

جامعة عبد الحميد بن باديس مستغانم

المرجع:.....

كلية الحقوق و العلوم السياسية

قسم: القانون الخاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

الإطار القانوني لحماية التوقيع الإلكتروني ومكافحة الجرائم المرتبطة به

ميدان الحقوق و العلوم السياسية

التخصص: القانون خاص

تحت إشراف الأستاذ(ة):

مرابط حبيبة

الشعبة: الحقوق

من إعداد الطالب(ة):

حمدود مدينة

أعضاء لجنة المناقشة

رئيسا

برابح هدى

الأستاذ(ة)

مشرفا مقرر

مربط حبيبة

الأستاذ(ة)

مناقشا

مشرفي عبد القادر

الأستاذ(ة)

السنة الجامعية: 2026/2025

تاريخ المناقشة : 2026-06-22



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة عبد الحميد بن باديس مستغانم



كلية الحقوق و العلوم السياسية
مصلحة التبرصات

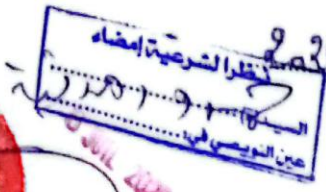
تصرح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب :
الاسم :
الحامل (ة) لبطاقة التعريف الوطنية رقم : والصادرة بتاريخ : 2025/03/10
المسجل (ة) بكلية : قسم :
والمكلف (ة) بإنجاز مذكرة ماستر بعنوان :
.....
.....

أصرح بشرفي أنني ألتمزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث المذكور أعلاه.

امضاء المعني



التاريخ : 2025/03/10

عن رئيس المجلس الأعلى للتعليم بالبلدي
28 جويلية 2014
* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2014
امضاء : كاشو بن شاعة محمد

شكر

قبل كل شيء أحمده الله تعالى الذي منحني الصبر والثقة ووفقني لإعداد هذه المذكرة
كما أتقدم بجزيل الشكر إلى كل من ساهم في هذا العمل سواء من قريب أو من بعيد ولو بكلمة
طيبة.

وأقدم بالشكر إلى أستاذتي المشرفة تفضلها "مرابط حبيبة" بقبولها للإشراف على هذه المذكرة رغم
التزاماتها

كما أشكر أيضا أعضاء لجنة المناقشة على قبولهم مناقشة هذا العمل المتواضع.

الإهداء

إلى والدي الحبيب أهديك هذا النجاح الذي كنت تحلم برؤيتي أحققه

إلى أُمي الغالية

مصدر الحب والقوة، التي وقفت بجانبني في كل خطوة، كانت لي الأب والأم، فاحتوتني بحنانها وقوتها. دعواتك، تعبك، وصبرك، كلها محفورة في قلبي، وهذا النجاح ثمرة جهدك وتضحياتك. شكرًا لك من أعماق قلبي، وأسأل الله أن يحفظك ويطيل في عمرك.

إلى أخواتي العزيزات،

قطعة من روحي، وصديقات عمري، وسندي الذي لا يميل. كنتم لي العائلة التي أستمد منها القوة، والدعم الذي منحني الأمل في كل لحظة. هذا النجاح أهديه لكن، فبكن تكتمل فرحتي، ومن دونكن لم تكن هذه الرحلة لتكون كما هي.

إلى صديقاتي الغاليات،

رفيقات الدرب اللواتي شاركنني اللحظات الصعبة والمبهجة، وكنّ لي العون والسند. شكرًا لوجودكن في حياتي، فقد جعلت هذه الرحلة أجمل.

وأخيرًا، إلى نفسي

التي صبرت وكافحت وسعت لتحقيق حلمها رغم كل التحديات. هذا النجاح ليس إلا بداية لطريق طويل من الطموح، وأسأل الله أن يوفقني لما هو قادم

مقدمة

إن التطور العلمي المذهل وخاصة في مجال تبادل المعلومات و التقنيات العلمية ووسائل الإتصال الفوري وظهور شبكة المعلومات العالمية (الإنترنت) فتح أبواباً عالمية لتسهيل التبادلات التجارية وغيرها، وجعل العالم يتحول إلى قرية صغيرة وقلص المسافات بين المتعاملين في مختلف الدول ، وأصبحت المعاملات القانونية بكل أشكالها تتم بوساطة شبكات الإتصال الإلكترونية . فإبرام التصرفات وتنفيذها تتم من خلال معلومات تتبادل بين الأطراف إلكترونياً.

وفي ظل هذه الخطوات السريعة التي خطتها وسائل الإتصال الحديثة و تقنيات الحاسوب الآلي من خلال السرعة والحداثة والدقة ، أصبحت خصائص الأمان والسرية والثقة في التعاملات التي تتم بوساطة شبكة الإنترنت من الضرورات الملحة أستوجبت توفرها، وخاصة المعاملات التجارية بغية محافظة مصالح المتعاملين من خلال الشبكة ، وحماية المستهلك من عمليات القرصنة الإلكترونية والإختراق المعلوماتي ، ودخول الفايروس في (داتا) المعلومات وتخريبها مما يؤدي إلى الإضرار بالمتعاملين ، وفقد الثقة بأمان الشبكة العالمية للمعلومات، مما يتطلب الأمر تنظيم هذه التحولات والتغيرات العالمية قانونياً . وهذا ما شهدته الحقبة الأخيرة، إذ صدر عدد من القوانين ذات صفة عالمية ونموذجية ، منها القانون النموذجي بشأن التجارة الإلكترونية عام 1996 ، والقانون النموذجي بشأن التوقيعات الإلكترونية عام 2001 وهما دليل تشريعي للدول التي سنت تشريعاتها في ظلها . ومن بين الموضوعات التي لها صلة وثيقة بالتعاملات التجارية الإلكترونية بشكل مباشر ، الذي تطرقت اليه قوانين معظم الدول من خلال التعاملات التجارية الإلكترونية او من خلال تشريعات خاصة به ، هو التوقيع الإلكتروني. (Electronic Signature)

مقدمة

إن استخدام الدعامات الورقية والحبر لتوقيع المحررات وفقاً لقوانين الإثبات التقليدية يكون عائقاً أمام تطور التجارة الإلكترونية¹، وخاصة ما تتمتع به المستندات الإلكترونية من توفير للوقت والنفقات ومنح الدول الفرص الكبيرة للدخول في التجارة العالمية، ومحاولة منهم لمواكبة التطورات المستمرة والسريعة في عالم المعلومات والتكنولوجيا وإضفاء المصادقية على التعاملات الإلكترونية. وهناك مبدأ متفق عليه في معظم قوانين الإثبات للدول المختلفة مفاده أن الكتابة والدليل الكتابي لا يكتملان في غياب التوقيع، لأن التوقيع يثبت الصلة بين الكتابة ومن تنسب إليه. ولما للتوقيع من كيان مادي ملموس يؤدي إلى استحالة توقيع السندات الإلكترونية، ولما للتوقيع من تأثير فعلي لمصادقية السند في الوجود والعدم، فمن المتعذر الاستغناء عن التوقيع بصفته ابتداءً قانونياً ذا مسوغات تفرض وجوده.

لذا استوجب الأمر ظهور صيغ جديدة للتوقيع تتفق مع البيئة الإلكترونية، ويسمى بالتوقيع الإلكتروني (Electronic Signature) وما يتعلق بموضوع مذكرتنا المقصود بالتوقيع الإلكتروني، وصوره، والتقنية المستخدمة لإنشائه ومدى عده نظيراً للتوقيع التقليدي ومدى معالجة قوانين الإثبات للمنازعات التي قد تحدث بين المتعاملين بالتقنيات الحديثة في مجالات التجارة الإلكترونية، ومدى حجية التوقيعات الإلكترونية في الإثبات على السندات الإلكترونية، ومدى تطبيق قوانين الإثبات التقليدي في المشكلات التي تحدث في التعاملات من خلال شبكة الإنترنت.

وفي ظروف انتشار التجارة الإلكترونية كان لازماً أن تتوفر وسائل حديثة تتناسب وهذا التطور التكنولوجي هائل في وسائل الاتصالات، يتم بواسطته تحقيق السرعة والأمان الضروريين للتجارة الإلكترونية، لذلك ونظراً لأهمية هذا الموضوع وحداثه، وعده من مواضيع العصر التي تستوجب الاهتمام والدراسة على التشريعات الدولية والداخلية وضع نظام قانوني جديد مواكب للتغيير والتطور المستمر فيه، ويتناسب مع التطورات الحديثة.

¹ محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الذكر الجامعي، الإسكندرية 2006، ص 9.

مقدمة

لذا وجدت من الضروري الشروع ببحث في هذا المجال، ولاسيما موضوع التوقيع الإلكتروني، الذي يعد المفتاح والمحرك للتجارة الإلكترونية، والدخول في تفاصيله وصوره وماهيته ومدى حجته في الإثبات. وما هو معلوم أن إصدار قانون التوقيع الإلكتروني يعد من أهم التغييرات العصرية التي جاءت بعد تعاون فقهاء القانون ورجال التكنولوجيا والمعلومات لأجل إيجاد منفذ لحل المشاكل التي تحدث في الإثبات. وفي غياب تنظيم قانوني للوضع الجديد سوف تنتشر الفوضى وتظهر مؤسسات وهمية تقوم بعمليات البيع والشراء لسلع ليس لها وجود في الحقيقة ، مما يؤدي إلى فقدان الثقة بين المتعاملين مع شبكة المعلومات العالمية، ويبعد هذه التقنية المتطورة عن هدفه الرئيس

نظراً لتعدد وسائل التوقيع الإلكتروني وتقنيات إنشائه من جهة والمخاطر التي تحيط به من جهة أخرى جعلته يستقل ويتميز بأحكام قانونية تتعلق بأساسه الإلكتروني. وتكمن أهمية هذه الدراسة في إتساع إطار التجارة الإلكترونية وإزدياد أهميتها في كل البلدان، وإنحسار التجارة التقليدية وتقلصها في عصر السرعة والتطور ، ويدفعنا ذلك إلى البحث في كل الأمور التي تخص التجارة الإلكترونية ، ويعد التوقيع الإلكتروني من أهم الأسس التي تعتمد عليه، وإزدهار التجارة الإلكترونية مرهون بمدى صدق التوقيع الإلكتروني ومدى حاجته لمصالح المتعاملين به. ومحاولة من خلال هذا ارتائنا الاشكال الاتي: إلى أي مدى يمكن التشريعات الوطنية والآليات التقنية المعاصرة من ضمان حجية التوقيع الإلكتروني في المعاملات الرقمية، وتحقيق حماية فعالة ضد الجرائم الإلكترونية المرتبطة به، في ظل التطور المتسارع لأساليب الاختراق والتزوير؟

ومن أسباب اختيارنا للموضوع أسباب موضوعية وأسباب شخصية

• الأسباب الموضوعية:

-قلة البحوث التي تناولت موضوع التوقيع الإلكتروني.

مقدمة

-الجدية والأصالة التي تتمتع بها الموضوع، وذلك من خلال دوره في تحريك عجلة التنمية الإقتصادية للعديد من الدول والتقليص من ظاهرة البيروقراطية،وتسهيل المعاملات الرقمية.

• الأسباب الشخصية:

- الرغبة الذاتية في البحث في هذا الموضوع.
- الرغبة في المبادرة العلمية لدراسة موضوع يتسم بالحدثة.
- توافق موضوع مع التخصص، وتطابقه مع واقع الحياة.

واعتمدنا في دراستنا هذه على المنهج التحليلي الوصفي، كونه الأنسب لمثل هذه الدراسات، من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في جريمة التوقيع الإلكتروني واختلافها عن النصوص الإجرائية التقليدية، وكذا وصف وتحليل مختلف الاتفاقيات الدولية والعربية من أجل مكافحة هذا النوع من الإجرام المعلوماتي

لقد تطرقت عدة دراسات سابقة إلى هذه الجرائم من الناحية الموضوعية فقط؛ مع وجود بعض الدراسات التي تطرقت لها من الناحية الإجرائية لكن ليست بالتفصيل، الأمر الذي جعلها قاصرة.

ومن أجل معالجة الإشكالية التي سبق طرحها وجب تقسيم هذه الدراسة وفقاً لخطة منهجية تتمثل في:

فصلين تطرقنا في الفصل الأول: إلى الإطار القانوني للتوقيع الإلكتروني والفصل الثاني: جرائم التوقيع الإلكتروني واليات الحماية منها.

الفصل الأول

الإطار القانوني للتوقيع الإلكتروني

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

يشكل التوقيع منذ نشأة الكتابة، الأداة الجوهرية لإضفاء الثقة والاطمئنان على المعاملات بين الأشخاص، ولا يزال يؤدي هذا الدور إلى الوقت الحاضر. وعند إطلاق مصطلح التوقيع، ينصرف الذهن مباشرة إلى التوقيع التقليدي المتمثل في الكتابة بخط اليد. غير أنّ التطور التكنولوجي وما صاحبه من انتقال من الوسيط المادي إلى الوسيط الإلكتروني، أفرز ضرورة ملحة لمراجعة قواعد الإثبات التقليدية، لاسيما في ما يتصل بالتوقيع الإلكتروني. وعلى هذا الأساس، بادرت عدة دول، من بينها الجزائر، إلى تكليف تشريعاتها بما يسمح بالأخذ بالتوقيع الإلكتروني كوسيلة من وسائل الإثبات المعاصرة. وانطلاقاً من ذلك، يقتضي البحث التعرّض لمفهوم التوقيع الإلكتروني قبل الخوض في بيان وظائفه

الفصل الأول لإطار القانوني للتوقيع الالكتروني

المبحث الأول: مفهوم التوقيع الالكتروني

إذا أردنا أن نعرف مصطلح التوقيع الالكتروني، علميا نجد انه عبارة عن القيام بعمل أو إجراء يقوم به المرسل بحيث يتم ربط هويته بالوثيقة ليتسنى للمستلم التحقق من صحة التوقيع

المطلب الأول: تعريف التوقيع الالكتروني

هناك فرق بين التوقيع الالكتروني والتوقيع الرقمي، وان المصطلحين لا يعنيان شيئا واحدا وليس مترادفين لبعضهما بعضا، كما إن التوقيع الالكتروني يشير إلى جميع الوسائل والأساليب المتاحة لإجراء الموقع توقيعه بصورة الكترونية، بقصد توثيق السند الموقع أو بقصد الالتزام بمضمون السند الموقع عليه، وهو ما نتعرض له في هذا المطلب مع إبراز موقف المشرع الجزائري.

الفرع الأول: التعريف الفقهي للتوقيع الالكتروني

برز اتجاهان فقهيان في تعريف التوقيع الالكتروني، الاتجاه الأول يركز على الوسيلة التي يتم بها إنشاء التوقيع بينما يركز الاتجاه الثاني على إبراز وظائف التوقيع الالكتروني فيرى بعض الفقهاء أن التوقيع الالكتروني عبارة عن تعبير شخص عن إرادته في الالتزام بتصرف قانوني معين عن طريق تكوينه لرموز سرية يعلمها هو وحده، تسمح بتحديد هويته. وهناك من الفقه من عرف التوقيع الالكتروني بأنه عبارة عن توقيع رقمي يرتبط بالمعلومات التي يرغب المرسل في إرسالها إلى الطرف الآخر ويتضمن التوقيع المعطيات، التي تدل على ارتباط صاحبه واعترافه بما ورد على الوثيقة الالكترونية المرسلة⁽²⁾.

¹ ازاد دزهبي، النظام القانوني للمصادقة على التوقيع الالكتروني، دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، كلية الحقوق

الإسكندرية، 2015، ص 25.

² محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، المرجع السابق، ص 12.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

و يعاب على هذين التعريفين قصورهما لكونهما حصرا التوقيع الإلكتروني في البعض من صوره، دون الصور الأخرى خاصة منها التي تعتمد على الخواص الذاتية (التوقيع البيومتري)، غالقين بذلك المجال أمام الاعتراف بها.

و هناك أيضا تعريف آخر للتوقيع الإلكتروني في الفقه الفرنسي الذي يرى أن التوقيع الإلكتروني هو مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات، و قبوله بمضمون التصرف الذي يصدر التوقيع بمناسبة¹.

و هذا التعريف يتبين من مضمونه أنه جامع مانع تضمن مفهوم واسع للوسيلة التي يتم بها إنشاء التوقيع، معترفا بذلك بجميع صور التوقيع الإلكتروني، كما أبرز بوضوح وظائف التوقيع الإلكتروني، من تحديد هوية الموقع و التعبير عن إرادته بالموافقة على مضمون السند الموقع عليه.

الفرع الثاني: تعريف التوقيع الإلكتروني في التشريعات المقارنة

جاء تعريف التوقيع الإلكتروني في كافة القوانين المنظمة له الدولية منها و الداخلية واحدا تقريبا، مع الاختلاف في الألفاظ و لكن موحدة في المضمون.

و نتعرض في هذا الفرع لتعريف التوقيع الإلكتروني من قبل المنظمات الدولية، ثم التشريعات المقارنة.

أولاً: تعريف التوقيع الإلكتروني من قبل المنظمات الدولي

دارت مناقشات ومداولات وحوارات مكثفة وشاقة على الصعيد الدولي من أجل إيجاد مخرج للوصول إلى اتفاق واحد وتعريف شامل وكامل لجامع للتوقيع الإلكتروني ومجالات استخدامه وهو إمكانية تطبيقه في كلاً من الدول والأقاليم لتستطيع الدول لإستناد اليه في تشريعاتها.

¹ علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر و التوزيع، عمان 2005، ص 30.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

وبهذا الخصوص نذكر من تلك المناقشات ما دار في لجنة الأمم المتحدة الدولية، بعد بحث عميق للمشكلات التي تتعلق بالتعاملات والالتزامات التي تنشأ بواسطة الاتصالات الحديثة وشبكة الإنترنت وفقاً للمعطيات المعلوماتية في التجارة الدولية وكرست اللجنة جهودها لإيجاد قانون موحد طيلة الدورات من الخامسة والعشرين إلى التاسعة والعشرين، وأقر مشروع القانون النموذجي للتجارة الإلكترونية، واعتمدت عليه الجمعية العامة للأمم المتحدة بقرارها المرقم 51/162 بتاريخ 12 كانون الأول 1996، وهذا القانون يشتمل على أحكام منظمة للتجارة الإلكترونية¹.

ويذكر أن هذا القانون لم يعرف وإنما أعتبر فبوظائف التوقيع على الدعامات الورقية، ولدى عدداً لقانون النموذجي جرى النظر في وظيفة التوقيع بتعيين هوية الشخص وتوفير ما يؤكد يقينا مشاركة ذلك الشخص في التوقيع، والربط بين مضمون المستند

1/ التوقيع الإلكتروني في قانون الأونيسترال النموذجي:

عرفته المادة الثانية من القانون النموذجي للتوقيع الإلكتروني الذي وضعته منظمة الأمم المتحدة لجنة القانون التجاري الدولي الأونيسترال بصدد تعريف المصطلحات بأنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات و بيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"

يقصد بالرسالة الإلكترونية في هذا القانون معلومات إلكترونية، ترسل و تستلم بوسائل أيا كانت وسيلة استخراجها في المكان المستلمة فيه.⁽²⁾

و يستهدف هذا القانون النموذجي توفير يقين قانوني إضافي بشأن استخدام التوقيعات الإلكترونية، و هذا القانون الذي يستند إلى مبدأ مرن يرسى افتراضاً بأن التوقيعات

¹ انظر النص الكامل لهذا القانون على الموقع الإلكتروني، <http://www.uncitral.org>، 11-03-2026 last visit

² محمد أمين الرومي، المرجع السابق، ص 11.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

الإلكترونية، يجب أن تعامل على أنها مناظرة للتوقيعات بخط اليد عندما تستوفي معايير معينة بشأن الموثوقية.⁽¹⁾

هذا و يلاحظ على تعريف الأونيسترال للتوقيع الإلكتروني ما يلي:

1. عدم تحديد نوع الطريقة التي يتم بها استخدام التوقيع الإلكتروني فاتحا المجال لإيراد أية طريقة تراها الدول ملائمة.

2. أن التعريف ركز على أن أية طريقة للتوقيع يجب أن تحقق وظائف التوقيع الإلكتروني، من تحديد هوية الشخص الموقع و التعبير عن إرادته بالموافقة على مضمون رسالة البيانات.⁽²⁾

2/ تعريف التوقيع الإلكتروني في المجموعة الإتحاد الأوربي:

وللمجموعة الأوربية أيضا عناية بهذا الشأن فقد أصدرت اللجنة الأوربية توصية تحت رقم 196 سعى الإتحاد الأوربي إلى تعريف التوقيع الإلكتروني الذي ورد في توجيهه الصادر من مجلس الإتحاد الأوربي تحت رقم 93 لسنة 1999، و الذي حث دول الإتحاد على إعداد تشريعاتها الداخلية وفقا له، و بما يحقق الأغراض المستهدفة به من إشاعة الثقة و الأمان داخل السوق الأوربية، و قد عرفت المادة الثانية منه التوقيع الإلكتروني على أنه "بيان أو معلومة إلكترونية ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى (كرسالة أو محرر)، والتي تصلح وسيلة لتمييز الشخص و تحديد هويته."⁽³⁾

كما جاء في نفس المادة أن التوقيع الإلكتروني المتقدم أو المؤمن هو عبارة عن توقيع إلكتروني، يشترط فيه أن يكون مرتبط ارتباطا فريدا من نوعه مع صاحب التوقيع قادر على تحقيق (تحديد) صاحب التوقيع، و التعرف عليه بإستخدامه، ثم إيجاد استخدام وسائل يضمن

(1) منير محمد الجنبهي، ممدوح محمد الجنبهي. تزوير التوقيع الإلكتروني. دار الفكر الجامعي، الإسكندرية 2006 ص 31.

(2) علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر و التوزيع، عمان، 2005، ص 23.

(3) علاء محمد نصيرات، المرجع السابق ص 24.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

فيها صاحبه السرية التامة، و مرتبط مع المعلومات المحتواة في الرسالة حيث أنه يكشف أي تغيير في المعلومات.⁽¹⁾

و يلاحظ على هذا التعريف أنه يميز بين التعريف العام للتوقيع الإلكتروني، و تعريف التوقيع الإلكتروني المتقدم أو المؤمن، و هذا المنهج استثنته تشريعات دول من الإتحاد الأوروبي.

فالتوقيع الإلكتروني العادي لم يشترط فيه سوى أن يكون مميزاً، و قادراً على تحديد شخص الموقع، أما التوقيع الإلكتروني المتقدم اشترط فيه أن تكون التقنية المستعملة جديرة بحماية صاحب التوقيع، و أن يضمن مع ما هو مرتبط به رابطة تمكن من اكتشاف أي تعديلات لاحقة على المحرر. و قد أعطت المادة "05" من التوجيه الحجية الكاملة للتوقيع الإلكتروني المتقدم مثله مثل التوقيع الخطي.

ثانياً: تعريف التوقيع الإلكتروني في التشريعات المقارنة:

رغم تشابه معظم التشريعات في تعريف التوقيع الإلكتروني، من حيث مضمونه تختلف في توسيع طرق إنشائه، و نطاق استخدامه في أنواع معينة من المعاملات دون الأخرى، و هو ما نستشفه من تطرقنا إلى تعريف التوقيع الإلكتروني في القانون الفيدرالي الأمريكي، ثم القانون الفرنسي و القانون السويسري و الفدرالي الألماني والدنمركي أخيراً القانون المصري.

1/ تعريف التوقيع الإلكتروني في القانون الفيدرالي الأمريكي:

ورد في القانون الفيدرالي الأمريكي تعريفان للتوقيع الإلكتروني الأول في القانون الفيدرالي للتوقيع الإلكتروني، الذي جاء في المادة 08/102 بأن التوقيع الإلكتروني هو التوقيع الذي يصدر في شكل إلكتروني، و يرتبط بسجل إلكتروني.

(1) علاء محمد نصيرات، المرجع السابق، ص 24.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

بينما الثاني ورد في قانون المعاملات الإلكترونية الموحد، و الذي عرفه بأنه صوت أو رمز أو إجراء يقع في شكل إلكتروني يلحق (يرتبط منطقياً) بعقد أو سجل آخر (وثيقة) ينفذ، أو يصدر من شخص بقصد التوقيع على السجل⁽¹⁾

و السجل الإلكتروني، كما عرفته القوانين الأمريكية هو أي عقد أو سجل آخر، جرى إنشاؤه أو إرساله أو استقباله أو تخزينه بالوسائل الإلكترونية⁽²⁾

و ما يلاحظ على التعريفين أنهما فتحا المجال أمام أية وسيلة تقع في شكل إلكتروني، متى كانت قادرة على تحقيق متطلبات التوقيع الإلكتروني، و من ثم الاعتراف بها كوسيلة صالحة للتوقيع، و هذا ما يجعل من التشريع الأمريكي يركز على الجانب التقني مع اشتراط ارتباط التوقيع بالسجل الإلكتروني ارتباطاً منطقياً.

2/ تعريف التوقيع الإلكتروني في التشريع الفرنسي:

تدخل المشرع الفرنسي بتعديل بعض نصوص القانون المدني لتتفق مع التوقيع على العقود والمحركات الإلكترونية، فنص في المادة 1316/4 الفقرة 02 المعدلة بالقانون الصادر في 13 مارس 2000 تحت رقم 230/2000 بتعريف التوقيع الإلكتروني، بأنه التوقيع الذي ينتج عن استخدام أية وسيلة مقبولة موثوق بها، لتحديد هوية الموقع و تكفل اتصال التوقيع بالعمل أو المستند المرتبط به.⁽³⁾

أما الفقرة الأولى من ذات المادة، عرفت التوقيع بأنه التوقيع الذي يميز هوية صاحبه وهو التعريف العام للتوقيع.⁽⁴⁾

(1) علاء محمد نصيرات، المرجع السابق، ص 25.

(2) علاء محمد نصيرات، المرجع السابق، ص 26.

(3) علاء محمد نصيرات، المرجع نفسه، ص 27.

(4) خالد ممدوح إبراهيم، إبرام العقد الإلكتروني دراسة مقارنة، دار الفكر الجامعي، الاسكندرية 2006، ص 19.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

كما عرف المرسوم الصادر عن مجلس الدولة الفرنسي في 2001/03/30 التوقيع الإلكتروني، بأنه مجموعة من البيانات تصدر عن شخص نتيجة للإلتزام بالشروط الواردة في الفقرة الثانية من المادة 4/1316 من القانون المدني الفرنسي⁽¹⁾.

و ما يلاحظ على المشرع الفرنسي، أنه عرف التوقيع مركزاً على وظائف التوقيع في الفقرة الأولى من المادة 4/1316، مما يسمح بإتساع نطاقه ليشمل التوقيعات التقليدية والإلكترونية، ثم جاء في الفقرة الثانية من نفس المادة ليضع شروط لتحقيق التعادل الوظيفي بين التوقيع الإلكتروني و التوقيع التقليدي، و هو أن تكون طريقة إنشاء التوقيع الإلكتروني موثوق بها، مع وجوب ارتباط التوقيع بالبيانات موضوع التوقيع.

3/ القانون الفدرالي السويسري: الصادر بتاريخ 19 ديسمبر 2004 عرف التوقيع الإلكتروني في المادة

2/منه علماً النحو الآتي " : التوقيع الإلكتروني هو التوقيع الذي تتمتع بالمتطلبات الآتية :
رابط صاحب فقط ويسمح من خلال التعرف على شخصيته، وقد أنشئ بسائل إلكترونية تتم من خلال حمايتها وحفظه من قبل الموقع بقاءاً وتحت سيطرتها المنفردة، وبالمعطيات التي تتعلق بها، وأي تغيير أو تحريف قد يحصل للبيانات مستقبلاً كإكتشافه.

4/ القانون الفدرالي الألماني: فإنه أخذ أيضاً بالفرقة بين التعريف² العام للتوقيع الإلكتروني والتوقيع الإلكتروني مؤمن، وأخيراً التوقيع الإلكتروني الموصوف فقد نص في المادة الثانية منه علماً أن :

- التوقيع الإلكتروني عبارة عن بيانات تعلن شكلاً إلكترونيًا وتتصل ببيانات أخرى إلكترونية، أو يرتبط منطقياً معه ويتحقق من خلال التصديق عليه

- التوقيع الإلكتروني لا من عبارة عن توقيع إلكتروني يختصر التوقيع إلى المال التوقيع الإلكتروني، ويكمن في حديد شخصية صاحب التوقيع، السيطرة الكلية والفعالية على التوقيع من قبل الموقع، ويرتبط التوقيع بالبيانات الموقعة بحيث أن أي تغيير يمكن إكتشافه

(1) أحمد أمين الرومي، المرجع السابق، ص 12.

(2) - القاضي حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية، الطبعة الأولى، دار وائل للنشر عمان، 2006، ص 177.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

-التوقيع الإلكتروني الموصوف أيضاً عبارة عن توقيع إلكتروني بحيث أنه يستند إلى قاعدة أو وصف كامل ودقيق

من وقت إنشائه، ويتمتع بإنشائه بطريقة آمنة للتوقيع

5/ تعريف التوقيع الإلكتروني في التشريع المصري:

عرف المشرع المصري التوقيع الإلكتروني بموجب قانون رقم 15/ 2004 المتعلق بتنظيم التوقيع الإلكتروني و إنشاء هيئة صناعة تكنولوجيا المعلومات، على أنه "ما يوضع على محرر إلكتروني، و يتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، و يكون له طابع متفرد يسمح بتحديد شخص الموقع، و يميزه عن غيره"⁽¹⁾

و ما يلاحظ على هذا التعريف، أنه ركز على تبيان صور التوقيع الإلكتروني مع اشتراط الطابع المتفرد، حتى تضمن السرية التامة، و تحديد هوية الموقع و تمييزه عن غيره، و هي إحدى وظائف التوقيع.

غير أن المشرع المصري أغفل الوظيفة الثانية للتوقيع، و هي التعبير عن إرادة الموقع بالموافقة على مضمون السند، مما يجعل إرادة الموقع مفترضة بمجرد وضع التوقيع على المحرر. كما أنه عرف التوقيع الإلكتروني بعبارة "ما يوضع على المحرر" و التي تدل على الغموض في تحديد فكرة الارتباط المنطقي بين التوقيع و المحرر.

الفرع الثالث: موقف المشرع الجزائري فيما يتعلق بتعريف التوقيع الإلكتروني.

المشرع الجزائري لم يعرف التوقيع الإلكتروني، و إنما استعمل عبارة "يعتد بالتوقيع الإلكتروني" في الفقرة الثانية من المادة 327 المعدلة بموجب القانون 10/05 المؤرخ في 20 جوان 2005 المعدل والمتمم للقانون المدني.

وربط شروط الاعتماد بالتوقيع الإلكتروني وفق الشروط الواردة في المادة 323 مكرر 1 من نفس القانون، و ذلك متى تأكد من هوية الشخص الذي صدر منه، و أن يكون محفوظا وفق شروط الأمان و السلامة، و لم يحدد تلك الشروط.

(1) خالد ممدوح إبراهيم، المرجع السابق، ص 192.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

فيلاحظ على المشرع الجزائري، أنه لم يخص التوقيع الإلكتروني بشروط منفردة و اكتفى بربطها بالشروط المتعلقة بالكتابة الإلكترونية، كأن التوقيع و الكتابة لهما نفس الوظيفة.

المطلب الثاني: شروط التوقيع الإلكتروني وصوره

إن التوقيع الإلكتروني حقيقة ملموسة، وعبرة عن فعل مادي من قبل الموقع وهو القيام بوضع التوقيع على وثيقة إلكترونية كالعقود والاتفاقات وأوامر البيع. بحيث يمكن لمسلم الوثيقة التحقق من صحة التوقيع واطمئنانه بشكل قاطع وأبدي¹.

ولكن ليس كما في التوقيع اليدوي بالنسبة لطريقة إنشائه والشك في صحته فقط في حالة حصول نزاع بشأنه. بل يتطلب ذلك أن يمنح التوقيع الإلكتروني الصبغة القانونية اللازمة ليتمكن مساواته مع التوقيع اليدوي²، وأصدرت منظمة الأمم المتحدة (أونسترال) القانون النموذجي للتوقيع الإلكتروني في عام 2001. ليكون مظلة تستطيع الدول أن تشرع قوانينها وفقها ليأخذ القانون شكلاً موحداً وعالمياً

ولكي يمكن الاعتماد على التوقيع الإلكتروني والاعتماد به من قبل جهة رسمية، يتطلب ذلك وجود بعض الشروط الخاصة بالتوقيع الإلكتروني.

الفرع الأول: شروط التوقيع الإلكتروني

أولاً: يشترط في التوقيع الإلكتروني أن يكون خاصاً بالموقع

¹ فهد عبد الله الحويماني، التوقيع الإلكتروني أو التوقيع اليدوي، مقال منشور في مجلة الاتصال العدد (11) في

2026/5/28 على الموقع: www.etesai.com.

² ثروت عبد الحميد، مصدر سابق، ص.51.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

ويلتزم بمضمون السند الإلكتروني الموقع عليه. ومن الضروري أن يكون التوقيع دالاً محدداً بشخص الموقع¹ ليتحقق بذلك تأثيره في الإثبات. وتعترف به قوانين الإثبات² وما نص عليه قانون أونسترال النموذجي الخاص بالتوقيع الإلكتروني في المادة 1(7/أ) منه هو أنه: "إذا ما استخدمت طريقة لتعيين هوية ذلك الشخص" وبما يؤكد سلطته في إبرام التصرف القانوني ورضائه بمضمونه.³

مع أن هناك اتجاه يرى عدم ملائمة التوقيع الإلكتروني للقيام بوظيفة الإثبات، وتحديد هوية الشخص والكشف عن إرادته وإلزامه بمحتوى المحرر بمجرد قيامه على وسيط إلكتروني غير مادي. ويختلف التوقيع الإلكتروني عن التوقيع التقليدي في أنه يؤكد هوية الموقع بشكل قاطع.⁴

في حين هناك رأي آخر يرى أن التوقيع الإلكتروني يؤدي ما يؤديه التوقيع اليدوي، وبدلة أكثر وثقة زائدة، وأمان أكبر مما في التوقيع التقليدي اليدوي، وقيل⁵ إن التوقيع الإلكتروني يعد من قبيل العلامات المميزة الخاصة بالشخص وحده دون غيره، ولا يشارك أحد فيه. مثلاً يقوم التوقيع البيومتري على الخصائص الذاتية للإنسان، التي لا يشترك فيها شخصان، كذلك الرقم السري، لا يمكن أن يتشابه شخصان بالرقم نفسه داخل نظام واحد. فعندما يشترط القانون وجود توقيع شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا أ- استخدمت طريقة لتعيين هوية ذلك الشخص، والتدليل على رضائه من المعلومات الواردة في رسالة البيانات

¹ محمد إبراهيم أبو الهيجاء، عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 68.

² المادة (11) من قانون البيئات الأردني والمادة (14) من قانون الإثبات المصري والمادة (19) من قانون البيئات السوري والمادة (25) من قانون الإثبات العراقي.

³ المادة (18/1) من قانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004.

⁴ مقال منشور في مجلة الاتصالات والعالم الرقمي. أسبوعية متخصصة تصدر عن صحيفة الجزيرة، الأحد (5) ربيع الثاني

1428 العدد (205) متوفر على الموقع www.al-Jazirah.com، تم الاطلاع 25-02-2026.

⁵ علاء محمد نصيرات، مرجع سابق، ص 26.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

ب- وكانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات¹

أي أن هذا التوقيع يعطي التوقيع الإلكتروني حجية التوقيع اليدوي نفسها بشرط

1. إمكانية تعرف شخص الموقع، وموافقه على مضمون المستند الموقع

2. إذا كانت الطريقة المستخدمة في التوقيع الإلكتروني لتعرف شخصية الموقع، موثوقة

وآمنة²

ونصت المادة (6/1) من قانون أونسترال الخاص بالتوقيع الإلكتروني لعام 2001 على

أنه "حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الشرط مستوفياً بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني موثق به بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة

وتنص المادة نفسها في الفقرة الثالثة منها على ما يأتي "يعد التوقيع الإلكتروني موثقاً به

لغرض الوفاء بالشرط المشار إليه من الفقرة السابقة إذا

أ- كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر.

وقد نصت المادة (1316/1) مدني فرنسي على تمتع الكتابة الإلكترونية بذات الحجية

بشرط إمكانية تعيين الشخص الذي صدرت منه

فيما نصت المادة الثانية من التوجيه الأوروبي على ربط التوقيع الإلكتروني ربطاً منطقياً

بمعلومات أو بيانات إلكترونية تصلح وسيلة لتمييز الشخص تحديد هويته³. وقد قضت محكمة

¹ انظر المادة (7) من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية

² نجلاه توفيق فليح، القيمة الثبوتية للتوقيع الإلكتروني، بحث منشور في مجلة الرافدين للحقوق التي تصدر عن كلية الحقوق

جامعة الموصل، مجلد 6، العدد 2004، ص 22، ص 33.

³ خالد مصطفى فهمي، مرجع سابق، ص 96.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

النقض المصرية أن ثبوت صحة توقيع يعد ما ورد به حجة على صاحب التوقيع بصرف النظر عما إذا كان بخطه أو بخط غيره.¹

ونصل إلى أن التوقيع الإلكتروني بصوره المختلفة إذا تم إنشاؤه بصورة صحيحة فإنه يعد من الإشارات المميزة، والخاصة بالشخص الموقع وحده دون غيره، فجوهر التوقيع الإلكتروني هو إثبات الربط بين صاحب التوقيع والمستند أو المحرر الإلكتروني، أي أن يسمح التوقيع الإلكتروني بتحديد هوية شخص الموقع على نحو يسمح بالاحتجاج بالمستند الإلكتروني وإعطاء محتوياته وآثاره القانونية بما يشمل من حقوق والتزامات، لغرض تمتع التوقيع الإلكتروني بالحجية القانونية في الإثبات لابد من استيفاء الشروط التي يؤدي غيابها إلى انعدام هذه الحجية، ومن هذه الشروط ارتباط التوقيع الإلكتروني بشخص الموقع.²

ثانياً: أن يتمتع التوقيع الإلكتروني بالسرعة والدقة والاستمرارية

بشرط المحافظة على التوقيع الإلكتروني، بأن يبقى بالصورة نفسها التي صدر بها من المرسل ووصله إلى المرسل إليه وذلك باللجوء إلى عملية الضبط الإلكتروني (HASH) وهي عبارة عن ضغط على بيانات لتأخذ شكل رسالة رقمية مختلفة تماماً عن صورتها البدائية، مما يؤدي ذلك إلى أن يتمتع التوقيع الإلكتروني بالثقة والأمان لا تقل عما في التوقيع اليدوي، وربما أفضل وأدق³

ولعل مفتاح إعلان الحرب النووية أكبر مثال على ذلك⁴

¹ نقض مدني مصري جلسة 13/11/1985، مجموعة أحكام النقض، 993-226-36. نقلا عن خالد مصطفى فهمي، مرجع سابق، ص. 22.

² ميلاد سامي، التوقيع الإلكتروني والحماية القانونية، بحث منشور في جريدة القبس، العدد 12614، الاثنين 23 يوليو 2007 متوفر على الموقع www.algabas.com : تم الاطلاع في 2026/04/09

³ عصمت عبد المجيد بكر، اثر التقدم العلمي في العقد، موسوعة القوانين العراقية، بغداد، العراق، 2007، ص. 100.

⁴ عصمت عبد المجيد بكر، مرجع سابق، ص. 103. ومحمد المرسي زهرة، مرجع سابق، ص. 114. وعبد الفتاح بيومي حجازي، الحكومة الإلكترونية، مرجع سابق، ص. 122.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

فإذا كان هناك شك في الأعضاء على الأشرطة المغنطة وأقراص التسجيل المستخدمة في الحاسبة الآلية لتعرضه لتلف السريع عند اختلاف الطاقة الكهربائية، إلا أن ذلك أمكن السيطرة عليه باستخدام أجهزة أكثر دقة وتطوراً، وبالتالي يمكن الاحتفاظ بالبيانات مدة طويلة قد تفوق التوقيع اليدوي¹ مع تحديد وقت إنشاء الكتابة الإلكترونية وتاريخها

ثالثاً: أن يتصل التوقيع الإلكتروني بالمرحّر أو السند الإلكتروني

وفي السند التقليدي هناك دمج وتفاعل بين السند والتوقيع، ويتحقق هذا الاتصال ما بين المرحّر والتوقيع بشكل يستحيل فصله على الورق، إلا بإتلاف المرحّر، وتكون الأحبار التي تتم بها الكتابة من مواد كيميائية قابلة للاتصال بشكل وثيق بالورقة بمجرد أن تجف، وهذا غير موجود في التوقيع الإلكتروني².

ففي السند الإلكتروني على الرغم من إمكانية الربط بينه وبين السند والتوقيع الإلكتروني وتأمينهما من حصول التلاعب فيهما، فإن هناك من يتحفظ على ذلك بقوله أن قبول السند الإلكتروني بواسطة القاضي بوصفه دليلاً كتابياً يقتضي مدى قبول القاضي لكفاءة التقنية المستخدمة في إنشاء التوقيع الإلكتروني التي تؤهله للقيام بدوره في الإثبات، يعد ذلك نقطة ضعف للسند الإلكتروني³. وهذا الشرط يثير مسألة مهمة وضرورية، وهي سلامة المرحّر الإلكتروني من أي تعديل أو تلاعب أو تحريف قد يطرأ عليه بعد توقيعه، وبالتالي إحداث أي تعديل على التوقيع الموضوع على المرحّر الإلكتروني يؤدي إلى تعديل بيانات المرحّر كاملة، وهذا يجعل صلاحية المرحّر في الإثبات محل شك⁴، من ثم فإن التطور والتعقيد الذي يشهده

¹ ميلاد سامي، مرجع سابق.

² محمد إبراهيم أبو الهجاء، مرجع سابق، ص. 69.

³ عصمت عبد المجيد بكر، مرجع سابق، ص. 101.

⁴ لورنس محمد عبيدات، مرجع سابق، ص. 131 و. أحمد شرف الدين، حجية الرسائل الإلكترونية في الإثبات، بحث منشور

في مجلة الأبحاث القانونية، متوفر على الموقع : www.easlaws.com تاريخ الاطلاع 2026/04/29.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

الحاسوب الإلكتروني يؤدي إلى ارتباط التوقيع الإلكتروني أكثر وأعمق مع المحرر ويعطيه ثقة وأماناً أكثر. وبحيث يتفوق السند التقليدي الذي يمكن أن يزور بآليات معينة لا يمكن كشفها رابعاً: سيطرة الموقع وحده على وسيلة التوقيع

ويشترط أن تكون وسائل التوقيع الإلكتروني تحت سيطرة الموقع وحده دون غيره، وإلا لا يعد هذا التوقيع حجة على الموقع ولا على غيره. واشترطت ذلك معظم التشريعات الدولية والعربية.¹ ويتطلب هذا الشرط انفراد صاحب التوقيع بحيث من غير الممكن لأي شخص آخر معرفة رموز التوقيع الخاص به أو الدخول عليه عند استعمال أو إنشاء هذا التوقيع² وفي هذا السياق أوضح قرار مجلس الدولة الفرنسي الصادر في 20/3/2001 في المادة (1/2) - أن التوقيع الإلكتروني يكون صحيحاً إذا تم بوسيلة تكون تحت السيطرة المباشرة للموقع وحده دون غيره.³ كما عرفت المادة (2) من التوجيه الأوروبي للتوقيع الإلكتروني " التوقيع الإلكتروني المقدم هو التوقيع الذي يستوفي الشروط المحددة".

الفرع الثاني: صور التوقيع الإلكتروني

إذا كان التوقيع التقليدي، و فق ما حددته معظم التشريعات يتمثل في التوقيع بالإمضاء أو بالختم أو ببصمة الأصبع، فإن التوقيع بالطريق الإلكتروني يأخذ صور عدة، و أهم ما توصلت إليه التكنولوجيا في سبيل تنويعها، تتمثل في التوقيع الرقمي Digital signature والتوقيع بالقلم الإلكتروني Pen - op، التوقيع بالخواص الذاتية، التوقيع الإلكتروني البيومتري، التوقيع بالرقم السري Pin في البطاقات البلاستيكية، و نتعرض لكل منها على التوالي:

¹ المادة (3) من القانون النموذجي بشأن التوقيعات الإلكترونية (أونسترال). والمادة (18/5) من القانون رقم (15) للتوقيع الإلكتروني المصري لسنة 2004. والمادة (5) من قانون المعاملات الإلكترونية لمملكة البحرين رقم (28) لسنة 2004. والمادة (20/2 ج) من قانون رقم (2) لسنة 2002 لإمارة دبي بشأن المعاملات والتجارة الإلكترونية

² لورنس محمد عبيدات، مرجع سابق، ص.13

³ عصمت عبد المجيد بكر، مرجع سابق، ص.101

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

أولاً: التوقيع الرقمي

يعتبر التوقيع الرقمي من أهم صور التوقيع الإلكتروني، لكونها الأفضل على الإطلاق لما يتمتع به من درجة عالية من الثقة و الأمان في استخدامه.

وهو عبارة عن رقم سري أو رمز سري ينشئه صاحبه، بإستخدام برنامج حاسب آلي ينشأ دالة رقمية مرمزة لرسالة إلكترونية، يجري تشفيره بإحدى خوارزميات المفاتيح العام و المفتاح الخاص.⁽¹⁾

ينشأ التوقيع الرقمي، و يتم التحقق من صحته بإستخدام التشفير (الترميز)، و بناء على ذلك إذا أراد الموقع إرسال رسالة بيانات عبر البريد الإلكتروني مثلاً فإنه يقوم بإعداد ملخص الرسالة بإستخدام برنامج تشفير، ثم يشفر الملخص بإستخدام المفتاح الخاص و يقوم بإرسالها للشخص المستلم، الذي بدوره يستخدم المفتاح العام للموقع للتحقق من صحة التوقيع، ثم ينشئ المرسل إليه ملخص رسالة بإستخدام نفس برنامج التشفير، و يقارن بين ملخص الرسالتين فإذا كانتا متطابقتان فهذا دليل على أن الرسالة وصلت سليمة كما هي، و لم يحدث بها أي تغيير أو تحريف، أما إذا تم إحداث تغيير في الرسالة، فسيكون ملخص الرسالة التي أنشأها المستلم، مختلفة عن ملخص الرسالة التي أنشأها الموقع.⁽²⁾

فالتوقيع الإلكتروني يتم من خلال معادلات رياضية، بإستخدام اللوغاريتمات يتحول بها التوقيع أو المحرر المكتوب من نمط الكتابة العادية إلى معادلة رياضية، لا يمكن لأحد أن يعيدها إلى الصيغة المقروءة، إلا الشخص الذي لديه المعادلة الخاصة بذلك أي المفتاح العام و الخاص.⁽³⁾

ثانياً: التوقيع بإستخدام بطاقات الائتمان بالرقم السري Pin

(1) -علاء محمد نصيرات ، المرجع السابق ص 37.

(2) خالد ممدوح إبراهيم، إبرام العقد الإلكتروني . دراسة مقارنة ،دار الفكر الجامعي ، الإسكندرية 2006، ص 199.

(3) -علاء محمد نصيرات ، المرجع السابق ص 38.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

درجت البنوك على منح عملائها بطاقات الائتمان الممغنطة، و لها رقم سري لا يعلمه إلا صاحب البطاقة ،و ذلك تسهيلا لإبرام صفقات تجارية بشكل عام، و الحصول على نقود في أي وقت على وجه الخصوص، و تستخدم هذه البطاقات إما في سحب مبالغ نقدية في الحدود المتفق عليها بين العميل و البنك، بموجب عقد إصدار البطاقة و الحساب الخاص بالعميل أوفي دفع قيمة المشتريات التي يقوم العميل بشرائها من أماكن تقبل الدفع بهذه البطاقة. و لكي يقوم العميل بإتمام أية عملية منهما، عليه أن يدخل البطاقة بالوضع الصحيح داخل الجهاز المخصص لتنفيذ العملية، ثم بعدها يقوم بإدخال رقمه السري الخاص، ثم يقوم بالضغط على الاختيار الخاص بإتمام العملية⁽¹⁾.

إن دقة هذا النظام تكمن في أنه يشتمل على رقم سري مميز و فريد بصاحبه، و بالتالي لو عثر على البطاقة فلا يستطيع أي شخص استخدامها، ما لم يكن على علم بالرقم السري، و هذا نادرا ما يحدث إلا بإهمال من قبل حامل البطاقة، الذي يمكنه تفادي ذلك عن طريق مخاطبة البنك بوقف العمل بهذه البطاقة، و إلا فإن هذه البطاقة و الرقم السري قد يحقق وظائف التوقيع بكفاءة عالية⁽²⁾.

ثالثا: التوقيع بالخواص الذاتية (البيومتري)

إن التوقيع البيومتري باستخدام الخواص الذاتية أو الطبيعية، كإجراء للتحقق يقوم بصفة أساسية على الخواص الفيزيائية و الطبيعية و السلوكية للإنسان³ و التي لا يمكن أن تتشابه من الناحية الإكلينيكية، بدلا من الانتقادات التي وجهت لنظام التعامل بالبطاقات الممغنطة المقترنة بالرقم السري، فالبديل الآن هو البصمة الصوتية للشخص أو بصمة إصبعه أو بصمات الشفاه. ووفقا لهذه الطريقة يتم تخزين بصمة الشخص داخل الدائرة الإلكترونية للجهاز، الذي يتم التعامل معه أو من خلاله، بحيث لا يتم الدخول إلا عندما ينطق الشخص كلمات معينة

(1) سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، 2006، ص 67.

(2) علاء محمد نصيرات، المرجع السابق، ص 36.

(3) سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، 2006، ص 70.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

أوضع بصمة الأصبع المتفق عليه، أو بصمة شفاه بحيث يتم التعامل عندما يتأكد الجهاز من عملية المطابقة الكاملة.⁽¹⁾

و ارتباط هذه الخواص الذاتية بالإنسان، تسمح بتمييزه عن غيره بشكل موثوق به إلى أقصى الحدود، و هو ما يتيح استخدامها في التوقيع على العقود الإلكترونية، و هذا النوع من التوقيع كشأن كل أنواع التوقيع الإلكتروني، يرتبط استخدامه و الوثوق فيه بمدى درجة تقدم التكنولوجيا التي تؤمن انتقاله، بدون القدرة على التلاعب به.

رابعاً: التوقيع بالقلم الإلكتروني

و هذه الطريقة عبارة عن قلم إلكتروني، يمكنه الكتابة على شاشة الكمبيوتر عن طريق برنامج هو المسيطر و المحرك لكل هذه العملية، و يقوم هذا البرنامج بوظيفتين أساسيتين، لهذا النوع من التوقيعات الأولى، و هي خدمة النقاط التوقيع و الثانية هي خدمة التحقق من صحة التوقيع، وتتمثل هذه الطريقة في نقل التوقيع المحرر بخط اليد عن طريق التصوير بالماسح الضوئي scanner، ثم تنقل هذه الصورة إلى الرسالة الإلكترونية المراد منها، إضافة هذا التوقيع إليها الحجية عليها.⁽²⁾

غير أن هذه الطريقة تواجه الكثير من المعوقات، تتمثل في عدم الثقة، حيث يمكن للمستقبل أن يحتفظ بهذا التوقيع الموجود على المحرر الذي استقبله، عن طريق شبكة الإنترنت عبر جهاز scanner، ووضعه على أي مستند آخر لديه دون وجود أي طريقة يمكن من خلالها التأكد من أن صاحب هذا التوقيع هو الذي وضعه على هذا المستند و قام بإرساله إلى هذا الشخص، و عليه فإن هذه الطريقة تضعف الثقة في المحررات الموقع عليها إلكترونياً، و بالتالي تقلل من حجية التوقيع الإلكتروني.⁽³⁾

⁽¹⁾ نفس المرجع، ص. 70.

⁽²⁾ - خالد ممدوح إبراهيم، إبرام العقد الإلكترونية (دراسة مقارنة) دار الفكر الجامعي، الإسكندرية، 2006، ص 200.

⁽³⁾ - محمد الجنبهي، ممدوح محمد الجنبهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 45.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

وأيا كانت الصورة التي يتخذها التوقيع، فإنه لضمان صحته ونسبته إلى الموقع يلجأ إلى التشفير عن طريق استخدام Algorithm، الأمر الذي تتعدد التقنيات المستخدمة فيه لئلا من المتخصصين فيه طريقته، وهو يتم بمرحلتين: مرحلة التشفير و مرحلة فكّه . وقد سبق وقشرنا بأن التشريعات قد تقف موقفا حياديا بالنسبة للتقنيات والتكنولوجيات المتوافرة لتحقيق التشفير، وتأمين التعامل بالرسائل والتوقيع الإلكتروني، وقد تذهبتشريعات منها إلى تبني صراحة أسلوب تكنولوجيا التوقيع الإلكتروني الرقمي.

الفرع الثالث: أهم تطبيقات التوقيع الإلكتروني

نظرا لما يحظى به التوقيع الإلكتروني من مزايا، كفلت له انتشارا واسعا و تزايدا مستمرا في الاستخدام، وذلك في مجالات عدة، سواء على مستوى المعاملات القانونية بين الأفراد أو المؤسسات، ومن أهم تطبيقاته نجد البطاقات البلاستيكية، التلّكس، الشيك الإلكتروني وسند الشحن الإلكتروني وغيرها .

نقتصر في دراستنا على عرض استخدام التوقيع الإلكتروني في البطاقات البلاستيكية، ثم التلّكس.

أولا: البطاقات البلاستيكية

اخترنا البطاقات البلاستيكية كدراسة تطبيقية، لانتشار استخدامها في البنوك و في المعاملات التجارية عبر الانترنت، و قد ظهرت أخيرا في البريد لتحل محل الشيك الورقي، ويمكن القيام بعمليات أخرى مثل الاطلاع على الرصيد، و السحب و التحويل. سنحاول التطرق لأنواعها ثم التوقيع الإلكتروني فيها، و مدى حجيته في النقاط التالية:

1/ أنواع البطاقات البلاستيكية

أ - البطاقات الائتمانية (المصرفية) CreditCard.

الفصل الأول لإطار القانوني للتوقيع الالكتروني

عرفها مجمع الفقه الإسلامي الدولي بأنها مستند الكتروني، يعطيه مصدره لشخص طبيعي أو اعتباري بناء على عقد بينهما، يمكنه من شراء السلع و الخدمات ممن يعتمد المستند دون دفع الثمن حالا، لتضمنه التزام المصدر بالدفع، و منها ما يمكن من سحب النقود من المصارف⁽¹⁾. فهي بطاقة بلاستيكية يمنحها المصدر للحامل، و يمنح له بموجبها خط ائتمان، فيستطيع من خلالها شراء مستلزماته ثم التسديد لاحقا، وإلا لم يستطع التسديد في أي شهر يسمح له بتدوير جزء أو كل المبلغ، مقابل دفع فائدة على رصيد المدين القائم، و يمكن استخدامها للدفع عبر الانترنت⁽²⁾.

ب- بطاقة الحساب "Charge Card"

وهي بطاقة تتيح للمستهلك الشراء على الحساب و التسديد لاحقا، و لا بد على حاملها تسديد المبلغ بكامله، عندما يرسل المصدر فاتورة له، و لا يتحمل المستهلك جراء ذلك أية فوائد⁽³⁾.

ج-البطاقة المدينة (بطاقة الوفاءdebitcard)

تسمح هذه البطاقة لحاملها بتسديد مشترياته من خلال السحب على حسابه الجاري في المصرف مباشرة، فالعميل عند العمليات المختلفة، من سحب النقد، ا و دفع قيمة المشتريات يحول الأموال العائدة له إلى حساب البائع التاجر مباشرة، فإذا كانت البطاقة متصلة -On "line على الخط يتم تحويل الأموال فورا، أما إن كانت خارج الخط "Off -line فإن التحويل يتم خلال عدة أيام لاحقة.

د- بطاقة الصراف الآلي "A.T.M"

تسمح هذه البطاقة بالدخول إلى مكنونات المصرف المؤتمنة، و إلى الشبكات المرتبطة بها العائدة للمصارف الأخرى، ويستطيع العميل إجراء العديد من المعاملات المصرفية النمطية، مثل التحويل من حساب لآخر، إيداع و سحب الأموال، وتسديد بعض الفواتير⁽¹⁾

(1) فيصل سعيد الغريب ، المرجع السابق ، ص 239.

(2) علاء محمد نصيرات ، المرجع السابق ، ص 42.

(3) نفس المرجع ، ص 42.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

هـ - البطاقة الذكية "SmartCard"

تعتبر هذه من أهم أنواع البطاقات، كونها تحتوي على شريحة ذكية تسمى ميكرو بروسيسور "Microprocessor puce"، مما يجعلها عبارة عن كومبيوتر مصغر لا يزيد حجمه عن الظفر، ويمكن طبع برمجته لتلبية بعض الوظائف بواسطة شركات مختصة، فتدخل بعض المعلومات في الذاكرة، مثل اسم صاحب البطاقة، مؤسسة العمل الجهة المصدرة للبطاقة، تاريخ سريانها، ثم ترمج دالة جبرية أو خوارزمية مسؤولة عن توليد الرقم السري، وعند كل استعمال يدخل العميل البطاقة في آلة قراءة مع إدخال الرقم السري المولد في البطاقة، فإذا كانا متطابقين تتم العملية المزمع القيام بها، وإذا كانا غير متطابقين يعطى حامل البطاقة محاولتين أخريين، فإذا أخطأ رغم هذا في إدخال رقم سري صحيح يطلق "Microprocessor" أمر لإفساد وتعطيب نفسه⁽²⁾.

2 / التوقيع الإلكتروني في البطاقة البلاستيكية.

يجمع بين كل أنواع البطاقات البلاستيكية، اعتمادها على الرقم السري عند استخدامها للقيام بعمليات معينة، ويتم ذلك بسلك الخطوات التالية:

- * إدخال البطاقة التي تحتوي على البيانات الخاصة بالعمل في جهاز مخصص .
- * كتابة الرقم السري المخصص لصاحب البطاقة .
- * إصدار الأمر للقيام بالعملية المراد إتمامها بالضغط على المفتاح المخصص، وبذلك يكتمل التعبير عن الإرادة في قبول إتمام العملية.

فالرقم السري يستعمل لتعريف و تحديد هوية المتعامل أو الزبون، بالإضافة إلى توقيع العمليات الحسابية دون استعمال ورق.

* ويتم إثبات عملية السحب على ثلاثة أنواع من المخرجات : على شريط ورقي موجود خلف الجهاز، على أسطوانة ممغنطة، و في حالة قيام نزاع بين البنك و العميل حول عملية السحب

(1) فيصل سعيد الغريب ، المرجع السابق ، ص 236.

(2) علاء محمد نصيرات ، المرجع السابق ، ص 43 .

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

ذاتها، أو مقدار المبلغ الذي تم سحبه، فإنه يكفي للمؤسسة المصرفية تقديم تسجيلا للعمليات التي تمت بواسطة جهاز الحاسب الآلي .

3 / مدى تعارض التوقيع الإلكتروني في البطاقات البلاستيكية مع مبادئ الإثبات

لما كان إثبات العملية أو مقدارها يتم بتقديم تسجيلا للعمليات التي تمت بواسطة جهاز الحاسب الآلي، و لما كان هذا الجهاز يخضع لسيطرة المؤسسة المصرفية، و لها حرية التصرف فيه، فإنه من المفروض ألا يعتد به، لأنه يتعارض مع مبدأ أساسي في الإثبات، وهو أنه لا يجوز للشخص أن يصطنع دليلا لنفسه، و مع ذلك ميزت محكمة النقض الفرنسية بين فرضين: حالة ما إذا كانت الأداة أو الجهاز المستمد منه التوقيع يخضع للسيطرة التامة لمقدم الدليل، أو أحد تابعيه في عمليتي التحضير و التشغيل، فتفرض على ذلك الأساس الاستناد إلى هذا الدليل و اعتبرته اصطناعا للدليل لصالحه.

أما الفرض الثاني ألا يكون لمقدم الدليل أي سيطرة على المنظومة المعلوماتية المتعلقة بتسجيل العمليات الواقعة من طرف العميل⁽¹⁾، فتقبله و لا تعتبره اصطناع للدليل.

و في رأينا المتواضع: نرى أنه بما أن الجهاز بمجرد وضعه في العمل يصبح أداة آلي، وذاتي، ويقتصر دور المؤسسة على صيانة الجهاز كعتاد دون المساس بالنظام المسؤول على القيام بالتعرف على منشأ البطاقة، و مدى توافقها مع الجهاز ثم التعرف على العميل بمطابقة الرقم السري الذي يحمله مع قاعدة البيانات المرجعية، التي كونتها المؤسسة بمناسبة طلبات الحصول على البطاقة، وذلك يعد بمثابة المرور على حاجز أمني، وفي حالة اجتيازه يمنح النظام مربع حوار لمجمل العمليات التي يمكن القيام بها عن طريق البطاقة ، بالإضافة أن الجهاز يقدم مستخرجا مكتوبا على الورق يمنح للعميل بمجرد الانتهاء من العملية التي قام بها. فإنه و الحال كذلك يمكن الاعتداد بما ورد في هذه الأجهزة لإثبات مختلف العمليات التي كانت قد أنجزها العميل ،دون أن يكون ذلك اصطناع المؤسسة دليلا لصالحها.

(1) ثروت عبد الحميد ، المرجع السابق ، ص 80/79.

الفصل الأول لإطار القانوني للتوقيع الالكتروني

ثانيا: التلكس

يعتبر التلكس من وسائل الاتصال الحديثة التي أصبحت تستخدم في عدة مجالات، ومنها إجراء الصفقات و العقود بين الأفراد والمؤسسات ، فما هو التلكس وما حجته في الإثبات ؟
نحاول الإجابة في النقاط التالية:

1/تعريف التلكس:

يعرف أنه جهاز الكتروني مبرق متصل بدعامة يطبع البيانات الصادرة من المرسل بلون أحمر ، والبيانات الصادرة من المرسل إليه باللون الأسود، و يستطيع المشترك الاتصال مباشرة مع أي مشترك آخر يملك نفس الجهاز، لإرسال إجابته و تلقي رده ، فلكل مشترك رقم و رمز نداء من الجهاز المرسل إليه⁽¹⁾.

2 /طريقة عمله:

يعمل التلكس عن طريق ما يسمى بالتشفير المتماثل فهو يستخدم نظام النداء الذهاب، ويقصد به أن رمزا معيناً يمكن أن ينتقل بين جهازين متصلين ببعضهما بخط واحد، وبهذا الأسلوب نفسه يمكن استلام النداء الراجع من أحدهما، و يقوم جهاز التلكس بتحويل الحروف المكتوبة التي تتم عن طريق الإرسال، والاستلام بالاتصال السلكي واللاسلكي، إلى نبضات كهربائية فيتحول الضغط على الحروف إلى إشارات كهربائية، تتحول إلى إشارات كهرومغناطيسية ، تمر خلال أمواج ليقوم بتسلمها جهاز التلكس الذي تنعكس فيه العملية إلى طبع الحرف المرسل⁽²⁾ استخدام التلكس في البنوك:

يحرر البنك الأمر بالدفع برقية إلى بنك المستفيد ،يطلب منه دفع مبلغ معين مع تحديد تاريخ التحرير و اسم المستفيد، ثم يوقعه بوضع عدد معروف بالمفتاح أو الشفرة، على زاوية في البرقية، و هو ناتج عن دالة رياضية تستند إلى قاعدة سرية لا يعرفها إلا البنك المرسل إليه ، و البنك الباعث، وحتى داخلهما لا يعرفونها إلا الموظفين المخولين للإذن بتلك العمليات ، يقوم

(1) علاء محمد نصيرات ،المرجع السابق ، ص 51.

(2) ثروت عبد الحميد ، المرجع السابق ، ص 142.

الفصل الأول لإطار القانوني للتوقيع الالكتروني

البنك المراسل عند تلقي التلكس بحل المفتاح أو الشفرة حسب القاعدة المتبادلة ، وبالسرية المتفق عليها مع البنك العميل الأمر بالدفع، فإذا وجد نفس العدد على البرقية أدرك أنها صادرة عن الأمر فينفذ العملية بكل أمان، أما إذا اختلف العددين فيرفض انجاز العملية و يتصل بالبنك الأمر للثبوت في أمر البرقية.

3 / مميزات التلكس :

يتمتع التلكس بالسرعة و السرية و الوضوح و أهم سمة له أنه يترك أثرا ماديا مكتوبا للوثائق المرسله عن طريقه ⁽¹⁾، فهو بذلك يعتبر بيئة آمنة لتبادل الرسائل، وخاصة أنه يستخدم في شبكة خاصة يتحكم في إدارتها ، ومراقبتها شخص وسيط محايد يقوم بدور شبيه لمكاتب البريد ، فالوسيط يحدد هوية طرفي الرسالة ، و يتحقق من تلقي جهاز المرسل إليه للرسالة ويؤرخ عملية الإرسال، ثم أن الوسيط يحتفظ بما يدل على تبادل الرسائل خلال مدة معينة ، وهذه الإجراءات تكفل حدا أدنى من الأمان فيما يتعلق بعملية الإرسال والاستقبال .

4 / الاعتراف التشريعي بحجية التلكس :

لقد كانت حجية التلكس محل جدل بين الفقه من مؤيد و معارض ، و كانت معظم قوانين الإثبات لا تعطيه أية حجية إلا على سبيل الاستثناء ⁽²⁾، لكن في ما بعد اعترفت به، و من ضمنها المشرع الجزائري في المادة 329 من القانون المدني التي تنص على أنه : تكون للبرقيات هذه القيمة أيضا (قيمة الأوراق العرفية) إذا كان أصلها المودع في مكتب التصدير موقعا عليها من مراسلها ، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك ، وإذا تلف أصل البرقية فلا تعتبر نسختها إلا لمجرد الاستئناس ، و نظام إرسال البرقيات هو نفسه النظام المستخدم في التلكس ، ما عدا أنه في حالة التلكس تكون الرسالة مشفرة أما في البرق فلا، لأن أطراف التعامل يلجئون إليها نظرا للسرعة و الأمان الذي يتمتع به و من نص المادة المذكورة نجد أن المشرع الجزائري قد أعطى المحررات الناجمة عن التلكس القيمة ذاتها

(1) علاء محمد نصيرات ، المرجع السابق ، ص 52.

(2) نفس المرجع ، ص 53.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

للمحركات الورقية ، و افترض أنها مطابقة لأصلها المودع في مكتب التصدير حتى يقوم العكس ، ويمكن الرجوع لمكاتب التصدير للتحقق من قيام المرسل و المرسل إليه بالعملية موضوع النزاع، ولا بد أن يكون الأصل موقع عليه تحت طائلة عدم اعتباره دليلا كتابيا كاملا . أما إن لم يكن أصل البرقية موجودا لدى مكتب التصدير فإن مستخرج التلكس حتى و إن كان ممهورا بالتوقيع، وجميع البيانات الضرورية المحددة فإنه يكفي إنكار التوقيع ليفقد قيمته كمحرر مكتوب .

المبحث الثاني: حجية التوقيع الإلكتروني

تتوقف حجية السجلات والتوقيع الإلكتروني على القوة التي يمنحها الشارع لها في الإثبات: فإذا أقر الشارع لها هذه القوة كأداة لإثبات الحقوق والواجبات أو كوسيلة لحفظ البيانات التي تكون له حجيتها في إثبات الوقائع كانت النتيجة المترتبة على ذلك أن المساس بهذه السجلات والتوقيعات يشكل فعلا مجرما⁽¹⁾.

يتعين التمييز بين الحجية و متطلبات التعويل على التوقيع الإلكتروني أو بعبارة أخرى متطلبات تحقق الحجية القانونية للتوقيع الإلكتروني.

و قبل البدء فيما تثيره هذه الحجية القانونية للتوقيع الإلكتروني نجد أن الغاية من دراسته هو التوصل بالتوقيع الإلكتروني و الرسالة الإلكترونية التي تحقيق ذات الحجية القانونية المقررة للتوقيع بخط اليد و السند المحرر على الورق ما يثير مدى هذه الحجية و متطلبات تحققها ونطاق أعمالها.

المطلب الأول: شروط إضفاء الحجية على التوقيع الإلكتروني و نطاقها

إن التوقيع الإلكتروني يمر بمرحلتين الأولى تتعلق بإنشاء التوقيع، و توفير التأمين اللازم لذلك، و الثانية مرحلة التحقق من صدوره من الموقع، و ذلك عند تلقي الرسالة الإلكترونية.

(1) شبكة قانونيون العرب، المرجع السابق، متاح على الرابط، www.arablalaw.com

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

غير أنه حتى تتحقق الحجية القانونية للتوقيع الإلكتروني، و يكون له ذات الحجية للتوقيع التقليدي، يتعين توافر عدة شروط، فضلا عن وجوب اشتراك طرف ثالث عن الراسل والمرسل إليه، يضطلع بمهمة إصدار شهادات التوثيق لتنفيذ صدور التوقيع من الموقع، و من ثم التعرف على هويته و نسبة الرسالة و التوقيع له.

الفرع الأول: الصفات الواجب توافرها على التوقيع الإلكتروني

أولاً: أن يكون التوقيع متميز و مرتبط بشخص الموقع

التوقيع الخطي عبارة عن إشارة خطية متميزة خاصة بالشخص الذي صدرت عنه و الذي اعتاد أن يستعملها للإعلان عن اسمه⁽¹⁾.

ففي التوقيع الإلكتروني يجب أن تكون أدوات إنشاء التوقيع، من رموز و أرقام وغيرها متميزة بشكل فريد و مرتبطة بالشخص الموقع وحده دون غيره، لضمان عدم قيام أي شخص آخر بإنشاء نفس التوقيع، لارتباط التوقيع بصاحبه ارتباطا وثيقا معنويا و ماديا بالارتباط بين البيانات المستخدمة لإنشاء التوقيع و الموقع هو العنصر الرئيسي⁽²⁾ و هو ما نجده في أعظم صور التوقيع الإلكتروني، بإعتبار أن التقنية المستخدمة فيه تعتمد على البيانات الشخصية للموقع فمثلا التوقيع البيومتري للموقع، و كذلك الشأن في التوقيع بالرقم السري فكل رقم سري يقابله شخص وحيد، و في التوقيع الرقمي المفتاح العام و الخاص المميزين لشخص موقع.

ثانياً: أن يكون التوقيع محدد لشخص الموقع

يعد هذا الشرط أمر بديهي لا بد منه بإعتباره من وظائف التوقيع بالمفهوم العام فالتوقيع الإلكتروني يجب أن يكون محدد لهوية شخص الموقع على الرسائل الإلكترونية، ويتحقق

(1) اليأس أبو عبيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية 2005،

ص 181.

(2) علاء محمد نصيرات، المرجع السابق، ص 133.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

بذلك من خلال الرجوع إلى الجهات التي تقوم بإصدار شهادات التوثيق المعتمدة من يريد إنشاء توقيع إلكتروني، للتأكد من هوية الشخص الذي يستخدم التوقيع⁽¹⁾.

و هو ما نصت عليه المادة 3/6 بند (أ) من القانون النموذجي لسنة 2001: يعتبر التوقيع الإلكتروني قابل للتحويل عليه، إذا كانت بيانات إنشاء التوقيع مرتبطة في سياق الذي تستخدم فيه بالموقع دون أي شخص آخر، و المادة 323 مكرر 1 من القانون المدني الجزائري نصت "... بشرط إمكانية التأكد من هوية الشخص الذي أصدرها..."

ثالثا: سيطرة الموقع على منظومة التوقيع.

ويقصد به من الناحية الفنية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني،⁽²⁾ حتى يضمن أن يكون صاحب التوقيع منفردا بذلك التوقيع سواء عند التوقيع ذاته أو استعماله بأي شكل من الأشكال⁽³⁾.

نصت المادة 3/6 البند "ب" من القانون النموذجي لسنة 2001 كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون غيره.

و هذا الشرط يعين وجوب خضوع أدوات إنشاء التوقيع الموثق بأي صورة من صور، لسيطرة صاحب التوقيع و لزوم رعايته لها بعدم نشرها و الإفصاح عندها لصالح الغير حفاظ على سلامة المستندات الموقعة إلكترونيا، و مثال ذلك أن من يستعمل البطاقات البلاستيكية (الممغنطة) عليه الاحتفاظ بسرية رقمه المعطى له لقبول دخوله والقيام بالعمليات المصرفية، و إلا أمكن استعمال البطاقة من شخص أجنبي.

وكذلك الأمر في التوقيعات الرقمية إذ يجب تأمين وحماية المفتاح الخصوصي وإبقائه سرا.

(1) علاء محمد نصيرات، مرجع السابق، ص 134.

(2) محمد أمين أحمد الشوابكة، جرائم الحاسوب و الانترنت ، دار الثقافة للنشر و التوزيع ، عمان 2004 ،

ص 61.

(3) عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة ، دار الجامعة الجديدة ، الأزاريطة، ص 444.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

رابعاً: إرتباط التوقيع بالسند الذي يتعلق مع إمكانية كشف أي تعديل أو تعديل في بيانات التوقيع الإلكتروني.

يتناول هذا الشرط مسألة سلامة التوقيع الإلكتروني، و سلامة المعلومات التي يوقع عليها إلكترونياً، حيث إذا تم توقيع مستند تكون سلامته و سلامة التوقيع مرتبطين ارتباطاً وثيقاً⁽¹⁾ نصت المادة 3/6 بند "د" الفقرة "ج" من القانون النموذجي لسنة 2001: إذا كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلاً للاكتشاف. الفقرة "د" كان الغرض من اشتراط التوقيع قانونياً هي تأكيد سلامة المعلومات التي يتعلق بها التوقيع، و كان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلاً للاكتشاف". و تضمين التوقيع الإلكتروني في السند الإلكتروني له طابع خاص، يتلاءم مع البيئة الإلكترونية.

ففي التوقيع الإلكتروني لا يوجد اتصال محسوس بين البيانات المكونة للكتابة وبيانات التوقيع فيما بينهما، و بين الدعامة التي يظهران فيها فكل منها كيان معلوماتي مستقل، لكن مع ذلك لا بد من ارتباطهما ارتباطاً منطقياً يمكن من تحديد هوية الموقع والتعبير عن إرادته في قبوله بمضمون السند، مع إمكانية الكشف عن أي تغيير في التوقيع في أي لحظة، كما أن هذا الإرتباط لا يسمح بإجراء تعديل في السند الموقع دون إحداث تغيير على التوقيع⁽²⁾.

الفرع الثاني: التوثيق

يفرض استخدام التوقيع الإلكتروني بطريقة آمنة و موثوقة، للتحقق من صحته فلا بد من وجود جهة موثوق بها، لربط شخص أو كيان بالتوقيع، و يتم ذلك عن طريق جهات التوثيق التي

(1) علاء محمد نصيرات، مرجع السابق، ص 136.

(2) علاء محمد نصيرات، مرجع السابق، ص 137.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

تصدر شهادات التوثيق، لإثبات نسبة التوقيع الإلكتروني إلى شخص معين إستنادا إلى إجراءات التوثيق المعتمدة، أو المتفق عليها بين الأطراف⁽¹⁾.

و الغرض من إجراءات التوثيق هو التحقق من أن التوقيع الإلكتروني لم يتعرض إلى التعديل أو التغيير، و هو ما يؤدي إلى إعطاء التوقيع الإلكتروني الحجية القانونية في مواجهة أطرافه و الغير⁽²⁾.

و تكون جهات التوثيق مسؤولة عن صحة المعلومات الموثقة بالشهادات التي تصدرها وعن صحة الربط بين الموقع و التوقيع الإلكتروني.

و تجدر الإشارة إلى أن التوقيع الإلكتروني غير المصادق على صحته من جهات التصديق، لا تنعدم قوته الثبوتية لإعطائه الحجية و تمتعه بالآثار القانونية للتوقيع الصحيح. و بالرجوع إلى الفقرة (02) من المادة 327 من القانون المدني الجزائري نجدها قد نصت على الاعتداد بالتوقيع الإلكتروني، وفق الشروط المذكورة بالمادة 323 مكرر 1 من نفس القانون، وبملاحظة هذه الشروط و مقارنتها مع الشروط التي سبق وأن شرحناها لتوافر صحة التوقيع الإلكتروني، نجدها تنطبق على شروط التوقيع الإلكتروني العادي بمعنى آخر أن المشرع الجزائري لم ينص على التوقيع الإلكتروني المحمي، كما فعل المشرع الفرنسي وغيره، لذلك نتساءل هل أن المشرع قصد إعطاء الحجية الكاملة للتوقيع الإلكتروني البسيط غير الموثق، خاصة مع عدم تنظيمه لمسألة التوثيق الإلكتروني.

وعليه نقول أن هناك فراغا كبيرا في القانون الحالي، فالمشرع الجزائري لم ينظم هيئات المصادقة ولم يبين الجهة المكلفة بتحديداتها، مما يجعل من النصوص المستحدثة في ظل القانون 10/05 تحمل بذور جمودها، إذ لا يتصور ثقة الأفراد في وسيلة لا توفر أدنضمان الأمر الذي يحد من تفعيل هذه النصوص بشكلها الحالي.

(1) خالد ممدوح إبراهيم، المرجع السابق، ص.ص 196-197.

(2) علاء محمد نصيرات، مرجع السابق، ص 126.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

و أخيراً يلاحظ أن التشريعات التي نصت على الأخذ بالتوقيع الإلكتروني، وفي سبيل إضفاء صفة أو عنصر الأمان عليه اتخذت وسائل تضمن ثقة المتعاملين بها⁽¹⁾ كما جعلت لها قوة في الإثبات مساوية للتوقيع التقليدي، غير انه لا محل لهذه القوة إلا إذا توافرت ضوابط تكفل ضمان صحة و سلامة التوقيع، و لتحقيق هذا الهدف أصدرت قوانين و لوائح إدارية تتضمن الضوابط و الإجراءات الواجب اتخاذها بشأن استخدام و توثيق التوقيع الإلكتروني، وتتمثل هذه الضوابط فيما يلي :

1/ الضوابط الفنية العامة:

هناك عدة ضوابط فنية عامة يجب أن تتوافر في التوقيع الإلكتروني، فيجب أن يكون التوقيع خاصاً بالشخص وحده ولا يشاركه فيه غيره، كما يجب ألا يكون قد سبق إستخدام هذا التوقيع من قبل حتى ولو من صاحبه، وعلة ذلك هي كفالة أكبر قدر من السرية على هذا التوقيع، ويجب على الشخص صاحب التوقيع أن يقر كتابة بأن توقيعه الإلكتروني ملزم قانوناً ويتساوى مع توقيعه بخط اليد من حيث الأثر القانوني، غير أن هذا الإقرار غير لازم في كل مرة يضع فيها الشخص توقيعه الإلكتروني. ويجوز للهيئة المسؤولة عن التوقيع الإلكتروني أن تطلب من صاحب التوقيع أن يقدم شهادة بصحة توقيعه بمناسبة تصرف معين، وفي هذه الحالة فإنه يجب عليه تقديمها، وبخضع التزوير في هذه الشهادة للقواعد العامة في جريمة التزوير.

2/ الضوابط الفنية الخاصة:

إلى جوار الضوابط العامة سالفة الذكر، فإنه يوجب ضوابط فنية خاصة للتوقيع الإلكتروني وهي تختلف من نظام تشريعي إلى آخر بحسب ما توفره من أمن وسلامة المعاملات من ناحية، ومرونة وعدم عرقلة هذه المعاملات من جهة أخرى، وتتصل هذه الضوابط بتشفير المستند، سواء أكان توقيعاً أم سجلاً إلكترونياً، ويلاحظ أنه لا يكفي لضمان سلامة إتمام

(1) فيصل سعيد الغريب، التوقيع الإلكتروني وحججه في الإثبات، المنظمة العربية للتنمية الإدارية، 2005، ص243.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

المعاملة الإلكترونية أن يتم تشفير الرسالة المنسوبة لشخص معين، وإنما يجب التأكد من نسبة هذه الرسالة لهذا الشخص، وأن مضمونها لم يتعرض لتبديل أو تشويه⁽¹⁾

المطلب الثاني: نطاق حجية التوقيع الإلكتروني.

معظم الدول التي أصدرت تشريعات خاصة بالمعاملات الإلكترونية قامت بإدراج شروط خاصة أخرجت من نطاقها بعض المعاملات، ولم تقبل فيها التوقيع الإلكتروني حتى ولو كانت مستوفية لكافة الشروط، واقتصرت على البعض الآخر وهو ما سنعرضه في فرعين.

الفرع الأول: المعاملات التي يقبل فيها التوقيع الإلكتروني .

إن قانون الأونيسترال قد أقر أن قواعده تطبق عندما يستخدم التوقيع الإلكتروني في سياق الأنشطة التجارية، أي جعله حجة في الإثبات التجاري فقط، أخذاً بذلك بالمفهوم الواسع للمصطلح "تجاري"⁽²⁾.

في حين أن القانون المصري الخاص بالتوقيع الإلكتروني، قد نص في المواد 14، 15 على أن التوقيع الإلكتروني له الحجية في الإثبات المنصوص عليها في قانون الإثبات إذا ما تم استخدامه في المعاملات التجارية و المدنية و الإدارية فقط، ولم ينص على حجيته في الإثبات إذا استخدم في المعاملات الأخرى التي تخرج عن نطاق المعاملات المدنية والتجارية و الإدارية⁽³⁾.

لذا نرى أن المشرع المصري حدد نطاق استخدام التوقيع الإلكتروني .

كما اختلفت معظم التشريعات فيما يصلح فيه استخدام التوقيع الإلكتروني من تعاملات دون الأخرى، إذ منها من أقر استخدامه في المعاملات المدنية و التجارية فقط، و منها من أقر

(1) راجع الموقع الإلكتروني: شبكة قانوني العرب متاح على الرابط : www.arablawninfo.com . تم الاطلاع في 2026/05/26.

(2) قانون الأونيسترال النموذجي بشأن التوقيع الإلكتروني لسنة 2001 .

(3) منير محمد الجنبهي وممدوح محمد الجنبهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الاسكندرية

الفصل الأول لإطار القانوني للتوقيع الالكتروني

استخدامه في المعاملات مع الجهات الحكومية، و منها من جمع بين الاثنين فالتوقيع الأمريكي و الإماراتي عمدا إلى فتح المجال أمام الدوائر الحكومية و المؤسسات الرسمية، لاستخدام الوسائل الالكترونية في انجاز المعاملات المختلفة التي تدخل ضمن نشاطها، وذلك بصورة كلية أو جزئية، و هو ما يعرف بمصطلح الحكومة الالكترونية حيث يمكن انجاز معظم الخدمات التي تقدمها عن طريق الوسائل الالكترونية، وهو ما يجعلها تستخدم التوقيع الالكتروني في أداء الخدمة الالكترونية، حتى تكون هذه المعاملات كاملة من الناحية القانونية. فضلا على اعتراف معظم التشريعات بسريان التوقيع الالكتروني في المعاملات التي يتفق فيها الأطراف على اجرائها بالوسائل الالكترونية، وهو ما يشمل جميع المعاملات المدنية و التجارية في غياب ما يستثنىها بنص قانوني، وذلك متى استوفى التوقيع الالكتروني لجميع الشروط والأوضاع التي اشترطها القانون⁽¹⁾.

الفرع الثاني : المعاملات التي لا يقبل فيها التوقيع الالكتروني

عمدت معظم التشريعات إلى إخراج بعض أصناف المعاملات في نطاق استخدام التوقيع الالكتروني، مركزة في ذلك على التصرفات التي تستوجب الشكلية الخاصة لإتمامها بالإضافة الى معاملات الأوراق المالية .

اذ نجد أن القانون الفيدرالي للولايات المتحدة الأمريكية الخاص بالتوقيع الالكتروني في مجال التجارة العالمية و القومية الصادر في 2000 جاء فيه أن هذا القانون، لا يطبق في انشاء وتنفيذ الوصايا و شهادات منح الثقة و التبنّي و الطلاق والأمور المتعلقة بالأسرة، نزع الحيازة و انتهاء الرهون .

أما التوجيه الأوربي الصادر في 1999/12/13 فقد قرر عدم تطبيق التوقيع الالكتروني على العقود المنشئة و الناقلة لحقوق عقارية فيما عدا حقوق الايجار، والعقود التي تتطلب تدخلا من

(1) - علاء محمد نصيرات، المرجع السابق، ص. 162- 164 .

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

المحاكم والسلطات العامة، وعقود الكفالة و العقود التي يحكمها قانون الأسرة أوقانون الميراث مثل الوصية، الهبة، الطلاق، الزواج، التبني⁽¹⁾.

أما على مستوى التشريعات العربية، فإن القانون الأردني للمعاملات الإلكترونية رقم 85 لسنة 2001 في مادته السادسة استثنى من نطاق قبول التوقيع الإلكتروني مايلي :

أ/ العقود والمستندات و الوثائق التي تنظم وفقا لتشريعات خاصة بشكل معين و تتم باجراءات محددة، ومنها انشاء الوصية وتعديلها ،وكذلك انشاء الوقف و تعديل شروطه وغيرها من المعاملات المتعلقة بالاحوال الشخصية، و الحقوق العينية والتأمين الصحي

ب/الأوراق المالية إلا ما تنص عليه تعليمات خاصة استنادا لقانون المالية⁽²⁾.

أما المشرع الجزائري فلا يزال بعيدا كل البعد عن المتغيرات الحديثة ،إذ اكتفى بالإشارة عرضيا إلى التوقيع الإلكتروني، مما يستنتج منه إبقاءه على القواعد الخاصة المتعلقة بالشكلية بالطرق التقليدية.

وعليه وفي ظل الوضع القانوني الحالي، يصعب وجود تعامل بالتوقيع الإلكتروني ومنه بالمحرر الإلكتروني ككل، لغياب تنظيم أهم شرط في صحة التوقيع الإلكتروني والمحرر على حد سواء ألا و هوالتوثيق .

خلاصة

يتناول هذا الفصل الإطار القانوني المنظم للتوقيع الإلكتروني، باعتباره أحد أهم مظاهر التحول نحو المعاملات الرقمية. حيث تم التطرق في البداية إلى مفهوم التوقيع الإلكتروني بجميع أنواعه مع إبراز الاختلاف بينه وبين التوقيع التقليدي، وبيان خصائصه التي تميزه، خطة من حيث اعتماده على وسائل تقنية حديثة تضمن سلامة البيانات وصحة نسبتها إلى صاحبها

(1) - شبكة قانوني العرب ،مرجع السابق، متاح عبر الرابط : www.arablawninfo.com، تاريخ الاطلاع 2026/05/20.

(2) - علاء محمد نصيرات _المرجع السابق ص 165، 169.

الفصل الأول لإطار القانوني للتوقيع الإلكتروني

كما عالج الفصل الشروط و خصائص وصوره القانونية الواجب توفرها في التوقيع الإلكتروني حتى يكتسب الحجية القانونية، ومن أبرزها: إمكانية تحديد هوية الموقع، وضمان ارتباط التوقيع بالمحرر الإلكتروني، وحماية البيانات من أي تعديل أو تزوير وفي الأخير، خلص الفصل إلى أن الاعتراف القانوني بالتوقيع الإلكتروني يشكل خطوة أساسية لتعزيز الثقة في المعاملات الإلكترونية، وتحقيق الأمن القانوني، مما يساهم في تطوير الاقتصاد الرقمي وتسهيل التعاملات الحديثة

الفصل الثاني

جرائم التوقيع الإلكتروني وآليات حمايتها

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

شهد العصر الحديث تطورا تكنولوجيا متسارعا مس مختلف مجالات الحياة، حيث أفرزت الثورة الرقمية بيئة جديدة تعتمد على تبادل المعلومات وإبرام المعاملات عبر الوسائط الإلكترونية. وفي ظل هذه التحولات، برز التوقيع الإلكتروني كأداة أساسية لضمان الثقة في المعاملات الرقمية، لما يوفره من سرعة ومرونة وأمان، إضافة إلى منحه حجية قانونية تعادل في كثير من الأحيان التوقيع التقليدي

غير أن هذا التطور، وعلى الرغم من مزاياه العديدة، صاحبه ظهور أنماط مستحدثة من السلوك الإجرامي، استهدفت النظم المعلوماتية بصفة عامة، والتوقيع الإلكتروني بصفة خاصة. فقد أصبح هذا الأخير عرضة لعدة اعتداءات، كالتزوير، وانتحال الهوية، والاستعمال غير المشروع، الأمر الذي يشكل تهديداً مباشراً لأمن المعاملات الإلكترونية، ويؤثر سلباً على الثقة في البيئة الرقمية

ومن هذا المنطلق، تبرز أهمية دراسة جرائم التوقيع الإلكتروني باعتبارها فئة متميزة من الجرائم المعلوماتية، لما تتسم به من خصوصية في طبيعتها، وتعقيد في وسائل ارتكابها، وصعوبة في إثباتها في كثير من الأحيان. وهو ما يستدعي تحليلاً قانونياً دقيقاً لفهم أركانها، وتحديد صورها، وبيان الأحكام القانونية التي تنظمها

وعليه، يهدف هذا الفصل إلى تسليط الضوء على مختلف الجرائم التي تمس التوقيع الإلكتروني، سواء تلك التي تستهدف سلامته وسريته بياناته، أو التي تنال من حجته القانونية.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

المبحث الاول: صور جرائم التوقيع الالكتروني

يهدف هذا المبحث إلى تسليط الضوء على مختلف الجرائم التي تمس التوقيع الإلكتروني، سواء تلك التي تستهدف سلامته وسريته بياناته، أو التي تنال من حجبيته القانونية.

المطلب الاول: جريمة سرقة التوقيع الالكتروني والدخول الغير مصرح

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

الفرع الاول: تعريفها

أ- لغةً: بأنها أخذ الشيء في الخفاء وتطلق مجازاً على الشيء المسروق سرق منه مالا، كما يطلق مجازاً على السمع تخفياً، إذ يقال: اسرق السمع ومنه قوله تعالى: "إلا من استرق السمع... شهاب مبین".¹

ب- فقهاً: تعرف السرقة في مفهومها الواسع بأنها: "اختلاس مال منقول مملوك للغير بغية تملكه وعرفها الفقه بأنها اعتداء ملكية المنقول وحيازته بنية التملك وذهب البعض الآخر في تعريفهم لمفهوم السرقة على أنها اختلاس مال منقول مملوك للغير بغية التملك"

أما في المجال المعلوماتي فقد انقسم الفقه إلى اتجاهين

- يذهب الاتجاه الاول ان سرقة البيانات عبر الإنترنت أو من يقوم بسرقة البيانات فإنه يقر بأخذ نسخة من البيانات أو المعلومات أو برامج معينة وإدخالها في حيازته

¹ دلهار صلاح الدين يوناني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2016، ص 76.

² سورة الحجر، الآية رقم 18.

³ حسان ناجي صالح الخليل، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2009، ص 172.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

• **بناء على هذا فإن السرقة بهذا المعنى تتعارض وتعريف السرقة المنصوص عليها في التشريعات العقابية وفي إمكانية أن تكون البيانات أو البرامج محلاً للسرقة لأنها أشياء غير محسوسة وغير مادية.**

في حين يذهب الاتجاه الثاني إلى أن جريمة السرقة بمفهومها التقليدي يمكن أن تقع على البرامج والمعلومات وبالتالي تخضع لذات أحكام جريمة السرقة ، فالركن المادي يتمثل في أخذ نسخة من المعلومات أو البرامج دون إذن صاحبها أو علمه أي أن السرقة في هي عبارة عن استيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي سواء كانت مخزنة على أشرطة ممغنطة أو أسطوانات مدمجة وبين هذين الاتجاهين رأى البعض حصر نطاق مفهوم هذه الجريمة حيث عرفها على أنها "الاستيلاء غير المشروع على الأرقام والمعلومات الخاصة بالبطاقات الائتمانية المملوكة للغير عبر شبكة المعلومات بهدف الحصول على السلع والخدمات

ومن هذا المنطلق، يمكن القول بان مفهوم سرقة البيانات الالكترونية من الممكن أن يأخذ بذات المفهوم التقليدي لجريمة السرقة إلا أنه يتوسع في تحديد المحل الذي تقع عليه هذه الجريمة المتعلقة بالبيانات الالكترونية

وعليه يمكن تعريف سرقة البيانات الالكترونية على أنها عبارة عن الاستيلاء على البيانات أو المعلومات بواسطة اختراق أنظمة الحاسب الآلي أو المواقع الالكترونية وحيازتها بطريقة غير مشروعة تمكن الغير من حرمان صاحب الحق منها والبعض من مكوناتها، وذلك بدون علم وعلى غير إرادة مالكيها أو حائزها².

¹ يوسف بن سعيد الكيلاني، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه، جامعة أبو بكر الصديق، تلمسان، الجزائر، ص70.

² أيمن عبد الله فكري، جرائم نظم المعلوماتية، دار الجامعة الجديدة، الطبعة الاولى، الإسكندرية، 2007، ص 52.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الفرع الثاني: أركان جريمة السرقة الالكترونية

أولاً: الركن المادي في جريمة السرقة الالكترونية

إن الفعل المادي لـ لسرقة، أي فعل الاختلاس ، يتكون من عنصرين هما: العنصر الموضوعي المادي الذي يتمثل في الاستيلاء على الحيازة على نحو يؤدي إلى إخراج الشيء من حيازة المجني عليه وإدخاله في حيازة أخرى، والعنصر المعنوي المتمثل في عدم رضا المالك أو الحائز.

ووفقاً للمفهوم التقليدي لفعل الاختلاس عرف البعض الاختلاس المعلوماتي بأنه "الاستيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي".¹

1- فعل الاختلاس:

إن الطبيعة المعنوية للمعلوماتية أثارت خلافات في الفقه حول مدى إمكانية ورود فعل الاختلاس على المعلوماتية المعالجة آلياً فانقسم الفقه إلى اتجاهين:

أ- الاتجاه الأول: يرى أنصار هذا الاتجاه في عدم خضوع المعلومات لفعل الاختلاس للاختلاف الواضح في الطبيعة بينهما، فالمعلومات ذات طبيعة معنوية، بينما الاختلاس ذو طبيعة مادية، ويسوق أنصار هذا الاتجاه عدة حجج منها

- المعلوماتية لا تعد من قبيل الأشياء وكونها يتم الحصول عليها إما عن طريق الالتقاط السمعي أو البصري أو بطريقة إعادة نسخها على دعائم يملكها الجاني ذاته
- أن الاختلاس اللازم لقيام جريمة السرقة غير متحقق في إطار اختلاس المعلوماتية بمعناه المعروف يؤدي إلى إخراج المال من حيازة مالكه أو حائزه وإدخاله في حيازة الجاني، بينما في حالة المعلوماتية فإن المالك أو حائز المعلومات لا يفقدها بل كل ما في الأمر هو ازدياد عدد المطلعين عليها

¹ دلهار صلاح يوناني، مرجع سابق، ص 86.

² عمر أبو الفتوح عبد العليم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009، ص 301.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

- إن من غير المتصور اختلاس شيء معنوي غير مادي على اسقلال من دعامته، ومرد ذلك بمفهومه التقليدي يقتضي حيازته داخل دعامة معينة بقصد الغرض لتحقيق جريمة السرقة بمفهومه التقليدي يخروجه من حيازة صاحبه إلى حيازة الجاني، بينما المعلومات الموجودة على شاشة الحاسب الآلي فلا تصلح محلاً للسرقة¹.
- ب- **الاتجاه الثاني:** وفق أنصار هذا الاتجاه فإن المعلوماتية تخضع لفعل الاختلاس، معتمدين في ذلك على التوسع في مفهوم الاختلاس، حيث تغطي حالات الاختلاس الوقتي للشيء بنية استعماله وإعادته بعد فترة زمنية قصيرة ومن ثم تجريمها لعمليات النسخ أو نقل المحتوى المعلوماتي ويستند هذا الاتجاه على عدة حجج
- المعلوماتية قابلة للتحديد والقياس مثل الطاقة الكهربائية، فمن الممكن قياسها عن طريق كمية المعلومات بالشريط أو الأسطوانة ويمكن قياسها عن طريق الشريط أو الفكرة المعبرة عنها أيضاً².
- الاختلاس ليس له طبيعة واحدة بل يتفق مع طبيعة المحل الذي يرد عليه، فإذا كان المحل شيئاً غير مادي (معنوي) فإن الاستيلاء عليه سيكون بالطرق غير المادية تبعاً لذلك، وبما أن المعلوماتية كونها ذات طبيعة فكرية، فإن الاختلاس الذي يرد عليها سيكون من نفس طبيعتها، أي حيازة فكرية للشيء المعلوماتي³.

2- ركن محل الاختلاس المعلوماتي:

وفقاً للمفهوم التقليدي لجريمة السرقة فإن محل الاختلاس يجب أن يكون مالاً منقولاً وأن يكون مملوكاً للغير تبعاً لذلك فإن محل السرقة المعلوماتية هو مال معلوماتي مملوك لغير الجاني

¹ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الجديدة، الكتاب الأول، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011-2012، ص 28.

² المرجع نفسه، ص 29.

³ هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية المنعقد بـ 25 أكتوبر 1993، القاهرة، مصر، ص 310.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

والمعروف أن جريمة السرقة المعلوماتية إنما تنص على المعلوماتية وعليه لبيان ركن المحل فلا بد من أن تبين ما مدى اعتبار المعلومات مالاً لغير الجاني أي مالاً من خلال ما يلي

• أن يكون محل السرقة المعلوماتية مالاً: مدى اعتبار المعلومات محل سرقة المعلوماتية مالاً:

إن القيمة الاقتصادية التي تتمتع بها المعلومات جعل منها قيمة مالية قابلة للتملك والاستغلال، وهذه القيمة تتعاضد يوماً بعد يوم، مما أصبح من غير المقبول التغاضي عن أهميتها في ظل اعتماد المجتمع عليها في شتى المجالات، الأمر الذي اقتضى إسباغ وصف المال على المعلومات.

• أن يكون محل السرقة المعلوماتية مالاً منقولاً : مدى اعتبار المعلومات محل جريمة السرقة المعلوماتية من قبيل المنقولات

من المعلوم أن النصوص الجنائية الخاصة بالسرقة لا توفر الحماية الجنائية سوى للأموال المنقولة، والتي تعني وفقاً للمفهوم التقليدي أية مادة كونية غير بشرية قابلة للنقل من مكان لآخر سواء كانت صلبة أو سائلة أو غازية أي أن تكون ذات طبيعة مادية. بيد أن القضاء قد وسع من مفهوم المنقول واتجه إلى القول أنه "لا يقتصر وصف المال المنقول على ما كان جسماً متحيزاً قابلاً للون طبقاً لنظريات الطبيعة، بل هو يتناول كل شيء مقوم قابل للتملك والحياسة والنقل من مكان إلى آخر".²

هذا ما دفع جانباً من الفقه إلى إسباغ وصف المنقول على المعلومات، وذلك بناءً على قابليتها للانتقال من مكان إلى آخر وإمكانية حيازتها والإطلاع عليها من خلال شاشة الحاسب الآلي، دون اشتراط انتقال المحتوى والهيكل، فالانتقال هنا يكون ذهنياً، أي بمجرد تشغيل الحاسب الآلي وإلى ورؤية المعلومات على شاشته تنتقل هذه المعلومات إلى ذهن هذا المتلقي³، على

¹ خالد ممدوح إبراهيم، جرائم السرقة في التشريع الجنائي، دار الفكر الجامعي، الاسكندرية الطبعة الاولى، 2015، ص 104.

² دلهار صلاح يوناني، شرح القانون الجنائي، القسم الخاص، دار هومة، الجزائر 2017، ص 90.

³ هدى حامد قشقوش، شرح قانون العقوبات، القسم الخاص، الطبعة الثانية، دار النهضة العربية، القاهرة 2016، ص 57.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

اعتبار أن المنقولات تختلف بحسب طبيعتها فيما يتعلق بطريقة انتقالها، فمنها ما ينتقل باليد كالبضائع، وما ينتقل بالتدوين عن طريق الفاكس، ومنها ما ينتقل عبر الدوائر أو الانقاط الذهني كالمعلومات

- ويمكن تاييد الاتجاه القائل بسباغ وصف المنقول على المعلومات المعالجة آلياً كونها شيئاً قابلاً للانتقال دون أن يطرأ عليها تلف سواء عن طريق الدعامة المادية المخزونة أو عن طريق عمليات النسخ واللصق أو الإرسال سواء نقل أصلها كما في النسخ والإرسال لا يضيع الأصل كما في النقل المادي للامر. والجدير بالذكر أن اعتبار المعلومات من قبيل المنقولات لا يعني إمكانية اعتبارها محلاً للاختلاس في جريمة السرقة، وبخاصة ضمن فكر الاتجاه المعارض لوقوع الاختلاس على المعلومات والتي تقتضي برأيهم انتقال المال من حيازة الشخص إلى آخر أي حرمانه منها، وهو ما قد لا يتحقق في إطار المعلوماتية كما في حالة نسخ المعلومات مع بقاء الأصل، فالمنقول يكتسب هذه الصفة لإمكانية نقله من مكان إلى آخر وليس لإمكانية اختلاسه من عدمه¹.

- أن يكون محل السرقة المعلوماتية مالا منقولاً مملوكاً للغير لتكون محلاً لملكية الغير: من المتفق عليه أن جريمة السرقة لا تقع إلا على شيء مملوك لشخص غير الجاني، سواء كان طبيعياً أو معنوياً، وقد اختلفت الآراء حول المعلومات كمحل لسرقة المعلوماتية ما إذا كانت تصلح لأن تكون ملكاً للغير، فذهب رأي إلى أن المعلومات لا يمكن أن تكون ملكاً لأحد، بدعوى أن المعلومات هي إنتاج فكري حر لا يمكن أن يكون ملكاً لأحد، بدعوى أن المعلومات في إنتاج فكري حر لا يمكن أن يكون ملكاً لأحد، فالأفكار حرة مطلقة لا فضل لأحد بإيجادها في حين أن خلاصة تجارب أشخاص متعددين، غير أن هناك رأي آخر يرى إمكانية أن تكون

¹ دلهار صلاح يوناني، مرجع سابق، ص 90.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

المعلومات محل ملكية للغير، فهي ليست مجرد فكرة وإنما مجموعة أفكار أنشأت عنها شيء معنوي، وهو ما يؤكد وجود معلومات ذات قيمة اقتصادية كبيرة يتم الاحتفاظ بها بعيداً عن متناول الجميع

ونحن بدورنا نؤمن بصلاحيية المعلومات لأن تكون محلاً لملكية الغير، فالمعلومة عند تخليقها أو استخدامها من قبل شخص فإنه يكون المسيطر عليها، ويمكن رفض إذاعتها، وهذه العلاقة بين المعلومات وصاحبها هي علاقة قانونية، وهي علاقة الحائز بما يحوزه وتنطبق عليه قاعدة الحيازة في المنقول الملكية، أضف إلى ذلك أن المعلومات أصبحت في مصاف الأموال الاقتصادية المهمة كما سبق بيانه¹

ثانياً: الركن المعنوي لجريمة السرقة المعلوماتية

تقوم جريمة السرقة المعلوماتية على ركن معنوي يتمثل أساساً في القصد الجنائي الذي بدوره يركز على عنصري العلم والإرادة بحيث يتعين على الجاني أن يدرك أنه يختلس مالاً مملوكاً لغيره وأن إرادته اتجه إلى إحداث ذلك السلوك أو يتمثل ذلك في جريمة سرقة البيانات عند انتهاك الأنظمة الآلية التي تحوي أرقاماً سرية، مما يدل على سوء نية مرتكب الفعل ويظهر القصد الجنائي عندئذ في فترة البقاء غير المشروع، ولكن ربما يشكل عبء الإثبات في هذه الحالة عقبة في توافر هذا القصد من عدمه

أما بخصوص القصد الجنائي الخاص في جريمة السرقة فهو يتمثل في "نية تملك الشيء" مما يعني أن جريمة السرقة من الجرائم العمدية التي تتطلب قصداً جنائياً خاصاً يتمثل في نية تملك الشيء المسروق² ويستدل على توافر هذا القصد من خلال القرائن والأدلة

¹ هدى حامد قشقوش، المرجع السابق، ص 68.

² خالد ممدوح إبراهيم، الحماية الجنائية للتوقيع الإلكتروني، مجلة الفكر الشرطي، عدد 88، يناير 2019، ص 305.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

وقد قضت محكمة النقض المصرية "أن القصد الجنائي" في جريمة السرقة ينحصر في قيام الجاني عند ارتكاب الجريمة باختلاس المنقول المملوك للغير رغم إرادة مالكه بنية أن يملكه هو نفسه¹.

ويذهب القضاء الفرنسي إلى أن انتهاك النظام الأمني الخاص بالأنظمة الإلكترونية يعتد به كسوء نية وقصد سرقة منفعة حق ولو كانت نية التملك وقتية ، و التي تتوافر بمجرد ارتكاب الشخص عمل من أعمال التصرف والتي يظهر فيها بمظهر المالك واشترطت بعض القوانين المقارنة توافر نية التملك في جريمة السرقة حيث استخدم قانون العقوبات الفرنسي في المادة 311/1 تعبير "من اختلس بسوء نية" وكذلك فإن القانون الإنجليزي استخدم مصطلح سوء النية للتعبير عن نية التملك حين نص في قانون السرقة لسنة 1968 "يعتبر الشخص مرتكباً للسرقة إذا استولى لنفسه بسوء نية على أموال تنتمي إلى الغير بنية حرمان هذا الأخير منها بشكل دائم"² والسرقة هنا يترتب عليها حيازة الغير لنسخة من البيانات والمعلومات دون أن تؤدي إلى حرمان صاحبها من حيازتها أو التصرف فيها، كما يوجد فقهاء يرون أن القصد الجنائي الخاص المتمثل في نية التملك لا يتوافر في حالة الالتقاط الذهني للبيانات والمعلومات أوسعها ويبرر ذلك بأن الجاني لم يقصد حرمان الحائز القانوني لها وإنما شاركه في الانتفاع بها من خلال الإطلاع عليها، فإثبات القصد الجنائي هو مزيج من إثبات الوعي بملاسات الفعل المجرم واتجاه الإرادة إلى تحقيق النتيجة المتوقعة من جراء هذا الفعل ولهذا فإن عناصر القصد الجنائي بعنصريه العام والخاص تتوافر في الشخص مرتكب جريمة سرقة البيانات الإلكترونية

¹ مجموعة أحكام محكمة النقض رقم 15 لسنة 23/06/1964، ص 66.

² خالد ممدوح إبراهيم، مرجع سابق، ص 306.

³ "a person is guilty of theft if the dishonesty appropriates property belonging to another with the intention of depriving the other of it; and "thief" and "steal" shall be construed accordingly".

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الفرع الثالث : جريمة الدخول غير المصرح به إلى النظام المعلوماتي لتوقيع الإلكتروني

يقتضي تناول ماهية الدخول غير المصرح به إلى النظام المعلوماتي لتوقيع الإلكتروني أن نتعرض أولاً لمفهوم الدخول ووسائل الاختراق والدخول غير المصرح به للنظام المعلوماتي لتوقيع الإلكتروني وكذا أسباب الاختراق والدخول غير المصرح به إلى النظام المعلوماتي للتوقيع الإلكتروني

أولاً: ماهية جريمة الدخول غير المصرح به إلى نظام التوقيع الإلكتروني

أ- مفهوم الدخول غير المصرح به للنظام المعلوماتي

ينصرف معنى مصطلح "الدخول access" في إطار المعلوماتية بصفة عامة لتشمل كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة أو السيطرة على المعلومات التي يتكون منها أو الخدمات التي يقدمها¹، أو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والمعطيات المخزنة بداخله، للاطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي².

وقد عرف المشرع السعودي الدخول، في المادة الأول من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بأنه "دخول شخص بطريقة تعمدية إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات إليه غير مرخص لذلك الشخص الدخول إليها" إن فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يعني الدخول المادي، كالدخول إلى مكان أو منزل وحديقة، في نفس الاتجاه الدخول إلى الحاسب الآلي أو مكان وجوده، إنما يقصد بالدخول هنا كظاهرة معنوية تشبه تلك التي يعبر عنها بقولها "الدخول إلى فكر أو مملكة

¹ نائلة عادل محمد فريد قورة، شرح قانون العقوبات، جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، الطبعة

الأولى، 2018، ص 242.

² خالد ممدوح إبراهيم، مرجع سابق، ص 84.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

التفكير لدى إنسان أي الدخول إلى العمليات الذهنية التي يقوم بها النظام المعلوماتي "فالدخول إلى النظام المعلوماتي يتشابه مع الدخول إلى ذاكرة إنسان ويتحقق الدخول غير المصرح به بوصول جهاز الكمبيوتر إلى المعلومات أو البيانات المخزنة داخل نظام الكمبيوتر والقوائم والم لفات والمكونات دون رضا المسئول عن هذا النظام أو المعلومات التي يحتوي عليها أو يسعى آخر إساءة استخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات الموجودة بداخله لاستخدامها في غرض ما¹.

وقد جاء في نص المادة 2 من قانون الاتحاد الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على أنه "كل فعل عمدي يتوصل بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب عليه بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين"

ويلاحظ أن تحديد فكرة الدخول غير المشروع من حيث دلالة المكان يمكن ان تعرف بأنها "التسلل في داخل النظام المعلوماتي" أما الدخول من حيث الزمان فيتمثل في "تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية.

كذلك قد يتحدد مضمون الدخول من زاوية فنية بحيث قد يتم الدخول بصور مختلفة منها الاعتداء على البرامج أو البيانات أو المكونات المادية ويتم الدخول بواسطة الغش المعلوماتي يتم بطريقة الكترونية من خلال كلمة السر password أو طريقة مادية فيزيائية مثل اقتحام الملفات وسرقة الهوية الشخصية والطريقة الأولى هي الأكثر شيوعاً وتستعمل من قبل الذين

¹ دلهار صلاح يوناني، مرجع سابق، ص 191.

² أحمد عصام عجيبة، شرح قانون العقوبات، الطبعة الاولى، دار النهضة العربية، القاهرة، 2017، ص 251.

³ خالد ممدوح إبراهيم، الحماية الجنائية للتوقيع الإلكتروني، مجلة الفكر الشرطي، عدد 88 يناير 2019، ص 166.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

يسرقون كلمات السر أو يستخدمون الحاسب الآلي في إدخال كلمات سر عشوائية لأجل التوصل إلى كلمة السر الصحيحة¹.

ويلاحظ أن الاختراق لا يطل أجهزة الكمبيوتر إلا إذا كانت موصولة بشبكة الانترنت التي تصل الجهاز بفراصة الانترنت، ويعتبر من ضعف جرائم الاختراق أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة أما مجرداً ولجبية ارتكاب فعل آخر هذا البرامج والبيانات وتخريب المعطيات والنقم والممتلكات فمن مفهوم تخريب الكمبيوتر وإيذاء الكمبيوتر وخلق البرمجيات الخبيثة².

ج- أسباب الاختراق والدخول غير المصرح به لنظام المعلوماتي لتوقيع الالكتروني

تختلف أسباب الاختراق والدخول لنظام المعلوماتي باختلاف أهداف المخترق، فقد يكون الهدف من عملية اختراق أجهزة كمبيوتر البعض أو مواقعهم على الشبكة لمجرد الفضول وقد يخترق بعض السرقة لمعلومات والبيانات، وهذا هو السبب الأبرز الذي يدفع قراصنة الانترنت إلى الدخول إلى مواقع أجهزة كمبيوتر الغير لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل بدل مالي للاضطلاع عليها وقد يكون الاختراق في بنية المخترق فيتغير أو تحريف أو تعطيل المعلومات في أجهزة الغير وقد يكون الاختراق تزوير البيانات ومعلومات التوقيع الالكتروني وفي هذا الصدد نصت المادة 4 من قانون اتخاذ رقم 2 لسنة 2006 "بشأن مكافحة جرائم تقنية المعلومات" يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترف بها قانوناً في نظام معلوماتي

وقد يكون الاختراق بهدف تعطيل الأجهزة والشبكات الخاصة بتشكيل التوقيع الالكتروني حيث يتم تعطيل أجهزة الكمبيوتر عبر تعطيل برامجها، كما قد يؤدي تعطيل البرامج والشبكات

¹ عبد الفتاح بيومي حجازي، النظام القانوني للجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، الطبعة الاولى 2014، ص 81-82.

² خالد ممدوح إبراهيم، مرجع سابق، ص 168.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

عن تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة، تتم عملية تعطيل الأجهزة أو الشبكات المراد تعطيلها عن طريق إرسال الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها، الأمر الذي يعيقها عن تأدية عملها¹.

ثانياً: أركان جريمة الدخول غير المصرح به إلى نظام التوقيع الإلكتروني

تتطلب جريمة الولوج غير القانوني للنظام المعلوماتي إلى توافر ركن مادي وركن معنوي بشقيه القصد العام والقصد الخاص، فتناولها على نحو ما يلي

أ- الركن المادي لجريمة الدخول غير القانوني لنظام التوقيع الإلكتروني:

يعد فعل الدخول بدون تصريح إلى النظام المعلوماتي سلوكاً إجرامياً يتحقق به الركن المادي لهذه الجريمة، والذي يطلق عليه الدخول المنطقي، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية، حيث يختلف المحل الذي يتخذه الركن المادي في جريمة الدخول غير المصرح به إلى نظام مواقع الويب "web site" ويتم عادة التفرقة في هذا الخصوص بين العمليات التي تنطوي على اعتراض عمليات الاتصال من أجل الدخول إلى أحد نظم الكمبيوتر وبين الدخول إلى أحد نظم الكمبيوتر وبين الدخول المباشر إلى هذه النظام ويمكن بالنظر إلى التشريعات المختلفة التي جرمت الدخول غير المصرح به أن نميز بين ثلاث صور للمحل في جريمة الدخول غير مصرح به وهذا ما سيتم بيانه كالاتي

ب- محل الدخول بدون تصريح إلى النظام المعلوماتي لتوقيع الإلكتروني

باستعراض التشريعات المختلفة في مجال مكافحة الجرائم المعلوماتية، والتي تناولت جريمة الدخول بدون تصريح إلى النظام المعلوماتي، نجد أنها تتميز بين ثلاث صور للمحل الذي ينص عليه فعل الدخول بدون تصريح تتمثل الصور الأولى في المعلومات ذاتها والثانية في أنظمة الحسابات الآلية أما الثالثة فليشبكة.

¹ المرجع نفسه، ص 170.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

1-الاتجاه الأول:

أن من هذا الاتجاه التشريعي يجمع بين الصور الثلاث التي أشرنا إليها، أي المعلومات وأنظمة الحسابات الآلية وشبكة المعلومات، فهذا الاتجاه يوسع من محل الدخول بدون تصريح، لذا أطلق عليه اسم الاتجاه الموسع ومن التشريعات التي أخذت باتجاه الموسع لمحل الدخول بدون تصريح، التشريع الجنائي الفرنسي إذ تجرم المادة 323/1 من قانون العقوبات الفرنسي لسنة 1992 فعل الدخول أو البقاء بدون تصريح داخل نظام المعالجة الآلية بالمعنى الواسع للكلمة، وقد اجتمع الفقه في فرنسا على نظام الآلية للمعلومات وفق منظور المادة 323/1 من قانون العقوبات الفرنسي الجديد ينصرف إلى المعلومات والنظام الذي يحتوي عليها بالإضافة إلى الشبكات¹.

2-الاتجاه الثاني:

وفق هذا الاتجاه فإن محل الدخول بدون تصريح ينصب على المعلومات وأنظمة الحاسبات الآلية دون شبكات المعلومات، حيث يستبعد هذا الاتجاه من نطاق تجريم الدخول بدون تصريح شبكة المعلومات، ومن أبرز التشريعات التي أخذت بهذا الاتجاه هو التشريع الانجليزي بشأن إساءة استخدام الكمبيوتر لسنة 1995 إذ تعاقب المادة الأول منه على الدخول غير المصرح به إلى البرامج والمعلومات التي يحتوي عليها الحاسب الآلي فقد فدون الإشارة إلى شبكة المعلومات²، الأمر الذي يعني عدم شمول النص لحالات الدخول بدون تصريح التي تتم بصورة غير مباشرة عن طريق اعتراض الاتصالات المتضمنة نقل المعلومات³

3 -الاتجاه الثالث:

يتمثل هذا الاتجاه في تجريم الدخول بدون تصريح إلى أنظمة الحاسبات الآلية عبر شبكات المعلومات ومن التشريعات التي انتهت جت هذا الاتجاه قانون عقوبات السويسري حيث تعاقب

¹ نائلة عادل محمد فريد قورة، مرجع سابق، ص 332.

² خالد ممدوح إبراهيم، مرجع سابق، ص 88.

³ دلهار صلاح يوناني، مرجع سابق، ص 194.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

المادة 143 مكرر منه على الدخول بدون تصريح إلى أنظمة الحاسبات الآلية بواسطة جهاز لنقل المعلومات، وتوضح المناقشات التي دارت من خلال الأعمال التحضيرية لهذا القانون أن هذا النص لا يقصد من ورائه تجريم اعتراض وسائل الاتصال فهذا النص لا يعالج سوى حالات الدخول بدون تصريح التي تتم عن طريق أشخاص خارج المؤسسات التي تحتوي على أنظمة بواسطة شبكات الاتصال، أما الحالات التي تنطوي على دخول مباشر إلى النظام والتي تتم عادة من العاملين بالمؤسسات التي تحتوي هذه الأنظمة فلا ينطبق عليها النص ما لم يكن الدخول قد تم من خلال شبكة داخلية تابعة إلى المؤسسة.

ومن خلال استعراضنا لهذه الاتجاهات الثلاثة والتي تتبعها التشريعات المختلفة من خلال نصوص تجريم الدخول بدون تصريح، فإننا نؤيد الرأي الذي يرى أن الاتجاه الأول هو الأصوب إذ ينبغي عدم التمييز بين الحالات الثلاثة للدخول بدون تصريح، وأن عملية التجريم يجب أن تظل جميعها طالما أن الدخول بدون تصريح وهو ما أكدته منظمة التعاون والتنمية الاقتصادية من خلال التوصية التي قدمتها للأعضاء في تقريرها الصادر سنة 1986 في شأن جرائم المعلوماتية، بأن تجرم قوانين العقوبات في دول الأعضاء الدخول بدون تصريح إلى الأنظمة المعلوماتية وأنظمة الاتصالات، وكذلك اعتراض الاتصالات بدون تصريح من المسؤول عن النظام².

ج- الركن المعنوي في جريمة الدخول غير المصرح به للنظام المعلوماتي الإلكتروني:

يشكل الركن المعنوي أهمية في قيام جريمة الدخول غير المصرح به إلى نظام الكمبيوتر فالأفعال التي تقوم بها هذه الجريمة يقوم بها كل يوم مستخدمو الكمبيوتر، ومن بين هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي فالركن المعنوي لجريمة

¹ نائلة عادل محمد فريد قورة، مرجع سابق، ص 337.

² دلهار صلاح يوناني، مرجع سابق، ص 195.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الدخول غير المصرح به لنظام معلوماتي في كل التشريعات التي تناولتها يتخذ صورة القصد الجنائي، باعتبارها من الجرائم العمدية، ولتحقق هذه الجريمة يجب توافر عناصر القصد الجنائي من علم وإرادة، فسننظر للقصد العام المطلوب تحققه في جريمة الدخول غير المصرح به إلى نظام الكمبيوتر ثم نتناول القصد الخاص في هذه الجريمة

1- القصد العام في جريمة الدخول غير المشروع لنظام المعلوماتي للموقع الإلكتروني:

عبرت جميع النصوص القانونية التي تناولت جريمة الدخول غير المصرح به إلى نظام الكمبيوتر عن القصد العام المتطلب في هذه الجريمة، وذلك على الرغم من الاختلاف في العبارات المستخدمة لهذا الغرض، فقد عبر النص الفرنسي عن القصد العام بأنه يتطلب أن يكون الدخول إلى النظام قد تم عن طريق الغش والخداع، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله إلى نظام الكمبيوتر غير مصرح به

وفي الدنمارك أشار النص إلى أن الفاعل يقوم بالدخول غير المصرح به إلى النظام على نحو مخالف للقانون، وفي فنلندا وسويسرا والبرتغال والو.م.أ. اشترط أن يتم الدخول إلى النظام بدون تصريح وفي السويد واليونان أن يتم الدخول إلى النظام بدون وجه حق وقد تطلب القانون الانجليزي أن يتم الدخول إلى النظام على نحو غير مصرح به مع العلم بذلك، ويتطلب القصد العام يحيط بكل جانب علم واقفة ذات أهمية قانونية في تكوين الجريمة، وكل ما يتطلبه القانون لاستكمال عناصرها، وعلم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة وإنما يتعين أن يحيط أيضاً بالتكليف الذي تتصف به بعض هذه الوقائع وتكسب به أهميتها في نظر القانون¹، حيث أن عدداً من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون، إلا إذا اكتسبت وصفاً معيناً، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية ولم تعد صالحة لتقوم بها الجريمة

¹ محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة لركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، مصر، 1989، ص 51.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

وتتطلب القصد الجنائي أيضاً أن يتوقع الجاني حيث يأتي فعله النتيجة الإجرامية التي يوف تترتب على الفعل، فتوقع النتيجة هو الأساس النفسي الذي تقوم عليه إرادته والنتيجة التي يجب أن تتجه إليها الفاعل في النتيجة التي يحددها القانون وإذا ما توفر العلم على النحو السابق، تعين بعد ذلك يتوافر القول يتوافر القصد الجنائي، بحيث تتجه إرادة الجاني نحو الدخول غير المصرح به بالدخول إليه أي أن نتيجة إرادته إلى تحقيق هذه النتيجة.

2- القصد الخاص في جريمة الدخول غير مشروع لنظام المعلوماتي لتوقيع الالكتروني

تتطلب بعض النصوص التي جرمت الدخول غير المصرح به إلى نظام الحاسب الآلي في التشريعات المختلفة قصداً خاصاً إلى جانب القصد العام وقد يترتب على توافر هذا القصد تشديد العقوبة في الدنمارك تشدد العقوبة ما ارتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالإسرار المتعلقة بعمل إحدى الشركات، وفي استراليا يوجد نص خاص يشدد العقوبة من ارتكب الفعل بنية الأضرار بالغير وفي النرويج تشدد العقوبة على نحو ملحوظ ما ارتكبت بنية حصول الفاعل له أو الغير على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة الاطلاع على المعلومات التي يحتوي عليها النظام.¹

أما في التشريع الجزائري فلا يبدو من نص المادة 394 مكرر أن المشرع يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول أو البقاء غير المصرح بها وأنه يكفي لقيامها توافر القصد العام القائم على العلم والإرادة وكذلك الشأن مع نص المادة 232/1 من قانون العقوبات الفرنسي المطابقة للمادة السابقة في هي لا تشترط قصد خاصاً²

¹ خالد ممدوح إبراهيم، مرجع سابق، ص 178.

² محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية 2007، ص 167.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

-موقف التشريعات العقابية من جريمة الدخول غير مصرح به لنظام معلوماتي
تختلف خطة التشريعات المقارنة كما قدمنا في معالجة جريمة الدخول غير المشروع لنظام
المعلوماتي، فتفاوتت من ناحية النص على الركن المادي للجريمة وفي محل الدخول غير
المشروع المنصوص عليه في نص التجريم وفي تطلب قصد خاص من عدمه، لذا فإننا سوف
نعرض إلى موقف التشريعات التالية

1-موقف التشريعات الأجنبية:

نص المشرع الفرنسي في المادة 232/1 من قانون العقوبات الجديد الصادر في 1994 على
أنه "يعاقب على الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية
بالحبس لمدة سنتين وبغرامة 30000 يورو" فإذا نجم عن الدخول محو أو تعديل في البيانات
أو إتلاف نظم تشغيل هذا النظام تكون العقوبة الحبس لمدة ثلاث سنوات وغرامة قدرها
45000 يورو" وتقرر المادة 232/3 من ذات القانون عقوبة بذات العقوبة المقررة للجريمة أو
المقررة للجريمة الأشد في حالة المساهمة في جماعة أو الاتفاق بين مجموعة من الأشخاص
للتحضير بعمل أو أعمال مادية لارتكاب جريمة أو أكثر من الجرائم السابقة وينبني على المواد
السابق ذكرها، أن المادة 323/1 من قانون العقوبات الفرنسي التي تجرم الدخول غير المصرح
به إلى جميع أنظمة الحاسبات الآلية تمثل الاتجاه الموسع الذي يشمل الدخول غير المصرح به
للمعلومات وعلى رأسها شبكة الانترنت، وكذلك البيانات المخزنة بطريقة الكترونية داخل
النظام¹.

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام، والتالي يجوز الدخول إلى النظام بأية
وسيلة، مثل الدخول عن طريق كلمة السر الحقيقية عندما يكون الجاني غير مخول له

¹أحمد عصام عجيلة، موقف التشريعات من التكنولوجيا المعلومات واتصالات، دار الفكر الجامعي، الاسكندرية، 2008، ص
315.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

استخدامها، واستخدام برامج شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر، سواء تم ذلك عن طريق شبكات الاتصال التليفونية أو محطات طرفيه سواء محلية وعالمية¹ أما في القانون الأمريكي فقد أصدرت الولايات المتحدة الأمريكية القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله في عام 1984 وتجرم المادة 1535 2 أ من القانون الفيدرالي الأمريكية الخاصة بإساءة استخدام الحاسب الآلية للحصول على المعلومات عن طريق الدخول غير المصرح به، كما تجرم المادة 1535 3 أ الدخول إلى الحاسبات الآلية التابعة للحكومة الفيدرالية أو تلك التي يؤدي الدخول غير المصرح به إليها المساس بأعمال تتعلق بحكومة، وبالتالي تم اعتبار كل دخول غير مشروع إلى معلومات مصنفة في حاسوب جنحة، أما إذا كان الدخول غير المشروع قاصداً سجلات مالية أو سجلات ائتمان في المؤسسات المالية أو انتهاك حرمة كمبيوتر الحكومة الفيدرالية فإن الجريمة تأخذ شكل جنائية

2 - موقف التشريعات العربية:

أما بالنسبة للمشرع السعودي ومن خلال نظام مكافحة جرائم المعلوماتية رقم 17 سنة 2007 نجده قد واجه جريمة الدخول غير المشروع بعدة نصوص، منها نص المادة الثالثة فقره 2 تنص على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية

- التصنت على ما هو مرسل من طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي
- الدخول غير المشروع أو الإلكتروني أو الدخول إلى موقع الكتروني لتغيير تصاميمه هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه

¹ أمين عزان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، رسالة دكتوراه، حقوق عين شمس، القاهرة، مصر، 2005، ص 91.

² خالد ممدوح إبراهيم، مرجع سابق، ص 179.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

كما جاء في نص المادة 5 على أنه "يعاقب بالسجن مدة لا تزيد على أربعة سنوات وبغرامة لا تزيد على 3 ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها أو تدميرها أو تسريبها، أو إتلافها أو تغييرها أو إعادة نشرها.
 - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو لتسريبها أو إتلافها، أو تعديلها.
 - إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها، بأي وسيلة كانت¹.
- أما في دولة الجزائر، وضمن سياق التعديل الذي أجراه المشرع على قانون العقوبات الجزائري فقد تناول جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي وذلك في المادة 394 مكرر والتي تنص على "يعاقب بالحبس من ثلاثة أشهر، إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة، وإذا ما ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة أشهر إلى سنتين وبغرامة من 50000 إلى 150000 دج، ويلاحظ أن المشرع الجزائري جرم فعل الدخول المجرد بدون تصريح إلى النظام المعلوماتي واعتبر السلوك بحد ذاته جريمة، فمجرد الدخول سواء كان بقصد الوصول إلى البيانات أو لمجرد التسلية يعد انتهاكاً لنظام المعلوماتي وأن لم يترتب على ذلك إضرار بالمعلومات أو النظام الذي تحويه²

كما جرم المشرع البقاء بدون تصريح في ذات النص، وذلك لمواجهة حالات الدخول عن طريق الخطأ أو السهو أو تجاوز التصريح واعتبر البقاء عن قصد مشكلاً جريمة تمت من عند إرادة

¹ دلهار صلاح يوناني، مرجع سابق، ص 218.

² ربيعة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى الجزائر 2011، ص 51.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الجاني في الإضرار بالغير. وكذلك من خلال استقراء نص المادة 394 مكرر من قانون العقوبات الجزائري نجد أنها قد نصت على طرفين مشددين لعقوبة جريمة الدخول أو البقاء بدون تصريح داخل النظام، حيث تضاعفت العقوبة في الحالة التي ينتج عنها محو أو تعديل للبيانات التي يحتويها النظام بينما تشدد العقوبة وتصبح الحبس من 6 أشهر إلى سنتين وبغرامة 50000 إلى 150000 دج، إذا ترتب على الدخول أو البقاء عدم قدرة النظام على تأدية وظائفه وتجدر الإشارة أن المشرع الجزائري لم يكتفي بتجريم الدخول أو البقاء بدون تصريح في النظام المعلوماتي بل تجاوز ذلك إلى إلى تجريم المحاولة وذلك بحسب العبارة أو يحاول ذلك بما معناه تجريم المشروع في جريمة الدخول أو البقاء بدون تصريح في النظام المعلوماتي

المطلب الثاني: جريمة الاحتيال المعلوماتي و جريمة التزوير

لقد تناولنا في هذا لمطلب فرعين حيث الفرع الاول جريمة الاحتيال بينما الفرع الثاني تناولنا فيه جريمة التزوير.

الفرع الاول:تعرف جريمة الاحتيال

الاحتيال المعلوماتي وصف يشير إلى صورة مستحدثة للاحتيال تقوم على إساءة استخدام الحاسبات الآلية والتلاعب في نظم المعالجة الآلية للمعلومات بغية الحصول بغير وجه حق على أموال أو أصول أو خدمات، وفي هذه الصورة تتميز من الاحتيال التقليدي بعدة سمات أهمها التعقيد الناجم عن استخدام المفاتيح والشفرات والوسائل الالكترونية في ارتكابه ومحاكاته ذو الطبيعة المعنوية المتمثل في المعلومات وكذا إمكانية ارتكابه عن بعد فيعرف الاحتيال المعلوماتي بأنه: "التلاعب بالبرامج أو البيانات بالتغيير بما يترتب عليه إيهام المجني عليه بصحتها والتسليم بها".

كما عرفه البعض الآخر الاحتيال المعلوماتي: "التلاعب العمدي بالمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها

¹ ربيحة زيدان، مرجع سابق، ص 52.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

التأثير في الحاسب الآلي حق يقوم بعمليات على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير¹.

مما تقدم يتبين لنا أن الاحتيال المعلوماتي يتمثل مع الاحتيال التقليدي فيما يتعلق باستخدام وسائل خداع من أجل الاستيلاء على أموال المجني عليه، ويختلف معه كونه ينطوي على استخدام الجاني للحاسب الآلي والوسائل التقنية في خداع وإيهام المجني عليه ودفعه إلى تسليم أمواله المتمثلة في القيم المعلوماتية - أركان جريمة الاحتيال المعلوماتي.

جريمة الاحتيال شأنها شأن باقي الجرائم ينبغي لقيامها أن تتحقق أركانها، لذا فلدراسة جريمة الاحتيال المعلوماتي تقتضي دراسة أركانها التالية

أ- الركن المادي لجريمة الاحتيال المعلوماتي:

الركن المادي لجريمة الاحتيال يتألف من ثلاثة عناصر هي السلوك الإجرامي والنتيجة الجرمية والعلاقة السببية وتثير هذه العناصر في مجال الاحتيال المعلوماتي الكثير من خلاف والجدل كونها جريمة على درجة من التعقيد سواء من حيث طبيعة المحل الذي يرد عليه ومن حيث الوسائل التي ترتكب من خلالها، الأمر الذي يقتضي البحث في مجموعة الإشكالات القانونية التي قد تواجهنا ونحن بصدد تطبيق القواعد العامة في جريمة الاحتيال التقليدية على جريمة الاحتيال المعلوماتي، والتي منها مدى انطباق وصف المال على المعلومات التي هي في محل الاحتيال المعلوماتي ومدى إمكانية ممارسة الوسائل الاحتيالية على الحاسب الآلي والنظام المعلوماتي المرتبطة به، ومدى اعتبار تسليم الأموال الكتابية بمثابة تسليم للمال؟ وهو ما سنحاول دراسته والتطرق إليه في الفقرات التالية².

¹ دلهار صلاح يوناني، مرجع سابق، ص 127.

² دلهار صلاح يوناني، مرجع سابق، ص 134.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

ب- السلوك الإجرامي:

استعمال الجاني وسيلة من وسائل الخداع المنصوص عليها في القانون وهي الأعمال والمظاهر الخارجية التي يلجأ إليها الجاني لدعم ما يصدر عنه من كذب أو تغيير في الحقيقة لتحقيق أغراض معينة تمكنه من الاستيلاء على مال الغير وإيقاعه في الغلط¹، والجدير بالذكر أنه من الصعب حصر المظاهر الخارجية الداعمة للاحتيال كونها متطورة ومتجددة تبعاً إلى التطورات التي تشهدها مختلف مجالات الحياة وبخاصة في ميدان الاختراعات التي يكشف عنها العلم².

الفرع الثاني: جريمة التزوير

مع تزايد المعاملات الالكترونية على المستوى المحلي والعالمي، والذي جاء نتيجة التطور المذهل في استعمال التكنولوجيا، كان من الضروري توفير الحماية القانونية والتشريعية لهذه المعلومات، فالقاعدة العامة تنص على أن التوقيع الالكتروني الذي لا يتمتع بالحجية في الإثبات ليس محلاً للتزوير، بينما التوقيع الالكتروني المتمتع بالحجية يقع محلاً للتزوير، وعليه فالحجية في الإثبات شرط لحصول التوقيع على الحماية الجنائية وتعد جريمة تزوير التوقيع أحد أهم الجرائم التي يمكن أن تقع على التوقيع الالكتروني والتي تؤدي إلى إهدار الثقة في المعاملات الالكترونية، ما دفع التشريعات والقوانين في دول العالم إلى حماية التوقيع الالكتروني من هذا الشكل من أشكال الغش المعلوماتي، وهذا ما سنوضحه فيما يلي:

نتيجة لظهور فكرة التوقيع الالكتروني والحاجة للحماية الجنائية لهذا التوقيع لجأ المشرع بعض التشريعات على صور مستحدثة لحماية الاعتداء عليه، لكنها انقسمت اتجاه المشرع الذي

¹ حسام محمد نبيل الشنراقي، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 2024، 3، ص 189.

² صباح رمضان، ياسين صالح، السياسة الجنائية في مواجهة الجرائم المعلوماتية: دراسة تحليلية، أطروحة دكتوراه، العراق، 2013، ص. 192.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

يقع في مجال المعلوماتية، حيث يرى فريق من الفقه عدم إمكانية تطبيق النصوص التقليدية على جرائم التزوير الإلكتروني، في حين يرى البعض الآخر إمكانية تطبيقها وفقاً للمفهوم السائد والمستقر للتزوير الإلكتروني، ولابد من تشريعات نصوص خاصة بجرائم التزوير الإلكتروني، وسنحاول في هذا الصدد بيان مفهوم جريمة تزوير التوقيع الإلكتروني وبيان أركانها فيما يلي

أولاً: تعريف جريمة تزوير التوقيع الإلكتروني

التزوير في مفهوم القانون العقوبات هو تغيير الحقيقة بقصد الغش بإحدى الطرق المقررة قانوناً في محرر يحميه القانون¹، ويعد من أخطر الجرائم التي تخل بالثقة الواجب توافرها في المحررات.

ولم يضع المشرع الجزائري تعريفاً محدداً لجريمة التزوير في المحررات ولم يتم بتحديد أركانها وإنما اكتفى بتحديد الطرق التي يقع بها، تاركاً هذه المهمة للفقه والقضاء. ويعتبر تغيير الحقيقة جوهر التزوير، فلا يتصور وقوع التغيير إلا بإبدال الحقيقة بما يغيرها فإذا انعدم تغيير الحقيقة لا تقوم جريمة التزوير.

والتزوير قد يكون مادياً أو معنوياً، حيث يقع التزوير المادي بوسيلة مادية يترتب عنها آثار في مادة المحرر أو في شكله، أما التزوير المعنوي فهو الذي يقع بتغيير الحقيقة دون أن يترك أثراً يدركه الحس، قد يقع التزوير المادي وقت أو بعد إنشاء المحرر، بينما التزوير المعنوي لا يقع إلا وقت إنشاء المحرر .

كما عرف التزوير الإلكتروني بأنه ذلك التزوير الذي ينصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه بشرط أن تطبع على دعامة مكتوبة أو مسجلة، أي يكون لها كيان مادي يمكن إدراكه، ولم يتم تغيير الحقيقة دون طباعة، وذلك أمر وارد، فلا يمكن أن يطلق عليه تزوير².

¹ منير محمد الجنيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الطبعة الأولى، مصر 2006، ص 209.

² عبد الفتاح بيومي حجازي، المرجع السابق، ص 164.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

وذهبت الغالبية العظمى من الفقه القانوني إلى عدم انطباق نصوص التزوير التقليدية على التعديل أو التغيير الواقع على المعطيات والبيانات المخزنة بشكل غير مرئي كونها بيانات إلكترونية مستنديين في ذلك إلى حجة عدم إمكانية القراءة البصرية لمحتويات المحرر وانتفاء الكتابة.

ولم يتناول كل من قانون العقوبات الجزائري وكذا القانون 15/04 جريمة التزوير الإلكتروني (المادة 23)، مما يطرح إشكالاً حول مدى إمكانية تطبيق أركان جريمة التزوير التقليدي على جريمة تزوير التوقيع الإلكتروني، أم أنها تعتبر صورة من صور جرائم المعالجة الآلية لنظم المعطيات المنصوص عليها في قانون العقوبات؟

ثانياً: أركان جريمة تزوير التوقيع الإلكتروني

سنحاول دراسة الركن المادي لجريمة التزوير ثم الركن المعنوي مع بيان مدى انطباق هذه الأركان على جريمة تزوير التوقيع الإلكتروني

أ- **الركن المادي في جريمة تزوير التوقيع الإلكتروني** الركن المادي في جريمة تزوير التوقيع الإلكتروني لا يختلف عن الركن المادي في جريمة التزوير التقليدية من حيث عناصره، فالركن المادي يقتضي عنصرين:

- **العنصر الأول:** أن يتم تغيير الحقيقة بإحدى الطرق المنصوص عليها قانوناً
- **العنصر الثاني:** هو ضرورة توافر الضرر الذي لا يكتمل الركن المادي إلا به، فيشترط تحقق الضرر للغير، وهذا الضرر قد يكون مادياً كخسارة مادية للمجني عليه وأيضاً قد يكون أدبياً بفقدان الثقة في المعاملات في المجتمع عموماً ولقد حددت المواد 214 إلى 216 من قانون العقوبات طرق التزوير المادي والمعنوي. وقد اعتمد المشرع الكتابة في الشكل الإلكتروني ضمن وسائل الإثبات المدني وكذا التوقيع الإلكتروني، ومن ثم يتصور أن يقع التلاعب أو التزوير على التوقيع الإلكتروني بحيث يمكن للقراصنة

¹ لامية محبوب، جريمة التزوير، دار الجامعة الجديدة، مصر 2013، ص 31.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

اختراق نظم المعلوماتية¹، وفك شفرته واستخدامه دون موافقة صاحبه، أو نقل إمضاء الشخص علناً لأوراق المسحوبة على الحاسب الآلي وتزويرها دون علم ورضا صاحبه خاصة في التعاملات الشبكية².

• لكن هناك من يرى أن التوقيع الإلكتروني عبارة عن مخرجات ليست ورقية بل إلكترونية تحتوي مجموعة من الرموز أو الأرقام تتضمن علامة مميزة لصاحبها في مجملها، وهي بذلك تعد بيانات تتضمن معلومات تنشأ أو تندمج أو تخزن بوسيلة الإلكترونية أو رقمية باعتبارها ومضات كهرومغناطيسية ذات طابع معنوي، وعليه فكل تزوير ينصب على هذه البيانات هو من قبيل التزوير المعنوي وليس تزويراً مادياً ومهما يكن من أمر فإن مناط التزوير سواء تعلق الأمر بتوقيع تقليدي أو توقيع إلكتروني فإن الأمر يتم بطريقة مختلفة، إذ أن التوقيع الإلكتروني لا يمكن تقليده، وإنما يمكن استخدامه دون علم مالكة كونه يتم بواسطة منظومة إلكترونية، تتخذ شكل حروف أو أرقام أو رموز أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر، وذلك لأن توقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يكون متماثلاً معه، ومن ثم فجريمة تزوير التوقيع التقليدي تختلف عن جريمة التوقيع الإلكتروني، سواء في طريقة التزوير أو في أسلوب اكتشافه، فالكشف عن التوقيع المزور يكون عن طريق المضاهاة، في حين لا يمكن استخدام هذه الطريقة في اكتشاف تزوير توقيع على محرر إلكتروني

ب- الركن المعنوي لجريمة تزوير التوقيع الإلكتروني

تعد جريمة التزوير بصفة عامة من الجرائم العمدية التي تتطلب قصداً جنائياً عاماً وقصداً جنائياً خاصاً، فلا يكفي القصد العام الذي يقوم على علم المتهم بأركان الجريمة، واتجاه

¹ هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، تأليف بحوث مؤتمر الأعمال المصرفية بين الشريعة والقانون المجلد الثاني، الإمارات العربية المتحدة، كلية العلوم والقانون، ص 528

² راضية مشري، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، مجلة حوليات للعلوم الاجتماعية والانسانية 2017، ص 130.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

إرادته إلى الفعل المكون لها وتحقيق نتيجته، بل تتطلب هذه الجريمة توافر قصد جنائي خاص، يتمثل في نية استعمال المزور فيما زور من أجله،¹ وعلى هذا فإن القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بأنه: "تعمد تغيير الحقيقة في محرر تغييراً من شأنه أن يسبب ضرراً وبنية استعمال المحرر فيما غيرت من أجله الحقيقة"² وانطلاقاً مما سبق نصل إلى نتيجة مفادها أنه لا يمكن القياس على جريمة التزوير التقليدي، لأن هذا يتنافى مع مبدأ الشرعية، والنصوص التقليدية، كون جريمة تزوير التوقيع الإلكتروني جريمة مستحدثة لا تنسجم مع النصوص التقليدية، ما يدعو إلى ضرورة تدخل المشرع الجزائري للنص على هذه الجريمة أخذاً بما ذهب إليه المشرع المصري من خلال القانون 15-2004 الخاص بتنظيم التوقيع الإلكتروني وأن ما قام به المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004 وإدخاله لجرائم المعالجة الآلية لمعطيات الحاسوب بموجب المادة 394 مكرر إلى 394 مكرر 7 غير كافٍ بالنسبة لجريمة تزوير التوقيع الإلكتروني.

الفرع الثالث: أساليب تزوير التوقيع الإلكتروني

نظراً لضعف إجراءات الأمان والثقة في التوقيع الإلكتروني، يكون من السهل تزويرها، بعد أن يتم مهاجمته أو نسخه من قبل قرصنة الحاسب الآلي، ومن أهم الصور الأكثر عرضة للتزوير التوقيع بالرقم السري وكذا التوقيع الرقمي

أولاً: تزوير التوقيع الإلكتروني الذي يتم بالرقم السري

أهم تطبيقات هذه الصورة بطاقات الصرف البنكي -بمختلف أنواعها- وأهم صور الاستخدام المشروع لهذه البطاقات هو تزويرها سواء تزويراً كلياً أو جزئياً ولعل أهمها بطاقات الدفع، التي يمكن أن تكون محلاً للاعتداء عليها عن طريق تزويرها، والمبدأ الأساسي لتزوير

¹ ياسر محمد ال حاكمي، الحماية الجنائية والأمنية للتوقيع الإلكتروني، في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، مصر جامعة حلوان، ص135.

² محمود نجيب حسني، شرح قانون العقوبات، دار النهضة العربية، جامعة حلوان 1994، ص271.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

هذه البطاقة هو سرقة بياناتها من خلال جهاز الحاسب الآلي باستخدام أدوات معينة، حيث يتم نقش هذه البيانات على بطاقة أخرى تكون معدة لهذا الغرض أو تكون بطاقة منتهية أو مسروقة ويتم استخدامها بعد ذلك في عمليات الدفع أو السحب¹.

وقد لا تكون البطاقة في حد ذاتها صحيحة لكن تم الحصول عليها بواسطة وثائق مزورة أو وضع توقيع مزور، فالطريقة الأولى يطلق عليها اصطناع المستند، وهذا بخلق محرر بأكمله ونسبته إلى غير محرره، أما الطريقة الثانية وتعد من طرق التزوير المادي الأكثر شيوعاً وذلك بتزييف أو تقليد الكتابة بتدوين عبارات أو وضع توقيعات مقلدة².

وقد يحدث وأن تستعمل هذه البطاقة البنكية المزورة وهي جريمة قائمة بذاتها، وقد فصل فيها المشرع الجزائري، إذ فصل تزوير المحررات عن استعمالها، كما نص على استعمال الأوراق العرفية أو التجارية أو المصرفية المزورة (المادة 22 من قانون العقوبات الجزائري) ويترتب عن فعل التزوير والاستعمال والفصل بينهما أن مرتكب التزوير يعاقب ولو لم يستعمل الورقة المزورة، وأن من يستعمل الورقة المزورة يعاقب حتى ولو لم يرتكب التزوير أو يشترك فيه.

ثانياً: تزوير التوقيع الرقمي

إن التوقيع الرقمي يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات حيث لا يمكن تقليدها إنما استعمالها دون علم مالكيها، عن طريق الحصول على منظومة التوقيع بطريقة التجسس الإلكتروني أو الدخول غير المشروع، والتوقيع هنا سليماً إلا أنه استخدم من غير صاحبه، وعليه يتم الكشف عن التوقيع الرقمي المزور بإثبات أنه لم يصدر من صاحب المنظومة، وإنما من شخص آخر قام بسرقتها وتكون جريمة تزوير التوقيع بالدخول إلى قاعدة البيانات وتعديلها، سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن

¹ راضية مشري، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، مجلة حوليات للعلوم الاجتماعية والإنسانية، 2017، ص 145.

² أسيا بن عبيد، الحماية الجنائية لبطاقات الدفع في جرائم التزوير في القانون الجنائي، مجلة دراسات، 2017، ص 210-211.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

موجودة من قبل، وتعد جريمة مركبة تتكون من جريمتين: جريمة سرقة منظومة التوقيع الإلكتروني (التجسس - الدخول غير المشروع عن طريق القرصنة الإلكترونية)، والتي يصعب اكتشافها إلا بعد استخدام غير المشروع لمنظومة التوقيع الإلكتروني¹

الفرع الرابع: جريمة تعطيل أو إفساد النظام المعلوماتي

تتحقق هذه الجريمة بتعطيل وإعاقة النظام المعلوماتي عن القيام بوظائفه المعتادة حيث يترتب على ذلك توقف النظام للحالة المعهودة لعمله بشكل تام أو تباطؤ واضطراب في عمله مما يؤدي إلى إصدار نتائج غير صحيحة ومخالف للحالة المعهودة لعمل النظام والوقوف على هذه الجريمة لا بد أن نستعرض مفهومها أولاً ثم أركانها ثم موقف القوانين العقابية منها

تعريف جريمة تعطيل وإفساد النظام المعلوماتي

تعرف جريمة تعطيل وإفساد النظام المعلوماتي بأنها "الاعتداء على نظم المعالجة الآلية للمعلومات بمنعها من أداء وظائفها بصورة تامة أو إجراء تعديل في تلك الوظائف"² أو تعرف بأنها "كل فعل يتسبب في توقف أو تباطؤ وارتباك عمل نظام المعالجة ومن ثم ينتج عن ذلك تغير في حالة النظام"³.

ولخطورة السلوكيات التي تنطوي عليها هذه الجريمة اتجه اغلب المشرعين إلى مواجهتها سواء من خلال التشريعات الصادرة لمواجهة الجرائم المعلوماتية أو من خلال إجراء تعديلات على التشريعات العقابية القائمة، ففي فرنسا مثلاً جرم المشرع فعل إعاقة النظام وإفساده في المادة 323 في 2-1⁴، وكذا في كندا أضيفت فقرة إلى المادة 430 من قانون العقوبات لسنة 1985 والخاصة بالإتلاف جرمت بموجبها الأفعال التي من شأنها منع أو إيقاف أو عرقلة نظام الحاسب الآلي أو إفادة آدائه، كما جرم المشرع في دولة الإمارات العربية المتحدة إعاقة وتعطيل

¹ راضية مشري، المرجع السابق، ص 151.

² دلهار صلاح يوناني، مرجع سابق، ص 227.

³ نائلة عادل محمد فريد، مرجع سابق، ص 225.

⁴ محمد خليفة، مرجع سابق، ص 167.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

النظام المعلوماتي من خلال المواد 5-6 من قانون مكافحة جرائم تقنية المعلومات، وكذا قانون مكافحة جرائم المعلوماتية في السودان 2007 حيث نصت المادة 8 من هذا القانون "كل من يدخل بأية وسيلة نظاماً أو وسائط أو شبكات المعلومات وما في حكمها ويقوم عمداً بإيقافها وتعطيلها يعاقب بالسجن مدة لا تتجاوز ستة سنوات أو بالغرامة أو بالعقوبتين معاً¹

المبحث الثاني: آليات الحماية الالكترونية للتوقيع الالكتروني

تعد مسألة الأمن المعلوماتي² من أهم الضمانات والتحديات التي تواجهها وسائل الدفع الالكتروني، لأن غياب الأمن المعلوماتي يعتبر من معوقات اعتماد التجارة الالكترونية على الرغم من المزايا التي توفرها. ويقصد بالأمن المعلوماتي حماية جميع المعلومات التي يتم التعامل معها والمعالجة من منظمة وغرفة تشغيل أجهزة، ووسائط التخزين من السرقة والتزوير والتلف والضياع والاختراق³.

فلا يكفي الاعتراف بحجية التوقيع الالكتروني في الإثبات، دون العمل على إيجاد الآليات الكفيلة التي تبعث الثقة والاطمئنان لدى المتعاملين به، وتحقيق الحماية الضرورية للتوقيع الالكتروني من أي تحايل أو اختراق، ما جعل المشرع يقر عملية التشفير كإجراء الكتروني تقني لحماية البيانات الالكترونية، إضافة إلى تنظيم مهام جهة التوثيق الالكتروني وتحديد مسؤولياتها قصد تحقيق الأمان القانوني للمتعاملين في المجال الالكتروني

المطلب الأول: نظام التشفير

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

¹ دلهار صلاح يوناني، مرجع سابق، ص 229.

² الحميدة محمد دباس، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، 2007، ص 34.

³ الحميد محمد دباس، المرجع السابق، ص 34.

⁴ عبد الفتاح بيومي حجازي، المرجع السابق، 202.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الفرع الاول: المقصود بالتشفير

يعرف التشفير بأنه: "كل العمليات التي تؤدي بفضل بروتوكولات سرية إلى تحويل معلومات أو إشارات مفهومة (مقروعة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية"، ويعرف أيضا بأنه: "آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس أو يمكن إرجاعها إلى حالتها الأصلي" أما بالنسبة للتعريف التشريعي للتشفير، فلم يتطرق المشرع الجزائري من القانون 18-05 المتعلق بالتجارة الالكترونية¹ إلى تعريف التشفير، واكتفى بتعريف مفتاح التشفير الخاص ومفتاح التشفير العمومي في القانون 15-04 للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني. (نصت على ذلك المادة 02 في فقرتها الثامنة بقولها: "مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي"

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

الفرع الثاني: ضوابط وطرق التشفير

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

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

1- مشروعية تشفير البيانات والمعلومات التي يتم تبادلها عن طريق الوسائط الالكترونية، إذ أقر المشرع الجزائري من خلال القانون 15-04 نصوصا تتناول نظام التشفير، وعرف التشفير

¹ القانون رقم 18/05 المؤرخ في 10 ماي 2018، المرجع السابق

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

الخاص والعام، وأجاز استخدامه في المراسلات الالكترونية والتعاملات التجارية الالكترونية، كما أكد على حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها من كل اعتداء سواء تم ذلك باستخدام عناصر التشفير الخاصة بالتوقيع من غير طرفي العلاقة، أو بسبب استخدام التشفير في ارتكاب جرائم احتيالية¹

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

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

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

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

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

¹ محمد عقوني، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة الفكر 2019، ص304.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

هذه الطريقة تقنية المفتاح الخصوصي، كونها تعمل بواسطة مفتاح واحد خصوصي يمتلكه كل من مرسل الرسالة ومتلقيها، وهذا ما يعاب على هذه التقنية، إذ أن استعمال هذا المفتاح من قبل شخصين مختلفين (المرسل والمرسل إليه) قد يضعف من حجية المستندات الرقمية والتوقيع الإلكتروني وقوتها الثبوتية¹

2-التشفير غير المتماثل: يطلق على هذه التقنية التشفير بالمفتاح العمومي وخلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث يستعمل مفتاحين سريين مختلفين من أجل فك تشفيرها، الأول خصوصي يمتلكه مستخدم معين لمستعمل الوسائط الإلكترونية ويبقيه سرياً وخاصاً به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منهم².

المطلب الثاني : التصديق الإلكتروني

إزاء تنامي مخاطر القرصنة الإلكترونية وإساءة استخدام الغير، استوجب الأمر توفير الوسائل التي تكفل تحديد هوية المتعاقدين والتعبير عن إرادتهم على نحو صحيح ثم الاستعانة بطرف ثالث محايد موثوق به، يتمثل في جهة مختصة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية، بإصدار شهادة تسمى بشهادة التصديق الإلكتروني وبناء على ما سبق سنحاول التطرق إلى تعريف التصديق الإلكتروني، ودور الجهة المختصة بإصدار شهادات التصديق في إضفاء الحماية على التوقيع الإلكتروني

الفرع الأول: تعريف التصديق الإلكتروني

التصديق الإلكتروني آلية تهدف إلى بناء الثقة في نظام الشهادات الرقمية وتشجيع المعاملات الإلكترونية بإضفاء المصادقية عليها، فالتصديق بمعناه العام يعني التوثيق والاعتماد ومجاله الطبيعي هو التصرفات القانونية في شكلها التقليدي أي السندات الورقية، حيث على الموظف التأكيد والتصديق على صحة ما ورد في المحرر المقدم للتصديق وصحة نسبته إلى

¹ محمد العقوني المرجع السابق، ص306.

² المطالقة محمد فواز، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر، والتوزيع الأردن، ص159.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

من وقع عليه، وبالتالي بالتصديق الإلكتروني يعني تدخل طرف ثالث لتأمين التبادل الإلكتروني وللمعطيات في المجال الإلكتروني لتحقيق السلامة والثقة في المعاملات الإلكترونية¹ ويعد التصديق أو التوثيق الإلكتروني وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر، حيث يتم نسبته إلى شخص معين أو جهة معينة أو طرف محايد يطلق عليه مقدم خدمات التصديق أو مورد خدمات التصديق أو جهة التوثيق ولم يعرف المشرع الجزائري التصديق الإلكتروني ولكنه عرف شهادة التصديق الإلكتروني وهذا من خلال المادة 02 من القانون 15/04 بأنها " وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع"

الفرع الثاني: دور الجهات المختصة بإصدار شهادات التصديق الإلكتروني في حماية التوقيع الإلكتروني
اختلف الفقه والقانون في الاصطلاح الذي يطلق على الجهة المختصة بإصدار شهادات التصديق الإلكتروني، حيث يستخدم جانب من الفقه اصطلاح سلطة الإشهار، ويطلق عليها جانب من الفقه مصطلح مقدم خدمات التصديق. أما قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، فاستخدم مصطلح مقدم خدمات التصديق. وعرفه في المادة 02 من هبأنه " شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية ". أما التوجه الأوروبي فعرف مقدم الخدمات بأنه كل " شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، ويتولى خدمات أخرى مرتبطة بالتوقيع الإلكتروني²."

أما المشرع الجزائري فقد استمد مصطلح وتعريف مقدم خدمات التوثيق من نصوص قانون اليونسترال بشأن التوقيعات الإلكترونية وأحكام التوجيه الأوروبي عند تعريفه بأنه :

¹ غزالي نزيهة، الآليات القانونية لحماية وسائل الدفع الإلكتروني، في التشريع الجزائري، مجلة البحوث السياسية والادارية 2017، ص 291.

² فواز المطلقة، المرجع السابق، ص 173.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

"شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة، ويقدم خدمات أخرى في مجال التصديق الإلكتروني" (المادة 2/11 من القانون 15/04).

ويكمن الهدف الأساسي من إنشاء جهات مختصة في إصدار شهادات التصديق الإلكتروني في تسهيل مراقبة التعاملات الإلكترونية، إضافة إلى ضمان الأمن القانوني وحماية التعاملات الإلكترونية وخاصة التوقيع الإلكتروني من الأخطار التي قد تواجهه بسبب طبيعة هذه المعاملات التي تتم عبر وسائط الكترونية ومجلس عقد افتراضي

ولعل من أهم الضمانات القانونية للحماية والمحافظة على سلامة التوقيع الإلكتروني هو إصدار شهادة التصديق الإلكتروني، والتحقق من هوية الشخص الموقع، إضافة إلى إثبات مضمون البيانات الإلكترونية وإصدار مفاتيح التشفير، نحاول هنا فيما يلي:

أ- إصدار شهادة التصديق الإلكتروني ميز المشرع الجزائري بين الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة - كما سبقت الإشارة - فالشهادة الإلكترونية البسيطة تتطلب إجراءات ترتبط بمعطيات ومعلومات تتعلق بالتحقق من توقيع شخص معين وتأكيد هوية هذا الشخص (المادة 03 مكرر من المرسوم التنفيذي 162/07 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001، 2007). أما شهادة التصديق الإلكترونية الموصوفة، فإنها ترتبط بإصدار الشهادة النوعية وفق شروط حددها المشرع من بينها أن تتضمن على الخصوص التوقيع الإلكتروني الموصوف (المادة 7 فقرة 2 من القانون 15/04 المتضمن تحديد القواعد العامة للتوقيع مادة 2/11 من القانون 15/04 المحدد للقواعد الخاصة بالتوقيع والتصديق الإلكترونيين)

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

وكل من الشهادتين تفي بوجوب ارتباط التوقيع الإلكتروني بشهادة الكترونية والتي تصدر حصريا من جهة تصديق الكتروني معتمدة، ومن ثم فلا بد من توافر شهادة التصديق الإلكتروني لكل يكون التوقيع الإلكتروني موصوفا¹.

ب- التحقق من هوية الشخص الموقع يتمثل الدور الرئيسي لجهات التصديق الإلكتروني في تمكين المرسل إليه من التأكد من هوية المرسل وصلاحيه توقيع، حيث تقوم بإصدار شهادة تصديق الكتروني تفيد التصديق على التوقيع الإلكتروني في تعاقد معين، كما تفيد وقد نص المشرع الجزائري من خلال المادة 44 من القانون 04-15 على أنه يجب على مؤدي خدمات التصديق الإلكتروني وقبل منح شهادة التصديق الإلكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، ويمنح مؤدي خدمات التصديق الإلكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته وعند الاقتضاء التحقق من صفاته الخاصة. أما في حالة الأشخاص المعنوية فإن مؤدي خدمات التصديق الإلكتروني يحتفظ بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني.

ج- إثبات مضمون التبادل الإلكتروني تقوم الجهة المختصة بإصدار شهادات التصديق الإلكتروني كذلك بالتحقق من مضمون التعامل أو التبادل الإلكتروني بين الأطراف المتعاقدة، وكذلك التيقن من سلامته وجديته وبعده عن الغش والاحتيال. إضافة إلى إثبات ومضمونه، حماية للمتعاملين من أي غش قد يقعون فيه أثناء تعاملاتهم².

وقد نص المشرع الجزائري على أن يلغي خدمات التصديق الإلكتروني الموصوفة عندما يتبين أنه قد تم منحها بناء على معلومات خاطئة أو مزورة أو إذا أصبحت المعلومات الواردة

¹ عقوني، المرجع السابق، ص 309.

² الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، مؤتمر الأعمال المصرفية الإلكترونية، المجلد الخامس، ص 178.

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

في شهادة التصديق الإلكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع (المادة 45 من القانون 15/04 المتعلق بالتوقيع والتصديق الإلكترونيين)

د- إصدار المفاتيح الإلكترونية تقوم جهات التصديق الإلكتروني بإصدار مفاتيح التشفير الإلكتروني، سواء المفتاح الخاص الذي من خلال يتم تشفير المعاملة الإلكترونية الذي يكون خاصا بصاحبه ولا يعلمه غيره، أهم المفتاح العام الذي يتم بواسطته فك هذه الشفرة، كما تتولى المصادقة على هوية الحائز على المفتاح العمومي وإصدار شهادات الكترونية من شأنها أن تضمن بأن المفتاح العمومي العائدة إلى الجهة الحائزة على المفتاح الخصوصي، ومن ثم استخدام المفتاح العام لفك تشفير الرسالة الأصلية والتأكد من عدم حصول أي تعديل عليها

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

خلاصة

يعتبر التوقيع الإلكتروني من أهم الوسائل التقنية والقانونية التي أسهمت في إضفاء الحجية القانونية على المعاملات الإلكترونية، إذ يمكن من التحقق من هوية الموقع والتأكد من سلامة المحرر الإلكتروني وعدم تعرضه للتعديل أو التحريف. ومع اتساع استخدامه في المجالات التجارية والإدارية والمالية، ظهرت مجموعة من الجرائم التي تستهدفه، سواء من خلال تزويره أو استعماله دون وجه حق أو اختراق الأنظمة التقنية التي تضمن سلامته

وتتمثل أهم جرائم التوقيع الإلكتروني في جريمة تزوير التوقيع الإلكتروني، التي تقوم عند اصطناع توقيع مزور أو تعديل توقيع صحيح بقصد استعماله على نحو يسبب ضرراً للغير، وجريمة الاستعمال الاحتيالي للتوقيع الإلكتروني باستخدام بيانات أو شهادات رقمية دون إذن صاحبها، فضلاً عن جرائم اختراق نظم المعلومات وسرقة المفاتيح الخاصة والشهادات الرقمية، وكذا جريمة انتحال الهوية الإلكترونية للحصول على توقيع إلكتروني أو استخدامه في إبرام تصرفات قانونية غير مشروعة. وتُعد هذه الأفعال اعتداءً على الثقة العامة وعلى أمن المعاملات الإلكترونية، لما يترتب عنها من أضرار مادية ومعنوية جسيمة

ولمواجهة هذه الجرائم، اعتمد المشرع الجزائري منظومة قانونية وتقنية متكاملة، من أبرزها القانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، والقانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، إلى جانب الأحكام الواردة في قانون العقوبات والقانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وقد خوّلت هذه النصوص للسلطات المختصة صلاحيات تنظيم خدمات التصديق الإلكتروني والرقابة عليها، وقررت عقوبات جزائية لكل من يعتدي على التوقيع الإلكتروني أو يستعمله بطريقة غير مشروعة

الفصل الثاني جرائم التوقيع الإلكتروني وآليات حمايتها

أما من الناحية التقنية، فنتحقق حماية التوقيع الإلكتروني من خلال استخدام تقنيات التشفير غير المتماثل، والمفاتيح العامة والخاصة، والشهادات الرقمية الصادرة عن جهات تصديق معتمدة، إضافة إلى وسائل التأمين مثل كلمات المرور القوية والمصادقة متعددة العوامل وأجهزة حفظ المفاتيح المشفرة. وتُعزّز هذه الحماية بالتوعية القانونية والتقنية للمستخدمين، ووضع سياسات أمن معلومات فعالة داخل المؤسسات

وخلاصة القول، فإن التوقيع الإلكتروني يمثل حجر الأساس في بناء الثقة في البيئة الرقمية، غير أن فعاليته تظل رهينة بتوفير حماية قانونية وتقنية متكاملة تكفل التصدي للجرائم التي تهدده. وقد سعى المشرع الجزائري إلى تحقيق هذا الهدف من خلال سن تشريعات خاصة وتنظيم آليات التصديق الإلكتروني وتجريم مختلف صور الاعتداء عليه، بما يضمن استقرار المعاملات الإلكترونية وتعزيز الأمن القانوني في الفضاء الرقمي

خاتمة

خاتمة

خاتمة:

يعد التوقيع الإلكتروني أحد الموضوعات المهمة التي لم تنل حتى الآن ما تستحقه من البحث والدراسة، وهو نتاج لما فرضه علينا الوجود الواقعي لنظم تكنولوجيا المعلومات والتجارة الإلكترونية، وما أفرزه لنا هذا الواقع من ظهور التعاقد عبر الإنترنت، حيث إن التعاقد لا يمكن تنفيذه إلا بوجود المحرر والتوقيع الإلكتروني

لذا حاولت هذه الدراسة تسليط الضوء على هذه المسألة من خلال تطرقي إلى تناولنا موضوعاً حديثاً نسبياً أفرزه العقد والمحرر الإلكتروني وهو التوقيع الإلكتروني حيث وضعنا ماهية التوقيع الإلكتروني وشروطه وبيننا فيها أهم التطبيقات والمعاملات التي تقبل التعامل بها والمعاملات التي لا تقبل التعامل بالتوقيع الإلكتروني، كما بينا مدى حجية هذا التوقيع في الإثبات طبقاً للقانون بالإضافة إلى موقف بعض التشريعات العربية والدولية، ومدى توافق القوانين

ومن خلال هذه الدراسة تبين للباحثة أن هناك في العقد والمحرر الإلكتروني بشكل عام والتوقيع الإلكتروني بشكل خاص بعض صور الغموض وعدم الانسجام في التطبيق بين القواعد التقليدية والإلكترونية في بيئة العقد، والمحرر والتوقيع، وبعد تلك الجولة العلمية دراسة وتمحيصاً للموضوع انتهت هذه الدراسة وتوصلت إلى مجموعة من النتائج والتوصيات وهي على النحو الآتي:

أولاً: النتائج:

1. عُرف العقد منذ زمن قديم، إلا أنه تطوره كان مع ظهور الثورة المعلوماتية، فتغير شكله من العقود التقليدية (الورق) إلى عقود تتم عن طريق الوسائط الإلكترونية، وبالتالي لا يختلف العقد الإلكتروني عن العقد التقليدي إلا من حيث الطريقة التي ينعقد بها وهي توقيعه إلكترونياً، ولم يعرف المشرع العقد الإلكتروني، وإنما اكتفى بتعريف العقد التقليدي .

خاتمة

2. إن **مجلس العقد** تعتبر من المراحل المهمة في تكوين العقد بعد مرحلة التفاوض، حيث استند عليه المشرع والتشريعات العربية المختلفة ورتبت عليه نتائجها، وهناك نوعان من مجلس العقد، **المجلس الحقيقي** الذي يجمع الطرفين في مكان واحد ويكونان على اتصال مباشر، و **المجلس الحكمي** الذي لا يجمعهما في مكان واحد ويكون أحد الأطراف غائباً عن المجلس.
3. يتفق القانون مع الفقه الإسلامي على أن الكتابة تعد وسيلة رئيسة من وسائل الإثبات، ولا يشترط أن تكون بطريقة معينة أو على دعامة محددة، كما أجاز الفقه الإسلامي الاعتماد على الكتابة الإلكترونية بأي وسيلة أو دليل

ثانياً: التوصيات:

- بعد الانتهاء من هذه الدراسة تحليلاً واستنتاجاً، هناك ثمة توصيات توصي بها هذه الدراسة وتتمنى الباحثة أن تتحقق مستقبلاً وهي على النحو الآتي
- 1 ضرورة أن يوضح المشرع مصطلح **العقد الإلكتروني** لكونه مصطلحاً حديثاً، فالتجارة الإلكترونية لا بد وأن تمارس في إطار بيئة قانونية معينة تتفق مع متطلباتها، مع إعادة صياغة مصطلح **الرسالة الإلكترونية** وأن يعرفها مقرباً بها **التوقيع الإلكتروني المحمي (الموثق)** لإعطائه القوة الثبوتية عند الاحتجاج به
 - 2 إعادة النظر بخصوص **التوقيع الإلكتروني** من قبل المشرع وذلك بذكر **التوقيع الإلكتروني غير محمي** وما شروطه حاله حال **التوقيع الإلكتروني المحمي (الموثق)**، وعدم تحديد شكل معين من التوقيع كالتوقيع: بالأحرف، أو أرقام، أو رموز أو إشارات، وإنما تركها مفتوحة كالتوجيه الأوروبي الذي لم يتطلب استخدام تقنية بعينها بل وضع شروطاً محددة لكي يتصف هذا التوقيع بالتوقيع الإلكتروني المحمي، وذلك لأن عملية التطور التكنولوجي دائماً أسرع كثيراً من عملية التطور التشريعي والتي تستغرق عادة زمناً ليس بالقصير.

خاتمة

3 إصدار المزيد من القوانين التي تنظم المعاملات الإلكترونية وخاصة التوقيع الإلكتروني،

مع ضرورة وضع جميع القوانين المتعلقة بالإلكترونيات في قانون المعاملات والتجارة الإلكترونية الإماراتية ومنها قانون الإثبات الإلكتروني

4 يجب على المشرع أن يشير إلى المعاملات التي تقبل التعامل بالتوقيع الإلكتروني

بشكل مفصل كما فعل المشرع الأردني، لأن هذا الأمر يسهل على القاضي تطبيق النصوص والرجوع إليها ويساعد في إتاحة استخدام التجارة الإلكترونية في جميع المجالات بين الدول

5 نوصي بالتوسع في تطبيق المعاملات الإلكترونية والتوقيع الإلكتروني دون إيراد

استثناءات في المعاملات مثلما فعل المشرع الفرنسي، فطالما اعترف القانون بالتوقيع الإلكتروني وقرر له الحجية في الإثبات مثله مثل التوقيع التقليدي، فليس هناك أي داعٍ في قصر تلك الحجية على بعض المعاملات دون المعاملات الأخرى، وإلا صارت هناك تفرقة بين أنواع المعاملات

6 تشديد الجزاءات الجنائية على الجرائم المتعلقة بالحاسب وتقنية المعلومات بخصوص

عمليات السرقة والتزوير التي تتم بواسطة الحاسب الآلي، والتي تؤثر سلباً أو تعيق انتشار التجارة الإلكترونية

تعرض المشرع إلى مزود خدمات التصديق ومسؤولياته، وهي خطوة جيدة من قبل المشرع، ولكننا نعتقد أن ذلك لا يكفي لإضفاء الحماية القانونية على التجارة الإلكترونية، لذا نوصي بإصدار تشريع عالمي موحد.

7 تطوير التشريعات القانونية المتعلقة بالتوقيع الإلكتروني بما يواكب التطور التكنولوجي

المستمر وأساليب الجرائم

8 تشديد العقوبات على جرائم تزوير واستعمال التوقيع الإلكتروني بطرق غير مشروعة

لضمان الردع وحماية المعاملات الإلكترونية.

خاتمة

- 9 تعزيز التعاون الدولي بين الدول لمكافحة الجرائم المرتبطة بالتوقيع الإلكتروني، نظراً للطبيعة العابرة للحدود للفضاء الرقمي.
- 10 رفع مستوى الوعي الرقمي لدى الأفراد والمؤسسات حول مخاطر إساءة استخدام التوقيع الإلكتروني وطرق حمايته.
- 11 اعتماد تقنيات أمنية متطورة مثل التشفير القوي والمصادقة متعددة العوامل لضمان سلامة التوقيعات الإلكترونية.
- 12 تكوين وتدريب القضاة وأعاون الضبط القضائي في مجال الجرائم الإلكترونية والأدلة الرقمية لتمكينهم من التعامل الفعال مع هذا النوع من الجرائم
- 13 تشجيع المؤسسات على تطبيق معايير الأمن السيبراني لحماية البيانات والوثائق الإلكترونية من الاختراق والتزوير.
- 14 وفي ختام هذه الدراسة، يتضح أن التوقيع الإلكتروني أصبح أداة أساسية في المعاملات الحديثة، إلا أن التطور التكنولوجي صاحبه ظهور جرائم جديدة تهدد الثقة والأمن القانوني للمعاملات الإلكترونية. ومن ثمّ، فإن مواجهة جرائم التوقيع الإلكتروني تتطلب تضافر الجهود التشريعية والتقنية والتوعوية لضمان حماية الحقوق وتحقيق الأمن الرقمي، بما يساهم في تعزيز الثقة في البيئة الإلكترونية ودعم التحول الرقمي

قائمة المراجع

قائمة المراجع

قائمة المصادر

أولاً: الآيات القرآنية

- سورة الحجر ، الآية رقم 18.

ثانياً: الكتب القانونية

- أحمد عصام عجيلة ، موقف التشريعات من تكنولوجيا المعلومات والاتصالات، دار الفكر الجامعي، الإسكندرية، 2008.
- أحمد عصام عجيلة ، شرح قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة الأولى، 2017.
- إلياس أبو عبيد ، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية، 2005.
- أيمن عبد الله فكري ، جرائم نظم المعلوماتية، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، 2007.
- أزد دزهيي، النظام القانوني للمصادقة على التوقيع الإلكتروني: دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، كلية الحقوق بالإسكندرية 2015.
- ثروت عبد الحميد، التوقيع الإلكتروني (مرجع سابق).
- جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الجديدة، الكتاب الأول، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011-2012.
- حسان ناجي صالح الخليل ، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2009.
- الحميد محمد دباس، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع 2007.
- خالد ممدوح إبراهيم ، إبرام العقد الإلكتروني: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006.
- خالد ممدوح إبراهيم ، جرائم السرقة في التشريع الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2015.
- دلهار صلاح الدين يوناني ، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر 2016.

قائمة المراجع

- دلهار صلاح الدين يوناني، شرح القانون الجنائي (القسم الخاص)، دار هومة، الجزائر، 2017.
- ربيعة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.
- سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، 2006.
- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الجامعة الجديدة، الأزاريطة.
- عبد الفتاح بيومي حجازي ، النظام القانوني للجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2014.
- علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر والتوزيع، عمان، 2005.
- عصمت عبد المجيد بكر، أثر التقدم العلمي في العقد، موسوعة القوانين العراقية، بغداد، العراق، 2007.
- القاضي حازم نعيم الصمادي ، المسؤولية في العمليات المصرفية الإلكترونية، الطبعة الأولى، دار وائل للنشر، عمان، 2006.
- لامية محبوب، جريمة التزوير، دار الجامعة الجديدة، مصر، 2013.
- محمد إبراهيم أبو الهيجاء، عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2005.
- محمد أمين أحمد الشوابكة ، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2004.
- محمد أمين الرومي ، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
- محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007.
- محمود نجيب حسني ، النظرية العامة للقصد الجنائي: دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، مصر، 1989.

قائمة المراجع

- **محمود نجيب حسني** ، شرح قانون العقوبات، دار النهضة العربية، جامعة حلوان، 1994.
- **المطالقة محمد فواز** ، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن.
- **منير محمد الجنيهي وممدوح محمد الجنيهي** ، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
- **منير محمد الجنيهي وممدوح محمد الجنيهي** ، التوقيع الإلكتروني وحجته في الإثبات، دار الفكر الجامعي، الإسكندرية، 2005.
- **نائلة عادل محمد فريد قورة** ، شرح قانون العقوبات (جرائم الاعتداء على الأموال)، دار النهضة العربية، القاهرة، الطبعة الأولى، 2018.
- **هدى حامد قشقوش** ، شرح قانون العقوبات (القسم الخاص)، الطبعة الثانية، دار النهضة العربية، القاهرة، 2016.
- **ثالثاً: الرسائل الجامعية والأطروحات**
- **أمين عزان** ، الحماية الجنائية للتجارة الإلكترونية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 2005.
- **صباح رمضان وياسين صالح** ، السياسة الجنائية في مواجهة الجرائم المعلوماتية: دراسة تحليلية، أطروحة دكتوراه، العراق، 2013.
- **عمر أبو الفتوح عبد العليم الحمامي** ، الحماية الجنائية للمعلومات المسجلة إلكترونياً، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.
- **ياسر محمد الحكومي** ، الحماية الجنائية والأمنية للتوقيع الإلكتروني في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق، جامعة حلوان، مصر.
- **يوسف بن سعيد الكيلاني** ، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه، جامعة أبو بكر الصديق، تلمسان، الجزائر.

قائمة المراجع

رابعاً: البحوث والمقالات العلمية والمؤتمرات

- آسيا بن عبيد ، الحماية الجنائية لبطاقات الدفع في جرائم التزوير في القانون الجنائي، مجلة دراسات، 2017.
- حسام محمد نبيل الشنراقي ، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 3، 2024.
- خالد ممدوح إبراهيم ، الحماية الجنائية للتوقيع الإلكتروني، مجلة الفكر الشرطي، العدد 88، يناير 2019.
- الدسوقي أبو الليل ، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، مؤتمر الأعمال المصرفية الإلكترونية، المجلد الخامس.
- راضية مشري ، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، مجلة حوليات للعلوم الاجتماعية والإنسانية، 2017.
- غزالي نزيهة ، الآليات القانونية لحماية وسائل الدفع الإلكتروني في التشريع الجزائري، مجلة البحوث السياسية والإدارية، 2017.
- فيصل سعيد الغريب ، التوقيع الإلكتروني وحجته في الإثبات، المنظمة العربية للتنمية الإدارية، 2005.
- محمد عقوني ، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة الفكر، 2019.
- نجلاء توفيق فليح ، القيمة الثبوتية للتوقيع الإلكتروني، بحث منشور في مجلة الرافدين للحقوق، كلية الحقوق، جامعة الموصل، المجلد 6، العدد 22، 2004.
- هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية، القاهرة، مصر 25 أكتوبر 1993.
- هدى حامد قشقوش ، الحماية الجنائية للتوقيع الإلكتروني، بحوث مؤتمر الأعمال المصرفية بين الشريعة والقانون، المجلد الثاني، الإمارات العربية المتحدة، كلية العلوم والقانون.

قائمة المراجع

خامساً: القوانين والتشريعات والأحكام القضائية النصوص القانونية :

- قانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004.
- قانون المعاملات الإلكترونية لمملكة البحرين رقم (28) لسنة 2004.
- قانون رقم (2) لسنة 2002 لإمارة دبي بشأن المعاملات والتجارة الإلكترونية.
- المادة (11) من قانون المعاملات الإلكترونية الأردني، والمادة (14) من قانون الإثبات المصري، والمادة (19) من قانون المعاملات الإلكترونية السوري، والمادة (25) من قانون الإثبات العراقي.
- محكمة النقض المصرية: نقض مدني، جلسة 1985/11/13، مجموعة أحكام النقض، 36-226-993.
- محكمة النقض المصرية : مجموعة أحكام محكمة النقض، رقم 15 لسنة 23/06/1964.
- النصوص القانونية الوطنية
- القانون الجزائري رقم 18/05 المؤرخ في 10 ماي 2018
- النصوص القانونية الأجنبية
- قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني لسنة 2001.
- القانون النموذجي بشأن التوقيعات الإلكترونية (أونسيترال).
- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية
- سادساً: المقالات الصحفية والمواقع الإلكترونية
- أحمد شرف الدين ، حجية الرسائل الإلكترونية في الإثبات، بحث منشور في مجلة الأبحاث القانونية، متاح على الموقع الإلكتروني: www.easlaws.com (تاريخ الاطلاع: 2026/04/29).
- فهد عبد الله الحويماني ، التوقيع الإلكتروني أو التوقيع اليدوي، مقال منشور في مجلة الاتصال، العدد (11) في 2026/5/28، متاح على الموقع الإلكتروني: www.etesai.com.

قائمة المراجع

- ميلاد سامي ، التوقيع الإلكتروني والحماية القانونية، بحث منشور في جريدة القبس، العدد 12614، الاثنين 23 يوليو 2007، متاح على الموقع الإلكتروني: www.algabas.com (تاريخ الاطلاع: 2026/04/09).
- مقال منشور في مجلة الاتصالات والعالم الرقمي (أسبوعية متخصصة تصدر عن صحيفة الجزيرة)، الأحد 5 ربيع الثاني 1428، العدد (205)، متاح على الموقع الإلكتروني: www.al-jazirah.com (تاريخ الاطلاع: 2026/02/25).
- شبكة قانوني العرب، متاح عبر الرابط الإلكتروني: www.arablawninfo.com.
- النص الكامل لقانون الأونسيترال متاح على الموقع الإلكتروني للجنة: www.uncitral.org (تاريخ الاطلاع: 2026-03-11).

سابعاً: المراجع الأجنبية (Foreign References)

- "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and 'thief' and 'steal' shall be construed accordingly."

فهرس المحتويات

.....1.....	مقدمة
الفصل الأول: الإطار القانوني للتوقيع الإلكتروني	
.....7.....	المبحث الأول: مفهوم التوقيع الإلكتروني
.....7.....	المطلب الأول: تعريف التوقيع الإلكتروني
.....7.....	الفرع الأول: التعريف الفقهي للتوقيع الإلكتروني
.....8.....	الفرع الثاني: تعريف التوقيع الإلكتروني في التشريعات المقارنة
.....14.....	الفرع الثالث: موقف المشرع الجزائري فيما يتعلق بتعريف التوقيع الإلكتروني.
.....15.....	المطلب الثاني: شروط التوقيع الإلكتروني وصوره
.....15.....	الفرع الأول: شروط التوقيع الإلكتروني
.....20.....	الفرع الثاني: صور التوقيع الإلكتروني
.....24.....	الفرع الثالث: أهم تطبيقات التوقيع الإلكتروني
.....30.....	المبحث الثاني: حجية التوقيع الإلكتروني
.....31.....	المطلب الأول: شروط إضفاء الحجية على التوقيع الإلكتروني و نطاقها
.....31.....	الفرع الأول: الصفات الواجب توافرها على التوقيع الإلكتروني
.....34.....	الفرع الثاني: التوثيق
.....36.....	المطلب الثاني: نطاق حجية التوقيع الإلكتروني.
.....36.....	الفرع الأول: المعاملات التي يقبل فيها التوقيع الإلكتروني .
.....37.....	الفرع الثاني : المعاملات التي لا يقبل فيها التوقيع الإلكتروني

الفصل الثاني: جرائم التوقيع الإلكتروني وآليات حمايتها

المبحث الاول: صور جرائم التوقيع الالكتروني	42
المطلب الاول: جريمة سرقة التوقيع الالكتروني والدخول الغير مصرح	42
الفرع الاول: تعريفها	42
الفرع الثاني: أركان جريمة السرقة الالكترونية	44
الفرع الثالث : جريمة الدخول غير المصرح به إلى النظام المعلوماتي لتوقيع الالكتروني	50
المطلب الثاني: جريمة الاحتيال المعلوماتي و جريمة التزوير	61
الفرع الاول: تعرف جريمة الاحتيال	61
الفرع الثاني: جريمة التزوير	63
الفرع الثالث: أساليب تزوير التوقيع الإلكتروني	67
الفرع الرابع: جريمة تعطيل أو إفساد النظام المعلوماتي	69
المبحث الثاني: آليات الحماية الالكترونية للتوقيع الالكتروني	70
الفرع الاول: المقصود بالتشفير	71
الفرع الثاني: ضوابط وطرق التشفير	71
المطلب الثاني : التصديق الالكتروني	73
الفرع الاول: تعريف التصديق الالكتروني	73
الفرع الثاني: دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع الالكتروني	74

فهرس المحتويات

.....81.....

خاتمة:

.....86.....

قائمة المراجع:

ملخص مذكرة الماستر

يعد التوقيع الإلكتروني من أهم الوسائل الحديثة التي فرضتها التطورات التكنولوجية في مجال المعاملات الإلكترونية، حيث أصبح أداة قانونية تضمن توثيق الهوية وتحقيق الثقة والأمان في التبادل الرقمي للمعلومات والعقود. وقد سعت التشريعات الوطنية والدولية إلى وضع إطار قانوني ينظم استعمال التوقيع الإلكتروني ويوفر الحماية القانونية له، من خلال تحديد شروط صحته وحجيته في الإثبات، إضافة إلى تنظيم الجهات المصدقة وآليات التفسير والأمن المعلوماتي.

وفي المقابل، أدى الانتشار الواسع للتوقيع الإلكتروني إلى ظهور العديد من الجرائم الإلكترونية المرتبطة به، مثل التزوير الإلكتروني، واختراق البيانات، وسرقة الهوية الرقمية، واستعمال التوقيع الإلكتروني بطرق غير مشروعة، مما استدعى تدخل المشرع لوضع نصوص قانونية تجرم هذه الأفعال وتحدد العقوبات المناسبة لها.

وتبرز أهمية الإطار القانوني لحماية التوقيع الإلكتروني في تحقيق الثقة في المعاملات الرقمية، وضمان سلامة وأمن البيانات الإلكترونية، وحماية حقوق الأفراد والمؤسسات من الجرائم المعلوماتية. كما تسهم هذه الحماية في تشجيع الاستثمار والتجارة الإلكترونية وتعزيز التحول الرقمي في مختلف القطاعات.

الكلمات المفتاحية:

- 1- التوقيع الإلكتروني 2- الجرائم الإلكترونية 3- الحماية القانونية 4- الإثبات الإلكتروني
- 5- أمن المعلومات 6- التفسير الإلكتروني

Master's Note Summary

The electronic signature is considered one of the most important modern tools imposed by technological developments in the field of electronic transactions. It has become a legal means that ensures identity verification and establishes trust and security in the digital exchange of information and contracts. National and international legislations have sought to establish a legal framework regulating the use of electronic signatures and providing legal protection for them by defining the conditions of their validity and evidentiary value, in addition to

regulating certification authorities, encryption methods, and information security mechanisms.

On the other hand, the widespread use of electronic signatures has led to the emergence of several cybercrimes associated with them, such as electronic forgery, data breaches, digital identity theft, and the unlawful use of electronic signatures. This has required legislators to enact legal provisions criminalizing such acts and imposing appropriate penalties.

The importance of the legal framework for the protection of electronic signatures lies in establishing trust in digital transactions, ensuring the integrity and security of electronic data, and protecting the rights of individuals and institutions from cybercrimes. Such protection also contributes to encouraging investment and electronic commerce, as well as supporting digital transformation in various sectors.

Keywords:

1-Electronic Signature 2-Cybercrime 3-Legal Protection 4-Electronic Evidence
5-Information Security 6-Electronic Encryption