولادي

، إلى كتاكيتي الصغار وسيم واية إلى

أساتذتي بن داود حسين ، إلى أخي

وصديقي بن عباس التوفيق دون أن أنسى

أن اهديها إلى روح الأخ المرحوم بن عباس

عثمان

إلى كل من قدم لنا يد المساعدة

والتسهيلات.

عبـد الـــــرؤوف

يوم الجمعة 2022/06/03

# مقـدمـــة

## مقــدمــة:

أن التطور التكنولوجي الذي نعيشه الآن، والذي يطلق عليه عصر المعلومات والبيانات، أدى إلى ظهور وسائل وأساليب جديدة في إبرام العقود، لم تكن معروفة منذ سنوات قليلة، وهذه الوسائل في تطور دائم ومستمر وسريع ، ومع تطور تقنيات وأساليب إبرام التصرفات القانونية ، كان من الضروري إيجاد وسيلة تقر بهذه التصرفات قوة ثبوتية لجعلها من الأدلة المقبولة أمام القضاء، خاصة مع تعذر استخدام التوقيع التقليدي في بعض التصرفات.

لذلك بحث المهتمون من قانونيين وتقنين عن وسيلة بديلة أخرى تقوم بهذه المهمة، وتوصلوا إلى وسيلة إلكترونية لها أشكال مختلفة يمكن أن تحقق الخصائص التي يقدمها التوقيع التقليدي سميت "بالتوقيع الإلكتروني"، والذي تكمن أهميته في زيادة مستوى الأمن والخصوصية في التعاملات ، نظرا لقدرة هذه التقنية على حفظ سرية المعلومات والرسائل المرسلة وعدم قدرة أي شخص أخر على الإطلاع أو تعديل أو تحريف الرسالة ، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكد من مصداقية الشخصية مما يسمح بكشف التحايل أو التلاعب .

ولقد أدركت الجزائر منذ أزيد من عشرية أهمية التحكم في تكنولوجيا الإعلام والاتصال، نظرا لعلاقة هذه الأخيرة بنجاح مسار التنمية المستدامة، و بغية التوصل إلى تحقيق أهداف التنمية أضحى التوجه صوب استعمال التكنولوجيات في جميع الميادين ضرورة من أجل تمكين كل المواطنين والمؤسسات من هذه الخدمات بدون تمييز.

وهذا ما كرسه المشرع الجزائري من خلال تعديل قواعد الإثبات بالقانون المدني رقم10/05 المؤرخ في20 جوان2005 المعدل والمتمم[1] ، حيث اعتبر الإثبات بالشكل الالكتروني كالإثبات بالكتابة بتوافر شروط معينة.

[1]- القانون رقم 05-05 المؤرخ في 06 فيفري2005 ، المتضمن القانون التجاري المعدل والمتمم الصادر بالجريدة الرسمية للجمهورية الجزائرية بتاريخ 26 جويلية 2005 ، عدد رقم 30.

ولتحقيق مبدأ الثقة والأمان في المبادلات التجارية الإلكترونية تم في هذا الإطار الاهتمام بمؤسسة التوقيع الإلكتروني، حيث أحاطه المشرع بجملة من شروط الأمان، ووضع له آلية آمنة لإنشائه، ثم حدّد الجهات المكلفة بالمصادقة الإلكترونية، من أجل اعتباره توقيعا إلكترونيا مؤمنا وحجّته في إثبات التصرفات القانونية بين المتعاقدين في التجارة الإلكترونية، هذا التوقيع الإلكتروني الآمن يعطي للأطراف المتعاقدة وخاصة المستهلك الأمان والاطمئنان، مما ينعكس إيجابا على المبادلات التجارية بالنظر إلى الحجية القانونية القوية التي يوفرها هذا التوقيع المستند إلى آلية لإنشائه، والمضمون بشهادة المصادقة الإلكترونية التي توضح صحته وسلامته وتؤكّد حجيته القانونية .

وعلى الرغم من الإيجابيات التي حملتها المعاملات الإلكترونية، إلا أنها لا تخلو من بعض السلبيات التي قد تقوّض جهود الأطراف المعنية أو الغير وتحول دون خلق بيئة آمنة وموثوقة لكافة المتعاملين، خاصةً مع تنامي ظواهر مثل القرصنة والتزوير الإلكتروني، الأمر الذي استدعى تدخّل المشرّع لسن قوانين كفيلة بوضع آليات ووسائل الحماية الجنائية للتوقيع والتصديق الإلكترونيين.

وفي إطار توجه المشرّع الجزائري نحو مسايرة هذه التغيرات في مجال المعاملات الإلكترونية ومواجهة الرهانات ذات العلاقة بالتوقيع والتصديق الإلكترونيين، عمل على سن قانون خاص بهما بعدما كانت مختلف القضايا القانونية المرتبطة بهما منظمة ضمن القواعد العامة لقانون العقوبات، أين صدر القانون رقم 04/15 المؤرخ في01 فيفري2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1] قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة المواتية لتعميم وتطوير المبادلات الإلكترونية وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في

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

الجزائر ، والذي يسمح بدوره بتعميم وتطوير التبادلات الإلكترونية بين المستعملين في مجالي التجارة الإلكترونية ، والذي يسهم في النهاية في تحقيق التنمية الاقتصادية.

كما يسمح الإطار القانوني لعدة قطاعات ، من بينها الإدارة الإلكترونية والتجارة الإلكترونية، بالانضمام للحوكمة الإلكترونية[1]، من أجل ضمان تسيير أفضل للهيئات والمؤسسات، وتسهيل الحياة اليومية للمواطنين والفاعلين الاجتماعيين والاقتصاديين.

و من أجل إنجاح تطبيق العمل بهذا القانون في المجتمع من خلال زيادة الوعي الاجتماعي به ، أي أن تكون لكل فئاته فكرة في مجال التعامل الالكتروني بالنظر لقلة وعي وثقة المجتمع به وخاصة المصارف والتجار وأبناء المجتمع بشكل عام في التعاملات الالكترونية بدل من أن تكون تعاملاتهم ورقية تقليدية وذلك من أجل اللحاق بركب المجتمعات المتقدمة التي سبقتنا في هذا المجال ليشتمل على كل ما له علاقة بالتوقيع والتصديق الإلكترونيين ووسائل الحماية الجنائية لهما سنحاول في هذا الموضوع تسليط الضوء على الحماية الخاصة به والآليات القانونية والتقنية التي يتمتع بها من أجل رفع البس عليه وتشجيع كل الشرائح لاستغلال هذه التقنيات في جو من الطمأنينة والأمان.

## أهميـة الموضـوع:

تثير مشكلة الأمن والخصوصية على شبكة الإنترنيت حيزا كبيرا من اهتمام التقنيين والفقهاء القانونيين، كما تثير قلق كثير من الأفراد والمتعاملين، وكذا المرشحين للنشاط في مجالات التجارة والمبادلات الالكترونية، مما يسبب نوع من عدم الثقة في هذه الشبكات والتصرفات القانونية الواقعة بواسطتها، أين تم اللجوء إلى تقنية التوقيع الالكتروني ليحل محل التوقيع التقليدي من حيث هو أحد أهم المظاهر الحديثة في مجال المعاملات الإلكترونية ويرفع مستوى الأمن والخصوصية على هذه الشبكات، من خلال قدرة التكنولوجيا الحديثة على

[1]- يقصد بمصطلح الحوكمة الالكترونية تلك الحوكمة المعتمدة على التكنولوجيا ،والحوكمة الالكترونية هي استخدام تكنولوجيا المعلومات والاتصالات (ITC) لتقديم الخدمات الحكومية، وتبادل معلومات معاملات الاتصالات ، وتكامل مختلف الأنظمة والخدمات القائمة بذاتها بين الحكومة والمواطن (G2C) ، وبين الحكومة والشركات (G2B) ، وبين الحكومات وبعضها البعض (G2G) ، وكذلك عمليات الأقسام الإدارية والتفاعلات داخل إطار عمل الحكومة بأكمله. على الرابط الالكتروني https://ar.m.wikipedia.org أطلع عليه بتاريخ 2022/06/02.

حفظ الخصوصية والسرية والمعلومات، وعدم قدرة أي شخص على سرقتها أو تحريفها أو تعديلها، وفي حالة الاعتداء عليها أوجدت له مختلف التشريعات الوطنية والدولية ضمانات قانونيـة وجزائيـة للحفـاظ علـى حقـوق المتعـاملين بهـا ، وردع المخـالفين والمعتـدين عليهـا بعقوبات صارمة ، مما يشجع الأفراد على التعامل بها والذي بدوره يساهم في رفع مستوى التنمية الاقتصادية من خلال سرعة وبساطة التعاملات عبر مختلف الشبكات وهو ما يظهر أهمية الدراسة.

بالإضافة إلى الوقوف على مختلف صور جرائم الاعتداء على التوقيع الإلكتروني، والوسائل التي كفلها المشرّع لضمان الحماية الجنائية له، والتصدي للتجاوزات التي قد تحول دون ترقية استعمال هذه الآليات والحد من مساهمتها في تسهيل المبادلات.

كما تتجلى أهمية البحث أيضا في محاولة الوقوف على توجهات المشرّع الجزائري في تنظيمه للتوقيع والتصديق الإلكترونيين ووسائل الحماية الجنائية التي اعتمدها لمواجهة جرائم الاعتداء على هذه المنظومة الإلكترونية، ومقارنتها مع توجهات التشريع الأجنبي، مما قد يساعد في بناء تصور حول واقع تنظيم التوقيع والتصديق الإلكترونيين وأهم التحديات التي تواجهه في الجزائر في هذا المجال، ما من شأنه توفير هوية رقمية لكل مواطن وحمايتها.

## أسبـاب اختيـار الموضـوع:

أسباب اختيار هذا الموضوع في ضوء بعدين موضوعي وذاتي، أما الأسباب الموضوعية فتمحورت 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 المشرّع لمواجهة جرائم الاعتداء على التوقيع الإلكتروني.

أمـا الـدوافع الذاتيـة فهـي الشـعور بأهميـة الموضـوع وضـرورة البحـث فيـه كـون مـن الموضـوعات المسـتجدة ممـا يولـد الرغبـة فـي التعمـق فيـه والاطـلاع علـى مـا هـو جديـد بخصوصه على المستويين الوطني والدولي، بغرض إثرائه ولو باليسير من خلال البحث في مـدى انسـجام توافـق النصـوص القانونيـة الحاليـة مـع التطـورات الحاصـلة مـع المسـتجدات العالمية، استعداد لدخول فئات معتبرة في المستقبل القريب لمجال المعاملات الالكترونية بعد توفر البنية التحتية وتحسن مناخ الأعمال، وكذا وصول فئات شبانية إلى مستويات تكوين عليا مما يسمح لهم بإثراء معارفهم وخوض تجاربهم لخلق الثروة.

## إشكـــالية الموضـــوع:

بـالنظر لأهميـة التوقيـع الالكترونـي فـي مسـتقبل التعـاملات الالكترونيـة سـواء منهـا المدنية أو التجارية، وحلوله محل التوقيع التقليدي في المستقبل القريب لا محالة بعد التزايد فـي نطـاق المعـاملات الموقعـة الكترونيـا ، وتشـجيع الأفـراد للتعامـل بـه اسـتغلالا لثـروة المعلومات التقنية التي يشهدها العالم ، ما يجعلنا نطرح الإشكال الجوهري في دراستنا حول:

1- ماهية التوقيع الإلكتروني ووظائفه وطرق إنشائه ؟.

2- ومـا هـي صـور الجـرائم التـي يمكـن أن تقـع علـى التوقيـع الالكترونـي ، وهـل كفـل المشرع الجزائري حماية جزائية فعالة لحمايته ؟.

## أهـــداف الموضـــوع:

محاولة التعرف على منهج التشريعات الأجنبية والوطنية وبخاصة التشريع الجزائري إزاء ضمان وسائل ذات فعّالية وكفاية للحماية الجنائية للتوقيع الإلكتروني من أجل مسايرة ومواكبة الأمـم المتقدمـة مـن النـاحيتين القانونيـة والتقنيـة للـتحكم فـي التقنيـات الحديثـة والسـعي إلـى تعميمها بين كل فئات المجتمع، مما ينعكس على الرقي الشخصي والتنمية وتحفيز الشباب على مواكبة التطورات وخلق الثروة، والغيرة على تطور مجتمعنا لمواكبة التطورات الحاصلة فـي الأمم ، بالإضـافة إلـى محاولـة إسـقاط التنظير والبحـوث الأكاديميـة علـى الحيـاة الواقعيـة والمهنية بطريقة مبسطة وتفعيل العمل بهاته الوسائل لتعزيز الحوكمة والقضاء على العراقيل

البيروقراطية ، وكذا الحد من مختلف النزعات في إطار المعاملات والتبادلات الالكترونية وحتى الإدارية باعتبار أن التكنولوجيا والآلة أكثر دقة من الإنسان وهامش الخطأ يكاد يكون منعدم.

## صعـوبات الموضـوع:

الأهمية البالغة للموضوع من الناحيتين التقنية والقانونية تطلب جهودا كبيرة جدا باعتبار مسائل التوقيع الالكتروني من المستجدات في التشريعات العربية مما حال دون الاطلاع على اكبر عدد من المراجع العلمية باللغة الوطنية ،وكذا التطرق للتشريعات الوطنية بالمراجع المتخصصة، بالإضافة إلى الحالة الاستثنائية بسبب جائحة كورونا مما حال دون الاستفادة من تجارب طلبة وباحثين في مختلف جامعات الوطنية ، وكذا المشاكل الصحية والارتباطات المهنية التي حالت دون تفرغنا بصفة كلية للبحث والله المستعان.

## منـــاهـج الموضـوع:

ومن أجل الإجابة عن الإشكالية المطروحة وتحقيق الاهداف المتواخاة اقتضت منا الدراسة إتباع المنهج الوصفي لبيان مفهوم التوقيع الالكتروني الإلكتروني، إضافة إلى الاستعانة بالمنهجين الاستقرائي التحليلي لما جاءت به مختلف النصوص القانونية المنظمة له والعقوبات الواجب تطبيقها في حال الاعتداء عليه بمختلف الجرائم على البعدين الدولي والوطني .

## تقسيم الموضـوع:

لدراسة موضوع البحث في ضوء الإجابة على التساؤلات التي خرجت بها الإشكالية والأهداف التي يسعى إلى تحقيقها، تم تقسيم الدراسة إلى الدراسة في فصلين، الأول منهما والموسوم بـ" الإطار المفاهيمي للتوقيع الالكتروني"، والذي انبثق منه مبحثين، تناول الأول ماهية التوقيع الإلكتروني من خلال مفهومه وتعريفه وخصائصه وتقنيات إنشائه، وكذا وظائفه وصوره ،والمبحث الثاني تطرق إلي بيان صوره .

أما الفصل الثاني والذي يحمل عنوان " الجرائم الماسة بالتوقيع الالكتروني وآليات حمايتة" فقد جاء هو الآخر في مبحثين، تناول الأول منه الحماية الجزائية الموضوعية للتوقيع الالكتروني من خلال الحماية الجزائية الموضوعية المستحدثة للتوقيع الالكتروني في ظل قانون المعالجة الآلية للمعطيات ، وكذا الحماية الجزائية له في ظل القانون 04/15 ، وفي المبحث الثاني الذي تناول الحماية الجزائية الإجرائية للتوقيع الالكتروني خلال مرحلة البحث والتحري وجمع الاستدلالات وصولا إلى إجراءات التحقيق و إثبات الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، إلى غاية الجهة القضائية المختصة بالمحاكمة في الجرائم الواقعة على التوقيع الالكتروني.

# الفصـــــل الأول

# الفصل الأول : الإطار المفاهيمي للتوقيع الإلكتروني

## تمهيد:

يتجه الواقع العملي بخصوص التوقيع الالكتروني إلى إدخال طرق ووسائل حديثة في التعامل لا تتفق تماما مع فكرة التوقيع التقليدي، وفي ظل هذه الظروف لا نجد للتوقيع التقليدي مكان أمام انتشار نظم المعالجة الالكترونية للمعلومات، التي بدأت تغزو العالم وتعتمد اعتمادا كليا على الآلية، ولا مجال للإجراءات اليدوية في ظلها.

أول ظهور للتوقيع الإلكتروني كان في قطاع البنوك لمرافقة التسديد عن طريق بطاقة الدفع، أما اليوم فإن استعمالها أصبح يعرف انتشارا واسعا عبر الشبكات العالمية التي تسمح بإجراء تبادل المعلومات بإرسال واستلام وتسديد كل ذلك باستعمال لغة معلوماتية موحدة والذي هو قاعدة الانترنيت TCP/IP [1] ، أو ما يعرف ببروتوكول، فاستجابة لدخول عنصر

---

[1] إن مصطلح TCP/IP هو اختصار لـ " Transmission Control Protocol/ Internet Protocol " وهو واقعيا يعتبر "بروتوكولين" مختلفين لكنهما يعملان معا دوما في أنظمة شبكة الإنترنت، ولهذا السبب أصبحا مقبولين لأن يوصفا بأنهما نظام واحد.

وعادة ما يتطلب تشغيل هذا البروتوكول وجود أجهزة "Hardware" وبرامج "Software" مستقلة، مما يعني أن أي شخص يمكنه الاتصال بالإنترنت ويشارك في المعلومات مستخدما أي نوع من أجهزة الحاسب الآلي ستعمل أجهزة TCP/IP على تحويل البيانات إلى اللغة التي يفهمها المتلقي.

ويقوم بروتوكول "TCP" بتحديد كيف سيتم تجزيء المعلومات إلى رزم وإرسالها عبر الإنترنت، وأيضا تحديد طريقة تجزئة الرسائل "messages" أو المستندات "documents" لتصبح بشكل ملفات أو رزم صغيرة "Packets" بحيث يتم إرسالها بأسرع الطرق من خلال الشبكات المختلفة على الإنترنت تحمل العنوان نفسه "وهو عنوان المتلقي" ،حيث يتكون كل "باكيت" من 1 إلى 1500 "بت"، بما فيها عنوان الحاسوب المرسل والحاسوب المستقبل.

وترسل تلك الرزم مستقلة عن بعضها بعضا من حاسوب إلى آخر، بأي اتجاه من أجل تفادي العوائق، وكذلك بأي سرعة متوافرة . هناك بعض أجهزة الحاسوب التي تسمى موجه"Router" ، تستعمل "البروتوكول " IP لكي تقوم بتحريك رزم المعلومات في اتجاهاتها الصحيحة. باعتبار أن كل رزمة لها عنوان "IP" خاص بالحاسوب الذي أرسل تلك الرزمة، وكذلك عنوان "IP" بالحاسوب المرسلة إليه تلك الرزمة.

ويلاحظ أن لكل حاسوب عنوان "IP" خاص به وهو يتكون من أربعة أرقام تفصل بين كل رقم وآخر نقطة، ونظرا لصعوبة تذكر هذه الأرقام، فقد تم اعتماد أسماء موازية لها، هذه الأسماء أسهل للحفظ، كما أنه يمكن أن يكون لها مدلول معين، سواء كان تجاريا أو تعليميا أو حكوميا أو غيره، وعندما تكتب اسما لحاسوب ما، وهو في الواقع عنوانه، فإنه في الواقع يترجم إلى اسمه الرقمي الأساسي.

وكما يحدث في البريد العادي، فإن الرسائل تأخذ وسائل توصيل متعددة، منها الطائرات أو القطارات أو السيارات وغيرها، ولذا فإن تلك المظاريف ستأخذ طرقا متعددة للوصول إلى ذلك الصديق. عندما تصل المظاريف إليه يقوم بإزالة المظروف ويبدأ بتجميع قطع الصورة حسب الأرقام، وإذا ما فقد أحدها في الطريق يعود ليسألك أن ترسلها مرة أخرى .

لذلك تعد هذه العملية مشابهة لطريقة ما يحدث في الإنترنت من حيث إرسال المعلومات خلاله، وهذا يعني أنه لا توجد ضمانة بأن جميع المعلومات ستصل في الوقت نفسه، ولذا فإنه يعمل على أن يعاد ترتيب رزم المعلومات بالشكل السليم، وذلك لإعادة تكوين المستند في وضعه الأصلي نفسه، وهذا تماما هو ما يقوم به "بروتوكولTCP ، ومما يميز بروتوكول TCP/IP أن جميع أساليب العمل تعتمد عليه خلال عملها على الإنترنت، وعلى أساس هذا "البروتوكول" تأسست "بروتوكولات" أخرى كونت عائلة واحدة من خلال بروتوكولTCP/IP ، من أهمها SMTP :وهو بروتوكول للتحكم.../.. .../... في طريقة إرسال واستقبال البريد الإلكتروني، وبروتوكول FTP الذي يعمل على نقل الملفات بين أجهزة الكمبيوتر، وأخيرا بروتوكول HTP الذي يعمل على تنظيم البث إرسال المعلومات إلى صفحات الإنترنت .

جديد للبشرية يجمع بين مجال المعلوماتية وقطاع الاتصال، وما لهما من انعكاس على التبادل التجاري الذي يقع عبر شبكة الاتصال الحديثة "الانترنيت"، صدرت تشريعات دولية وإقليمية ووطنية لمواكبة التطور الذي لحق بمجال المعلوماتية والقطاع التكنولوجي من جهة، ومن جهة أخرى لكي توفر الأمان والثقة والخصوصية لهذه الوسيلة الجديدة ولإقناع المستهلك بأن هناك قانونا يحميه ويحافظ على مصالحه من الغش والخداع.

إن ظهور التوقيع الالكتروني كمصطلح جديد يقتضي منا محاولة بيان المقصود بهذا المصطلح ، فقد بذلت جهود كبيرة لبيان ذلك من قبل المنظمات الدولية المتخصصة في هذا المجال، وكذلك من قبل الكثير من القوانين الدولية والوطنية ومن طرف الفقهاء، ونظرا للأهمية القصوى التي أصبح يحظى بها التوقيع الالكتروني كآلية للتوقيع على المحررات الالكترونية و كبديل للتوقيع العادي في إثبات حجية هذه الوثائق وإضفاء الحماية القانونية لها، وحتى يؤدي هذا التوقيع وظائف التوقيع التقليدي، سعت التشريعات الوطنية والدولية إلى تبيان مفهومه، صوره، وشروطه ،وتم تقسيم الفصل الأول إلى مبحثين، تناول الأول ماهية التوقيع الإلكتروني والثاني صوره .

## المبحث الأول : ماهية التوقيع الالكتروني

التوقيع الالكتروني هو كل كتابة مدرجة في شكل الكتروني وتتخذ هيئة حروف أو أرقام أو رموز أو إشارات ويمكن عن طريقها نسبة هذه الكتابة إلى موقعها ويختلف التوقيع الالكتروني عن الخط التقليدي في الناحيتين :

**من ناحية الشكل:** التوقيع الالكتروني هو نتاج حركة يد الموّقع في صورة إمضاء أو بصمة عبر وسيط مادي يتم عبر وسيط الكتروني عن طريق جهاز الحاسب الآلي.

---

يذكر أن بروتوكول " TCP/IP" الذي تم ابتكاره عام 1970 كان جزءا من أبحاث مؤسسة "DARPA" التي أنشئت لتوصيل أنواع مختلفة من الشبكات وأجهزة الحاسوب، وكان تمويل هذه المؤسسة عاما من أجل تطوير هذا البروتوكول، ولذلك فإنها تتصف بعدم تبعيتها لأحد، والنتيجة أنها أصبحت ملكا عاما، وبالتالي لا يمكن لأحد ادعاء الحق باستخدامها له فقط، نقلا عن مجلة العرب الاقتصادية الدولية على الرابط الالكتروني https://www.aleqt.com أطلع عليه بتاريخ 2022/04/24.

**من ناحية الخصائص المادية:** التوقيع الالكتروني عبارة عن بيانات مدونة على وسائط الكترونية وللقاضي سلطة واسعة في تقدير مدى قيمة الدليل الالكتروني المقدم أمامه وكذا مراعاة توفر ضوابط الكتابة الالكترونية.

ولتفصيل ماهية التوقيع الالكتروني فقد جاء المبحث الأول في ثلاث مطالب تناول الأول مفهومه، والثاني تقنيات إنشائه ، أما الثالث فقد تناول وظائفه.

**المطلب الأول: مفهوم التوقيع الالكتروني**

إن صفة الإلزام لعقد أو محرر الكتروني ما يتطلب بالضرورة قيام الأطراف بالتوقيع عليه، أين اختلف الفقه والتشريعات في تعريفه ومفهومه في مختلف الأنظمة والقوانين .

وفي النظام الانجلوسكسوني لم يرد في قانون الأمم المتحدة النموذجي بشأن التجارة الالكترونية لعام 1996 تعريفا للتوقيع الالكتروني واكتفى في المادة السابعة منه بتحديد الشروط الواجب توافرها في التوقيع ، إلا أنه بتاريخ 05 جويلية 2001 صدر قانون الأمم المتحدة النموذجي بشأن التوقيعات الالكترونية[1]، والذي تضمنت المادة الثانية منه فقرة " أ" تعريف التوقيع الالكتروني بأنه " بيانات في شكل الكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموّقع بالنسبة لرسالة البيانات، ولبيان موافقة الموّقع على المعلومات الواردة في رسالة البيانات ".

وقد ورد في الفقرة "د" من هذه المادة تعريف الموّقع بأنه " شخص حائز على بيانات إنشاء توقيع، ويتصرف إما بالأصالة عن نفسه، وإما بالنيابة عن الشخص الذي يمثله".

مما سبق يتضح أن قانون الأمم المتحدة قد وضح المقصود بالتوقيع الالكتروني وحدد الشروط الواجب توافرها فيه على نحو يتفق مع مفهوم وشروط التوقيع التقليدي ، كما أنه

[1]- صدر هذا القانون عن لجنة الأمم المتحدة للقانون التجاري الدولي، الدورة 34 ، المعقودة في فيينا في الفترة من 25 إلى 13جويلية 2001، ويمثل هذا القانون مجموعة من القواعد التي ينبغي على الدول الأعضاء في الأمم المتحدة أن تضعها في الاعتبار عند تعديل قوانينها الحالية، أو وضع قوانين جديدة بشأن تنظيم المعاملات والتوقيعات الالكترونية ، نقلا عن الموقع الرسمي للجنة الأمم المتحدة للقانون الدولي على الرابط الالكترونيhttps://uncitral.un.org/ar/general_assembly أطلع عليه بتاريخ 2022/04/24.

يستوي أن يكون الشخص الموّقع شخصا طبيعيا أو معنويًا، وأنه يجوز للشخص أن يقوم بالتوقيع بنفسه أو بواسطة شخص يمثله قانونا.

كما عرف الفقه الأمريكي التوقيع الالكتروني بأنه " وحدة قصيرة من البيانات التي تحمل علاقة رياضية مع البيانات الموجودة في محتوى الوثيقة".

أما القانون الأمريكي الصادر في 30 جوان 2000 فقد عرف التوقيع الالكتروني بأنه " شهادة رقمية تصدر عن إحدى الهيئات المستقلة وتميز كل مستخدم يمكن أن يستخدمها في إرسال أي ووثيقة أو عقد تجاري أو تعهد أو قرار"[1].

أما القانون النموذجي العربي فقد عرف التوقيع الالكتروني على انه " بيانات في شكل الكتروني مدرجة في رسائل بيانات أو مضافة إليها أو متصلة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[2] .

أما مفهوم التوقيع الالكتروني في النظام اللاتيني فقد صدر بتاريخ 13 ديسمبر 1999 للتوجه الأوروبي رقم 193/99 بشأن التوقيع الالكتروني[3]، والتي تنص المادة الثانية فقرة 2 منه على أن التوقيع الالكتروني هو"عبارة عن بيان أو معلومة معالجة الكترونيا ترتبط منطقيًا بمعلومات أو بيانات الكترونية أخري (كرسالة أو محرر) ، والتي تصلح كوسيلة لتميز الشخص وتحديد هويته".

وقد أضفى هذا التوجه على التوقيع الالكتروني نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي، كما تبنى مفهوما واسعا للتوقيع الالكتروني حيث جاء عاما وشاملا لجميع صور التوقيع، والتي من شأنها أن تحدد صاحب التوقيع، وتميزه عند استخدام تقنيات الاتصال الحديثة ، بيد أن هذا التوجه قد ميز بين التوقيع الالكتروني المتقدم و

---

[1]- عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي** ، دار النهضة العربية ،القاهرة ، مصر ،2009، ص 73- 74 .

2- المرجع نفسه ، ص 72 .

[3]- يتكون هذا التوجيه من خمس عشرة مادة، متبوعة بأربعة ملاحق ووفقا لأحكام هذا التوجيه فانه ينبغي على الدول الأعضاء في الاتحاد الأوربي اتخاذ الإجراءات اللازمة لتطبيق أحكامه وتطويع قوانينها الداخلية لتتلائم معه في مدة أقصاها 18شهرا من تاريخ نفاذ هذا التوجيه أي بتاريخ 19 جويلية2001 ، للاطلاع على نصوص قانون التوجيه الأوربي ، أنظر الموقع: http://www.ec.europa.eu. و http://www.fs.dk/uk/acts/eu/pdf/esign-fr.pdf.

التوقيع الالكتروني البسيط . فالأول هو الذي يكون معتمدا من أحد مقدمي خدمات التصديق الالكتروني، ويمنح شهادة تفيد صحته، وذلك بعد التحقق من انتساب التوقيع لصاحبه[1] ، و ينبغي أن يتوافر في التوقيع المتقدم المتطلبات الآتية وفقًا لنص المادة الثانية فقرة 2 من ذات القانون وهي:

- ✓ أن تكون له القدرة على تحديد شخصية الموّقع ، ومميزا له عن غيره من الأشخاص.
- ✓ أن ينشأ باستخدام وسائل و إجراءات تقنية تقع تحت سيطرة الموّقع .
- ✓ أن يرتبط بالمعلومات التي يتضمنها المحرر الالكتروني بطريقة تسمح بكشف أية محاولة تعديل هذه البيانات[2] .

ومتى توافرت هذه الشروط يكون للتوقيع المتقدم الحجية القانونية الكاملة في الإثبات، أما التوقيع البسيط فيتمتع بالحجية القانونية في حالة عدم إنكاره، وفي حالة إنكاره يقع على عاتق من يتمسك به إقامة الدليل بأنه قد تم بطريقة تقنية موثوقة، وفي حالة ما إذا وجدت ازدواجية بين توقيعين الكترونيين، أحدهما متقدم والآخر بسيط، فإن الأولوية تكون للأول لأنه يتمتع بعناصر أمان وثقة لا تتوافر في النوع الثاني.

يتبين مما سبق أن التوجه الأوربي قد وضع تعريفا وصفيا للتوقيع الالكتروني، يسمح بالاعتراف به بمجرد أدائه لوظائفه وهي تمييز وتحديد هوية موقعه[3]، كما أنه قد أنشأ قرينة قانونية بسيطة على صحته وحجيته القانونية في الإثبات، بشرط أن يتم تقديم شهادة باعتماده من جهة متخصصة تخضع في إنشائها وممارستها أو عمالها لرقابة الدولة.

وعرف قانون اليونيسترال[4] النموذجي في المادة الثانية منه التوقيع الالكتروني " بأنه بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا،

---

[1]- سمير حامد عبد العزيز الجمال، **التعاقد عبر تقنيات الاتصال الحديثة**، دراسة مقارنة ، دار النهضة العربية، مصر، 2006، ص 208.

[2] - FAUSSE Yanaon: **La signature électronique**, DUNOD, Paris, 2001, P 87 , et s.

[3]- حسن عبد الباسط جميعي، **إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت**، دار النهضة العربية، مصر القاهرة، 2000 ،ص 94-95 .

4- اليونسترال هي لجنة قانون التجارة الدولية التابعة للأمم المتحدة ،وتضم عضويتها غالبية دول العالم الممثلة لمختلف النظم القانونية المختلفة ،وغرضها الرئيسي تحقيق الانسجام بين القواعد القانونية المنظمة للتجارة الالكترونية ،وتحقيق وحدة القواعد المتبعة وطنيا في التعامل مع مسائل التجارة الالكترونية على الموقع : http://www.uncitral.org اطلع عليه بتاريخ 2022/05/26.

يجوز أن تستخدم لتقييم هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات" [1].

**الفرع الأول: تعريف التوقيع الالكتروني**

تباينت تعريفات التوقيع الالكتروني، و ذلك بحسب الزاوية التي ينظر منها إليه، فهناك من عرفه بناء على الوسيلة التي يتم بها إجراء التوقيع الالكتروني، في حين عرفه آخر بحسب ما يقوم به من وظائف، فتنوعت تعريفات التوقيع الالكتروني سواء من منظور الاتفاقيات الدولية أو التشريعات الوطنية الخاصة بالتوقيع الالكتروني، إضافة إلى ما قام به الفقه من اجتهادات حول هذا الموضوع ،و سنعرض فيما يلي هذه التعريفات إذ سنتطرق إلى التعريف الاصطلاحي (أولا) ، ثم التعريف التشريعي (ثانيا).

**أولا: التعريف الاصطلاحي**

تعددت التعريفات الفقهية لمفهوم التوقيع الإلكتروني، إلا أنها تدور حول محور واحد ألا وهو عدم الخروج عن تحديد وظيفتي التوقيع وهما تحديد هوية الموّقع ، والتعبير عن رضاه بالالتزام بمحتوى المحرر .

و تطرقت بعض التعريفات إلى الجانب التقني للتوقيع الإلكتروني فعرفته بأنه" مجموعة من الأرقام التي تختلط مع بعضها البعض في إطار علاقة رياضية معينة ومعقدة ، مكونة بذلك كود سري يتعلق بشخص معين" [2].

وعرفه جانب آخر من الفقه بأنه " وحدة مقيدة من البيانات التي تحمل علاقة رياضية مع البيانات الموجودة في محتوى الوثيقة"[3] ، ويرتكز هذا الجانب من الفقه على أحد أشكال التوقيع الإلكتروني ألا وهو التوقيع الرقمي الذي يقوم على التشفير غير التماثلي، أي التشفير القائم على زوج من المفاتيح (العام و الخاص).

---

1- إيهاب فوزي السقا ، **جريمة التزوير في المحررات الالكترونية** ، دار الجامعة الجديدة ، الإسكندرية ، مصر ،2008 ، ص 81-82 .

2- فيصل سعيد الغريب ،**التوقيع الالكتروني وحجيته في الإثبات** ،منشورات المنظمة العربية للتنمية الإدارية ، مصر ، 2005 ، ص 216 .

3- عبد الفتاح بيومي حجازي، مرجع سابق ،ص 73.

وعرفه جانب آخر بأنه "مجموعة من الإجراءات التقنية التي تمكن من تحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بشأنه"[1] .

ويذهب اتجاه آخر بأنه " حروف أو رموز أو أرقام أو إشارات لها طابع منفرد، تسمح بتحديد الشخص صاحب التوقيع وتميزه عن الغير ، وهو الوسيلة الضرورية للمعاملات الالكترونية في إبرامها وتنفيذها والمحافظة على سرية المعلومات والوسائل"[2] .

كما عُرف 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 الموّقع ويميزه عن غيره "[3] .

وعُرف أيضا بأنه " طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الانترنيت "[4] .

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"[5].

و من هذه التعاريف، يمكن استخلاص العناصر الجوهرية للتوقيع الالكتروني وهي " أن يكون علامة خطية وشخصية لمن ينسب إليه المحرر، ثم أن يترك أثر متميز يبقى ولا يزول".

**ثانيا: اختلاف التشريعات في التعريف التشريعي للتوقيع الالكتروني**

أصبح اعتماد التوقيع الإلكتروني ضرورة عالمية إذ سارعت معظم التشريعات إلى الاعتراف به، وتنظيمه في قوانين خاصة كما هو الحال عليه مع التشريع الفرنسي و المصري، و ضمن قانون التجارة الالكترونية مثل التشريع التونسي و الأردني، و اختلفت كذلك المصطلحات الواردة بشأنه؛ فالبعض يسميها المستندات الإلكترونية مثل القانون

1- إيهاب فوزي السقا ، مرجع سابق ، ص 32.
2- المرجع نفسه ، ص 32 .
3- أمير فرج يوسف، **التوقيع الإلكتروني**، دار المطبوعات الجامعية، مصر،الإسكندرية، 2008، ص14.
4- المرجع نفسه ، ص 17 .
5- لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، دار الثقافة، الأردن، 2009 ، ص 120 .

الإماراتي، و البعض الآخر يسميها رسالة بيانات كقانون اليونيسترال النموذجي ، والبعض الآخر بالإمضاء الإلكتروني كما ورد في التشريع التونسي، أما المصطلح الشائع الاستعمال فهو مصطلح التوقيع الالكتروني الذي تبناه القانون الفرنسي و الأردني و الجزائري و المصري، وسنحاول استعراض بعض التعريفات التشريعية كما يلي:

وضع **المشرع الفرنسي** مفهوما موسعا للتوقيع ولم يفرق بين التوقيع التقليدي والالكتروني، ولهما نفس الحجية القانونية في الإثبات[1]، ويرتب أثاره سواء كان مستندا عرفيا أو رسميا، وهو ما تناوله المشرع الفرنسي بموجب القانون رقم 230/2000 الصادر في 13 مارس 2000 الخاص بالمبادلات والتجارة الالكترونية المعدل والمتمم للقانون المدني في نص المادة 4/1316 منه ، والتي تنص على أن " التوقيع الالكتروني إنما يدل على شخصية صاحبه ويضمن علاقته بالواقعة التي أجراها، ويؤكد شخصية صاحبه وصحة الواقعة المنسوبة إليه إلى أن يثبت عكس ذلك"[2] .

و نستعرض مفهوم التوقيع الالكتروني في التشريعات العربية التي أصدرت قوانين لتنظيم التوقيع الالكتروني والتجارة الالكترونية وذلك على النحو التالي:

– **عرف المشرع المصري التوقيع الالكتروني** في المادة الأولى فقرة "ج" من القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بأنه " ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموّقع ويميزه عن غيره[3]" .

**عرف المشرع الإماراتي** التوقيع الالكتروني في المادة الثانية من القانون رقم 2 لسنة 2002 بشأن المعاملات والتجارة الالكترونية بأنه" توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل الكتروني وملحق أو مرتبط منطقيا برسالة الكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة" [4].

1- فيصل سعيد الغريب ،المرجع السابق ، ص 216 .
2- ماجد راغب الحلو، **العقد الإداري الإلكتروني**، دراسة تحليلية مقارنة ، دار الجامعة الجديدة،مصر،2007 ، ص 81-82.
3- محمد الشهاوي ، **شرح قانون التوقيع الالكتروني رقم 15 لسنة 2004** (دراسة مقارنة) ، ط 1 ، دار النهضة العربية ، القاهرة ، مصر ، 2010، ص 7 .
4- عبد الفتاح بيومي حجازي،المرجع السابق ،ص7 .

**بالنسبة للمشرع التونسي** لم يرد نص في القانون التونسي رقم8 لسنة 2000 بشأن المبادلات والتجارة الالكترونية يتضمن تعريفا للتوقيع الالكتروني واكتفى بتعريف العناصر المؤدية له، حيث تناولت المادة الثانية منه تعريف منظومة أحداث الإمضاء بأنها " مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات الشخصية المهيأة خصيصا لإحداث إمضاء الكتروني"[1] .

**بالنسبة للمشرع الجزائري** فاعتد بالتوقيع الإلكتروني لأول مرة بنص المادة 2/327 من القانون المدني، ثَم في القانون المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية بمقتضى المرسوم التنفيذي رقم 162/07 المؤرخ في 30 ماي 2007 المعدل والمتمم للمرسوم التنفيذي رقم 123/01 المؤرخ في 09 ماي 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات[2] ، بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، وحسب المادة **3** مكرر منه فإنه يقصد بالتوقيع الالكتروني" معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكررو323 مكرر 1 من الأمر 58/75 المؤرخ في 26 سبتمبر 1975 "[3].

وصولا إلى تعريف المشرّع الجزائري للتوقيع الإلكتروني في قانون خاص رقم 04/15 بالتوقيع والتصديق الإلكترونيين.

واعترف كذلك بالتوقيع الإلكتروني في القانون المدني رقم10/05 في المواد323 مكرر، و323 مكرر1 و 327 ونصت المادة 323 مكرر المستحدثة بموجب هذا القانون على ما يلي:

---

1- منية بن ترايديت غمارسة ، **جرائم المعلوماتية في القانون التونسي القانون المقارن والقانون الدولي** ،دار الكتاب ، تونس ، 2015 ، ص 9 .

2- المرسوم التنفيذي رقم 162/07 المؤرخ في 30 ماي 2007 المعدل والمتمم للمرسوم التنفيذي رقم 123/01 المؤرخ في 09 ماي 2001 ،المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية الصادربالجريدة الرسمية للجمهورية الجزائرية في 7 جوان 2007 ، العدد 37.

3- الأمر رقم 58/75 المؤرخ في 26 سبتمبر 1975المتضمن القانون المدني، المعدل والمتمم بالقانون رقم 05/07 المؤرخ في 13 ماي 2007الصادربالجريدة الرسمية للجمهورية الجزائرية في 13 ماي 2007 ، العدد 31 .

" ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها ".

ونصتّ المادة 323 مكرر1 من القانون نفسه على أنه " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

وتناول المشرّع الجزائري التوقيع الإلكتروني المؤّمن من خلال المرسوم التنفيذي رقم162/07 بنص المادة 3 فقرة 2 منه، التي عرفته بأنه توقيع إلكتروني يفي بالمتطلبات الآتية:

- أن يكون خاصا بالموّقع .
- يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموّقع تحت رقابته الحصرية.
- يضمن مع الفعل المرتبط به صلة، بحيث يكون أي تعديل لاحق للفعل قابلا للكشف.

أما تعريف المشرع الجزائري للتوقيع الإلكتروني من خلال القانون 04/15 فقد كان بنص المادة 02 التي جاء فيها أن التوقيع الإلكتروني هو" بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".

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

أما بالنسبة لمعظم الدول الأوربية فلم تفرّق بين التوقيع التقليدي والالكتروني، من حيث الحجية القانونية في الإثبات، طالما كان هذا التوقيع يميز صاحبه، ويتم بإجراءات آمنة تضمن سرية بيانات هذا التوقيع ، وبالتالي فقد قامت في تعريفها للتوقيع الالكتروني بنقل التعريف الوارد بتوجيه اللجنة الأوربية رقم 93/1999، ومن بين تلك الدول نذكر منها النمسا التي أصدرت قانون خاص بالتوقيع الالكتروني في01 جانفي2000 ، وفي بلجيكا صدر

[1]- يمينة حوحو، عقد البيع الإلكتروني دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه ، كلية الحقوق، جامعة الجزائر، الموسم الجامعي 2012/2011، ص1 .

قانون في 30 نوفمبر 2001 ، وكذا الدنمارك في القانون رقم 417 في 31 ماي 2000 ،و في ايرلندا أيضا تم نقل هذا التوجيه بالقانون رقم 27 لسنة 2000 الخاص بالتجارة الالكترونية وكذلك انجلترا نقلت التوجيه بالقانون الخاص بالتجارة الالكترونية.

**الفرع الثاني : خصائص التوقيع الالكتروني**

يتميز التوقيع الالكتروني بأنه لا يتم عبر وسيط مادي ، بحيث تذيل به الكتابة، كما هو الحال بالنسبة للتوقيع الكتابي ، ويتم إنشاؤه عبر وسيط الكتروني من خلال أجهزة الكمبيوتر أو عبر الانترنيت ، بحيث يكون بإمكان أطراف العقد الاتصال ببعضهم البعض ، والاطلاع على وثائق العقد، والتفاوض بشأنه وشروطه وإفراغ هذا العقد في محررات الكترونية والتوقيع عليه بنفس الصفة[1].

واستلزمت ضرورة الأمن القانونية وجوب استخدام تقنية آمنة في التوقيع الالكتروني تسمح بالتعرف على شخصية الموّقع [2] ، بحث أن التوقيع الالكتروني يتميز عن غيره بمجموعة من الخصائص وهي :

**أولا: الخصوصية و التعرف على المستخدم**

خاصية الخصوصية توفر حماية البيانات ضد الاستخدام غير المشروع ، أي تحديد صلاحيات الوصول للبيانات وعدم السماح للأشخاص بتنفيذ أي إجراء على البيانات التي لا يملكون صلاحيات المساس بها ، وتتم عملية تفعيل صلاحية الوصول أثناء حفظ البيانات الخاصة بالتوقيع الالكتروني الموجود على بطاقة ذكية، ولا يغادرها أبدا ومحمي برقم سري أو تشفير البيانات أثناء إرسالها، وهي إحدى المزايا التي تجعل من الشخص المقصود هو الوحيد الذي يطلع على المستند المرسل[3].

---

[1]- يونس عرب ، منازعات التجارة الالكترونية ،" الاختصاص والقانون الواجب التطبيق وطرق التقاضي "، ورقة عمل مقدمة إلى مؤتمر التجارة الالكترونية الذي أقامته منظمة الأمم المتحدة ، الفترة ما بين 08-10 نوفمبر سنة 2000 ،بيروت لبنان ص 17-18 منشور على موقع http://www.aeab-low.com اطلع عليه بتاريخ 2022/03/06.

[2]- محمد بودالي ، التوقيع الالكتروني ، مجلة الإدارة ، العدد الثاني ،الجزائر ، 2003 ، ص 57 .

[3]- قارة مولود ، "الإطار القانوني للتوقيع والتوثيق الالكترونيين في قانون المعاملات والتجارة الالكترونية "، مقال منشور عبر موقع : www.minshawi.com اطلع عليه بتاريخ 2022/03/06 .

كما تتم عملية التحقق من هوية الأشخاص أو التعرف على مصادر البيانات عن طريق كلمات السر في البطاقات الذكية ، أو عن طريق شهادة التصديق الالكتروني الصادرة من جهة تصديق الكتروني ، وكلما زادت الحاجة لدقة تحديد الهوية يتم اللجوء إلى جمع عدة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم .

**ثانيا: عدم القدرة على الإنكار و ثبوت تاريخ المعاملة**

عدم قدرة الشخص الموّقع الكترونيا أو الشخص الذي قام بإرسال رسالة الكترونية لوجود طرف ثالث يمكنه إثبات قيام طرف معين بفعل الكتروني معين، وكذا عدم قدرة مستلم رسالة معينة على إنكار استلامه لرسالة ما، حيث أن المفتاح العام يثبت استلام الرسالة من قبل المستقبل وذلك بإرسال الرد (وصل استلام) إلى المرسل، فعدم الإنكار يعني حماية المستند أو العقد الالكتروني من إنكار أحد الطرفين (المرسل أو المستقبل)[1].

بالإضافة إلى ذلك لا يستطيع مرسل الرسالة تغيير تاريخ توقيع وإرسال الرسالة وكذلك الأمر بالنسبة لمستقبلها ، بحيث أن ذلك له أهمية كبيرة في مجال التجارة الالكترونية والعقود الالكترونية ، أي عدم قدرة مرسل الرسالة أو مستقبلها من إجراء أي تعديل عليها أو على تاريخ إرسالها واستلامها بالنسبة للطرفين.

**ثالثا:السرعة ودقة انجاز المعاملات و توفير وحدة البيانات**

يزيد التوقيع الالكتروني من سرعة ودقة المعاملات الالكترونية ويقلل من تأخر إرسال واستلام العقود والمستندات التجارية وغيره من العقود حول العالم ، كما أنه يوفر عملية حماية البيانات ضد التغيير أو تعويضها وتعديلها ببيانات أخرى، وتتم هذه العملية باستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة المرسلة ببصمة الرسالة المستقبلة (عدم تغيير بيانات الرسالة أثناء نقلها)، و أن مستقبل الرسالة يمكنه معرفة ذلك عند تلقي الرسالة، بحيث

[1]- منائي فراح ، **العقد الالكتروني وسيلة إثبات حديثة في القانون المدني الجزائري** ، دار الهدى للطباعة والنشر والتوزيع ، الجزائر ، 2009 ، ص 196-197 .

أنه يمكن اكتشاف إذا حصل أي تغيير أو تعديل على المستند أثناء إرساله وهذا ما يعتبر تزويرا[1] .

**المطلب الثاني :تقنية إنشاء التوقيع الالكتروني**

حرص المشرع الجزائري على ضمان أمن التوقيع الإلكتروني و صحته لينتج آثاره القانونية مثل التوقيع التقليدي، و نعني به أنه يتم إنشاؤه وفقا لإجراءات خاصة وظروف تضمن حفظه و سلامته، وتؤكد صلة معطيات التوقيع الإلكتروني بالموّقع عندئذ تتحقق حجيته القانونية، فتكون له الحجية ذاتها للتوقيع المكتوب بخط اليد مهما كانت التقنية المستخدمة في إنشائه[2].

ويتعين أن يستجيب التوقيع الإلكتروني لمعطيات إنشائه، هذه المعطيات تتمثل في جميع البيانات والعناصر الخاصة بالموّقع والتي تميزه عن غيره ، و المستخدمة في إنشائه و تكوينه ،وهي الوسائل التقنية و الفنية التي تضمن الصلة بينها و بين موقعها، و تتم بواسطة أدوات خاصة بالموّقع و مميزة له بصفة انفرادية، ولتفصيل تقنيات إنشائه قسمنا المطلب إلى فرعين، سنتطرق في الأول إلى جهاز إنشاء التوقيع الالكتروني ، وفي الثاني إلى استخدام التقنيات المؤّمنة في إنشائه، وفي الثالث جهاز فحص التوقيع الالكتروني .

**الفرع الأول: جهاز إنشاء التوقيع الالكتروني**

يقصد بالعناصر التقنية للتوقيع الالكتروني من قبل الموّقع حسب نص المادة 3 مكرر فقرة 4 من المرسوم رقم162/07 الأدوات والأساليب التقنية التي يستخدمها الموّقع نفسه لإنشاء توقيعه، والمتمثلة في جهاز تقني ومناهج تقنية معينة، كما نصت المادة 1/3 من

[1]- صلاح عبد الحكيم المصري ، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة ، أطروحة مقدمة لنيل شهادة الماجستير في إدارة الأعمال ، كلية التجارة ، الجامعة الإسلامية غزة ، فلسطين ،2007 ، ص 24-25.

[2] - Il s'agit d'une définition générale qui englobe également la stéganographie, technique particulière qui consiste à cacher un message dans un autre message d'apparence anodine. Les signatures numériques et le chiffrement constituent deux applications importantes de la cryptographie. Les signatures numériques permettent de prouver l'origine des données (authentification) et de vérifier si les données ont été altérées (intégrité). Le chiffrement peut aider à maintenir la confidentialité des données et des communications. Enfin, la cryptographie peut aussi bien assurer la protection de données stockées dans un ordinateur que transmises dans le cadre d'une communication". Elisabeth –FOLY –PASSANT .

المرسوم نفسه على جهاز إنشاء التوقيع الالكتروني و جاء فيها بأنه" جهاز لإنشاء التوقيع الإلكتروني يفي بالمتطلبات المحددة و يقصد بالمتطلبات المحددة ، تلك التي نص عليها المشرع الجزائري في المادة 3 مكرر فقرة 1 من ذات المرسوم، وهي أن تكون خاصة بالموّقع وأن يتم إنشاؤها بوسائل يمكن أن يحتفظ بها الموّقع تحت رقابته الحصرية، و أن يضمن مع الفعل المرتبط به علاقة بحيث يكون أي تعديل لاحق للفعل قابلا للكشف.

ويعد جهاز إنشاء التوقيع الإلكتروني عتاد MATERIEL أو برنامج معلوماتي LOGICIEL مخصص و معد لإنشاء معطيات التوقيع الإلكتروني قادر على تخزين المعلومات و معالجتها، أو تخزينهاأو إرسالها، أو استقبالها، أو تصفحها.

و يتنوع العتاد بتنوع التقنية المستخدمة المخصصة لذلك[1] ، كالمفتاح العام والمفتاح الخاص أو البطاقات الذكية مثلا، و اشترط المشرع الفرنسي مجموعة من الشروط الصدد بالإضافة إلى ما سبق ذكره قصد تقوية صحة و سلامة التوقيع الإلكتروني ، نص عليها بالماة 3 من المرسوم 272/2001 المؤرخ في 2001/03/30 ، يتعين أن تكون في التقنية المستخدمة لإنشاء التوقيع الإلكتروني من بينها، مع شرط الاستخدام الحصري من قبل الموّقع وشرط عدم الاستعمالها من قبل الغير[2] .

و لتحقيق ذلك غالبا ما تستعمل تكنولوجيا التقطيع أو الفرم Hachage المستخدمة في تشفير المعطيات و البيانات الإلكترونية، مثلا طريقة فرم المعطيات من خلال التقنية المسماة SHA-1 et RIMED- 160 ، هذا يعني أن الموّقع له أدوات تمكنه من إنشاء توقيعه

[1]- يوجد عدة أنواع من البرمجيات المخصصة لهذا الغرض مثل برنامج Logiciel Adesium Société Messenge Signature Safe ،أو برنامجPENFLOW IDENTI'SIGN ،Dhimyoti Société FORTIGNAالتابعين للشركات المتخصصة في ذلك.

[2] -Art. 3 du Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. “ Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est ertifié conforme à ces exigences dans les conditions prévues au II. Un dispositif sécurisé de création de signature électronique doit .

إذ تضمن له سيطرته على توقيعه و مراقبته الحصرية له، مما يضمن سلامة توقيعه فيكون المفتاح الخاص به تحت سيطرته و رقابته الحصرية[1] .

**الفرع الثاني: استخدام التقنيات المؤّمنة**

من أهم معطيات إنشاء التوقيع الإلكتروني هو أن يتم فيه استخدام تقنيات يتعين أن تكون مؤّمنة، إذ على الموّقع أن يتأكد من استعمال وسيلة تقنية مؤّمنة، و تعني مؤّمنة أنها وسيلة موثوق بها تحقق الضمان و السلامة و الحفظ من أي تغيير، حتى تضمن ارتباط التوقيع الإلكتروني بموّقعه.

هذا و تتنوع تقنيات تأمين التوقيع الإلكتروني بتنوع التقنيات المعروفة في هذا المجال كما سبق ذكره ، و التي تقوم في مجملها إما من خلال إدخال معلومات سرية كالكود ( UN CODE) أو البين(PIN) أو رقم أو كلمة المرور، أو استعمال أدوات محمولة مثل مفتاح (USB) ،أو استعمال الخواص البشرية البيومترية التي تعتمد على خواص الجسم البشري ، أو المواصفات الحيوية (Biometric) مثل شكل الوجه أو بصمة اليد أو قزحية العين .

**الفرع الثالث: جهاز فحص التوقيع الالكتروني**

يعد جهاز فحص التوقيع الإلكتروني من معطيات إنشائه، و الذي له علاقة مباشرة مع البنية التقنية الخاصة في توفير خدمة المصادقة الإلكترونية من أجل أمن المعلومات، و قد نصت المادة 3 فقرة 7 من المرسوم التنفيذي رقم 162/07 المؤرخ في 2007/05/09 الخاص بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات، بما فيها اللاسلكية الكهربائية وعلى مختلف أنواع الخدمات السلكية و اللاسلكية في تعريفها لجهاز فحص التوقيع الإلكتروني بأنه " عتاد أو برنامج معلوماتي معد لوضع معطيات فحص التوقيع الإلكتروني موضع التنفيذ "، و يعمل جهاز فحص التوقيع الإلكتروني وفقا لمعايير تقنية و إجراءات

[1] - 2-SHA-1 (Secure Hash Algorithm) est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA),et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (Federal Information Processing Standard du National Institute of Standards and Technology (NIST)). Elle produit un résultat (appelé « hash » ou condensat) de 160 bits.

- معلومات مأخوذة من الموقع http://fr.wikipedia.org/wiki/SHA ، راجع أيضا علاء محمد نصيرات ،**حجية التوقيع الإلكتروني في الإثبات** ،دراسة مقارنة ،دار الثقافة للنشر و التوزيع،الأردن، 2005، ص 135 .

عمل معتمدة عالميا من قبل منظمات عالمية متخصصة في هذا الميدان، مثل المنظمة العالمية للمعايير ISO التي أنشأت لجنة دولية إلكتروتقنية[1]، أو الإتحاد الدولي للاتصالات ITU [2]، أو المعهد الوطني لمعايير التكنولوجيا NIST[3] ، وغيرها من المنظمات المتواجدة في العالم .

**المطلب الثالث:وظائف التوقيع الالكتروني**

سبق التطرق إلى ماهية التوقيع الالكتروني والتعريف التشريعي والفقهي له، ولاحظنا أن الكثير من التشريعات عرفت التوقيع من خلال الوظائف التي يؤديها ، وهي تمييز الشخص الموّقع والتعبير عن إرادته بصفته أصيلا عن نفسه أو ممثلا لغيره بالموافقة على مضمون التصرف، لذا نلخص وظائف التوقيع الالكتروني على هذا الأساس فيما يلي:

**الفرع الأول: تحديد الشخص الموّقع**

وهو الشخص الملتزم بالتوقيع الذي يعتبر من أساسيات التوقيع، إذ أن الغاية من التوقيع هو أن ينسب ما ورد في المحرر أو المستند للشخص الموّقع .

و يرى جانب من الفقه أن التوقيع الالكتروني يتم بواسطته تحديد هوية الموّقع ، إذا ما تم مراعاة وسائل الأمان المتبعة، كما أن التوقيع يستطيع تأدية هذه الوظيفة باختلاف نوع التواقيع الالكترونية المستخدمة، فمثلا استخدام تقنية الماسح الضوئي الذي يقوم بنقل التوقيع

---

[1]- اللجنة الإلكتروتقنية الدولية للتعامل مع النتائج المترتبة من التداخل الكبير في مجالات المعايير والأعمال المتصلة بتكنولوجيا المعلومات، شكلت الإسو واللجنة الإلكتروتقنية الدولية اللجنة الفنية المشتركة المعروفة باسم الإسو\اللجنة الإلكتروتقنية الدولية (jtc1) كانت أول لجنة مشتركة من هذا القبيل، وحتى الآن لا تزال الوحيدة.

[2]- يعد الاتحاد الدولي للاتصالات، منظمة تقنية عالمية ، و هي من أقدم المنظمات، إذ يعود تاريخ إنشاؤها إلى سنة 1865، حيث كان يطلق عليها آنذاك بالاتحاد الدولي للتلغراف، وعند ظهور الهاتف و تطويره أصبح يطلق عليه بالاتحاد الدولي للاتصالات سنة 1932 و تم ربطه بالأمم المتحدة سنة1947 .

[3] المعهد الوطني للمعايير والتقنية بالإنجليزية NIST المعروف بين عام 1901 وعام 1988 بالمكتب الوطني للمعايير، وهو مختبر معايير القياس وهي وكالة غير اعتيادية لإدارة التجارة في الولايات المتحدة، ومهمة المعهد الرسمية هي تشجيع الابتكار بالولايات المتحدة والقدرة التنافسية الصناعية من خلال تطوير علم القياس والمعايير والقنيات في السبل التي تعزز الأمن الاقتصادي وتحسين نوعية الحياة.
وامتلكت NIST ميزانية تشغيلية للعام المالي 2007 (1 أكتوبر 2006 ، 30 سبتمبر 2007) حوالي 843.3 مليون دولار، ووصلت ميزانيته في عام 2009 حوالي 992 مليون دولار، لكنها تلقت أيضاً 610 مليون دولار كجزء من الإنعاش وإعادة الاستثمار الأمريكي، و توظف نحو 2,900 من العلماء والمهندسين والفنيين، والموظفين الإداريين وموظفي الدعم، فضلاً عن حوالي 1,800 ملحق (باحثين ضيوف ومهندسين من الشركات الأميركية والدول الأجنبية) تكملة لموظفيها.
بالإضافة إلى ذلك فهي شريكة مع 1,400 من متخصصين التصنيع والموظفين في ما يقرب من 350 مركزاً تابعاً في أنحاء البلاد نقلا عن موقع ويكيديا على الرابط الالكتروني https://ar.wikipedia.org/wiki اطلع عليه بتاريخ 2022/04/24 .

الصادر إلى شاشة الكمبيوتر لا يمكنه تأدية هذه الوظيفة في ظل التقدم التكنولوجي وإمكانية استخدام هذه التقنية من قبل بعض المخترقين، ذلك عكس ما عليه الحال في التوقيع الرقمي الذي يستخدم وسائل أكثر أمانا[1].

و تجدر الإشارة إلى أنه قد ظهرت في مختلف الدول شركات متخصصة وتقنيات متطورة من أجل تنفيذ عملية حماية التوقيع الالكتروني وتأمينه، وقد أشار المشرع الأردني في المادة 32 فقرة "ب" من قانون المعاملات الالكترونية إلى ضرورة إصدار شهادة التوثيق من هيئة مرخصة أو معتمدة سواء في الأردن أو في دولة أخرى ، كما أن المشرع المصري أشار إلى هيئة التصديق في المادتين 7 و 9 من اللائحة التنفيذية والخدمات التي تقدمها هيئة تنمية تكنولوجيا المعلومات من أجل تأمين التوقيع الالكتروني وخدمات الفحص الالكتروني وتحديد شخص الموّقع على المحرر الالكتروني[2] .

وعرف المشرع الجزائري الموّقع في المادة 3 مكرر من المرسوم التنفيذي رقم 162/07 بأنه " شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله ويضع موضع التنفيذ جهاز إنشاء التوقيع الالكتروني"، فحدد المشرع الجزائري هوية الموّقع أو شخصيته بتعبير عن الحساب الخاص للموّقع أو حساب الشخص الطبيعي أو المعنوي الذي يمثله، فهو تحديد لذاتية الشخص أو ذمته.

كما عرف المشرع الجزائري في نفس المادة مصطلح الشهادة الالكترونية بأنها " وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الالكتروني والموّقع "ويعني به بها التحقق من هوية الشخص الموّقع من خلال الشهادة الالكترونية.

**الفرع الثاني: الالتزام بما ورد عليه التوقيع لإثبات سلامة العقد**

[1]- حسن عبد الباسط جميعي، مرجع سابق، ص45

[2]- يوسف أحمد النوافلة، **الإثبات الالكتروني في المواد المدنية والمصرفية**، الطبعة الأولى، دار الثقافة ، الأردن ، 2012 ، ص 99.

يعد التوقيع الإلكتروني تعبيرا عن إرادة الموّقع في الالتزام بما وّقعه، أي يلتزم بالتصرف الذي تضمنه ذلك التوقيع، فهو لا يعد وسيلة لتحديد الشخص الموّقع فقط، و إنما هو وسيلة لإثبات موافقته على مضمون توقيعه[1] المتمثل في تصرف قانوني معين.

ولا يقصد بذلك أن التوقيع يضفي الحجية على سلامة العقد وصحته وحجيته، إنما قرينة تقبل إثبات العكس على سلامة محتوى العقد وصحته وعدم المساس بمضمونه أو العبث به، إذ أنه حتى لو ثبتت سلامة العقد من خلال استخدام التوقيع الالكتروني المؤّمن والمشفّر، الذي يضمن عدم العبث بمحتوى العقد فإنه من الممكن إثبات عدم حجية المحرر الالكتروني أو بطلانه[2].

فقد نصت المادة 31/د من قانون المعاملات الالكترونية الأردني على أن التوقيع الالكتروني يكون موثقا عندما يرتبط بالسجل بصورة لا تسمح بإجراء أي تعديل على المحرر بعد توقيعه، وتضمنت المادة 2/هـ من اللائحة التنفيذية لقانون التوقيع الالكتروني المصري على ذات المضمون حيث أنه وفي المحررات الالكترونية تختفي بيئة الورق وتظهر بيئة الحاسبات وشاشات الكمبيوتر التي تحفظ المعلومات على دعامات يسهل التلاعب بها، وهنا تظهر أهمية التوقيع الالكتروني ، الذي يستطيع أن يؤدي دوره في الإثبات خاصة أن وسائل الأمان في مجال العقود الالكترونية مهمة صعبة وشاقة[3].

## الفرع الثالث: التعبير عن إرادة الموّقع

1- قانون اليونسيترال النموذجي بشأن التجارة الإلكترونية (1996) هو أول نص تشريعي يعتمد المبادئ الأساسية لعدم التمييز والحياد التكنولوجي والتكافؤ الوظيفي التي يراها الكثيرون أسس قانون التجارة الإلكترونية الحديثة.
ويكفل مبدأ عدم التمييز ألاّ يُنكر الأثر القانوني لأي وثيقة أو تُنفى صحتها أو قابليتها للإنفاذ لمجرّد كونها في شكل إلكتروني ، ونصت المادة 1/2 منه على وظائف التوقيع الالكتروني و هي أنه أداة لتحديد شخصية الموّقع ، و إثبات موافقته على فحواه بقولها " التوقيع الإلكتروني نوع من المعلومات تأخذ شكل الكتروني متضمن في رسائل إلكترونية أو مصحوبة بتلك الرسائل.
و يمكن استخدامها من أجل معرفة هوية صاحب التوقيع الإلكتروني وإما توضح أنه يؤيد و يوافق على المعلومات المتضمنة في الرسائل الإلكترونية." نقلا عن الموقع الرسمي للجنة الأمم المتحدة للقانون التجاري الدولي على الرابط الالكتروني https://uncitral.un.org/ar/texts/ecommerce/modellaw/electronic_commerce اطلع عليه بتاريخ 2022/04/24 .

2- يوسف أحمد النوافلة، مرجع سابق، ص101

3- ضياء أمين مشيمش، **التوقيع الالكتروني**، دراسة مقارنة، المنشورات الحقوقية، لبنان ، 2003 ، ص155

التوقيع الالكتروني الموّثق والمؤّمن الصادر وفق الضوابط الفنية والتقنية قرينة على أن الشخص الموّقع قد وافق على مضمون المحرر الالكتروني، والبيانات الواردة فيه ما لم يثبت خلاف ذلك، فقد نصت المادة 32/ب من قانون المعاملات الأردني على أنه " **إذا لم يكن السجل الالكتروني أو التوقيع الالكتروني موثقًا فليس له أي حجية**"، كما تضمنت المادة 11من قانون البيانات الأردني بخصوص حجية السند العادي في الإثبات بأن من يريد إنكار مضمون السند المحتج به اتجاهه، عليه أن ينكر توقيع الشخص الوارد عليه ، وبالتالي فإن التوقيع الالكتروني له وظيفة هامة في التعبير عن إرادة الشخص الموّقع بالالتزام والقبول بما ورد في المحرر الالكتروني، وأن قيام الشخص الموّقع بالتوقيع الالكتروني على المحرر متى كان التوقيع موّثقا ومؤّمنا حسب الأصول يعتبر أداة للتعبير عن رضا الشخص الموّقع بما ورد في المحرر الالكتروني[1]، و يؤدي الوظيفة ذاتها التي يؤديها التوقيع التقليدي وهي التعبير عن رضا الموّقع بما ورد في السند، خاصة إذا اقترن التوقيع الالكتروني بوسائل الأمان والثقة خوفا من إساءة استخدام التوقيع من قبل الآخرين وإتباع إجراءات التوثيق والأمان للحفاظ على التوقيع الالكتروني وضمان عدم إساءة استخدامه[2] .

## المبحث الثاني : صور التوقيع الالكتروني

أوجدت التقنيات الحديثة صورا عديدة من التوقيعات الالكترونية لمحاولة استيفاء التوقيع الالكتروني للشروط اللازم توافرها في التوقيع التقليدي، وبالتالي اعتماده والاعتداد به قانونا ،ولا يمكن حصر كل صوره في هذا المبحث نظرا للتطور التكنولوجي الهائل خاصة من الناحية التقنية أكثر منها قانونية، وقد تم تقسيم هذا المبحث إلى أربعة مطالب إذ سنتناول في الأول التوقيع البيومتري وفي الثاني التوقيع الرقمي، وفي الثالث التوقيع اليدوي المحول إلى الرقمي، وأخيرا التوقيع بالرقم السري والبطاقة المغناطيسية.

### المطلب الأول: التوقيع البيومتري

[1]- سعيد السيد قنديل، **التوقيع الالكتروني، ماهيته، صوره، حجيته في الإثبات**، دار الجامعة الجديدة ، مصر، 2004 ، ص50

[2]- حسن عبد الباسط جميعي، مرجع سابق، ص 46.

يتم التوقيع البيومتري بأحد الخواص الذاتية المميزة لكل شخص( مسح العين البشرية " Iris & Retina Iris de l'œil Scanning " ، البصمة الشخصية " Empreinte digitale, Finger Printing "، خواص اليد البشرية Hand Gesmetry ،التحقق من نبرة الصوت "Voice recognnition "، التعرف على الوجه البشري "Facial Recognition " ،التوقيع الشخصي " Handwritten Signature "، وغير ذلك من الصفات الجسدية والسلوكية، أي باستخدام الخواص السلوكية والجسدية للشخص، وذلك لتميزه وتحديد هويته[1] ، لذا يطلق عليه التوقيع بالخواص الذاتية.

ويقوم هذا التوقيع، على حقيقة مفادها أن لكل فرد صفاته الجسدية الخاصة التي تختلف من شخص لآخر، والتي تتميز بالثبات النسبي، مما يجعل لها قدراً كبيراً من القوة الثبوتية في التوثيق والإثبات.

ويتم التوقيع بالتقاط صورة دقيقة لصفة جسدية للشخص الذي يريد استعمال الإمضاء البيومتري، ويتم تخزين هذه الصورة على جهاز الحاسب الآلي، وذلك بطريق التشفير، ويعاد فك هذا التشفير للتحقق من صحة التوقيع، وذلك بمطابقة صفات العميل المستخدم للتوقيع مع الصفات التي يتم تخزينها على الحاسب الآلي[2] ، حيث تتم برمجته على أساس ألا يتم فتح القفل المغلق إلا بعد أن يطابق هذه البصمة على البصمة المبرمجة في ذاكرته، وبذلك لا يمكن لغير صاحب هذه الميزة الدخول إلى النظام، أو حتى استخدام الجهاز في الحدود المطلوبة[3] ، عكس التوقيع المعتمد على المفاتيح السرية الذي يمكن أن يتعرض لخطر النسيان أو التزوير أو سرقة أرقام أو كلمات السر[1].

---

[1]- إبراهيم الدسوقي أبو الليل،" توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر"، بحث مقدم بمؤتمر" الأعمال المصرفية الالكترونية بين الشريعة والقانون المنعقدة بدولة الإمارات العربية، غرفة تجارة صناعة دبي، في الفترة 10-12 ماي 2003 الجزء الخامس، ص 1854.

[2]- يتم تخزين بصمة هذا الشخص على سبيل المثال داخل الدائرة الالكترونية للجهاز circuit المراد التعامل معه بحيث لا يمكن أن يستجيب للشخص إلا بعد النطق بكلمات محددة، أو بوضع البصمة، أو المرور أمام الجهاز عندما يتأكد من عملية المطابقة الكاملة نقلا عن نجوى أبو هيبة، **التوقيع الإلكتروني و مدى حجيته في الإثبات**، دار النهضة العربية ، مصر، 2004 ، ص 35 .

[3]- جدير بالذكر أنه بتاريخ 2010/10/30 اعتمد على الخواص الذاتية لأول مرة في العالم في المجال الانتخابي، وذلك في الانتخابات الرئاسية في البرازيل، حيث اعتمدت على الخواص البيوميترية لتحديد هوية الناخبين والتصويت عن طريق

وبوجود التوقيع البيومتري، يمنع أي استخدام غير قانوني أو غير مرخص به لأي معلومات أو بيانات سرية أو شخصية موجودة في نظام المعلومات الخاصة بإحدى الجهات، ولما كانت الخصائص الذاتية لكل شخص تميزه عن غيره من الأشخاص، فإن النتيجة المترتبة عن ذلك تقتضي بأن التوقيع البيومتري يعد وسيلة موثوق بها لتمييز الشخص وتحديد هويته، نظراً لارتباط الخواص الذاتية به، كما يعد من أحدث الصيغ المبتكرة في ظل التطور الحاصل في البطاقة ذات الشريحة[2].

وبالرغم من كل هذا، يعاب على التوقيع البيومتري في إمكانية مهاجمته أو نسخه، إذ من الممكن أن تخضع الذبذبات الحاملة للصوت أو صورة بصمة الإصبع أو شبكة العين للنسخ وإعادة الاستعمال، كما يمكن إدخال تعديلات عليها من قراصنة الحاسب الآلي عن طريق فك شفراتها، كما أنه على الرغم من ادعاء الشركات المصنعة للأجهزة البيومترية من أن نسبة الأمان التي توفره هي100%، إلا أنه تم اكتشاف حالات احتيال باستخدام البصمة الشخصية المقلدة أو ما يعرف بالبصمة البلاستيكية والمطاطية، والتي لم تستطع بعض أجهزة التحقق البصرية المصنوعة من رقائق السيلكون كشفها أو تمييزها[3] .

ونظرا لإمكانية نسخ التوقيع البيومتري على نحو ما ذكرنا، فإن تأمين الثقة بهذا النوع من التوقيع مرهون بإيجاد التقنية التي تؤّمن انتقاله دون التلاعب فيه، ومن ناحية أخرى بإقرار المشرع بكفاءة التقنية في تأمين التوقيع، وبالتالي إمكان الاعتداد به في الإثبات.

إلا أن التكلفة الباهضة نسبياً التي يتطلبها وضع نظام آمن في شبكات للمعلومات باستخدام الوسائل البيومترية، قد حدت من انتشارها إلى درجة كبيرة، وجعلته يقتصر على بعض الاستخدامات المحدد من قبل بعض الجهات كأجهزة الأمن والمخابرات.

---

جهاز كشف البصمات، لمزيد من التفصيل راجع البرازيل تنتخب رئيساً جديداً، مقال على الموقع http//www.moheet.com/show_news.aspx? nid: اطلع عليه بتاريخ 2022/03/14 .

[1]- علاء التميمي، **التنظيم القانوني للبنك الالكتروني على شبكة الإنترنيت**، دار الجامعة الجديدة، الإسكندرية، مصر ، 2012، ص 653 .

[2]- وسيم شفيق الحجار، **الإثبات الالكتروني**، منشورات صادر، بيروت، لبنان، 2002 ، ص 142.

[3]- بشار محمود دودين، **الإطار القانوني للعقد المبرم عبر شبكة الانترنت**، أصل الكتاب رسالة ماجستير، دار الثقافة ، مصر، 2006 ، ص 254.

وكذلك من ضمن الانتقادات الموجهة للتوقيع البيومتري أنه قد لا يعبر بشكل صحيح على الرضا الحقيقي بالالتزام بمضمون ما وقع عليه، فقد يجبر شخص على الوقوف أمام الجهاز الخاص بمسح الخواص البيومترية وبالتالي أخذ بصمته دون رضاه ، إلا أن هذا الانتقاد لا ينال من حجية التوقيع البيومتري في الإثبات، حيث انه يمكن أن يطال التوقيع العادي تحت طائلة الإكراه أو التهديد[1].

ولقد اعتمد المشرع الجزائري هذا النمط من التوقيع بغرض الاستفادة من هذه التقنية لما تنطوي عليه من سمات تحديد هوية الموّقع بدقة، بعد إصدار قرار[2] مؤرخ في 26 ديسمبر 2011 استجابة للمنظمة العالمية للطيران، التي دعت دول العالم إلى إصدار جواز السفر البيومتري.

إن تقنية التوقيع الإلكتروني عن طريقة الترقيم marquage أو وضع علامة أو سمة ، تقوم أساسا على تقنية الستغنوغرافيا steganographie ، و هي تعني عموما إخفاء البيانات في بيانات أخرى cacher l' information dans l' information ،و له عدة أنواع مثل watermarking أوfingerprinting الذي يقوم أساسا على تخزين علامة من علامات المستخدم في علامة أخرى، يتم وضعها بعد ذلك في قرص يوضع في الحاسب الآلي تكون بمثابة علامة لتوقيعه حيث يتمكن الموّقع بواسطتها السيطرة على عناصر إنشاء توقيعه بصورة حصرية، عندئذ يمكن من خلالها التوصل إلى تمييز صاحب التوقيع عن غيره بشكل موثوق به إلى درجة كبيرة بحيث تمتاز بسهولة الكشف عن أي تزوير أو تحريف عليها، لكن تبقى عرضة للتغيير و التحريف[3].

**المطلب الثاني: التوقيع الرقمي**

[1]- تامر محمد سليمان الدمياطي، **إثبات التعاقد الالكتروني عبر الانترنت**، دراسة مقارنة، الطبعة الأولى 2000، مصر ، ص 348.

[2]- قرار صادر عن السيد وزير الداخلية والجماعات المحلية مؤرخ في 26 ديسمبر سنة 2011 يحدد تاريخ بداية تداول جواز السفر الوطني البيومتري الالكتروني .

[3]- ماجد راغب الحلو، مرجع سابق ، ص45 .

يعرف التوقيع الرقمي بأنه " بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة (كود)، والذي يسمح للمرسل إليه إثبات مصدرها وتأكيد سلامة مضمونها وتأمينها ضد أي تعديل أو تحريف"[1]، فهو صورة من صور التوقيع الالكتروني التي تستخدم في إبرام الصفقات القانونية عبر الوسائط الالكترونية[2] ، أو هو "عبارة عن وحدة قصيرة من البيانات التي تحمل علاقة رياضية مع البيانات المتضمنة في محتوى الوثيقة "[3]، كما يمكن تعريفه أيضاً بأنه "طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الانترنيت[4]"، بحيث يعتبر الأوسع نطاقا والأكثر استخداما نظرا لطابع الأمان والثقة التي يوفرهما ، وهذا النوع يعتمد على نظام التشفير cryptologie [5]، لذا يسمى بالتوقيع الرقمي القائم على التشفير .

والتوقيع الرقمي عبارة عن مجموعة أرقام أو حروف يختارها صاحب التوقيع بها، ويتم تركيبها أو ترتيبها في شكل كودي معين، ويتم عن طريقه تحديد شخصية صاحبه، بحيث لا يكون هذا الكود معلوما إلا له فقط.

ويتم الحصول على التوقيع الرقمي عن طريق التشفير[6] ، وذلك بتحويل المحرر المكتوب والتوقيع الوارد عليه من نمط الكتابة العادية إلى معادلة رياضية وذلك باستخدام مفاتيح سرية وطرق حسابية معقدة (لوغاريتمات)، ومؤدى ذلك تحول المستند الإلكتروني من صورته المقروءة والمفهومة إلى صورة رسالة رقمية غير مقروءة وغير مفهومة، ولا يكون بمقدور أي شخص إعادة هذه المعادلة اللوغارتمية إلى صورتها المقروءة إلا الشخص الذي

---

[1]- وفقا للمواصفات القياسية رقم ISO 7498-2029 الصادرة عن المنظمة الدولية للمواصفات والمقاييس لعام 1988 الاطلاع على الموقع الالكتروني www.iso.org .

[2]- يطلق على التوقيع الرقمي باللغة العربية ويسمى أيضا بالتوقيع الكودي ، وبالفرنسية signature numerique وبالانجليزية signature digital .

[3]- عمر خالد زريقات، **عقد البيع عبر الانترنت**، دار الحامد للنشر والتوزيع، عمان، 2007، ص 257.

[4]- محمد خالد جمال رستم، **التنظيم القانون للتجارة والإثبات الالكتروني في العالم**، منشورات الحلبي الحقوقية، بيروت، 2006 ، ص39 .

[5]- جاء في المادة الأولى بند 9 من اللائحة التنفيذية لقانون التوقيع الالكتروني المصري رقم 2004/15 بان التشفير " هو منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة" .

[6]- يجب ألا نخلط بين تشفير التوقيع، وتشفير الرسالة، فإذا كان كل منهما عملية رياضية تهدف إلى تغيير المحتوى المراد تشفيره على نحو يحفظ عليه سريته، إلا أنهما يختلفان في أن تشفير الرسالة يشملها بالكامل بما في ذلك التوقيع، في حين أن تشفير التوقيع فقط دون مضمون الرسالة، وعلى ذلك يمكن أن نتصور توقيعاً مشفر ورسالة الكترونية غير مشفرة. إيمان مأمون سليمان، المرجع السابق، ص 271 .

لديه المعادلة الخاصة بذلك والتي تتمثل في المفتاح، فالشخص المالك لمفتاح التشفير هو الذي يمكنه فقط فك التشفير[1] .

ويتم التشفير بمفتاحين، أحدهما للتشفير ويسمى المفتاح الخاص، والثاني لفك التشفير ويسمى المفتاح العام [2]، ويرتبط المفتاح العام بالمفتاح الخاص، ولكن يتميز عنه بعدم الاحتفاظ بسريته حيث يبلغ إلى المرسل إليه ليتمكن عن طريقه من فك شفرة الرسالة، وقد اصطلح على تسمية هذا النظام بنظام المفتاح العام، وميزة هذه الطريقة أنه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الأخر حسابيا[3].

و التوقيع الرقمي يحقق أعلى درجات الثقة والأمان باعتبار أن علم التشفير كان خاصا بالمجال العسكري و الأمني[4] لعدة أمور هي:

**أولا** :باستخدام التوقيع الرقمي يتحقق الارتباط بين المستند الكتابي والتوقيع الوارد عليه.

**ثانيا:** يضمن عدم إمكان التدخل في مضمون التوقيع أو مضمون المحرر الذي يرتبط به.

**ثالثا** :يؤدي إلى التحقق من هوية الموّقع وأن الرسالة الموّقعة منه تنسب إليه، فلا يمكن للموّقع إنكار أن المستند الموّقع منه لا ينسب إليه، ويرجع ذلك إلى الارتباط التام بين المفتاحين العام والخاص.

**رابعا** :يعبر بطريقة واضحة عن إرادة صاحبه للالتزام بالتصرف القانوني وقبوله لمضمونه، وبذلك فهو يحقق كافة الشروط التي يتطلبها القانون في المحرر لكي يصلح لأن يكون دليلا كتابيا كاملا.

---

[1]- ثروت عبد الحميد، **التوقيع الإلكتروني**، دار النيل للطباعة والنشر، مكتبة الجلاء الجديدة، المنصورة، 2001 ، ص62 .

[2]- آلاء يعقوب يوسف،" المسؤولية المدنية لمجهز خدمات التصديق على التوقيع الرقمي تجاه الغير"، مجلة الحقوق،جامعة البحرين، المجلد الثالث، العدد الأول جانفي 2006 ، ص 306.

[3]- محمد أحمد محمود إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية،أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة عين شمس، 2005 ، ص 73.

[4]- استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب؛ خوفاً من وقوع الرسائل الحساسة في أيدي العدو .وقام يوليوس قيصر بتطوير خوارزميته المعيارية المعروفة باسم شفرة قيصر (Caesar Cipher) التي كانت نصّا مشفَّراً (Cipher text) لتأمين اتصالاته ومراسلاته مع قادة جيوشه، وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير، ومنها آلة التلغيز Enigma machine وتطور علم التشفير سنة 1466 من طرف العالم Leone Bastia Alberti و نظريته الخاصة بفن الأدوار الثلاثي في الرسم ثم حاول بعد ذلك قام بربط نظريته هذه و التشفير فوضع عبارات طويلة يقبلها كود سري فيقوم المرسل إليه بتشفير الكود باستخدام الجدول الذي أعده هذا العالم الموقع http://www.startimes.com/f.aspx?t= 5287300 اطلع عليه بتاريخ 2022/03/13 .

**خامسا** :التوقيع الرقمي يحقق سرية المعلومات التي تتضمنها المحررات الإلكترونية بحيث لا يمكن قراءة تلك المحررات إلا لمن أرسلت إليه وباستخدام المفتاح العام للمرسل.

ويرى البعض الآخر أن تشفير البيانات "يعني تغيير في شكل البيانات عن طرق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من الاطلاع عليها أو تعديلها أوتغييرها"[1]، وينقسم التشفير إلى نوعين التشفير بالمفتاح المتماثل والتشفير بالمفتاح غير المتماثل وسوف نتناولهما على النحو التالي:

**الفرع الأول: التشفير المتماثل**

التشفير بالمفتاح المتماثل ويسمى أيضا بالنظام السيمتري[2] ، ويتمثل هذا النوع في استخدام كل من المرسل والمستقبل نفس المفتاح السري للتشفير ، فطريقة تشغيل هذا النظام تعتمد على مفتاح واحد يستخدمه المرسل في عملية تشفير بيانات المحرر الالكتروني ، كما يستخدمه المرسل إليه في عملية فك هذا التشفير، حيث يحرر المرسل الرسالة ثم يقوم بتشفيرها بالمفتاح المماثل ، وذلك بتحويل الرسالة من صورتها المقروءة والمفهومة إلى صورة رسالة رقمية غير مقروءة تتخذ أشكال ورموز وعلامات غير مفهومة ، ثم يقوم بإرسال الرسالة وكذلك المفتاح المتماثل الذي شفر به بيانات المحرر الالكتروني إلى المرسل إليه ليتمكن هذا الأخير من فك شفرة المحرر وإعادته إلى حالته الأصلية، والتعامل بالنظام " السيمتري" مقصور على الأشخاص الذين تربطهم علاقة تعارف مسبقة، وأيضا هذا النظام فعال في الشبكات المختلفة كشبكة الأنترانات والإكسترانات[3].

---

[1]- هدى حامد قشقوش ، "الحماية الجنائية للتوقيع الالكتروني "، بحث مقدم بمؤتمر ( الأعمال المصرفية الالكترونية بين الشريعة والقانون)، المنعقد بدولة الإمارات العربية المتحدة ، غرفة تجارة وصناعة دبي ، الفترة من 10-12 ماي 2003، الجزء 2 ، ص 590.

[2]- نجوى أبو هيبة ، مرجع سابق ص 72.

[3]- شبكة الانترانت هي عبارة عن سلسلة من شبكات معلومات يمتلكها مشروع او مؤسسة واحدة وهذه الشبكات قد تكون شبكات داخلية محدودة النطاق تتصل بعضها ببعض داخل نفس المكان او تكون شبكات واسعة النطاق تتصل بعضها ببعض في أماكن مختلفة ومتعددة .

أما الاكسترانت هي شبكات خاصة مملوكة لمنشأة معينة تلتزم بذات البروتوكولات التي تستخدمها شبكة الانترنيت في إجراء عملية الاتصال أو تبادل المعلومات بين المنشأة وموزعيها أو مورديها أو فروعها أو شركائها بصورة آمنة ، إذ أن هذه البيانات تتعلق في غالب الأمر بصفقات وعقود ومعاملات تجارية، وعروض وكذلك بيانات سرية تخص العملاء وغير ذلك، وقد أمعن من خلال استخدام شبكة الاكسترانت إتمام العديد من صفقات التجارة الالكترونية انظر قدري عبد الفتاح الشهاوي، قانون التوقيع الإلكتروني ولائحته، دار النهضة العربية، 2005 ، ص 380-381 .

**الفرع الثاني: التشفير غير المتماثل**

التشفير بالنظام غير المتماثل أو كما يسمى أيضا الاستيميتري Asymetriquo[1] الصورة الحديثة المعمول بها لإجراء التوقيع الرقمي، فهو نظام يعتمد على خلق وإنشاء مفتاحين لكل متعامل ، احدهما يسمى بالمفتاح الخاص clé privé[2] ، يكون سريا لدى صاحبه لاستخدامه في التشفير والتوقيع الالكتروني على المحررات الالكترونية المرسلة[3]، والمفتاح الآخر يسمى المفتاح العام clé publique [4]، وهذا المفتاح يكون معروفا للمرسل إليه بحيث يمكن استخدامه لفك التشفير و التحقق من شخصية الموّقع على المحرر الالكتروني ، والتأكد من صحة وسلامة المحرر الالكتروني[5]، وبالتالي فالمفتاح العام يكون معروفا لكلا الطرفين وهذا لوجود رابطة مباشرة بينهما، فإذا استعمل المفتاح الخاص لتشفير المحرر فلا يمكن فك التشفير إلا باستعمال المفتاح العام والعكس صحيح[6]، ولو عرف احد المفتاحين فلا يمكن معرفة الآخر حسابيا[7].

**المطلب الثالث: التوقيع اليدوي المحول إلى الرقمي**

التوقيع بالقلم الالكتروني هو طريقة حديثة من طرق التوقيع البيومتري ويتم هذا التوقيع بقيام الشخص بالتوقيع على شاشة جهاز الحاسب الآلي باستخدام قلم الكتروني خاص، بواسطة جهاز حاسب آلي بمواصفات خاصة تمكنه من أداء مهمته في التقاط التوقيع من شاشته، ويتم حفظ صورة توقيع الشخص بذاكرة الحاسب الآلي، وعندما يرسل مستند الكتروني موقع بخط يده عن طريق القلم الالكتروني يتم المضاهاة بين التوقيع المرسل

---

[1] -sedalin valérie preuve et signature électronique , paris ; sur le cite www.juriscom.net/chr2/fr20000509htm

[2]- يسمى بالانجليزية key private ويظل هذا المفتاح سريا لدى صاحبه ويتكون المفتاح الخاص من مجموعة من الأرقام الحسابية يتشكل منها التوقيع الالكتروني ، ويخزن عادة المفتاح الخاص في بطاقة ذكية، يتم الوصول إليه عن طريق الرقم الشخصي، انظر إبراهيم الدسوقي أبو الليل ، المرجع السابق ص 162 .

[3]- المادة الأولى بند 11 من اللائحة التنفيذية لقانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بجمهورية مصر العربية رقم 15 سنة 2004.

[4]- يسمى المفتاح العام باللغة الانجليزية public key ويتميز هذا المفتاح بعدم سريته وإنما يبلغ للمرسل إليه ليتمكن من فك شفرة الرسالة.

[5]- المادة الأولى بند 12 من اللائحة التنفيذية لقانون التوقيع الالكتروني المصري السالف الذكر.

[6]- وسيم شفيق الحجار ، مرجع سابق ، ص 190 .

[7]- إيمان محمود احمد سليمان ، الجوانب القانونية لعقد التجارة الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه،جامعة المنصورة، 2005-2006، ص 167.

والتوقيع المخزن بذاكرة الحاسب، يتم التحقق من صحة التوقيع بالاستناد إلى حركة القلم الالكتروني والأشكال التي يتخذها من انحناءات أو إلتواءات وغير ذلك من سمات خاصة لتوقيع الموّقع .

ويعتبر التوقيع بالقلم الإلكتروني من بين أهم أنواع التوقيع الإلكتروني، ويعد واحدا من بين الأوجه الحديثة له، يتم فيه الاعتماد على قلم خاص يستعمل على حاسب آلي مزّود بماسح ضوئي لقراءة المعلومات التي يضعها الشخص صاحب التوقيع ممثلة في توقيعه حيث" يعتمد التوقيع بالقلم الإلكتروني على نفس الخاصية التي تقوم عليها التوقيعات الخطية التقليدية"[1] .

ويتم ذلك" باستخدام قلم إلكتروني يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي متخصص يقوم بالتقاط التوقيع والتحقق من صحته، إذ يتم نقل التوقيع بخط اليد عن طريق الماسح الضوئي ، ثم تُنقل هذه الصورة إلى الرسالة الإلكترونية المراد التأشير عليها بهذا التوقيع لإضفاء الحجية لها[2].

من خلال ما سبق ذكره نستشف أن هذا البرنامج الذي يتوفر عليه الحاسوب المزود بماسح ضوئي يقوم بوظيفتين أساسيتين، الأولى تتمثل في التقاط التوقيع من القلم الإلكتروني بخط يد الموّقع ، والثانية هي التحقّق من صحة هذا التوقيع.

وحتى يؤدي نظام التوقيع بالقلم الإلكتروني وظيفته بالشكل المطلوب فإنه بحاجة إلى حاسوب بمواصفات وتقنيات خاصة ومزود بمرفقات تقنية تضمن له استقبال الرسالة المعلوماتية وقراءتها، لكن هذا النوع لا يتمتع بأي درجة من الأمان، كذلك لا يتضمن حجية في الإثبات[3] .

---

1- محمد سعيد أحمد إسماعيل، **أساليب الحماية القانونية لمعاملات التجارة الإلكترونية** دراسة مقارنة ، ط1 ، منشورات الحلبي الحقوقية، لبنان، 2009، ص 270 .

2- إبراهيم إسماعيل الربيع، علاء موسى علي نالي،" التوثيق الإلكتروني– قرارات التحكيم في التوقيع الإلكتروني" ، دراسة، مقارنة ، مجلة المحقق الحلي للعلوم القانونية والسياسية، بابل، العراق ، العدد رقم01 ، 2012، ص 170 .

3- محمد مدحت عزمي، **المعاملات التجارية الإلكترونية الأسس القانونية والتطبيقات**، مركز الإسكندرية للكتاب، مصر، 2009، ص 275 .

وأهم ميزة لهذا النوع من التوقيع تكمن في التحقّق من صحته كل مرة يتم فيها، ولكن يؤخذ عليه أنه يحتاج إلى أجهزة مرفقة بالحاسوب وهي غير متوفرة دائما، كما أن استخدامه عبر شبكة الانترنيت سيحتاج إلى جهة توثيق تضمن عدم التلاعب به أو تزويره .

وإذا كان تزوير هذه الصورة من صور التوقيع الالكتروني يفوق في الصعوبة تزوير التوقيع على المستندات الورقية ،ذلك أن عملية المقارنة بين التوقيع بالقلم ونسخة التوقيع بخط اليد تتم من خلال تقنية تتسم بدقة كبيرة بحيث يسهل اكتشاف التزوير، فإنه لا يمكن أن نحيطه بدرجة كبيرة من الأمان اللازم توافرها بالتوقيع حتى يمكن الاعتداد بها في الإثبات، وتبقى عملية الأمان من الاعتداء عليه نسبية، إذ أن المرسل إليه صورة التوقيع يستطيع أن يحتفظ بصورة منه ثم يعيد وضعها على أي وثيقة من الوثائق المحررة على الوسائط الالكترونية وينسبها لصاحب التوقيع ، و يفضل استعمال هذا الإمضاء عبر شبكات Extranet أو Intranet إذ أن المتعاملين عليها بصفة عامة يعرفون بعضهم البعض وهي شبكات أكثر أمانا من شبكة Internet [1].

**المطلب الرابع: التوقيع بالرقم السري و البطاقة المغناطيسية**

التوقيع عن طريق البطاقة المقترنة بالرقم السري (التوقيع الكودي) غالبا ما يرتبط التوقيع السري بالبطاقات البلاستيكية والبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية، ويتم توقيع التعاملات الالكترونية وفقا لهذه الطريقة باستخدام مجموعة من الأرقام أو الحروف أو كليهما، يختارها صاحب التوقيع لتحديد شخصيته ولا تكون معلومة إلا له ولمن يبلغه به[2] ، وتسمى هذه الطريقة بالإنجليزية اختصار (PIN) .

ينتشر استعمال التوقيع السري أو الكودي في عمليات المصارف والدفع الالكتروني ، حيث تحرص البنوك على تنظيم عملية الإثبات بمقتضى اتفاق مع حامل البطاقة في العمل

[1]- المنصف قرطاس، "حجية الإمضاء الالكتروني أمام القضاء"، مجلة التجارة الالكترونية والخدمات المصرفية والمالية عبر الانترنيت ، اتحاد المصارف العربية، 2000 ، ص237 .
[2]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 185 .

، توجد صور عدة لهذه البطاقات[1] مثل VISA card وMaster card وAmerican Express ، تعمل هذه البطاقات بنظامين هما نظام Off-Line ونظام On-Line وتنحصر إجراءات التوقيع بالموافقة على عمليات السحب النقدي أو السداد بالبطاقة[2] في:

- ✓ إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل في جهاز الصرف الآلي.
- ✓ إدخال الرقم السري الخاص بالعميل والذي لا يعلم به سواه.
- ✓ إصدار الأمر بالسحب أو بالتسديد بالموافقة على العملية بالضغط على المفتاح الذي يكتمل به التعبير عن الإرادة في قبول العملية حيث يتم صرف المبلغ المطلوب أو تسديده ثم تعاد البطاقة للعميل.

وقد أقر القضاء الفرنسي مبكرا بحجية التوقيع الالكتروني بالبطاقات الالكترونية المقترنة بالرقم السري واعترف لها بالحجية الكاملة في الإثبات، حيث استند القضاء الفرنسي في منحه الحجية القانونية على الاتفاقات التي تبرم بين ذوي الشأن، وعليه فإن هذا النوع من أنواع التوقيع لا يصلح لإعداد الدليل (المستند) الكتابي المهيأ للإثبات، لأنه لا يتم إلحاقه بأي محرر كتابي، إنما يتم تسجيله في وثائق البنك منفصلا عن أي وثيقة تعاقدية .

هذا و تقوم البطاقة البنكية بعدة وظائف مثل الوفاء بالمبيعات أو سحب النقود أو الائتمان[3] ، و سنحاول استعراض بعض بطاقات السحب و الوفاء المعروفة في الجزائر، دون بطاقة الإئتمان التي لا تصدرها البنوك الجزائرية، وعرف المشرع الجزائري بطاقة الدفع في المادة 543 مكرر 23 من القانون التجاري[4] التي تنص على ما يلي" تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال".

---

[1]- نجوى أبو هيبة، مرجع سابق، ص67 .

[2]- إيمان مأمون أحمد سليمان، مرجع سابق، ص263 .

[3]- إن بطاقة الائتمان هي عبارة عن قروض محددة بنقطة استدلالية حسب مداخيل العميل و يستطيع أن يستعملها حتى ولو لم يكن في حسابه البنكي مالا حيث يضع له البنك مبلغ أقصى يستطيع استعماله و عليه بإرجاعه مضافا له عمولة و على العموم أصبح مصطلح بطاقة الائتمان شاملا لكل أنواه البطاقات التي تصدرها البنوك على اختلاف أنواعها رغم أن بطاقة الائتمان هي واحدة منها لهذا نفضل مصطلح البطاقة البنكية التي تشمل جميع أنواع البطاقات، خالد عبد التواب عبد الحميد ، نظام بطاقات، الدفع الإلكتروني من الناحية القانونية، دون دار النشر ،2006 ، ص42 .

[4]- القانون رقم 05-05 المؤرخ في 06 فيفري2005 ، المتضمن القانون التجاري المعدل والمتمم الصادر بالجريدة الرسمية للجمهورية الجزائرية بتاريخ 26 جويلية 2005 ، عدد رقم 30 .

من خلال المادة المذكورة أعلاه تناول المشرع الجزائري بطاقة الدفع بالتعريف دون أن يتدخل في تنظيمها ، ليفتح المجال للمؤسسات المالية المختصة في إصدارها كالبنوك أو مصالح البريد كما هو معمول به في الجزائر، و تصدر هذه البطاقات حسب التطور الحاصل في البيئة التجارية و المصرفية وهذا ما أكدته المادة 71 من الأمر 11/03المؤرخ في 2003/08/26 المتعلق بالنقد والقرض[1] والتي تنص على أنه" لا يمكن للمؤسسات المالية تلقي الأموال من العموم، ولا إدارة وسائل الدفع أو وضعها تحت تصرف زبائنها، وبإمكانها القيام بسائر العمليات الأخرى " [2]، واهم البطاقات المعروفة في الجزائر هي:

تضمنت المادة 543 مكرر 23 تعريفا لبطاقة السحب بأنها" البطاقة التي تعتبر بطاقة السحب كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أموال" ؛ أي أنها بطاقة تصدرها هيئة مختصة هي غالبا مؤسسات مصرفية و مالية، وفي الجزائر تصدرها البنوك و بريد الجزائر[3] ، بعد أن يتم فتح حساب باسم الشخص.

- تضمنت المادة 543 مكرر 23 تعريفا لبطاقة الوفاء ، وجاء فيها ما يلي: " تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا[4] ،وتسمح لصاحبها بسحب أو تحويل أموال "، و تسمى بطاقة الوفاء البنكية كذلك ببطاقة الدفع.

ملاحظة: قد يوجد النوعان المذكوران أعلاه من البطاقات في بطاقة واحدة فتصبح بطاقة سحب و وفاء في آن واحد.

---

[1]-الأمر 11/03المتعلق بالنقد والقرض المؤرخ في 2003/08/26 الصادر بالجريدة الرسمية للجمهورية الجزائرية لسنة 2003عدد رقم 52 .

[2]- يعرف المجلد الإنجليزي longman dictionary of contempory English البطاقة فيزا كارد بما يلي:
"a type of credit card (plastic card used to obtain goods and services, which the buyer pays for later) which can be used all over the world".

[3]- باشرت مصالح البريد في الجزائر ابتداء من الفاتح جانفي2007 عملية توفير بطاقات السحب، واختيرت الجزائر العاصمة كمرحلة أولى قبل تعميم العملية على باقي المناطق الأخرى .إلا أن النتائج بعد سنتين ظلت محدودة مع بروز تردد وعزوف خاصة لدى فئات الشباب، بينما لوحظ بأن المتقاعدين هم الفئة الأكثر استخداما للبطاقات .معلومات مأخوذة من الموقع الآتي: http://www.elkhabar.com/quotidien/?idc=49&ida=149052&date_insert=20090323

[4]- لقد و ضع بنك القرض الشعبي الجزائري CPA أنواع من بطاقات السحب الأولى بطاقة عادية تسمى CPA/VISA CLASSIC و ثانية هي البطاقة الذهبية لكبار رجال الأعمال CPA/VISA/GOLD. اطلع عليه بتاريخ 2002/03/14.

**خلاصة الفصل التمهيدي:**

من خلال كل ما تم تناوله في ما سبق يمكن الخروج بتعريف عام للتوقيع الالكتروني في كونه عبارة عن ملف رقمي صغير مؤلف من حروف أو أرقام أو رموز الكترونية ،يصدر عن إحدى الجهات المستقلة المعترف بها يسمى بالشهادة الالكترونية الرقمية ، تخزن فيها كافة معلومات الشخص وتاريخ ورقم شهادة مصدرها ، ويسلم مع هذه الشهادة مفتاحان مفتاح عام ينشر في الدليل لكل الناس ،

ومفتاح خاص هو التوقيع الالكتروني لا يعلمه إلا صاحبه ويدل على شخصيته وصحة الواقعة المنسوبة إليه.

والهدف من إنشاء التوقيع الالكتروني هو تحقيق اكبر قدر من السلامة والأمن الرقميين ، وإبعاد المتطفلين والقراصنة من سرقة البيانات الالكترونية، أو التلاعب بها من خلال توثيق التوقيع الالكتروني كل شخص[1] ورفع مستوى الأمن و الخصوصية بين المتعاملين عبر شبكة الانترنيت من خلال المحافظة على سرية المعلومات بما فيها معلومات التجارة الالكترونية ، والحكومة الالكترونية وسرية الرسائل المرسلة ، وعدم إمكانية تداولها إلا بالتوقيع عليها لأجل معرفة أو تحديد هوية المرسل والمرسل إليه الكترونيا[2].

[1] -http:/news. maktoob. com /article 620364 ، 2022/05/25 مقال منشور عبر الرابط اطلع عليه بتاريخ

[2]- عبد الفتاح بيومي حجازي ، مرجع سابق ، ص 72-73 .

# الفصل الثاني

# الفصل الثاني: الجرائم الماسة بالتوقيع الالكتروني وآليات حمايتة

## تمهيد:

إن الانتشار الواسع والسريع لاستخدام التكنولوجيا والتقنية الحديثة جعل المشرع يتدخل مرة أخرى لأجل بسط الحماية خاصة في المعاملات التجارية، لأجل الحث على الإقبال على إبرام العقود الالكترونية التي أصبحت قابلة للتوقيع والتشفير والمصادقة الالكترونية من قبل أجهزة حددت صلاحيتها وشروط اعتمادها، والمشرع أقر حمايتها من خلال تعداد مختلف الجرائم المتعلقة بالتوقيع والتصديق الالكترونيين، وطالما أن المشرع لم يعتمد أي تصنيف لهذه الجرائم إلا أنّ قرائتنا لهذه النصوص والجرائم المتضمنة لها، نميز بين تلك التي تلحق التوقيع الالكتروني ومؤدي خدمات المصادقة، وبين تلك التي تجرم بعض الممارسات المرتبطة بطالبي الخدمة، كما أن الاطلاع على تلك النصوص القانونية نجد وأن الجرائم التي نظمها المشرع تتفق في أنها جرائم عمدية يتطلب قيامها توافر الركن المعنوي الذي يقوم على القصد الجنائي العام بعنصريه العلم والإرادة ، ولا تحتاج إلى القصد الخاص، ويتمثل في العلم الواجب توافره في القصد الجنائي العام في إحاطة الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، أي كل واقعة يتطلبها القانون لبناء أركان الجريمة واستكمال عناصرها، وإضافة إلى ذلك لابد أن يشمل العلم أيضا التكييف الذي تتصف به بعض هذه الوقائع من الناحية القانونية، أو بعبارة أخرى يتعين على الجاني العلم بموضوع الحق المعتدى عليه.

أما الإرادة التي يتطلبها القصد العام فهي" حالة ذهنية أو نفسية يكون عليها الجاني ساعة إقدامه على ارتكاب الجريمة لتحقيق النتيجة المطلوبة "، وعليه فقد تم تقسيم هذا الفصل إلى مبحثين تناول الأول الحماية الجزائية الموضوعية للتوقيع الالكتروني ، أما المبحث الثاني فسنتطرق فيه إلى الحماية الجزائية الإجرائية للتوقيع الالكتروني.

## المبحث الأول: الحماية الجزائية الموضوعية للتوقيع الالكتروني

أضفى المشرع الجزائري حماية جزائية للأنظمة المعلوماتية ومعطيات الحاسب الآلي بوجه عام ضمن تعديل قانون العقوبات لسنة 2004 في نص المواد 394 مكرر إلى 394 مكرر7، ولأن التوقيع الالكتروني بإمكانه أن يكون ضمن نظام معلوماتي فهو يتمتع بحماية جزائية ومصلحة قانونية محمية وفقا لقواعد المساس بالنظام المعلوماتي ومعطياته ، وجرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني تندرج ضمن الإطار العام للجريمة المعلوماتية .

ولتفصيل الحماية الجزائية الموضوعية للتوقيع الالكتروني فقد جاء المبحث الأول في مطلبين تناول الأول الحماية الجزائية الموضوعية المستحدثة للتوقيع الالكتروني في ظل قانون المعالجة الآلية للمعطيات ، والثاني الحماية الجزائية للتوقيع الالكتروني في القانون رقم 04/15 .

### المطلب الأول: الحماية الجزائية الموضوعية المستحدثة للتوقيع الالكتروني في ظل قانون المعالجة الآلية للمعطيات

بعد أن اعتد المشرع الجزائري بالتوقيع الالكتروني طبقا للمادة 237 من القانون المدني التي تنص في الفقرة الثانية منها على أنه" يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 232 مكرر5 أعلاه"، وقبل صدور القانون 04/15 لم ينظم المشرع الجزائري التوقيع الالكتروني ولم يخصه بحماية جزائية خاصة على غرار التشريع الفرنسي، مما جعل حمايته تخضع للقواعد العامة المقررة في قانون العقوبات من خلال جرائم الاعتداء، والجرائم الماسة بالمعالجة الآلية لمعطيات التوقيع الالكتروني التي تندرج ضمن الإطار العام للجريمة المعلوماتية، وسنتطرق في هذا المطلب إلى جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني، وكذا جريمة الاتفاق الجنائي للمساس بأنظمة المعالجة الآلية للمعطيات، وأخيرا سنتناول جريمة التعامل في معطيات غير مشروعة.

**الفرع الأول: جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني**

جرم المشرع الجزائري الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات من دون أن يفرد نص خاص بذلك للتوقيع الالكتروني، على عكس بعض التشريعات التي جرمت الدخول بطريق الغش إلى نظام أو قاعدة بيانات تتعلق بالتوقيع الالكتروني بنص خاص[1]، وسنتطرق لهذه الجريمة من خلال بيان أركانها وعقوبتها.

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 للجريمة رغم أن الدخول في بداية الأمر كان مشروعا "[2]، وهي تقوم على ركنين مادي ومعنوي، بالإضافة إليهما فمحل الجريمة هو النظام المعلوماتي كركن مفترض، لذلك سنتطرق إلى ركنيها المادي والمعنوي.

**أولا: الركن المادي:** "هو نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح به[3] " .

**أ- الركن المفترض (النظام المعلوماتي):** نظرا لأهمية المعلومات في الوقت الحاضر، فقد استحدثت وسائل كثيرة لحمايتها، وحماية أنظمة معالجتها وقد تنوعت هذه الوسائل بين مادية

---

[1]- مثل التشريع المصري الذي جرم الدخول إلى قاعدة بيانات تتعلق التوقيع الالكتروني في نص المادة 26 من قانون التجارة الالكترونية التي تنص على " مع عدم الإخلال بأي عقوبة أشد وردت في أي قانون آخر يعاقب بالحبس وبغرامة لا تقل عن 300 جنيه أو بإحدى هاتين العقوبتين ، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الالكترونية ، ويعاقب بنفس العقوبة من اتصل أو بقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة.

[2]- 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،ص 137.

[3]- صالح شنين، الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة تلمسان،الموسم الجامعي 2012 -2013، ص74 .

ومعنوية، و يلجأ أصحاب الأنظمة المعلوماتية كثيرا إلى مثل هذه الأساليب وغيرها لتأمين الحماية للمعلومات التي تحويها أنظمتهم [1].

وقد عرفت الفقرة ب من المادة 2 من القانون رقم 04/09 بأنه " يقصد بمنظومة معلوماتية أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

و النظام المتعلق بالتوقيع الالكتروني عبارة عن بيانات أو معلومات تم معالجتها بعد إتباع طرق وإجراءات الكترونية معينة، فصارت برنامجا تطبيقيا تم تحميله على الحاسب الآلي من أجل تشغيله والحصول على نتائج معينة خاصة بالتوقيع الالكتروني، لذلك فإن قاعدة البيانات عبارة عن معلومات مخزنة يتم الرجوع إليها عند الحاجة، والنظام المعلوماتي قد يكون في صورة برنامج تطبيقي لتشغيل الحاسب الآلي ، وكلاهما يتعلق بالتوقيع الالكتروني[2].

ويمثل نظام أو نظم المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة الاعتداء على نظام متعلق بالتوقيع الالكتروني، فإذا ثبت تخلف هذا الشرط الأولي لا يكون هناك مجال للبحث في جريمة الاعتداء على نظام التوقيع الالكتروني، وبتوافر شرط النظام يمكن الانتقال والبحث في مدى توافر أركان جريمة الاعتداء على النظام أو الجرائم الملحقة والمرتبطة به[3]".

**ب- السلوك الإجرامي :** ويمكن أن يكون الفعل المجرم في صورتين:

**1-فعل الدخول غير المصرح به:** هو الوصول إلى المعلومات أو البيانات المخزنة داخل نظام الحاسب دون رضاء المسؤول عن هذا النظام أو المعلومات التي يحتويها أو بمعنى

---

[1]- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن**، دار الجامعة الجديدة،الإسكندرية،2007 ، ص 136.

[2]- عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها الجنائية**،دار الفكر الجامعي، الإسكندرية،2004، ص 185.

[3]- علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، الإسكندرية، 2010 ،ص 110.

آخر إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزونة بداخله[1] .

فالدخول له طبيعة معنوية غير مادية، أي أنه يختلف عن مفهوم الدخول كما هو متصور في العالم المادي، والحقيقة أن هذه النظرة هي التي تتفق مع العالم المعلوماتي ومكوناته غير المادية[2].

بالإضافة أيضا أن الدخول لابد أن يكون غير مصرحا به، فمجرد الدخول إلى نظام الحاسب الآلي لا يشكل فعلا غير مشروع، وإنما يشكل الفعل عدم مشروعيته من كونه غير مصرح به أو بدون وجه حق، ويرتبط أساسا من له الحق في الدخول إلى نظام الحاسب الآلي أو في التصريح بالدخول إليه فمناط التجريم هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك، ويكون الدخول غير مصرح به في حالتين:

**الأولى:** إذا كان هناك مسؤول عن نظام الحاسب الآلي وكان دخول الفاعل إلى هذا النظام قد تم دون الحصول على تصريح منه، أي الدخول يكون من قبل أشخاص خارج المؤسسة التي يوجد بها نظام الحاسب الآلي.

**الثانية:** إذا كان دخول الفاعل إلى نظام الحاسب الآلي في غير الحالات المرخص له بذلك، أي يتجاوز التصريح الممنوح له بالدخول إلى معطيات لا يشملها التصريح[3] ، إلا أن المشكلة تكون في حالة الدخول غير المصرح به من قبل العاملين في المؤسسة الذي يوجد بها نظام الحاسب الآلي الذي تم الدخول إليه، ففي هذه الحالة يتجاوز العامل السلطة المخولة له بدخوله إلى هذا النظام في غير الحالات المرخص له فيها بذلك، ويصعب في كثير من الأحيان معرّفة ما إذا كان العامل قد تجاوز بالفعل اختصاصه، ولهذا ينبغي تحديد اختصاصات العاملين بالمؤسسة في شأن استخدام الحاسب الآلي بها تحديدا دقيقا حتى يسهل تحديد التجاوزات، كما يتعذر في كثير من الأحيان معرّفة ما إذا كان العامل قد تجاوز

---

[1]- نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية** -دراسة نظرية وتطبيقية، ط 1 ، منشورات الحلبي الحقوقية، بيروت، 2005، ص 317.

[2]- محمد خليفة، مرجع سابق ، ص 82-83.

[3]- نائلة عادل فريد قورة ، مرجع سابق، ص333 .

اختصاصه عمدا نظرا لكثرة احتمالات دخوله إلى نظام الحاسب الآلي ودخوله إلى معلومات غير مرخص له الوصول إليها بطريق الخطأ أو الصدفة [1].

**2- البقاء في النظام المعلوماتي:**

البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، والسلوك الإجرامي في البقاء يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والاطلاع فقط ، ويتحقق أيضا بالنسبة للخدمات الموجهة للجمهور مثل الخدمات التليفونية والتي يستطيع فيها الجاني الحصول على خدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة[2]، وقد يجد شخص نفسه داخل نظام لحاسب آلي غير مسموح له بالدخول إليه عن طريق الخطأ معتقدا أنه في نظام له الحق في الدخول إليه، وفي هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تنبيهه للخطأ الذي وقع فيه، وقد يستمر البقاء في هذا النظام على الرغم من معرفته بأن هذا النظام غير مصرح له بالدخول إليه[3] .

وما يجمع بين حالة البقاء بعد دخول مصرح به أو بعد دخول عن طريق الصدفة أو الخطأ أن الدخول في جميع الحالات كان مشروعا، وبالتالي لا يمكن أن نطبق بشأنه أحكام جريمة الدخول غير المصرح به، لذلك تدخل المشرع الجنائي ليضيف سلوكا آخر إلى جانب الدخول غير المشروع وهو البقاء غير المشروع أو وغير المصرح به لأن المصلحة القانونية المحمية هي واحدة بالنسبة للفعلين معا[4].

---

[1]- المرجع نفسه، ص 334.

[2]- علي عبد القادر القهوجي ، مرجع سابق، ص122 .

[3]- نائلة عادل فريد قورة ، مرجع سابق، ص 346.

[4]- محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، دراسة مقارنة ، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق،جامعة عنابة، الموسم الجامعي 2010-2011 ، ص 161.

**ب .الركن المعنوي في جريمة الدخول**

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[1] .

**ثانيا :عقوبة الدخول أو البقاء في النظام المعلوماتي للتوقيع الإلكتروني**

هناك عقوبات أصلية وعقوبات تكميلية.

**أ .العقوبات الأصلية :** وهي العقوبات الواجب على القاضي النطق بها في جريمة معينة، فلا عقوبة جنائية بدون عقوبة أصلية ، وتقسم إلى عقوبات أصلية بسيطة ومشددة.

**1-العقوبات الأصلية البسيطة:** تعاقب المادة 394 مكرر إذا لم ينجم عن الدخول أو البقاء غير المصرح بهما إعاقة أو أفساد لنظام المعالجة الآلية للمعطيات أو إزالة أو تعديل لمعطياته، فإن العقوبة تكون الحبس من ثلاث أشهر إلى سنة، وغرامة من 50000 إلى 100000دينار جزائري.

**2- العقوبات الأصلية المشددة:** تعاقب المادة394مكرر فقرة01 و 02 إذا ترتب عن الدخول أو البقاء غير المصرح بهما إزالة أو تعديل لمعطياته فإن العقوبة تكون الحبس من ستة 06 أشهر إلى سنتين02 وغرامة من 100.000إلى400.000 دينار جزائري.

والظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة القصدية الأساسية وهي جريمة الدخول أو البقاء علاقة سببية للقول بتوافره، كما لا يشترط أن تكون النتيجة غير مقصودة أي على سبيل الخطأ غير العمدي، إلا إذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن إزالة أو تعديل المعطيات يرجع للقوة القاهرة أو الحادث المفاجئ ، كما لا يشترط أن تكون النتيجة غير مقصودة أي على سبيل الخطأ غير العمدي، ويكفي لتوافر هذا

[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 ، ص65.

الظرف وجود علاقة سببية بين الدخول أو البقاء غير المشروع والنتيجة الضارة المتمثلة في إعاقة أو إفساد النظام، أي بمعنى عدم قدرة هذا النظام للقيام بوظيفة المعالجة الآلية لمعطيات التوقيع الالكتروني، مع عدم اشتراط القصد للنتيجة لأن الظرف المشدد هنا هو ظرف مادي[1]، وإذا ترتب عنه إعاقة أو أفساد لنظام المعالجة الآلية للمعطيات فتكون العقوبة مشددة.

وتضاعف وتشدد أيضا العقوبات المشار إليها في المادة 394 مكرر و 394 مكرر 01 و 02 إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر 3 مع إمكانية تطبيق عقوبات على الشخص المعنوي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر 4 .

**3- العقوبات التكميلية:** العقوبات التكميلية هي التي لا يمكن النطق بها دون العقوبات الأصلية، وتكون دائما لتكملة العقوبات الأصلية، بهدف إعطاء أكثر فعالية للردع، وتشمل في جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني عقوبة المصادرة، وإغلاق المواقع.

- **المصادرة :** وهي نقل ملكية مال أو أكثر للدولة كعقوبة ناقلة للملكية جوهرها حلول الدولة محل المحكوم عليه أو غيره في ملكية مال[2]، وقد نصت عليها المادة 394 مكرر 06 بمصادرة الأجهزة والبرامج والوسائل المستخدمة في جريمة الدخول أو البقاء في نظام المعالجة الآلية لمعطيات التوقيع الالكتروني.
- **غلق المواقع:** نصت عليها أيضا المادة 394 مكرر 06 بإغلاق المواقع التي تكون محلا لجرائم المساس بالمعالجة الآلية للمعطيات، مع إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

[1]- علي عبد القادر القهوجي، مرجع سابق، ص 126-127.
[2]- محمود نجيب حسني ، **شرح قانون العقوبات** -القسم العام ، ط 8 ، دار النهضة العربية، القاهرة، 2018، ص 146.

**الفرع الثاني: جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني**

تضمن التشريع الجزائري تجريم الاعتداء القصدي على معطيات التوقيع الالكتروني في نص المادة 394 مكرر 01 بقولها " كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

**أولا :التمييز بين الاعتداء على النظام والاعتداء على المعطيات**

جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني مماثلة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للتوقيع الإلكتروني وتهدف العقوبة إلى الحماية من أفعال التخريب والقرصنة، إلا أنهما يختلفان في أن محل الاعتداء على النظام إن كانت تقع على البرامج وشبكات الاتصال فينتج عنه أيضا الاعتداء على المعطيات، والعكس فإن المساس بالمعطيات لا يترتب عنوه المساس بالنظام[1] .

وقد ضع جانب من الفقه معيار المحل الذي تقع عليه، فإذا كان الفعل يقع على العناصر المادية للنظام فإن الجريمة تكون الاعتداء القصدي على النظام، أما إذا كانت تقع على عناصر معنوية فإننا نكون أمام جريمة اعتداء على المعطيات، وما يؤخذ على هذا المعيار أن كلا من الجريمتين قد تقع على العناصر المادية والمعنوية معا، لذلك ذهب جانب من الفقه إلى الأخذ بمعيار الغاية، فإذا كان غاية الجاني الاعتداء على النظام نكون أمام جريمة الاعتداء القصدي على نظم المعالجة الآلية لمعطيات التوقيع الإلكتروني، وإذا كان غاية الجاني الاعتداء على معطيات التوقيع الإلكتروني نكون أمام جريمة الاعتداء على معطيات التوقيع الإلكتروني[2].

**ثانيا :أركان جريمة الاعتداء القصدي على معطيات التوقيع الالكتروني**

تضمن نص المادة 394 فقرة 01 ثلاث أفعال بطريق الغش وهي الإدخال، المحو، التعديل، سنتطرق لهم كصور للركن المادي، ثم ركنها المعنوي.

[1]- علي عبد القادر القهوجي ، مرجع سابق، ص 135-136.
[2]- المرجع نفسه، ص 136.

**أ- الركن المادي:** النشاط الإجرامي يتخذ ثلاث ولا يشترط اجتماعها فإحدى الصور تكفي لتوافر الركن المادي وهي:

**1- الإدخال** :يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أو يوجد عليها معطيات من قبل، كإدخال برنامج غريب يضيف معطيات جديدة.

**2- المحو** :ويقصد به إزالة جزء من المعطيات المسجلة على دعامة موجودة داخل النظام أو تحطيم تلك الدعامة ،أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

**3- التعديل** :وهو تغيير المعطيات داخل النظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة أو برامج الفيروسات بصفة عامة.

والأفعال السابقة وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة بصور أخرى.

**ب- الركن المعنوي:** جريمة قصدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة إلى فعل الإدخال أو المحو أو التعديل وعلمه إلى أن نشاطه الإجرامي يترتب على التلاعب في المعطيات بما ليس له الحق في ذلك، وباعتدائه على صاحب الحق والسيطرة على تلك المعطيات أو بدون موافقته[1].

أما عن الركن المعنوي للجريمة في صورتها المشددة فيتضح من خلال الفقرتين2 و3 من المادة 290 مكرر قانون العقوبات أن النتيجة المشددة هي نتيجة غير عمدية وهو الأمر الذي ذهب إليه جانب من الفقه الفرنسي بأن هذه الجريمة تقع عن طريق الخطأ، ولا يتطلب المشرع فيها توافر القصد الجنائي العمدي، بحيث يعد الخطأ كافيا لقيام الجريمة، ومن هنا

[1]- المرجع نفسه، ص 133.

فهي من جرائم الإهمال، وبالتالي فبمجرد ارتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذا استطاع الجاني إثبات وجود قوة قاهرة أدت إلى حدوثها[1].

**ثالثا :عقوبة الاعتداء القصدي على معطيات التوقيع الالكتروني**

تعاقب المادة 394 مكرر 01 بالحبس من 06 ستة أشهر إلى03 ثلاث سنوات وبغرامة من 500.000 دج إلى4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر 3 مع إمكانية تطبيق عقوبات على الشخص المعنوي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر 4 ،وتطبق أيضا العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة اعتداء قصدي على معطيات التوقيع الالكتروني بعلم مالكها وفقا لنص المادة 394 مكرر.

**الفرع الثالث: جريمة الاتفاق الجنائي للمساس بأنظمة المعالجة الآلية للمعطيات**

المشرع الجزائري لم يكتف بتجريم الشروع في الجريمة فقط وإنما جرَم قبل ذلك الاتفاق على الإعداد لارتكاب هذه الجريمة إذا تجسد في أعمال مادية، وجرَم التعامل في معطيات غير مشروعة والتي تعتبر من جرائم الخطر ومن خلالهما بهدف التجريم الوقائي لسد كل الأبواب أمام ارتكاب جريمة التواجد غير المشروع، وامتد أيضا التجريم إلى مراحل لاحقة بالجريمة وهو ما يتجلى في الصورة الثانية من جريمة التعامل في معطيات غير مشروعة، والمتمثلة في التعامل في المعطيات المتحصلة من الجريمة [2]، لذلك سنتطرق إلى الحكمة من تجريم الاتفاق، وتمييزه عما يشابهه، ثم أركان الاتفاق لارتكاب الجرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني، ثم عقوبتها.

[1]- نائلة عادل فريد قورة، مرجع سابق ، ص473

[2]- محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، مرجع السابق، ص 202-203.

**أولا :الغاية من تجريم الاتفاق على الإعداد لارتكاب جريمة التواجد غير المشروع للأنظمة المعلوماتية**

رغبة من المشرع في تفعيل الوقاية من الجريمة تواجد في مرحلة مبكرة تسبق الشروع، ذلك أن الاتفاق على ارتكاب تلك الجريمة يعطي لهذه الأخيرة بعدا تنظيميا يتطلب التصدي المسبق له، لأنه يشكل خطرا جديا وحقيقيا، ومن شأن تركه أن يؤدي إلى ارتكاب جريمة التواجد وإلحاق ضرر، فتجريم الاتفاق هو حرب استباقية من المشرع ضد جريمة التواجد غير المشروع في الأنظمة المعلوماتية[1].

**ثانيا :التمييز بين الاتفاق وما يشابهه:** هناك ما يشابه الاتفاق في ارتكاب الجرائم كالاشتراك والشروع.

**أ- الاتفاق الجنائي والاتفاق كوسيلة اشتراك:** يتلخص وجه الشبه بين الاتفاق الجنائي والاتفاق كوسيلة اشتراك في أن كليهما من صنف واحد، فليس ثمة فارق بين النوعين من حيث طبيعتهما ،أما من حيث الاختلاف بينهما يتلخص في:

-أن الاتفاق الجنائي على خلاف الاتفاق كوسيلة اشتراك محدد بجرائم معينة.

-لا يقوم الاتفاق الجنائي إلا في الجرائم العمدية بينما في الاتفاق كوسيلة اشتراك قد يكون موضوعه الجرائم العمدية كالجنايات أو الجنح أو المخالفات وهي في الغالب غير عمدية.

-أن الاتفاق الجنائي قد يكون موضوعه الأعمال التحضيرية المحضة على خلاف الاتفاق كوسيلة اشتراك.

-أن الاتفاق قد يكون موضوعه جريمة معينة أو غير معينة، أما الاتفاق كوسيلة اشتراك فيتعين أن يكون موضوعه جريمة معينة.

-أن الاتفاق الجنائي لا يتطلب نتيجة معينة فيه من قبيل الجرائم ذات الطابع الشكلي، أما الاتفاق كوسيلة اشتراك فيه على خلاف ذلك لأنه يحدد المسؤولية عن جريمة ارتكبت فعلا[2].

---

[1]- المرجع نفسه ص 205.

[2]- مصطفى عبد اللطيف إبراهيم، **الاتفاق الجنائي**، جريمة الاتفاق الجنائي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية،2011، ص 84-85.

**ب- الاتفاق الجنائي والشروع :** يتشابه الاتفاق الجنائي والشروع في أن كليهما يعتبر من الجرائم الناقصة، وذلك لعدم إتمام الفعل الإجرامي الذي قصده الجاني، كما أنهما يعتبران من قبيل جرائم الخطر نظرا لأن طبيعتهما تتنافى مع تحقيق الضرر، وأخيرا فإن كليهما يتطلب تنفيذ الغرض غير المشروع، أما من حيث الاختلاف فالشروع ليس جريمة قائمة بذاتها بل يضيع ضمن الجريمة الأخرى التي يقع فيها الشروع، لأنه يأخذ طابع تلك الجريمة من حيث التجريم والعقاب، في حين أن الاتفاق الجنائي يعتبر جريمة قائمة بذاتها ولا يضيع في ثنايا الجريمة موضوع الاتفاق، لأن تنفيذ الجريمة موضوع الاتفاق لا ينهي جريمة الاتفاق، كما أن الشروع بخلاف الاتفاق محدد بالجرائم معينة[1].

**ثالثا :أركان الاتفاق لارتكاب الجرائم المساس بالمعالجة الآلية للمعطيات**

يقوم الاتفاق الجنائي لارتكاب الجرائم المساس بالمعالجة الآلية لمعطيات التوقيع الالكتروني على ركنين مادي ومعنوي.

**أ- الركن المادي:** يتمثل في اتفاق بين شخصين على الأقل نحو هدف محدد هو التحضير لارتكاب إحدى جرائم الاعتداء على نظم المعالجة الآلية للتوقيع الالكتروني، ويستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، كما يستوي أن يعرف أعضاء الاتفاق بعضهم بعض أو لا، ولكن اتفقوا في ما بينهم على القيام بالنشاط الإجرامي المتمثل في الاعتداء على نظام التوقيع الالكتروني، فإذا ارتكب الفعل التحضيري شخص بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا باجتماع شخصين فأكثر، ويجب أن يتخذ هذا النشاط صورة العمل التحضيري المادي والذي لا يختلط مع البدء في التنفيذ الذي يتحقق به الشروع أو المحاولة في ارتكاب الجريمة أو المساهمة الجرمية ، وإلا لما كانت الحاجة لهذا النص، ومن أمثلة العمل التحضيري المادي المعاقب عليه تبادل المعلومات اللازمة لتنفيذ الجريمة من الكشف عن الرقم الكودي أو السري للدخول إلى النظام أو كيفية تجاوزها، فلا يكفي أن يكون الشخص عضوا في جماعة أو منظما لها،

[1]- المرجع نفسه ص 82.

وإنما يجب أن يصدر عنه فعل تحضيري مادي حتى ولو تمثل في حضور اجتماع تناقش فيه مثل تلك الأفعال[1].

**ب- الركن المعنوي:** يجب أن يتوافر القصد الجنائي لدى أعضاء الجماعة والذي يتمثل في توافر العمل لدى كل منهم أنه عضو في جماعة إجرامية ، وأن تتجه إرادة كل عضو من أعضائها إلى تحقيق نشاط إجرامي معين، مع علمه بنشاط الأخر[2]، فمن ينظم إلى اتفاق معتقدا أنه للاتجار في برامج حاسب آلي ومعطيات عادية ثم يتبين أن الاتجار كان ببرامج خبيثة أو برامج اختراق، مثل هذا لا يعد القصد الجنائي متوافر لديه، وذلك لانتفاء علمه بموضوع الاتفاق الجنائي، لكن القصد الجنائي يتوافر لدى هذا الشخص إذا علم بعد دخوله الاتفاق بموضوعه غير المشروع ومع ذلك بقي في الاتفاق[3].

**رابعا :العقوبة :** تعاقب المادة 394 مكرر5 على جريمة الاتفاق الجنائي لارتكاب الجرائم المساس بالمعالجة الآلية للمعطيات ، بالعقوبات المقررة للجريمة ذاتها التي تم الاتفاق و الإعداد لارتكابها ، فإذا كان موضوع الاتفاق الدخول أو البقاء في منظومة المعالجة الآلية للمعطيات وفقا لنص المادة 394 مكرر تكون العقوبة الحبس من ثلاثة أشهر إلى سنة والغرامة من 50000 دج إلى 200000 دج ، في صورتها البسيطة.

وتشدد العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، وإذا ترتب على هذه الأفعال تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 300000 دج.

ويعاقب على جريمة الاتفاق لإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها وفقا لنص المادة 394 مكرر1 ، بالحبس من ستة إلى ثلاث سنوات بغرامة من 50000 دج إلى 4000.000 دج.

كما يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 إلى 10.000.000دج على الاتفاق كل من يقوم عمدا وبطريق الغش بتصميم أو بحث أو تجميع

[1]- علي عبد القادر القهوجي، مرجع سابق، ص118 .
[2]- المرجع نفسه، ص 119.
[3]- محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، مرجع سابق، ص220 .

أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، أو حيازة أو أنشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها وفقا لنص المادة 394 مكرر 2 فقرة 1 و2 ، وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة 394 مكرر3 ، مع إمكانية تطبيق عقوبات على الشخص المعنوي الذي ينضم إلى اتفاق جنائي لارتكاب الجرائم المساس بأنظمة المعالجة الآلية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر4 ،وتطبق أيضا على جريمة الاتفاق الجنائي العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة اتفاق بعلم مالكها وفقا لنص المادة 394 مكرر2 فقرة 1و2.

وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة394 مكرر3، مع إمكانية تطبيق العقوبات على الشخص المعنوي الذي ينضم إلى اتفاق جنائي لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات بغرامة تعادل خمس مرت الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر4 ، وتطبق أيضا على جريمة الاتفاق الجنائي العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة اتفاق بعلم مالكها وفقا لنص المادة 394 مكرر6.

**الفرع الرابع: جريمة التعامل في معطيات غير مشروعة**

تعاقب المادة 394 مكرر 02 كل من يقوم عمدا وبطريق الغش بما يلي:

**1**-تصميم أو بحث أو تجميع أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أو ترتكب بها الجرائم المنصوص عليها في هذا القسم

**2**-حيازة أو أنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من

إحدى الجرائم المنصوص عليها في هذا القسم ، وبالتالي تتخذ جريمة التعامل في معطيات غير مشروعة صورتين:

**الأولى:** هي التعامل في معطيات صالحة لارتكاب جريمة.

**الثانية:** هي التعامل في معطيات متحصلة من جريمة [1]، لذلك سنتطرق إلى أركان جريمة التعامل في معطيات غير مشروعة، ثم عقوبتها.

**أولا :أركانها:** تقوم جريمة التعامل في معطيات غير مشروعة على ركنين مادي ومعنوي.

**أ- الركن المادي** : الركن المادي يقوم على محل الجريمة، والسلوك الإجرامي.

**1- محل الجريمة:** المعطيات في جريمة الدخول أو البقاء غير المصرح بهما هي المعطيات الموجودة داخل النظام، أما المعطيات في جريمة التعامل في معطيات صالحة لارتكاب جريمة فهي المعطيات المخزنة أو المرسلة، والمشرع لم يرد حصر هذه الجريمة في المعطيات المعالجة وفق نظام معالجة آلية، وإنما أراد أن يتسع مجالها إلى مختلف المعطيات مهما كانت حالتها سواء كانت مخزنة ثابتة أو مرسلة متحركة أو معالجة، وهذا مسلك يبرره أن كثير من المعطيات التي يمكن أن ترتكب بها الجرائم قد لا توجد داخل النظم للمعالجة الآلية للمعطيات، وإنما تكون مخزنة داخل وسائط أخرى أو تكون مرسلة بين نظم المعلومات ، وإذا كان قانون العقوبات الجزائري قد اقتصر على المعطيات كمحل للجريمة فإن قانون العقوبات الفرنسي كان أكثر توسعا في ذلك عندما أقر في مادته 323-3-1 أن التعاملات المجرمة يمكن أن تقع على تجهيزات أو أدوات أو برنامج معلوماتي وعلى معطيات مصممة أو معدة لارتكاب واحدة أو أكثر من جرائم الدخول غير المصرح بهما أو إعاقة أو أنساد أنظمة المعالجة الآلية للمعطيات أو التلاعب بالمعطيات[2].

**2- السلوك الإجرامي:** السلوك الإجرامي يكون بأحد الأفعال المنصوص عليها في الفقرة 01 و 02 من المادة 394 مكرر 02 و تحقق الأفعال الإجرامية المكونة لجريمة التعامل في معطيات صالحة لارتكاب جريمة بما يلي:

[1]- محمد خليفة،" دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري"، المجلة النقدية للقانون والعلوم السياسية، العدد 01 ، المجلد 13 ، جوان 2018 ،ص74 .

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، مرجع سابق، ص 196-197.

✓ **التصميم والبحث والتجميع:** التصميم هو أول عملية في سلسلة التعامل في المعطيات، وهي تتمثل في إخراج المعطيات إلى الوجود، أي القيام بخلق وإيجاد معطيات صالحة لارتكاب جريمة، وهذا العمل يقوم به مختصون في هذا المجال كالمبرمجين ومصممي البرامج، ومثاله تصميم برنامج يحمل فيروسا وهذا ما يطلق عليه بالبرامج الخبيثة أو تصميم برنامج اختراق، أما البحث في كيفية البحث عن هذه المعطيات وإعدادها وليس مجرد البحث عن هذه المعطيات ولهذا جاءت عبارة البحث بعد عبارة التصميم مباشرة وان كان النص قد جاء عاما، وفيما تعلق بفعل التجميع فيه القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول أو البقاء في نظام معالجة آلية للتوقيع الالكتروني، ويفترض في هذا السلوك أن صاحبه يحتفظ بمجموعة من المعطيات التي تشكل خطرا والتي ممكن استعمالها في ارتكاب تلك الجرائم ، وقد قدر المشرع أن تعدد المعطيات من شأنه أن يرفع درجة الخطر التي تشكلها[1].

✓ **التوفير(الوضع تحت التصرف أو العرض) و النشر و الاتجار:** الاتجار بالمعطيات هو تقديمها للغير بمقابل ولا يشترط أن يكون هذا المقابل نقديا بل قد يكون عينيا أو قد يتمثل في خدمات أو غير ذلك، فالاتجار كل المعاملات التي قد تقع على المعطيات الصالحة لارتكاب الجريمة، أما التوفير فيه من الأفعال التي تجرمها المادة 394 مكرر02 من قانون العقوبات الجزائري أيضا فعل التوفير، أي توفير معطيات يمكن أن ترتكب بها جريمة دخول أو بقاء داخل نظام معلوماتي للتوقيع الالكتروني، أو جريمة تلاعب، وتعاقب المادة323 فقرة 3 و1 من قانون العقوبات الفرنسي على السلوك نفسه، كما تعاقب عليه المادة السادسة من اتفاقية بودابست تحت عبارة " أي شكل للوضع تحت التصرف"، والحقيقة أن الترجمة الفرنسية للمادة 394 مكرر2 من قانون العقوبات الجزائري توافق هذه العبارة وهي الوضع تحت التصرف met a disposition ، والمراد بذلك هو تقديم المعطيات وإتاحتها لمن يريدها أي جعلها في متناول الغير، ووضعيا تحت تصرفه، أما صورة فعل النشر فيقصد به إذاعة

[1]- المرجع نفسه ، ص 200-201.

المعطيات محل الجريمة وتمكين الغير من الاطلاع عليها وذلك عن طريق مختلف الوسائل التي يتصور النشر بها مهما كانت طبيعتها[1]، والفرق بين النشر والوضع تحت التصرف أن هذا الأخير يشير إلى وضع أجهزة على الخط ليتم استخدامها بواسطة الغير، كما يضم المصطلح من ناحية أخرى إنشاء وتجميع الروابط المتشعبة من أجل تسهيل الوصول إلى هذه الأجهزة ، وذلك عن طريق الإحالة لبرنامج يتصل ببرامج مصممة لإتلاف بيانات التوقيع الالكتروني، أو من أجل التدخل في عمل النظام، كبرامج الفيروسات أو البرامج المصممة من أجل الوصول إلى نظام الحاسب المتعلق بالتوقيع الالكتروني[2] .أما الصورة الثانية لأفعال التعامل في معطيات غير مشروعة هي الأفعال المنصوص عليها في المادة 394 مكرر 02 فقرة 02 وهي الحيازة، الإنشاء، النشر، الاستعمال.

**ب- الركن المعنوي:** جريمة عمدية تتطلب قصدا جنائيا عاما وخاصا في صورة التعامل في معطيات صالحة لارتكاب جريمة، بينما يكفي في صورتها الثانية وهي التعامل في معطيات متحصلة من جريمة توافر القصد الجنائي العام، كما أنه لا يكفي لقيام جريمة التعامل في معطيات صالحة لارتكاب جريمة أن يتوافر لدى الفاعل القصد الجنائي العام وحده، وإنما يلزم فضلا عن هذا القصد أن يتوافر لدى الفاعل القصد الخاص، لأن التعامل في المعطيات الصالحة لارتكاب الجريمة لابد أن يكون بقصد الإعداد أو التمهيد لاستعمالها في ارتكاب هذه الجريمة[3] ، وأن الصورة الثانية تتطلب قصد عام، لأن طبيعة هذه المعطيات واحدة، فكلها متحصلة من جريمة، وصفتها الثابتة هذه تجعل من القصد العام كافيا لقيام الجريمة، إذ لا يسأل الفاعل عن قصده الخاص من التعامل في هذه المعطيات ما دام يعلم أنها متحصلة من جريمة، وهذا ما يكون القصد العام[4].

**ثانيا : العقوبة:** يعاقب بالحبس من شهرين إلى ثلاث سنوات بغرامة من 1000000 دج إلى 10.000.000 دج كل من يقوم عمدا وبطريق الغش بتصميم أو بحث أو تجميع أو توفير أو

---

[1]- المرجع نفسه ، ص 202-204.

[2]- هلالي عبد الله أحمد، **جرائم المعلوماتية التقليدية و المستحدثة وتطبيقاتها في النظام البحريني** ، دار النهضة العربية ، القاهرة، 2013 ، ص263 .

[3]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، مرجع سابق، ص 213.

[4]- المرجع نفسه ، ص 215.

نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، أو حيازة أو إنشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها وفقا لنص المادة 394مكرر2 فقرة 1و2، وتضاعف العقوبات المشار إليها أعلاه إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد وفقا لنص المادة394 مكرر3، مع إمكانية تطبيق عقوبات على الشخص بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وفقا لنص المادة 394 مكرر4 وتطبق أيضا العقوبات التكميلية المتمثلة في المصادرة وإغلاق المواقع أو المحل أو مكان الاستغلال التي تكون محلا لجريمة التعامل في معطيات غير مشروعة بعلم مالكها وفقا لنص المادة 394مكرر6 .

**المطلب الثاني: الحماية الجزائية للتوقيع الالكتروني في ظل القانون 04/15 .**

نظم المشرع الجزائري جميع أحكام التوقيع الالكتروني ضمن قانون التوقيع والتصديق الالكترونيين رقم 04/15 من بينها أحكام الحماية الجزائية الموضوعية له، والتي تشمل نماذج صور التجريم الواقعة على التوقيع الالكتروني وبياناته، وباعتبار التوقيع الالكتروني يمر بجهة أخرى تسمى جهة التصديق الالكتروني لإعطائه أكثر مصداقية و موثوقية، فقد يتم الاعتداء على التوقيع الالكتروني سواء قبل المصادقة عليه أو أثنائها أو بعدها، وصور الاعتداء على التوقيع الالكتروني في قانون التوقيع الالكتروني هي جريمة إنشاء أو استعمال أو حيازة بيانات التوقيع الالكتروني المنصوص عليها في المادة 86 من قانون التوقيع الالكتروني.

إن التوقيع الالكتروني يتمتع بدرجة عالية من الأمان الفني والقانوني، وبصورة تمنع التلاعب به والاعتداء عليه بأي شكل كان، ولذلك حرص المشرع الجزائري على تضمين نص القانون04/15 مجموعة من العقوبات الإدارية والمالية[1] والجزائية لكل من يمس بيانات التوقيع الالكتروني، بما يشكل جريمة في أحكام القانون السالف الذكر وسوف نكتفي بعرض

[1]- للاطلاع على العقوبات الإدارية و المالية المفروضة على مقدمي خدمات التصديق و التوقيع الالكتروني انظر المواد 64-65 من القانون 15-04 السالف الذكر.

الأحكام الجزائية لأنها محور اهتمامنا وموضوع دراستنا أين نص المشرع الجزائي على مجموعة من العقوبات الجزائية في الفصل الثاني المعنون بأحكام جزائية في المواد من 66 إلى 45 من القانون السالف الذكر وهي كالآتي:

**1-** يعاقب بالحبس من ثلاثة أشهر(3) إلى ثلاث سنوات (3) وبغرامة من عشرين ألف (20 000.00 دج ) إلى مائتين ألف دينار جزائري(200 000.00 دج ) أو بإحدى هاتين العقوبتين على جريمة الادعاء بإقرارات كاذبة للحصول على شهادة التصديق الالكتروني الموصوفة[1].

**2-** يعاقب بالحبس من شهرين (2) إلى سنة واحدة (1) وبغرامة من مائتين ألف دينار جزائري(200 000.00 دج ) إلى مليون دينار جزائري (1 000 000.00 دج ) أو بإحدى هاتين العقوبتين فقط على إحلال مؤدي خدمات التصديق الالكتروني بالتزام إعلام السلطة الاقتصادية بالتوقف عن النشاط في الآجال المحددة في المادتين 58-59 من هذا القانون[2] .

يعاقب بالحبس من ثلاثة أشهر(3) إلى سبع سنوات (7) وبغرامة مليون دينار جزائري (1 000 000.00 دج ) إلى خمسة مليون دينار جزائري (5 000 000.00 دج ) أو بإحدى هاتين العقوبتين كل من يقوم بحيازة أو أنساد أو استعمال أثناء التوقيع الالكتروني موصوف خاص بالغير[3].

**3-** يعاقب بالحبس من شهرين (2) إلى ثلاث سنوات (3) وبغرامة من عشرين ألف (20 000.00 دج ) إلى مائتين ألف دينار جزائري(200 000.00 دج ) أو بإحدى هاتين العقوبتين فقط كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق الكتروني موصوفة[4] .

**4-** يعاقب بالحبس من ثلاثة أشهر(3) إلى سنتين (2) وبغرامة من مائتين ألف دينار جزائري(200 000.00 دج ) إلى مليون دينار جزائري (1 000 000.00 دج ) أو بإحدى هاتين

[1]- المادة 66 من القانون 15-04
[2]- المادة 67 من نفس القانون .
[3]- المادة 68 من نفس القانون .
[4]- المادة 69 من نفس القانون .

العقوبتين فقط كل مؤدي خدمات التصديق الكتروني اخل بأحكام المادة 43 من هذا القانون[1].

**5-** يعاقب بالحبس من ستة أشهر(6) إلى ثلاث سنوات (3) وبغرامة من مائتين ألف دينار جزائري(200 000.00 دج ) إلى مليون دينار جزائري (1 000 000.00 دج ) أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الكتروني اخل بأحكام المادة 42 من هذا القانون[2].

**6-** يعاقب بالحبس من سنة واحدة (1) إلى ثلاث سنوات (3) من مائتين ألف دينار جزائري(200 000.00 دج ) إلى مليونين دينار جزائري (2 000 000.00 دج ) أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الكتروني سيستأنف أو يواصل نشاطه بالرغم من سحب ترخيص تصادر التجهيزات التي تستعمل في ارتكاب الجريمة طبقا للتشريع المعمول به[3].

**7-** يعاقب بالحبس من ثلاثة أشهر(3) إلى سنتين (2) وبغرامة من عشرين ألف (20 000.00 دج ) إلى مائتين ألف دينار جزائري(200 000.00 دج ) أو بإحدى هاتين العقوبتين فقط كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق[4] .

**8-** يعاقب بغرامة من ألفين (2000.00 دج ) إلى مائتين ألف دينار جزائري(200 000.00 دج ) كل شخص يستعمل بشهادته للتصديق الالكتروني الموصوفة لغير الأغراض التي منحت لها[5].

**9-** يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة مالية تعادل خمس مرات (5) الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي .

---

[1]- المادة 70 من نفس القانون .
[2]- المادة 71 من نفس القانون .
[3]- المادة 72 من نفس القانون .
[4]- المادة 73 من نفس القانون .
[5]- المادة 74 من نفس القانون .

يتجلى من أحكام القانون04/15 انه يهدف إلى إرساء الثقة وتأمين المبادلات عبر الانترنيت، ووضع المشرع ثلاث مبادئ أساسية وهي التوثيق، السلامة، وعدم الإنكار بجعل التوقيع الالكتروني موثقا وغير قابل للتزوير ولا يمكن إعادة استعماله[1] .

## المبحث الثاني: الحماية الجزائية الإجرائية للتوقيع الالكتروني

تعتبر مرحلة ما قبل المحاكمة الجزائية أهم مراحل الخصومة الجزائية أين يتم فيها تجميع الأدلة التي يتم عرضها في مرحلة المحاكمة، وبقدر ما يكون التحقيق الابتدائي محيطا بحقيقة الجريمة كلما كان الحكم معبرا عن الحقيقة القضائية والقانونية، وتخضع جرائم الاعتداء على التوقيع الالكتروني للأحكام الإجرائية التقليدية المنصوص عليها في قانون الإجراءات الجزائية إذا ما ارتكبت خارج البيئة الالكترونية، وباعتبارها تقع في بيئة الكترونية سنحاول إضفاء الخصوصية في إجراءات التحقيق الابتدائي للجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، سواء في مرحلة جمع الاستدلالات أو البحث والتحري أمام الضبطية القضائية، أو أمام جهات التحقيق القضائي، لذا سنتطرق في المطلب الأول لمرحلة البحث والتحري وجمع الاستدلالات، وفي المطلب الثاني لإجراءات التحقيق، وفي المطلب الثالث إثبات الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، وأخيرا في المطلب الرابع الجهة القضائية المختصة بالمحاكمة في الجرائم الواقعة على التوقيع الالكتروني.

### المطلب الأول: مرحلة البحث والتحري وجمع الاستدلالات

مرحلة جمع الاستدلالات أو ما يعرف عمليا أيضا مرحلة البحث والتحري تختص بها الشرطة القضائية في إطار صلاحياتها المنصوص عليها في قانون الإجراءات الجزائية، وتكتسي هذه المرحلة أهمية بالغة في الإجراءات بعد وقوع الجريمة لاتصالها المباشر واقترابها إلى ميدان ومسرح الجريمة، ولأن جرائم التوقيع الالكتروني تقع ضمن بيئة الكترونية فمرحلة البحث والتحري فيها تتميز بطبيعة خاصة تبدأ من ضبطية قضائية متخصصة في

[1]- مقال بعنوان حكومة سلال تعيد بعث مشاريع التصديق و التوقيع الإلكترونيين منشور على الرابط الالكتروني http://yagool.dzLAr/article 2071.html تاريخ الاطلاع 2022/05/15.

مجال الجرائم المرتكبة بالوسائل الالكترونية واختصاصاتها في مجال الضبط والتحري وأساليب التحري .

والضبطية القضائية لها صلاحية البحث والتحري في كافة الجرائم بواسطة أجهزتها، لكن طبيعة الإجرام الالكتروني وجريمة الاعتداء على التوقيع الالكتروني اتجهت غالبية التشريعات فيها إلى منح التحري إلى ضبطية مختصة في الجرائم المرتكبة بالوسائل الالكترونية، وهو ما يجعله أكثر من ضرورة لضبطية قضائية مختصة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني بصفة خاصة، نظرا لصعوبات الضبطية القضائية المختصة في الجرائم المرتكبة بوسائل عادية و المسندة لها في قانون الإجراءات الجزائية والقوانين المساعدة لها، والتي منحها المشرع الجزائري ضرورة استحداث ضبطية قضائية مختصة بمكافحة الجرائم المرتكبة بالوسائل الالكترونية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009، وأصبح لها جهاز متخصص بمكافحة الجرائم المرتكبة بالوسائل الالكترونية ومنها جرائم الاعتداء على التوقيع الالكتروني، بسبب الطبيعة الخاصة لهذه الجرائم التي يكون مرتكبيها يتمتعون بقدرات ذهنية عالية ومتمكنين من المعلوماتية، ما يجعل الضبطية القضائية غير المختصة في هذا النوع المستحدث من الجرائم لا تستطيع مواجهتها بالطرق التقليدية لوحدها كسماع الشهود والمعاينات الميدانية ورفع البصمات وغيرها، فلا بد من إجراءات مستحدثة لمواجهتها تمارسها ضبطية قضائية لها القدرة على استعمالها ولذلك سنتطرق في الفرع الأول لإجراءات التحري العادية ، وفي الفرع الثاني المراقبة الالكترونية، أما الفرع الثالث سنتناول فيه إجراء التسرب.

**الفرع الأول: إجراءات التحري العادية**

منحت المادة 17 من قانون الإجراءات الجزائية للشرطة القضائية صلاحية تلقى الشكاوى والبلاغات والقيام بجمع الاستدلالات و إجراء التحقيقات الابتدائية، والشكاوى والبلاغات كما هو معروف في الجرائم التقليدية يكون كتابيا أو شفهيا، غير أنه في الجرائم

المرتكبة في الوسط الالكتروني ونظرا لما تتسم به من خطورة فقد أورد المشرع الجزائري و التشريعات المقارنة طرق جديدة للتبليغ أو الشكوى كالتي تتم عبر الانترنيت بالبريد الالكتروني، لذا سنتناول الشكوى أو التبليغ في جرائم الاعتداء على التوقيع الالكتروني.

الشكوى هي إجراء يعبر به المجني عليه في جرائم معينة عن إرادته في رفع العقبة الإجرائية التي تحول دون ممارسة السلطات المختصة لحريتها في المطالبة بتطبيق القانون[1]، أما البلاغ فهو إخبار السلطات بوقوع جريمة حتى ولو كان الشخص المبلغ ليس من وقع عليه الاعتداء، والفرق بينها وبين الشكوى أن البلاغ يكون من الضحية أو الغير، في حين أن الشكوى لا تكون إلا من الضحية.

وهذا ما يجعل النيابة ليست دائما لها الحرية في تحري الدعوى العمومية قد تكون مقيدة بشكوى من الضحية في الجرائم التي يشترط فيها القانون الشكوى، لكن بالرجوع إلى جرائم التوقيع الالكتروني سواء الواقعة على النظام المعلوماتي للتوقيع الالكتروني، أو الجرائم المعاقب عنها في قانون التوقيع والتصديق الالكترونيين، فإنه لا يشترط فيه شكوى مسبقة من الضحية، وهذا ما يعطي للنيابة العامة الحرية في تحري في الدعوى العمومية من دون التقيد بشكوى الضحية.

التبليغ والشكوى كما هو سائد في غالبية النظم القانونية يكون إما كتابيا أو شفهيا، لكن التطور التكنولوجي مكن من ظهور آليات جديدة للتبليغ والشكوى عن طريق الانترنت بواسطة البريد الالكتروني للضبطية القضائية والنيابة المختصة ، بعد صدور قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 ، كما تم تأسيس مصالح شرطة قضائية متخصصة في الجريمة المرتكبة بالوسائل الالكترونية، سواء على مستوى جهازي الشرطة أو الدرك الوطني، ويتم التبليغ عن طريق الهاتف للضبطية ( 1548 بالنسبة

[1]- محمد زكي أبو عامر، **الإجراءات الجنائية مرحلة جمع الاستدلالات** - سير الدعوى الجنائية والدعوى المدنية المرتبطة بها - التحقيق والحكم والطعن في الحكم الصادر في الدعوى الجنائية ، ط 1 ، منشورات الحلبي الحقوقية، لبنان،2010 ،ص 386.

لمصالح الشرطة و 1055 بالنسبة لمصالح الدرك الوطني)[1]، أو الولوج إلى البريد الالكتروني ppng.mdn.dz، وفي حالة الشكوى يحدد موعد للشاكي أمام جهة الاختصاص عن طرق البريد الالكتروني، وإذا لم يتقدم لتأكيد شكواه خلال ثلاثين يوما بعد الموعد المحدد، تلغى الشكوى تلقائيا[2]، وقد سايرت وزارة العدل استخدام التكنولوجيا في تسيير قطاع العدالة وعصرنته، عبر إطلاق خدمة الأرضية الرقمية للنيابة الالكترونية على الربط الالكتروني e-nyaba. mjustice بتاريخ 28 جويلية 2020 .

وفي إطار عملية التحري يمكن التنقل من طرف الضبطية إلى مكان وقوع الجريمة لإثبات الحالة وإجراء المعاينة لمكان وقوعها، أو جمع الأدلة التي تخلفت من الجريمة كرفع البصمات، والانتقال إلى المعاينة في الجرائم المرتكبة بالوسائل الالكترونية يعد من الموضوعات الجديدة، ذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي وإنما عبر العالم الافتراضي، وهناك عدة طرق يستطيع بواسطتها المحقق الوصول إلى مرتكب أو مكان الجريمة من مكتبه بواسطة الكمبيوتر الخاص بالعمل أو من مزود خدمة الانترنيت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة[3] .

ونص قانون الإجراءات الجزائية المعدل سنة 2006 على مجموعة من إجراءات التحري الخاصة ببعض الجرائم الخطرة، منها الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني، كاعتراض الاتصالات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 05، كما نصت أيضا في المادة 65 مكرر 12 على إجراء أسلوب التسرب، ومع تطور خطورة الجرائم المرتكبة في وسط الكتروني، نص المشرع في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 على إجراء المراقبة الالكترونية كأحد أساليب البحث والتحري الخاصة،وهو ما سنتناوله في الفرع الثاني.

---

[1]- المصدر الموقع الرسمي للشرطة الجزائرية على الرابط http://algeriepolice.dz اطلع على الموقع بتاريخ 2022/05/17

[2]- http://ppgn.mdn.dz اطلع على الموقع بتاريخ 2022/05/17

[3]- خالد ممدوح إبراهيم، **فن التحقيق في الجرائم الالكترونية** -دراسة مقارنة، ط 1 ، دار الفكر الجامعي، الإسكندرية،2018 ، ص106.

**الفرع الثاني: المراقبة الالكترونية**

يقصد بها كل عمل أمني له نظام معلوماتي إلكتروني يعتمد على التقنية الالكترونية، لتولى المراقبة عن طريق الأجهزة الالكترونية وعبر شبكة الانترنت باستخدام البرمجيات الالكترونية وذلك لتحقيق غرض معين، ولكي تحقق المراقبة الالكترونية أهدافها يجب أن يتوافر أمرين الأول التعاون والتنسيق بين الشخص المناط به كشف الجريمة والبحث عنها وبين فريق المراقبة الذي يتولى التأهيل الفني للقائم بها ولفريق المراقبة[1].

وقد منح المشرع الجزائري في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لسنة 2009 العديد من السلطات والصلاحيات للضبطية القضائية، تحت إشراف السلطة القضائية في اختيار أسلوب إجراء التحري وبالطريقة التي تراها مناسبة لإتمام العملية بصورة إيجابية ، ودون المساس بحرمة الحياة الخاصة للأفراد للحصول على أكبر عدد من المعلومات حول الواقعة محل البحث.

والجرائم التي يجوز فيها اللجوء إلى المراقبة الالكترونية وفقا للمادة 4 فقرة "ب" من القانون السالف الذكر هي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، لذلك فإجراء المراقبة الالكترونية في جرائم التوقيع الالكتروني يتم اللجوء إليه في حالة احتمال الاعتداء على منظومة معلوماتية متعلقة بالتوقيع الالكتروني، بشرط أن يكون هذا الاعتداء يهدد ويمس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، والتي تخضع للسلطة التقديرية للآمر بالإجراء و تتخذ صورتين:

**الأولى** هي الإرشاد الجنائي عبر الانترنت.

**والثانية** هي المراقبة عبر التقنيات الالكترونية الحديثة[2] .

وتتخذ المراقبة أشكال تتمثل في استخدام وسائل تقنية من خلال ما يسمى بقلم التسجيل أو ما يسمى بالفخ والمتابعة، وفي هذه الحالة يتم تسجيل أسماء المتراسلين مع

[1]- محمد كمال شاهين، **الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي** - دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2018، ص 251.

[2]- المرجع نفسه ، ص 251.

مشتبه معين من خلال بريده الالكتروني أو ما يقوم به من محادثات ودردشات، أو عن طرق استخدام وسائل للتنصنت على محتوى الرسالة الالكترونية أو المحادثة الفورية بوسائل الاعتراض والتصنت وباعتبار أن تطور وسائل التحقيق يقابله تطور في الجرائم وآليتها تواجه الضبطية مشكلة تشفير المراسلات الالكترونية في حال ارتكاب جريمة من فاعلها عن طريق برامج تشفير متوفرة بسهولة و بأثمان رخيصة ، ما يثير مشكلات عدم القدرة على الاطلاع على محتواها كونها مشفرة[1].

**الفرع الثالث: إجراء التسرب**

يقصد بالتسرب وفقا للمادة 65 مكرر12 قيام ضابط الشرطة القضائية أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكاب جنحة أو جناية بإيهامهم بأنه فاعل معهم أو شريك.

ويمكن تجسيد عملية التسرب في جريمة اعتداء على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، بقيام عون أو ضابط شرطة قضائية بإيهام المشتبه فيه بأنه يريد الحصول على ما توصل إليه من الجريمة ، كإيهام من يحوز على توقيع الكتروني خاص بالغير تحصل عليه عن طريق اختراق نظام معلوماتي للتوقيع الالكتروني، أنه يريد شراءه مقابل مبلغ مالي مغري، أو يكون شريك معهم بعلاقات ومحادثات الكترونية وأن له قدرا في مجال المعلوماتية تساعدهم على الاختراق والدخول لنظام معلوماتي متعلق بالتوقيع الالكتروني، وشروط صحة التسرب حددتها المواد65 مكرر 11و 15و 17 من قانون الإجراءات الجزائية والتي يمكن إجمالها في:

- أن يكون الإذن مكتوب من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار هذا الأخير لوكيل الجمهورية.
- ذكرهما للأسباب التي دفعتهما للجوء إلى إجراء التسرب وذلك تحت طائلة البطلان.

[1]- شيماء عبد الغني محمد عطا الله ، **الحماية الجنائية للتعاملات الالكترونية**، دار الجامعة الجديدة، الإسكندرية،2007 ، ص 257-258.

- ذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، مع الإشارة بأنها جريمة اعتداء على نظام معالجة آلية لمعطيات للتوقيع الالكتروني.
- التحديد في الإذن بالمدة الزمنية للتسرب التي لا يمكن أن تتجاوز أربعة 04 أشهر، على أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط ، ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة .

أما عن طريقة تنفيذ التسرب في الجرائم الواقعة على نظم المعالجة الآلية لمعطيات التوقيع الالكتروني فيتم بدخول عون أو ضابط شرطة قضائية بآليات مختلفة لمتابعة الجريمة وتحديد هوية الجناة، من خلال الولوج لقاعات الدردشة واستخدام برمجيات الاتصال المباشر المستقلة والتنكر على الانترنت، واستخدام أسماء وصفات مستعارة ، والدخول إلى مواقع ترويج البرمجيات المسروقة والبيانات والمعلومات المستولى عليها بطريقة غير مشروعة من النظم المعلوماتية، حيث يتم عرضها للبيع عن طريق هذه المواقع و التي تكون معروفة لمعتادي شراء هذه العائدات كأرقام بطاقات ائتمان مسروقة أو برامج إعداد توقيعات إلكترونية مسروقة، ويقوم المتسرب بتقصي المعلومات كأن يسأل المخترق عن كيفية حصول الاختراق [1]، أو يقوم بعرض مبالغ مالية لشراء التوقيعات الالكترونية المخترقة والمسروقة، أو شراء البرامج التي يستعملها المجرمون في الدخول إلى أنظمة التوقيع الالكتروني.

ومن التطبيقات الواقعية على التسرب في الجرائم المرتكبة عبر الانترنت قيام المباحث الفيدرالية الأمريكية بدس عضو ضبطية قضائية عن طريق أسلوب التسرب بين جماعة إجرامية مختصة بقرصنة البرمجيات وتحميلها على مواقع قرصنة عبر الانترنت، أين تَم فعلا ضبط هذه الجماعة الإجرامية[2] .

[1]- حسام محمد نبيل الشنراقي، مرجع سابق، ص 382.
[2]- محمد كامل شاهين، مرجع سابق، ص252 .

**المطلب الثاني: إجراءات التحقيق**

التحقيق الابتدائي في الدعوى الجزائية هو عمل إجرائي تتخذه سلطة التحقيق وموضوعه الجريمة الواردة في محضر الاستدلالات، بهدف الكشف والوصول إلى الحقيقة بصدد هذه الجريمة بغية إحالة الدعوى إلى المحكمة المختصة في حالة رجوح أدلة الإدانة، أو إصدار أمر بانتفاء وجه الدعوى إذا رجحت أدلة البراءة[1]، وهناك نوعان من أعمال التحقيق الهادفة إلى الكشف عن الحقيقة ويطلق عليها إجراءات جمع الأدلة كالانتقال للمعاينة وندب الخبراء وسماع الشهود وضبط الأشياء والتفتيش والاستجواب، أما الثانية فهي أوامر التحقيق الهادفة إلى تأمين الأدلة ويطلق عليها إجراءات التحقيق الاحتياطية، ومثالها أوامر الضبط والإحضار والحبس المؤقت[2]، وعليه سنتناول في الفرع الأول الاستجواب، وفي الفرع الثاني التفتيش، أما الفرع الثالث سنتناول فيه ضبط الدليل الالكتروني.

**الفرع الأول: الاستجواب**

لقد نظم المشرع الجزائري أحكام الاستجواب في المواد من 100 إلى108 من قانون الإجراءات الجزائية، والذي يكون عبر مراحل منها الاستجواب عند مثول المتهم لأول مرة أمامه ، ويعتبر سماع أكثر منه استجواب و يتحقق فيه قاضي التحقيق من هوية المتهم وإحاطته بكل واقعة من الوقائع المنسوبة إليه، وينبهه بحريته في عدم الإدلاء بأي إقرار، أما إذا أراد ذلك يتلقى قاضي التحقيق منه ذلك ، وينبهه أيضا بأن له الحق في اختيار محام عنه حسب المادة 100 من قانون الإجراءات الجزائية، ثم في مرحلة أخرى من استجواب المتهم في الموضوع ومواجهته بحضور محاميه ووكيل الجمهورية الذي يجوز له أن يوجه مباشرة ما يراه لازما من أسئلة، على عكس محامي المتهم والمدعى المدني اللذان لا يجوز لهما الكلام ما عدا توجيه أسئلة بعد إذن قاضي التحقيق، وفقا لمقتضيات المواد 105 ، 106 ، 107 من قانون الإجراءات الجزائية .

---

[1]- جلال ثروت ، سليمان عبد المنعم ، **أصول المحاكمات الجزائية**، ط 1 ، المؤسسة الجامعية للدراسات، بيروت،1997، ص 460.

[2]- المرجع نفسه ، ص 491.

ويقصد بالاستجواب مواجهة المتهم بالأدلة المرصودة ضده ومناقشته فيها مناقشة تفصيلية بهدف استجلاء ظروف وملابسات الجريمة ،وكشف الحقيقة فيما تعلق بالجرم الواقع والأدلة التي أمكن لرجال الضبطية القضائية التوصل إليها، والاستجواب على هذا النحو قد يفضي بالمتهم إلى الاعتراف بجرمه وقد يحد به على العكس إلى إنكار الجرم المنسوب إليه[1]، واستجواب المتهم في جرائم التوقيع الالكتروني تحكمه ذات القواعد العامة للاستجواب في أي جريمة تقليدية ، وهذا الإجراء يتطلب من قاضي التحقيق الحنكة والتبصر فيه من خلال مواجهة المتهم بالدلائل القائمة ضده، ومواجهته أيضا بالشهود وأي شخص يراه ضروريا لإظهار الحقيقة.

وما يمكن أن يساعد قاضي التحقيق ويعطي له إضافة في الاستجواب مواجهته بالخبرة الالكترونية والخبراء في مجال الحاسب الآلي والجرائم الالكترونية ، ذلك باعتبار أن المجرم الالكتروني على عكس المجرم التقليدي يتميز بالذكاء ومتمرس بتفاصيل الحاسب والشبكات والبرمجيات، وتشير المعلومات إلى أن أغلب مرتكبي الجرائم المرتكبة بالوسائل الالكترونية يقيمون في دول العالم الثالث المتخلفة في كل شيء إلا في مجرميها الالكترونيين الأذكياء[2].

**الفرع الثاني: التفتيش**

التفتيش هو عمل من أعمال التحقيق التي تستهدف كشف الحقيقة بشأن الجرم الواقع ومدى ثبوته في مواجهة المتهم، ولقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، وإما أن يأذن بذلك للضبطية القضائية من خلال الندب[3] ، أو هو إجراء من إجراءات التحقيق يهدف إلى البحث عن دلائل أو أشياء موجودة في مكان مغلق تفيد في كشف الحقيقة عن الجريمة، فهو ليس من إجراءات كشف الجرائم قبل وقوعها بل هو من إجراءات تحقيقها بعد

[1]- المرجع نفسه ، ص 502.
[2]- خالد ممدوح إبراهيم،مرجع سابق ، ص 240.
[3]- المرجع نفسه ، ص 499.

ارتكابها[1]، ويشترط لمباشرة إجراء التفتيش للأشخاص والأماكن أو الإذن به باعتباره إجراء من إجراءات التحقيق توافر عدة شروط[2]وهي:

– أن يكون إجراء التفتيش متعلقا بجريمة وقعت فعلا وتشكل في القانون إما جناية أو جنحة أيا كانت جسامتها أو طبيعتها أو أيَ ما كانت العقوبة المقررة لها ولو كانت الغرامة ، كما لا يجوز التفتيش لضبط جريمة مستقبلية ولو ترجح وقوعها بالفعل أو قامت الدلائل أو التحريات على أنها ستقع لا محالة، لأن التفتيش إجراء من إجراءات التحقيق، وليس وسيلة لاكتشاف الجرائم وضبط مرتكبيها.

– أن يكون هناك اتهام موجه إلى الشخص المراد تفتيشه أو تفتيش مسكنه، أو أن توجد قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، فلا يكفي أن تكون هناك جناية أو جنحة قد وقعت، بل يلزم لإجراء التفتيش أو الإذن به أن تتوافر لدى المحقق دلائل كافية لاتهامه أو حيازته لأشياء تتعلق بالجريمة حتى يمكن تفتيشه.

– أن يكون الغرض من التفتيش هو ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة.

و التفتيش هو البحث عن الحقيقة الذي يكون محله سواء شخصا أو مكانا، لذا فإن التفتيش ينقسم إلى نوعين تفتيش الأشخاص والأماكن.

✓ **تفتيش الشخص** : يكون بالبحث في كيانه المادي الذي يشمل أعضاءه الخارجية والداخلية، ويتصل بهذا الكيان ما يرتدي من ملابس أو يحمله من أمتعة أو أشياء منقولة سواء في يديه أو في جيبه، أو ما يستعمله مثل مكتبه الخاص وسيارته الخاصة.

✓ **تفتيش الأماكن:** كل مكان خاص يقيم فيه الشخص بصفة دائمة أو مؤقتة، وينصرف المسكن إلى توابعه كالحديقة وحظيرة الدواجن والمخزن، ويمتد إلى الأماكن الخاصة التي يقيم فيها ولو لفترة محدودة من اليوم[3] ،وهذان النوعان من التفتيش يكون غالبا في الجرائم التقليدية، أما في الجرائم الماسة بالنظام المعلوماتي للتوقيع الالكتروني فيكون التفتيش ضمن النظام المعلوماتي بحثا عن دليل يتناسب وطبيعة الجرم المرتكب، فهل يمكن تصنيف تفتيش

[1]- أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية** ، دار النهضة العربية، القاهرة، مصر ،1985، ص 946.
[2]- محمد زكي أبو عامر، مرجع سابق،ص 634-635.
[3]- أحمد فتحي سرور، مرجع سابق ، ص 956.

النظام المعلوماتي ضمن تفتيش الأشخاص أو المساكن ؟، وهذا ما سنحاول الإجابة عليه في ما سيأتي.

وأدرج التشريع الجزائري تفتيش نظام الحاسب الآلي في نص المادة 11 من القانون 04/09 " أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04، الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية."

ولقد شرعت العديد من الدول الأوربية التي سبقت المشرع الجزائري إلى إعادة النظر في قانون الإجراءات الجزائية ليتماشى مع التطور السريع في مجال تكنولوجيا الحاسب والانترنت فأصدر المجلس الأوروبي التوصية رقم 95 الصادرة في 11 سبتمبر 1995 في شأن مشاكل الإجراءات الجزائية الوطنية لتتلائم مع التطور في هذا المجال وأهم ما ورد في التوصية أن توضح القوانين إجراءات تفتيش أجهزة الحاسب وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها ، وتسمح الإجراءات الجنائية لجهات التفتيش بضبط برامج الحاسب والمعلومات الموجودة والأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بان النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها، كما يسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش وأن يسمح أثناء عملية تنفيذ التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمدة التفتيش إلى أنظمة الحاسب الأخرى في دائرة اختصاصه والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات بشرط أن يكون هذا الإجراء ضروريا[1].

والحاسب الآلي يتكون من مكونات مادية ومعنوية منطقية، يجعلنا نتطرق إلى مدى خضوع المكونات المادية، وكذلك المعنوية المنطقية للتفتيش،والواقع أن الولوج إلى المكونات

[1]- مدحت رمضان، **الجرائم الاعتداء على الأشخاص والانترنت**،دار النهضة العربية، القاهرة، 2000، ص 80.

المادية لمحاسب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت على التوقيع الالكتروني ويفيد في كشف الحقيقة عنها وعن مرتكبها، يدخل ضمن نطاق التفتيش العادي وفقا لقواعد قانون الإجراءات الجزائية وهذا ما نصت عليه 81 من قانون الإجراءات الجزائية على أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، ويجوز أن يشمل التفتيش على المكونات المادية للحاسب مثل وحدة الإدخال، لوحة المفاتيح، شاشات اللمس، الإدخال المرئي، الإدخال الصوتي، الفأرة، القلم الضوئي، القراءة الضوئية، القراءة المغناطيسية.... [1]، كما أن قواعد تفتيش الحاسب تختلف بحسب نوع الوسيلة المراد إجراء التفتيش عليها إذا كان الحاسب ثابتا أو محمولا.

والمكونات المادية للحاسب المكتبي تخضع لقواعد تفتيش الأماكن وهو ما يتوقف على طبيعة المكان الموجود فيه إن كان خاصا أو عاما ، فإذا كان موجود في مكان خاص lieux privé كان لها حكم هذا المكان، وهنا يجب التفرقة بين ما إذا كان هذا المكان الخاص هو منزل المتهم أو أحد ملحقاته، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم وبنفس الضمانات المقررة قانونا للتفتيش في هذا المكان.

أما المكونات المادية للأجهزة التقنية المحمولة كالحاسب المحمول فتخضع لقواعد تفتيش الأشخاص، مع مراعاة إذا كان هذا الشخص هو شخص المتهم أو شخص غير المتهم، إذ يجب مراعاة كل حالة مع مراعاة أحكام المواد45 و47 من قانون الإجراءات الجزائية، كما يجب التفرقة أيضا ما إذا كانت المكونات المادية لهذه الأجهزة متصلة بنهاية طرفية موجودة مع شخص أخر حيث تخضع لقواعد تفتيش شخص غير المتهم بالنسبة لهذه النهاية الطرفية، وبين ما إذا كانت متصلة بنهاية طرفية موجودة في مكان أخر حيث تخضع لقواعد تفتيش الأماكن بالنسبة لهذه النهاية الطرفية[2].

[1]- هلالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي** - دراسة مقارنة، ط 2، دار النهضة العربية، القاهرة، 2008، ص 73، وكذلك بكري يوسف بكري، **التفتيش عن المعلومات في وسائل التقنية الحديثة**، ط 1، دار الفكر الجامعي، الإسكندرية ، 2011 ، ص 68.

[2]- بكري يوسف بكرى، مرجع سابق، ص 70.

**الفرع الثالث: ضبط الدليل الالكتروني**

يحقق التفتيش غايته في جمع الأدلة على الجريمة التي ارتكبت فلا بد من وسيلة بموجبها يتم وضع اليد على شيء يتصل بها ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهذه الوسيلة تتمثل في الضبط الذي يقصد به ضبط الأشياء بوجه عام أن تقوم سلطة التحقيق بوضع يدها على كافة الأشياء المتعلقة بالجريمة، والتي تفيد في كشف حقيقة الجرم الواقع أو في إثبات أو نفي التهمة في مواجهة المتهم، ويستوي أن تكون الأشياء المضبوطة مملوكة للمتهم أو لغيره، كما لا يهم طبيعتها أو نوعها سواء أكانت منقولا أو عقار، أو كانت من وسائل الجريمة أو متحصل عنها[1] .

والضبط بالنسبة لجرائم التوقيع الالكتروني التي تقع على الوسائل الإلكترونية أو عن طريقها يشتمل على كل ما استعمل في ارتكابها أو أعد لهذا الغرض كأجهزة نسخ وتسجيل برامج الحاسب الآلي، أجهزة الربط مع الشبكات الإلكترونية، أجهزة اختراق الاتصالات وتحميل الشفرات وكلمات السر، كافة البرامج المقلدة والمنسوخة، المحررات الإلكترونية، التوقيعات الإلكترونية المزورة والملفات المعنوية التي تعد وسيلة لارتكاب الجريمة، والضبط هنا يقصد به الضبط القضائي الذي يستهدف الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة، والضبط قد يقع على مكونات الوسائل الإلكترونية، وقد يكون محله أيضا المراسلات الإلكترونية[2] .

أما بالنسبة للمكونات المعنوية فيمكن ضبطها وحجزها حسب نص المادة 11 من قانون الوقاية من تكنولوجيات الإعلام والاتصال لسنة 2009 التي نصت على أنه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، إذ يتم نسخ المعطيات محل البحث، وكذا اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع تحت أحراز.

[1]- جلال ثروت، سليمان عبد المنعم، مرجع سابق، ص 497.
[2]- أشرف عبد القادر قنديل، **الإثبات في الجريمة الالكترونية**، دار الجامعة الجديدة، الإسكندرية،مصر، 2015، ص 60-61.

**المطلب الثالث: إثبات الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني**

سنتطرق في الفرع الأول إلى تطبيق أدلة الإثبات في جرائم التوقيع الالكتروني المستحدثة، أما الفرع الثاني فسنتناول فيه حجية الدليل الالكتروني في الإثبات الجزائي .

**الفرع الأول: تطبيق أدلة الإثبات في جرائم التوقيع الالكتروني المستحدثة**

**أولا: الاعتراف و القرائن:** الاعتراف في جرائم التوقيع الالكتروني هو إقرار المتهم بأنه ارتكب أحد جرائم التوقيع الالكتروني، كأن يقر متهم في جريمة تزوير توقيع الكتروني بأنه هو من قام بتغيير الحقيقة في التوقيع، والاعتراف في القانون الجزائري كجميع عناصر الإثبات متروك لحرية تقدير القاضي حسب المادة213 من قانون الإجراءات الجزائية[1] ، كما أن تراجع صاحب الاعتراف لا يلغي وجوده لو عدل عنه، وللقاضي السلطة التقديرية في أن يعتد بالإنكار اللاحق لهذا الاعتراف[2] .

أما القرائن فهي صلة ضرورية بين واقعتين، يكون ثبوت الأولى فيها دليلا على حدوث الثانية، أو الصلة بين واقعة ونتيجتها يكون ثبوت الواقعة فيها دليلا على حدوث نتيجتها، وهذه القرائن قد ينشئها القانون فتسمى حينئذ بالقرائن القانونية، وقد يقيمها القضاء، فتسمى عندئذ بالقرائن القضائية أو الدلائل، و القرائن بأنواعها هي من طرق الإثبات غير المباشر أي التي لا تنصب دلالتها على الواقعة المراد إثباتها وإنما على واقعة أخرى تسبقها أو تنتجها بمحض اللزوم العقلي[3] .

**ثانيا: الشهادة والمعاينة :**أجازت المادة 88 من قانون الإجراءات الجزائية لقاضي التحقيق في جرائم التوقيع الالكتروني صلاحية استدعاء كل شخص يرى فائدة من سماع شهادته، و يعرف الفقه الشهادة بأنها إدلاء الشخص أمام القضاء بعد أداء اليمين بما يكون قد رآه أو سمعه بنفسه[4]، أما الشاهد في الجرائم المعلوماتية فيقصد به الفني صاحب الخبرة في تقنية

---

[1]- المادة 213 من قانون الإجراءات الجزائية التي تنص على أن" الاعتراف شأنه شأن عناصر الإثبات يترك لحرية تقدير القاضي.

[2]- أحمد شوقي الشلقاني، **مبادئ الإجراءات الجزائية في التشريع الجزائري**، ج 2 ، ط 5 ، ديوان المطبوعات الجامعية ، الجزائر، 2010، ص 442.

[3]- محمد زكي أبو عامر، مرجع سابق، ص 263.

[4] - Coralie Ambroise Castérot, **la procédure pénal**, 2 eme édition, gualino l'extenso,paris, 2009,p 162.

وعلوم الحاسب، والذي تكون له معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذ مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذه النوعية الجديدة من الشهود مصطلح الشاهد المعلوماتي le témoin informatique وذلك تمييزا له عن الشاهد التقليدي[1] .

والمعاينة هي إدراك الشيء بالعين لغة ، وفي الاصطلاح هي الانتقال إلى مكان معين لفحصه واثبات حاله، وهي من الوسائل التي يصح للمحكمة أن تركن إليها إذا قدرت ضرورتها أوجدتها للكشف عن الحقيقة التي تسعى إلى معرفتها ، وعلى المحكمة إذا انتقلت لمعاينة إحدى الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني أن تراعي السرعة في الانتقال إلى مسرح الجريمة الالكتروني، و أن تصطحب معها أحد خبراء الحاسب بهدف ضبط ومعاينة أدلة الجرم المرتكب، التي قد تكون أدلة مادية كجهاز الحاسب، أو الأقراص الممغنطة، أو الصلبة، أو ذاكرة تحزين البيانات، أو معاينة الكيانات المنطقية كبيانات التوقيع الالكتروني الواقع عليها الاعتداء الموجودة داخل نظام الحاسب.

**ثالثا: الخبرة و استعمال الذكاء الاصطناعي**

أجازت المادة 143 من قانون الإجراءات الجزائية لقاضي التحقيق عند مباشرته تحقيق في جريمة واقعة على التوقيع الالكتروني أن يأمر بندب خبير بناء على طلب النيابة العامة أو من تلقاء نفسه أو من الخصوم في المسائل العلمية والتقنية التي لا يكون القاضي ملما أو على دراية بها، باعتبارها وسيلة لكشف بعض الدلائل أو الأدلة أو تحديد مدلولا بالاستعانة بالمعلومات العلمية كونها رأي فني للخبير للاستعانة به في المسألة موضوع الخبرة ويعد ندب المحقق للخبير إجراء من إجراءات التحقيق يقطع التقادم وذات الشأن بالنسبة لإيداع تقارير الخبرة، لكن أعمال الخبرة ذاتها لا أثر لها على التقادم لأنها أعمال مادية[2] .

وبالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية الواقعة على التوقيع الالكتروني فإن البحث على جزئياتها وملابساتها يحتاج في أغلب الحالات إلى خبرة فنية تظهر الحاجة إليها

[1]- هلالي عبد الله أحمد، **التزام الشاهد بالإعلام في الجرائم المعلوماتية** -دراسة مقارنة، ط 5 ، دار النهضة العربية القاهرة، 2008، ص 23.

[2]- أحمد فتحي سرور، مرجع سابق، ص 385.

منذ بدأ مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[1]، بهدف الكشف عن الدليل الرقمي وعمل نسخة منه لمعرفة جميع الآثار الواقعة خلال الجريمة من تزوير أو غش أو تعديل في التوقيع الالكتروني.

كما يمكن الاستعانة بالذكاء الاصطناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومنه استنتاج النتائج على ضوء معاملات حسابية يتم تحميلها بالحاسب وفق برامج صممت خصيصا لهذا الغرض[2]، ويقوم البرنامج بكشف كافة أكثر الاحتمالات وصولا إلى حقيقة الجريمة[3]،وتبقى دائما السلطة التقديرية للقاضي الجزائي في تقدير الأدلة المطروحة أمامه.

**الفرع الثاني: حجية الدليل الالكتروني في الإثبات الجزائي**

يتنازع قوة وسائل الإثبات المختلفة نظامان نظام الأدلة القانونية ونظام الاقتناع الشخصي[4]،ففي نظام الأدلة القانونية يحدد المشرع الأدلة المقبولة في الإثبات، كضرورة الاعتراف في بعض الجرائم أو تعدد الشهود، أو توافر شروط خاصة فيهم كالذكورة أو السن أو المهنة، ومتى توافرت هذه الأدلة حكم القاضي بالإدانة أو بالبراءة، ويتضح أن دور القاضي يقف عند التحقق من توافر هذه الأدلة بشروطها القانونية دون اعتداد برأيه أو باقتناعه الشخصي، وقد نشأ هذا النظام في عهد الإمبراطورية الرومانية إثر العدول عن نظام المحلفين وتركيز السلطة القضائية في أيدي القضاة المحترفين، ثم ساد في التشريعات المختلفة في القرون الوسطى وما بعدها.

ويسيطر على الإثبات الجنائي في النظم اللاتينية مبدأ حرية القاضي في الاقتناع، فالقاضي الجنائي يستطيع أن يستمد عقيدته من أي دليل يرتاح إليه وجدانه، وهذه الحرية التي يتمتع بها القاضي الجنائي ليست مقررة لكي تتسع سلطته من حيث الإدانة والبراءة،

[1]- أشرف عبد القادر قنديل، مرجع سابق، ص 58.
[2]- خالد ممدوح إبراهيم، مرجع سابق، ص 308.
[3] -John. r josephson and susan josephson , abductive inference computation , philosophie ndtechnologie , combridge , 1994 . p 86.
[4]- أحمد شوقي الشلقاني، مرجع سابق، ص 440-441.

وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية، فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على التوصل إلى الحقيقة، والقاضي على الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه يلتزم ببيان الأدلة التي استمد منها اقتناعه، فليس الحرية أن يطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر في استخلاص الحقيقة من أي مصدر مشروع، فهناك طرق للإثبات نص عليها قانون الإجراءات الجزائية وهي التي تعتبر مشروعة والتي يجوز له استخلاص الحقيقة منها[1].

ولذلك فالمخرجات المحصلة من الوسائل الإلكترونية لا تمثل مشكلة في النظام اللاتيني حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع، فالفقه والقضاء الفرنسي يتناول حجية هذه المخرجات في المواد الجنائية ضمن مسألة قبول الأدلة المحصلة من الآلة أو ما يسمى بالأدلة العلمية والتي يجب ألا تقبل كطرق إثبات إلا إذا توفرت الشروط المقررة بذلك، وما توصل إليه الفقه والقضاء الفرنسي يصدق الأخذ به في التشريع الجزائري[2] .

ولا يجوز للقاضي بحسب المادة 212 فقرة 2 من قانون الإجراءات الجزائية أن يبني قراره إلا على الأدلة المقدمة له في عرض المرافعات وحصلت المناقشة فيها حضوريا أمامه، فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات في الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم، ويترتب على ذلك أن هذه المخرجات سواء أكانت مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات فيلمية تكون محلا للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة.

**المطلب الرابع: الجهة القضائية المختصة بالمحاكمة في الجرائم الواقعة على التوقيع الالكتروني**

الجرائم التي ترتكب على الإقليم الجزائري فقط من قبل جزائريين التي لا يثير فيها إشكال في الاختصاص الإقليمي والنوعي والتي يختص بها القضاء الجزائري ، ولكن مع ما تأخذه الجرائم الالكترونية الواقعة على التوقيع الالكتروني من امتداد دولي، قد يكون هنالك

[1]- أشرف عبد القادر قنديل، مرجع سابق، ص 70-71.
[2]- المرجع نفسه ، ص 314.

تداخل في الاختصاص بين القضاء الجزائري والأجنبي، لذلك سنتطرق في الفرع الأول إلى المبادئ المطبقة على الاختصاص القضائي في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، ثم الاختصاص الإقليمي بالمحاكمة في جرائم التوقيع الالكتروني في الفرع الثاني أما الفرع الثالث فسنتناول فيه الاختصاص النوعي بالمحاكمة في جرائم التوقيع الالكتروني.

**الفرع الأول: المبادئ المطبقة على الاختصاص القضائي في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني**

الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني تأخذ في أغلب حالاتها طابع دولي، في حين أن المعلومات في حد ذاتها هي معطيات نظمها القانون الوطني، ففي هذه الحالة تدفق المعلومات الحر والسريع يرجع إلى قدرة سلطات التحقيق والحكم المربوط أساسا بقدرتها على الإقليم الوطني وعلى مبدأ السيادة[1] ، وتطبيق الاختصاص القضائي المكاني يحكمه أربع مبادئ وهي الإقليمية، الشخصية، العينية، العالمية.

والجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني التي ترتكب في إقليم دولة وتكون نتيجتها في إقليم دولة أخرى تثير مشاكل وتنازع في الاختصاص على عكس الجرائم المرتكبة على إقليم واحد، وهو ما سنتطرق له من خلال بيان المقصود بمبدأ الإقليمية، وتنازع الاختصاص بين القضاء الوطني و الأجنبي.

**أولا :المقصود بمبدأ الإقليمية:** يقصد بمبدأ الإقليمية تطبيق التشريع الجزائي الوطني على كافة الجرائم المرتكبة في إقليم الدولة بصرف النظر عن جنسية الجاني أو المجني عليه سواء كان وطنيا أم أجنبيا، وبصرف النظر أيضا عن المصلحة التي أهدرتها الجريمة ، ولو كانت مصلحة تخص دولة أجنبية[2] ،و يشمل إقليم الدولة أجزاء ثلاثة الأرضي، المائي،

[1] -Mohamed chawki, essai sur la notion de cyber criminalite sur le cite https ://www.ie-ei-eu. اطلع عليه بتاريخ 2022/04/12.

[2]- سليمان عبد المنعم، **النظرية العامة لقانون العقوبات** - دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003، ص 89.

الجوي، فالإقليم الأرضي هو المنطقة من الكرة الأرضية التي تعينها الحدود السياسية للدولة كذلك طبقات الأرض دون هذه المنطقة إلى مركز الكرة الأرضية، والإقليم المائي هو مساحات الماء التي تقع داخل حدود الدولة، وهو كذلك بحرها الإقليمي وتشمل مساحات الماء الداخلية الأنهار الوطنية والأجزاء التابعة للدولة من الأنهار الدولية، والبحيرات، والبحار المغلقة، والقنوات والمضايق والخلجان الداخلية والموانئ البحرية، أما البحر الإقليمي فيه الجزء من البحر العام الذي يلاصق شواطئ الدولة وعرضه وفقا للعُرّف الدولي ثلاث أميال بحرية تحسب من آخر نقطة ينحصر عنها البحر وقت الجزر والمقدر ب اثنا عشر ميلا، ويشمل الإقليم الجوي كل طبقات الهواء التي تعلو الإقليم الأرضي والمائي إلى ما لا نهاية في الارتفاع[1] ،ويعد مبدأ الإقليمية القاعدة الأساسية في اختصاص قضاء الدولة الجزائري طبقا للقاعدة العامة المنصوص عليها في المادة 20 من قانون العقوبات " يطبق قانون العقوبات على كافة الجرائم التي ترتكب على إقليمها، سواء أكان مرتكبها جزائريا أو أجنبيا".

وتطبيقا لذلك يطبق قانون العقوبات الجزائري على كافة جرائم التوقيع الالكتروني المرتكبة على الإقليم الجزائري بغض النظر عن جنسية مرتكبها سواء كان جزائريا أم أجنبيا.

**ثانيا :تحديد مكان ارتكاب الجريمة وتنازع الاختصاص بين القضاء الوطني و الأجنبي**

الإشكالية الرئيسية في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني هي كيف نحدد مكان ارتكابها، وموقف المشرع الجزائري أنه إذا كانت الجريمة المرتكبة مكتملة الأركان داخل الإقليم الوطني فإن القضاء الوطني هو المختص تطبيقا لنص المادة 03 من قانون العقوبات، ولكن قد يكون كل عنصر من عناصر جرائم التوقيع الالكتروني مرتكب داخل إقليم دولة تختلف عن الأخرى، كمن يقوم في الجزائر بتزوير توقيع الكتروني ويتم استعماله في إنجلترا أو كندا، وفي هذه الحالة يختص القضاء الجزائري بها حسب المادة 586 من قانون الإجراءات الجزائية التي تعتبر أن الجريمة مرتكبة على الإقليم الجزائري إذا كان أحد الأعمال المميزة لها مرتكبا داخل الإقليم الجزائري.

[1]- محمود نجيب حسني ، مرجع سابق، ص 956.

كما أن القضاء الجزائري يختص بجرائم التوقيع الالكتروني المرتكبة في الخارج وفقا للمادة 585 قانون الإجراءات الجزائية إذا كان فاعلها شريكا في الإقليم الجزائري ، بشرط أن تكون الواقعة معاقب عليها في الدولتين، وأنه قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية.

**الفرع الثاني: الاختصاص الإقليمي بالمحاكمة في جرائم التوقيع الالكتروني**

الأصل في الاختصاص الإقليمي للمحكمة حسب المادة 329 من قانون الإجراءات الجزائية أنه يتحدد إما بمكان إقامة أحد المتهمين أو شركائهم أو محل الجريمة أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

إلا أن التطور وخطورة بعض الجرائم والتي من الممكن أن ترتكب في عدة أقاليم قام المشرع بتعديل المادة 329 من قانون الإجراءات الجزائية بإضافة الفقرة 05 في القانون 14/04، والتي تنص على جواز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تشمل نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، وجرائم المخدرات والجريمة المنظمة عبر الحدود، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

**الفرع الثالث: الاختصاص النوعي بالمحاكمة في جرائم التوقيع الالكتروني**

المحاكم العادية هي صاحبة الاختصاص الأصيل في نظر كافة الدعاوى الجزائية ولا يكفي لسلب ولايتها بالقضاء لبعض الأشخاص أو بعض الجرائم أن يقرر القانون اختصاص جهة خاصة ببعض الدعاوى ، وإنما يلزم أن يكون القانون صريحا في اختصاص تلك الجهة للفصل في تلك الدعاوى[1]، كاختصاص الأقطاب الجزائية المتخصصة في بعض الجرائم الخطرة بموجب تعديل قانون الإجراءات الجزائية لسنة 2004 ، على هذا الأساس فهناك محاكم عادية ومتخصصة في الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني.

[1]- محمد زكي أبو عامر، مرجع سابق، ص 779.

تتم محاكمة المتهمين في جرائم الاعتداء على التوقيع الالكتروني أمام المحاكم العادية، وبما أن جل هذه الجرائم من الجنح سواء بالنسبة لجريمة الاعتداء على نظام المعالجة الآلية لمعطيات التوقيع الالكتروني، أو في جريمة إفشاء أو استعمال أو حيازة بيانات توقيع الكتروني موصوف خاص بالغير، أو في جرائم التصديق الالكتروني، وبالتالي إذا لم ترتبط هذه الجرائم بجنايات فإن المحاكمة تكون أمام محكمة الجنح، وتكون محكمة الأحداث مختصة إذا كان المتهم مرتكب إحدى جرائم التوقيع الالكتروني حدث لم يبلغ سن الرشد الجزائي وهو ثماني عشرة سنة.

وبعد تعديل قانون الإجراءات الجزائية 14/04المؤرخ في 10 نوفمبر 2004 ، وسع في الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة في المواد 37،40،329 من قانون الإجراءات الجزائية في الجرائم الخطرة منها جريمة المساس بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني والتي تبقى خاضعة للتنظيم، ليأتي فيما بعد تنظيمها بالمرسوم التنفيذي رقم 384/06 المؤرخ في05 أكتوبر 2006 المعدل بالمرسوم التنفيذي رقم 267/16 المؤرخ في 17 أكتوبر 2016 [1] المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق، لمحكمة سيدي محمد الجزائر، محكمة قسنطينة، محكمة ورقلة، محكمة وهران.

[1]- الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 10 ، الصادر بتاريخ 23 أكتوبر 2016 ، ص10.

**خلاصة الفصل الثاني:**

نظرا لأهمية التوقيع الالكتروني في المعاملات الالكترونية بصفة عامة ، والتصرفات القانونية بصفة خاصة ، فقد توجهت اغلب التشريعات العالمية إلى تنظيم مواضيع التوقيع الالكتروني في قوانين مستقلة ، وهو الحال كذلك بالنسبة للمشرع الجزائري الذي عمل على إضفاء حماية التوقيع الالكتروني بالتدرج ، حسب تطور استعمال هذا الأخير باعتباره من المسائل المستحدثة في النظم القانونية الدولية والوطنية ، وحاول حمايته في بادئ الأمر بنصوص قانون العقوبات العام ، ثم عن طريق .... ، إلى غاية صدور القانون ... الذي خصه بالحماية بصفة خاصة ، بهدف إرساء جو من الثقة والأمان في ضمان المبادلات عبر الانترنيت واضعا بذلك ثلاث أهداف رئيسية وهي السلامة ، التوثيق ، وعدم الإنكار بجعل التوقيع الالكتروني موثقا وغير قابل للتزوير ولا يمكن إعادة استعماله .

# خاتمـــــــة

## خاتمـــة:

نخلص من هذه الدراسة أن التوقيع الالكتروني مصلحة من المصالح الجديرة بالحماية لكونه عنصر أساسي تقوم عليه التجارة الالكترونية و المعاملات القانونية الالكترونية بعد انتقال العالم بشكل متسارع إلى استخدام التقنيات الالكترونية الحديثة، بل أصبح إحدى أهم وسائل الحماية المدنية لمعاملات التجارة الالكترونية، مما سينتج عنه اعتداءات أو محاولات اعتداء مختلفة ومتطورة ومتسارعة ، وعلى هذا الأساس بات التفكير في حماية متكاملة للتوقيع الالكتروني من مختلف الجرائم الواقعة عليه بنوعيها التقليدية والمستحدثة، و إزاء هذه الأهمية المتزايدة توجهت أغلب التشريعات العالمية إلى إقرار حماية قانونية وتقنية شاملة لحماية هذه المنظومة المتكاملة ، وهذا ما نتج عنه تنظيم التوقيع والتصديق الالكترونيين في قوانين خاصة في اغلب التشريعات العالمية ، على غرار المشرع الجزائري الذي سن القانون رقم 04/15 ، والذي تضمن مختلف التعريفات وكذا اقرار وسائل حماية خاصة نراها من منظورنا الخاص غير كافية لحماية تامة وشاملة له ، وقد توصلنا بعد دراستنا إلى النتائج التالية:

-إقرار مختلف التشريعات الدولية والوطنية بحجية التوقيع الإلكتروني في الإثبات بالدرجة نفسها للتوقيع التقليدي.

-مواكبة المشرع الجزائري للتوجهات الدولية باعترافه بالمحررات الالكترونية وتعديل القوانين الوطنية لا سيما القانون المدني للاستفادة من ثروة المعلومات الهائلة.

-يصطدم إثبات التوقيع الالكتروني بمجموعة من العقبات الفنية والقانونية في ظل غياب نصوص تشريعية تنظم ذلك لا سيما القانون الوطني الجزائري.

-يعتبر التوقيع الالكتروني مجموعة من الحروف أو الأرقام أو الرموز أو الأصوات ، أو أي معالجة الكترونية أخرى بحيث يمكن أن يعبر عن رضا أطراف التصرف القانوني ، ويميز ويحدد هوية شخص موقعه ، كما يرتبط بمضمون المحرر على أي دعامة الكترونية.

-للتوقيع الالكتروني صور عديدة تختلف باختلاف التقنية المستخدمة في تشغيل منظومة التوقيع الالكتروني ،ومن هاته الصور ما يعتمد على الأرقام او الحروف أو الرموز ....، مثل التوقيع بالرقم السري المقترن بالبطاقة المغناطيسية ومنها ما يعتمد على الخواص الفيزيائية للإنسان كالتوقيع البيومتري.

-اختلاف طبيعة جرائم الاعتداء على التوقيع الالكتروني عن بقية الجرائم التقليدية كونها تقع في بيئة الكترونية مفتوحة على الجميع ، وليس لها أي وجود مادي يمكن من تحديد هوية المتعاملين فيها .

-محاولة المشرع الجزائري إحاطة التوقيع الالكتروني حماية جزائية موضوعية في موضعين،الأول في قانون العقوبات من خلال التجريم الخاص بأنظمة المعالجة الآلية للمعطيات من ضمنها معطيات التوقيع الالكتروني في نص المادة 394 مكرر من قانون العقوبات، وأيضا تجريم تزوير التوقيع الالكتروني المطبق عليه النصوص التقليدية العامة المتعلقة بالتزوير التي نص عليها المشرع الجزائري في المواد من 214 إلى 229 من قانون العقوبات، أما الموضع الثاني في قانون التوقيع والتصديق الالكترونيين لسنة 2015 من خلال الجرائم الواقعة على التوقيع الالكتروني في المواد من 66 إلى 74، وفي نظرنا لا يزال يحتاج إلى إثراء وتعديل لإرساء حماية شاملة .

-محاولة المشرع الجزائري إحاطة التوقيع الالكتروني حماية جزائية إجرائية سواء في تعديل قانون الإجراءات الجزائية لسنة 2006 من خلال إجراءات التحري الخاصة في الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات التوقيع الالكتروني وتشمل إجراءات التسرب والتقاط الصور، والمراقبة التلفونية ، وبعدها منح المشرع سلطات وصلاحيات للضبطية القضائية تحت إشراف السلطة القضائية في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 باستحداث إجراءات تتلائم وطبيعة الجرائم المرتكبة في نطاق الكتروني ، كتفتيش أنظمة الحاسب الآلي وامتدادها إلى نطاق دولي وإجراء المراقبة الالكترونية للاتصالات الالكترونية للجرائم الالكترونية الواقعة على التوقيع الالكتروني .

-على الرغم من تنظيم المشرع الجزائري لكل ما يتعلق بالتوقيع الالكتروني في القانون 04/15 إلا أن المشرع لم يتمكن من وضع حماية جزائية كاملة لجميع صور الاعتداء على هاته المنظومة ، على غرار الجرائم المتعلقة بالاحتيال والتزوير... مما يلزم العودة إلى قانون العقوبات ، وفي ظل النتائج المتوصل إليها من خلال الدراسة يمكن تقديم الاقتراحات التالية:

-إقرار وسائل حماية جنائية إضافية بما يتماشى وخصوصيات التعاملات الالكترونية المتطورة باستمرار في ظل اختلاف الجرائم الواقعة على التوقيع الالكتروني عن بقية الجرائم المعلوماتية والتقليدية الأخرى.

-إقرار تشريعات خاصة من أجل التنسيق بين التقنين في مجال المعلوماتية والقانونيين بغرض تعزيز وسرية ونجاعة وسرعة التحقيقات في هذه الجرائم ، مع الأخذ بعين الاعتبار استحداث أقسام خاصة على مستوى مختلف درجات التقاضي بهذه الجرائم نظرا لتزايدا ، بالإضافة إلى تكوين قضاة متخصصين ومتحكمين في مجال المعلوماتية.

-تدارك الثغرات ذات العلاقة بالإحاطة القانونية في القانون 04/15 لجرائم تقع على التوقيع الالكتروني على غرار الاحتيال والتزوير، سرقة وإتلاف بيانات التوقيع الالكتروني، أو صنعه ... إلخ ، بصياغة جنائية جديدة لمواجهة الإجرام المستحدث بما في ذلك الخاصة بحماية التوقيع الالكتروني للسماح بدخول الصور المستحدثة مستقبلا في النص، مع ضرورة استحداث وتعزيز نص قانوني خاص بالتجارة الالكترونية في الجزائر على غرار مختلف التشريعات العربية والدولية التي سبقتنا في هذا المجال.

وبعد استعراض النتائج والمقترحات التي خرجت بها الدراسة ، يمكن أن نستخلص أنها أجابت على التساؤلات التي جاءت بها الإشكالية على النحو التالي:

**الإجابة على السؤال الأول:** من خلال ما جاءت به مختلف التعريفات الفقهية والاصطلاحية للتوقيع الالكتروني توصلنا التوصل إلى أن " التوقيع الالكتروني هو ما يوضع على محرر الكتروني متخذا شكل حروف أو أرقام أو رموز أو غيرها ، ويكون له طابع مميز ومنفرد

يسمح بتحديد هوية صاحبة والتعبير عن تصرفاته القانونية ، وله نفس حجية الإثبات بالنسبة للتوقيع التقليدي"، وله عدة صور ويتم إنشاؤه بتقنيات مختلفة.

**الإجابة على السؤال الثاني:** حاول المشرع الجزائري بسط حماية قانونية موضوعية وجزائية للحفاظ على سلامة وبيانات التوقيع الالكتروني من خلال التدرج في نظام الحماية من قانون العقوبات إلى القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الصادر سنة 2009 ، إلى قانون خاص ينظم التوقيع والتصديق الالكترونيين مع الأخذ بعين الاعتبار أن كل جرائم التوقيع الالكتروني تتطلب لقيامها ركن مادي ومعنوي يختلف بحسب نوع الجريمة الواقعة عليه ،كما يعاقب مرتكب الفعل الجرمي سواء كان شخصا طبيعيا أو معنويا من خلال عقوبات أصلية وأخرى تكميلية.

كما حاول أيضا بسط حماية جزائية إجرائية له من خلال تعديل قانون الإجراءات الجزائية لسنة 2006 ، وإقرار إجراءات التحري الخاصة في جرائم المساس بأنظمة المعالجة لمعطيات التوقيع الالكتروني ،ومنح صلاحيات للضبطية القضائية تحت إشراف السلطة القضائية القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، باستحداث إجراءات تتلائم وطبيعة الجرائم المرتكبة في بيئة الكترونية.

وكخلاصة عامة عدم فعالية وكفاية وسائل الحماية الجزائية التي اقرها المشرع الجزائري لحماية التوقيع الالكتروني من خلال مختلف النصوص التي جاء بها سيما نص القانون 04/15 ،على الرغم من تداركه من خلال هذا القانون لكنه لم يشمل مختلف صور الاعتداء التي يمكن ان تقع على التوقيع الالكتروني ،خاصة جرائم الاحتيال ، السرقة والتزوير التي لا تزال منظمة في إطار القواعد العامة لقانون العقوبات .

# قائمـة المراجـــع

# قائمـة المراجـع

## أولا:باللغــة العربيــة

### 1- النصوص القانونية

- **النصوص التشريعية**


- ✓ القانون رقم 05-05 المؤرخ في 06 فيفري2005 ، المتضمن القانون التجاري المعدل والمتمم الصادر بالجريدة الرسمية للجمهورية الجزائرية بتاريخ 26 جويلية 2005 ، عدد رقم 30.
- ✓ القانون رقم 10/05 المؤرخ في 2005/07/02 المعدل للأمر 58/75 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني الصادر بالجريدة الرسمية لسنة 2005 العدد رقم 44 .
- ✓ القانون رقم 04/09 المؤرخ في05 غشت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ✓ قانون الإجراءات الجزائية 14/04المؤرخ في 10 نوفمبر 2004 المعدل والمتمم.
- ✓ القانون رقم 15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06 .
- ✓ الأمر11/03المتعلق بالنقد والقرض1 المؤرخ في 2003/08/26 الصادر بالجريدة الرسمية للجمهورية الجزائرية لسنة 2003.


- **النصوص التنظيمية**


- ✓ المرسوم التنفيذي رقم 162/07 المؤرخ في 30 ماي 2007 المعدل والمتمم بالمرسوم التنفيذي رقم 123/01 المؤرخ في 09 ماي 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية الصادر بالجريدة الرسمية للجمهورية الجزائرية في 7 جوان 2007 ، العدد 37 .
- ✓ المرسوم التنفيذي رقم 384/06 المؤرخ في05 أكتوبر2006والمعدل بالمرسوم التنفيذي رقم 267/16 المؤرخ في 17 أكتوبر 2016المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق، لمحكمة سيدي محمد الجزائر، محكمة قسنطينة، محكمة ورقلة، محكمة وهران، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 10 ، الصادر بتاريخ 23 أكتوبر 2016.


- **النصوص التشريعية للدول الأجنبية**


- ✓ قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بجمهورية مصر العربية رقم 15 سنة 2004.


### 2- الكتــب العامة


- ✓ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة،1985.
- ✓ أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج 2 ، ط 5 ، ديوان المطبوعات الجامعية ، الجزائر، 2010.
- ✓ أمير فرج يوسف،التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، مصر ،2008.

# قائمة المراجع


- ✓ إيهاب فوزي السقا ، جريمة التزوير في المحررات الالكترونية ، دار الجامعة الجديدة ، الإسكندرية ، مصر ،2007.
- ✓ أشرف عبد القادر قنديل، الإثبات في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.
- ✓ إيمان مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته الجوانب القانونية لعقد التجارة الالكترونية، دار الجامعة الجديدة، الإسكندرية،2008 .
- ✓ ثروت عبد الحميد، التوقيع الإلكتروني، دار النيل للطباعة والنشر، مكتبة الجلاء الجديدة، المنصورة،مصر، 2001 .
- ✓ جلال ثروت ، سليمان عبد المنعم ، أصول المحاكمات الجزائية، ط 1 ، المؤسسة الجامعية للدراسات، بيروت،1997.
- ✓ حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة،مصر، 2000 .
- ✓ خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية -دراسة مقارنة، ط 1 ، دار الفكر الجامعي، الإسكندرية،2018.
- ✓ فيصل سعيد الغريب ،التوقيع الالكتروني وحجيته في الإثبات ،منشورات المنظمة العربية للتنمية الإدارية ، مصر ، 2005 .
- ✓ خالد عبد التواب عبد الحميد ، نظام بطاقات الدفع الإلكتروني من الناحية القانونية، دون دار النشر ،2006.
- ✓ لورنس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة، الأردن، 2009، ص 120.
- ✓ ماجد راغب الحلو، العقد الإداري الإلكتروني ، دراسة تحليلية مقارنة ، دار الجامعة الجديدة،مصر ، 2007 .
- ✓ محمد خالد جمال رستم، التنظيم القانون للتجارة والإثبات الالكتروني في العالم، منشورات الحلبي الحقوقية، بيروت،لبنان، 2006.
- ✓ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة،الإسكندرية،2007.
- ✓ مصطفى عبد اللطيف إبراهيم، الاتفاق الجنائي، جريمة الاتفاق الجنائي دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية،2011.
- ✓ محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية دراسة مقارنة ، ط1 ، منشورات الحلبي الحقوقية، لبنان، 2009 .
- ✓ مدحت رمضان، الجرائم الاعتداء على الأشخاص والانترنت،دار النهضة العربية، القاهرة، 2000.
- ✓ محمد مدحت عزمي، المعاملات التجارية الإلكترونية الأسس القانونية والتطبيقات، مركز الإسكندرية للكتاب، مصر، 2009 .
- ✓ محمود نجيب حسني ، شرح قانون العقوبات -القسم العام ، ط 8 ، دار النهضة العربية، القاهرة، 2018.
- ✓ مناني فراح ، العقد الالكتروني وسيلة إثبات حديثة في القانون المدني الجزائري ، دار الهدى للطباعة والنشر والتوزيع ، الجزائر ، 2009 .
- ✓ منية بن ترادیت غمارسة ، جرائم المعلوماتية في القانون التونسي القانون المقارن والقانون الدولي ،دار الكتاب ، تونس ، 2015 .

- ✓ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية -دراسة نظرية وتطبيقية، ط 1 ، منشورات الحلبي الحقوقية، بيروت، 2005.
- ✓ نجوى أبو هيبة، التوقيع الإلكتروني، مدى حجيته في الإثبات، دار النهضة العربية، مصر، 2004.
- ✓ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي - دراسة مقارنة، ط 2، دار النهضة العربية، القاهرة، 2008، وكذلك بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 1، دار الفكر الجامعي، الإسكندرية ، 2011 .
- ✓ وسيم شفيق الحجار ، الإثبات الالكتروني ، المنشورات الحقوقية ، بيروت ، لبنان 2002.
- ✓ يوسف أحمد النوافلة، الإثبات الالكتروني في المواد المدنية والمصرفية، دار الثقافة الطبعة الأولى، الأردن، 2012 .
- ✓ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية،دار الفكر الجامعي، الإسكندرية، مصر،2004.
- ✓ علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الإنترنيت، دار الجامعة الجديدة، الإسكندرية، مصر ، 2012.
- ✓ علاء محمد نصيرات ، حجية التوقيع الإلكتروني في الإثبات ،دراسة مقارنة ،دار الثقافة لنشر و التوزيع، الأردن، 2005 .
- ✓ عمر خالد زريقات، عقد البيع عبر الانترنت، دار الحامد للنشر والتوزيع، عمان، الأردن،2007 .
- ✓ سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة ، دار النهضة العربية ، 2006.
- ✓ سليمان عبد المنعم، النظرية العامة لقانون العقوبات - دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.
- ✓ سعيد السيد قنديل، التوقيع الالكتروني، ماهيته، صوره، حجيته في الإثبات، دار الجامعة الجديدة ، مصر، 2004 .


### 3- الكتــب المتخصصة


- ✓ 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.
- ✓ محمد الشهاوي ، شرح قانون التوقيع الالكتروني رقم 15 لسنة 2004 (دراسة مقارنة) ، ط 1 ،دار النهضة العربية، ، القاهرة ، مصر ، 2010.
- ✓ محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي - دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2018.
- ✓ محمد زكي أبو عامر، الإجراءات الجنائية -مرحلة جمع الاستدلالات - سير الدعوى الجنائية والدعوى المدنية المرتبطة بها - التحقيق والحكم والطعن في الحكم الصادر في الدعوى الجنائية ، ط 1، منشورات الحلبي الحقوقية، لبنان،2010 .
- ✓ هلالي عبد الله أحمد، جرائم المعلوماتية التقليدية و المستحدثة وتطبيقاتها في النظام البحريني ، دار النهضة العربية ، القاهرة، 2013 .
- ✓ هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية -دراسة مقارنة، ط 5 ، دار النهضة العربية القاهرة، 2008.
- ✓ عبد الفتاح بيومي حجازي،مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي ، دار النهضة العربية ،القاهرة ، مصر.

- ✓ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2010 .
- ✓ قدري عبد الفتاح الشهاوي، قانون التوقيع الإلكتروني ولائحته، دار النهضة العربية،مصر، 2005 .
- ✓ ضياء أمين مشيمش، التوقيع الالكتروني، دراسة مقارنة، المنشورات الحقوقية، الأردن ، 2003.
- ✓ شيماء عبد الغني محمد عطا الله ، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية،2007 .


## 4- المقالات والبحوث العلمية


- ✓ إبراهيم إسماعيل الربيع، علاء موسى علي نالي،" التوثيق الإلكتروني– قرارات التحكيم في التوقيع الإلكتروني ، دراسة، مقارنة ، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد رقم01 ، بابل، العراق ، 2012
- ✓ آلاء يعقوب يوسف، المسئولية المدنية لمجهز خدمات التصديق على التوقيع الرقمي تجاه الغير، مجلة الحقوق،جامعة البحرين، المجلد الثالث، العدد الأول جانفي 2006 .
- ✓ المنصف قرطاس، حجية الإمضاء الالكتروني أمام القضاء، بحث منشور بمجلة" التجارة الالكترونية والخدمات المصرفية والمالية عبر الانترنيت"، اتحاد المصارف العربية، 2000 .
- ✓ بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الانترنت أصل الكتاب رسالة ماجستير، دار الثقافة ، 2006 .
- ✓ قارة مولود ، الإطار القانوني للتوقيع والتوثيق الالكترونيين في قانون المعاملات والتجارة الالكترونية ، مقال منشور عبر موقع : www.minshawi.com .
- ✓ محمد بودالي ، التوقيع الالكتروني ، مجلة الإدارة ، العدد الثاني 2003 .
- ✓ محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 13 ، العدد 01 ، جوان 2018 .


## 5- المؤتمرات العلمية


- ✓ إبراهيم الدسوقي أبو الليل، توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق اتجاه الغير المتضرر، بحث مقدم بمؤتمر" الأعمال المصرفية الالكترونية بين الشريعة والقانون "المنعقدة بدولة الإمارات العربية، غرفة تجارة صناعة دبي، في الفترة 10-12 ماي 2003 الجزء الخامس.
- ✓ هدى حامد قشقوش ، الحماية الجنائية للتوقيع الالكتروني ، بحث مقدم بمؤتمر ( الأعمال المصرفية الالكترونية بين الشريعة والقانون)، المنعقد بدولة الإمارات العربية المتحدة ، غرفة تجارة وصناعة دبي ، الفترة من 10-12 ماي 2003، الجزء 2 .
- ✓ يونس عرب ، منازعات التجارة الالكترونية ، الاختصاص والقانون الواجب التطبيق وطرق التقاضي ، ورقة عمل مقدمة إلى مؤتمر التجارة الالكترونية الذي أقامته منظمة الأمم المتحدة ، الفترة ما بين 08-10 تشرين الثالث بيروت ص 17-18 منشور على موقع -http://www.aeab low.com .

### 6- الرسائل والمذكرات الجامعية


- ✓ إيمان محمود احمد سليمان ، الجوانب القانونية لعقد التجارة الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه ، جامعة المنصورة، مصر، الموسم الجامعي 2005-2006 .
- ✓ محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، دراسة مقارنة ، أطروحة مقدمة لنيل شهادة الدكتوراه ، كلية الحقوق،جامعة عنابة، الموسم الجامعي2010-2011.
- ✓ محمد أحمد محمود إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه ، كلية الحقوق، جامعة عين شمس، مصر، الموسم الجامعي2004-2005 .
- ✓ صالح شنين، الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه ، جامعة تلمسان، الموسم الجامعي2012-2013 .
- ✓ يمينة حوحو، عقد البيع الإلكتروني دراسة مقارنة،أطروحة مقدمة لنيل شهادة الدكتوراه ، كلية الحقوق، جامعة الجزائر، الموسم الجامعي 2012/2011.
- ✓ صلاح عبد الحكيم المصري ، متطلبات استخدام التوقيع الالكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة ، أطروحة مقدمة لنيل شهادة الماجستير في إدارة الأعمال ، كلية التجارة ، الجامعة الإسلامية غزة ، الموسم الجامعي 2006-2007.


### ثانيا:باللغات الأجنبية


- ✓ Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil .
- ✓ Coralie Ambroise Castérot, la procédure pénal, 2 eme édition, gualino l'extenso,paris, 2009.
- ✓ FAUSSE Yanaon: La signature électronique, DUNOD, Paris, 2001, P.87ets.
- ✓ John. r josephson and susan josephson , abductive inference computation , philosophie ndtechnologie , combridge , 1994
- ✓ sedalin valérie preuve et signature électronique , paris ; sur le cite
- ✓ www.juriscom.net/chr2/fr20000509htm
- ✓ Mohamed chawki, essai sur la notion de cyber criminalite ,p 3-4. https ://www.ie-ei-eu.


### 7- المواقع الالكترونية


- ✓ http://fr.wikipedia.org/wiki/SHA
- ✓ http://www.uncitral.org
- ✓ http://news. maktoob. com /article 620364
- ✓ http://www.ec.europa.eu.
- ✓ http//www.moheet.com/show_news.aspx? nid
- ✓ www.iso.org
- ✓ http://www.startimes.com/f.aspx?t=5287300
- ✓ www.juriscom.net/chr2/fr20000509htm
- ✓ http://www.elkhabar.com/quotidien/?idc=49&ida=149052&date_insert=20090323
- ✓ www.juriscom.net/chr2/fr20000509htm

- ✓ http://www.ec.europa.eu.
- ✓ http://www.fs.dk/uk/acts/eu/pdf/esign-fr.pdf
- ✓ http://www.aeab-low.com
- ✓ www.minshawi.com

# فهرس المحتويات

# فهرس المحتويات

# فهرس المحتويات

# فهرس المحتويات

**ملخص :**

يلعب التوقيع الالكتروني دورا محوريا في خلق بيئة تعاملات آمنة وموثوقة و التي تتم بواسطة تكنولوجيات حديثة تستدعي تأكيد هوية الأطراف وأهليتهم القانونية لإبرام مختلف التصرفات القانونية الكترونيا ، خاصة مع الانتشار المتزايد للتعاملات الموقعة الكترونيا وحلول التوقيع الالكتروني محل التوقيع التقليدي كنتيجة حتمية لهذه التطورات ، مما سينتج عنه لا محالة اعتداءات مختلفة عليه ومتزايدة بواسطة هذه التقنيات والتكنولوجيات نفسها في بيئة ذات خصائص مميزة مما يستوجب حماية جزائية له من الجرائم الواقعة عليه.

وعلى هذا الأساس سارعت مختلف التشريعات الدولية والوطنية إلى تنظيمه في قوانين خاصة ، على غرار المشرع الجزائري الذي أعطى للتوقيع الالكتروني نفس حجية إثبات التوقيع التقليدي من خلال تعديل نص القانون المدني، ثم حاول إضفاء حماية جزائية موضوعية وإجرائية على التوقيع الالكتروني لحمايته من الجرائم المستحدثة ،إلى أن نظمه قانون خاص ( 04/15) المتعلق بالتوقيع والتصديق الالكترونيين ، والذي لا يزال بحاجة إلى تعديل وإثراء لبسط حماية كاملة وشاملة للتوقيع الالكتروني و التي تم إغفالها في ذات القانون.

**الكلمات المفتاحية:**التوقيع الالكتروني ، التوقيع التقليدي ،حماية جزائية موضوعية وإجرائية ،الجرائم المستحدثة ، التوقيع والتصديق الالكترونيين .

**Résumé :**

La signature électronique joue un rôle central dans la création d'un environnement de transaction sécurisée et fiable qui s'effectue à l'aide de technologies modernes qui nécessitent la confirmation de l'identité des parties et de leur capacité juridique à conclure diverses actions en justice par voie électronique, en particulier avec la diffusion croissante des signatures électroniques. transactions et solutions de signature électronique en lieu et place de la signature traditionnelle comme conséquence inévitable de ces évolutions, qui n'aboutiront à aucune attaque diverse et croissante à son encontre rendue impossible par l'utilisation de ces mêmes techniques et technologies dans un environnement aux caractéristiques particulières, qui nécessite des sanctions pénales et protection contre les crimes commises.

Sur cette base, diverses législations internationales et nationales se sont empressées de l'organiser en lois spéciales, à l'instar du législateur algérien qui a donné à la signature électronique la même autorité de preuve qu'à la signature traditionnelle en modifiant le texte du Code civil puis il a tenté d'ajouter une protection pénale objective et procédurale à la signature électronique pour la protéger des Nouveaux délits émergents, jusqu'à ce qu'elle soit réglementée par sa propre loi (15/04) relative à la signature et à la certification électroniques, qui doit encore être modifiée et enrichie pour étendre la protection pleine et entière de la signature électronique, qui a été négligée dans la même loi.

**Les mots clés :** La signature électronique , La signature traditionnelle , protection pénale objective et procédurale , Nouveaux délits , la signature et à la certification électroniques.