الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العالي
المركز الجامعي علي كافي تندوف
معهد الحقوق والعلوم السياسية
قسم الحقوق

الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري

مذكرة تخرج لنيل شهادة الماستر في الحقوق
تخصص قانون عام

إعداد الطالب (ة) :
زكراوي عبد الله
زكراوي محمد

تحت إشراف الأستاذ
بوحزمة كوثر

لجنة المناقشة

محمد فاضل علي سالم نورالدين	أستاذ محاضر ب	المركز الجامعي علي كافي تندوف	رئيسا
بوحزمة كوثر	أستاذ محاضر ب	المركز الجامعي علي كافي تندوف	مشرفا ومقررا
ناصيري ربيعة	أستاذ محاضر ب	المركز الجامعي علي كافي تندوف	مناقشا

السنة الجامعية:2025/2024

((رَبَّنَآ ءَاتِنَا مِن لَّدُنكَ رَحْمَةً وَهَيِّئْ لَنَا مِنْ أَمْرِنَا رَشَدًا))

صدق الله العظيم

دعـــــــاء ورجـــــاء

بسم الله الرحمن الرحيم والصلاة والسلام على خاتم الأنبياء

وإمام

المرسلين سيدنا محمد وآله وصحبه أجمعين.

ربِّ أَوْزِعْنِي أَنْ أَشْكُرَنِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ

"اللهمَّ اجعلْنِي شكورًا، واجعلنِي صبورًا، واجعلنِي في عَينِي

صغيرًا، وفي أعينِ الناسِ كبيرًا"

اللهم إذا رزقتنا نجاحا فلا تأخذ تواضعنا، وإذ ا مننت علينا

بالتواضع فلا تحرمنا

اعتزازنا بكرامتنا إنك واسع العطاء

ربنا وتقبل دعاء

الإهـــــداء

اهدي هذا العمل إلى .....

إلى روح ابي رحمه الله

إلى أمي إكراما وإرضاء، برا و اقرارا بالفضل

إلى جدتي التي لم تبخلني من دعائها أطال الله في عمرها

اخواني واخواتي حبا واحتراما

إلى زوجتي التي كانت الداعم الاكبر لي في هذه الرحلة

شكرا لصبرك وتفهمك ودعمك المستمر

الى ابنائي فاطمة الزهراء ومحمد صديق مصدر

سعادتي.

العائلة الكريمة كبيرا وصغيرا

إلى كل طالب علم .... إلى أصحاب القضايا النزيهة

المدافعين عن الوطن

إلى من يراها الناس تنزف ،وأراها تتبرع بدمها لأمة

أصبحت بلا دم غزة الكفاح

إلى وطني الغالي الجزائر

إليكم جميعا أهدي ثمرة هذا العمل .

عبد الله زكراوي

الإهـــــداء

اهدي هذا العمل إلى .....

الوالدين الكريمين إكراما وإرضاء، برا واقرارا بالفضل

اخواني واخواتي حبا واحتراما

إلى زوجتي التي كانت الداعم الاكبرلي في هذه الرحلة شكرا لصبرك وتفهمك ودعمك المستمر

الى ابنائي غفران، المنتصربالله، علي نورين، صفوان مصدر سعادتي.

العائلة الكريمة كبيرا وصغيرا

إلى كل طالب علم .... إلى أصحاب القضايا النزيهة المدافعين عن الوطن

إلى من يراها الناس تنزف، وأراها تتبرع بدمها لأمة أصبحت بلا دم غزة الكفاح

إلى وطني الغالي الجزائر

إليكم جميعا أهدي ثمرة هذا العمل.

محمد زكراوي

أولا الشكر لله الواحد القهار صاحب الفضل والإكرام أكرمنا بنعـمة الإسـلام ويسر لنا سبيل العلم، فله الشكر حتى يرضى وله الشكر بعد الرضا والصلاة والسلام على المصطفى صل الله عليه وسلم تسليما كثيرا.

ثم كامل الشكر والتقدير للأستاذة الفاضلة **كوثر بوحزمة** لتفضلها بالإشراف على هذا العمل، ولما لها من جهود ومقترحات و ملاحظات قيمة أثمرت إيجابا فيما قدمنا، فجزاها الله عنا أفضل الجزاء.

كما نتوجه بالشكر إلى كل من ساعدنا من قريب أو من بعيد لإتمام هذا العمل.

كما أتوجه بالشكر لأعضاء لجنة المناقشة لقبولهم مناقشة هذا العمل، وتسخيرهـم وقتا لقراءته وتقييمه.


المقدمة

دخل العالم في مرحلة متطورة ضمن آفاق عصر التكنولوجيا والمعلومات بهدف تحقيق أقصى استفادة من التقنيات المتاحة في مجال نظم وتقنيات المعلومات والاتصالات، حيث أصبح هذه الأخيرة من أهم المعايير التي تقاس بها مدى تقدم الأمم.

حيث ألقى هذا التقدم بظلاله مختلف الجوانب الاقتصادية والتجارية وغيرها من الأنشطة التي أصبحت تتم دون الحضور المادي للأطراف، حيث أصبحت الوسائط الالكترونية للاتصال ذات أثر فعال وهام في إبرام العقود.

إن ظهور الحاسب وشبكة الانترنت واعتماد الافراد عليهما في اصدار المحررات الالكترونية والتوقيع والمصادقة عليها الكترونيا، اوجب على الدول من بينها الجزائر العمل على خلق الثقة في مثل هذه التطورات حيث عملت على ضبط هذه المعاملات وفقا لنصوص قانونية.

ولكن ما دامت الجريمة ظاهرة اجتماعية، تتأثر طبيعتها وحجمها بالتحولات الاقتصادية والاجتماعية والثقافية والتكنولوجية على المستويين الدولي والوطني، فقد ظهر شكل جديد من أشكال الجريمة، يتمثل في انتشار الجرائم المعلوماتية أو الإلكترونية، والتي تعتبر من أعظم السلبيات التي خلفتها الثورة المعلوماتية، لأن هذه الجرائم تتضمن في اعتداءاتها قيماً أساسية تهم الأفراد والمؤسسات وحتى الدول في جميع مناحي الحياة، كما خلفت هذه الجرائم لدى الافراد شعوراً بعدم الثقة في كيفية التعامل مع ثمار هذه الثورة الجديدة والاستفادة منها.

في ظل هذا الوضع المقلق، أصبح المجتمع الدولي مهتمًا بمكافحة الجرائم الإلكترونية. وفي هذا الصدد، نشير إلى أن الأمم المتحدة أولت هذه القضية اهتمامًا بالغًا، لا سيما في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، الذي عُقد في فيينا من 10 إلى 17 نيسان/أبريل 2000، ومؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، الذي عُقد في بانكوك من 18 إلى 25 نيسان/أبريل 2005.

من جهة أخرى، وضعت اللجنة الأوروبية المعنية بمشاكل الجريمة ولجنة الخبراء المعنية بجرائم الحاسوب مسودة اتفاقية دولية بشأن جرائم الحاسوب. وأعلن المجلس الأوروبي عن هذه المسودة في 27 أبريل/نيسان 2000. وأكد المجلس أن الهجمات الأخيرة على المواقع الإلكترونية التجارية قد لفتت انتباه المجتمع الدولي إلى المخاطر والتحديات التي تواجه شبكات الحاسوب وشبكات المعلومات الدولية، وأن جرائم الإنترنت أصبحت أكثر خطورة من أي وقت مضى. وبناءً على ذلك، بادر المجلس الأوروبي بوضع مسودة اتفاقية بشأن جرائم الحاسوب، مع مراعاة الطابع الدولي لهذا النوع من الجرائم. وبعد نحو عام ونصف من المناقشات والتعديلات على هذه المسودة، وُقّعت اتفاقية بودابست بشأن الجرائم الإلكترونية أو الحاسوبية في 23 نوفمبر/تشرين الثاني 2001، اقتناعًا من الدول الأعضاء في المجلس الأوروبي والدول الموقعة الأخرى بضرورة مكافحة هذا النوع الجديد من الجرائم.

لقد تأثرت الجزائر، كغيرها من البلدان، بالثورة المعلوماتية، بإيجابياتها وسلبياتها. ما دفع بالمشرع الجزائري الى مواكبة هذا التطور في الجرائم الماسة بالتوقيع الإلكتروني، فالمواجهة التشريعية

ضرورية للتعامل من خلال خلق قواعد قانونية غير تقليدية لمواجهة هذا النوع من الجرائم المستحدثة، ويعمل المشرع على إدخال تعديلات على قانون العقوبات لجعله أكثر استجابة للتطورات الجنائية في مجال تكنولوجيا المعلومات والاتصالات، وإنشاء قوانين جديدة. لضمان الحماية الجزائية للتوقيع الالكتروني.

إن الحداثة القانونية والتشريعية للحماية الجنائية للتوقيع والتصديق الالكترونيين، من هنا جاء اختيارنا للموضوع لمعرفة مدى انسجام النصوص التشريعية مع المستجدات الراهنة في مجال المعاملات الالكترونية خاصة مع بروز المحررات الالكترونية وضرورة التوقيع والمصادقة عليها الكترونيا.

وتهدف دراسة موضوع الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري، إلى معرفة السياسات المنتهجة من قبل المشرع الجزائري خاصة في مجال مكافحة الجرائم الماسة بالتوقيع الالكتروني وما يقابلها في التشريعات المقارنة. من خلال قراءة للنصوص القانونية المرصودة لمثل هذه الجرائم مع بيان ما تم اتخاذه مقارنة مع ما قامت به بعض التشريعات الدولية. حتى تكون المنظومة الجزائية قادرة على تحقيق الهدف المبتغى منها.

ورغم الأهمية الكبيرة التي يحظى بها موضوع الدراسة قد واجهتنا بعض الصعوبات والعراقيل أولها صعوبة الفصل بين التوقيع الالكتروني والمعاملات الالكترونية وكذلك الجرائم الماسة بالتوقيع الالكتروني والجرائم الالكترونية.

والأكيد ان هناك العديد من الدراسات السابقة التي تناولت موضوع الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري. والتي كان الفضل في ابراز كيفية معالجة موضوع الدراسة حيث التقينا في نقاط خاصة ما تعلق بالمفاهيم الأساسية للتوقيع والتصديق الالكتروني واختلفنا معها في بعض النقاط خاصة فيما تعلق بالجرائم الماسة بالتوقيع الالكتروني وكذا الاحكام الجزائية لمكافحة جرائم التوقيع الالكتروني ومن بين الدراسات السابقة نجد:

الدراسات الوطنية في الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة لترجمان نسيمة أطروحة لنيل شهادة دكتوراه طور الثالث تخصص التجريم في قانون الأعمال كلية الحقوق والعلوم السياسية جامعة ابن خلدون تيارت 2020-2021، بالإضافة الى دراسة لمعاشي سميرة، آليات مكافحة الجريمة المعلوماتية (دراسة مقارنة)،أطروحة دكتوراه تخصص قانون أعمال، جامعة محمد خيضر بسكرة،2020، ودراسة بعنوان جريمة التزوير الوثيقة الإدارية الرسمية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي، لبراهمي حنان جامعة محمد خيضر بسكرة،2015،

أما الدراسات العربية فتمثلت في دراسة تحت عنوان التنظيم القانوني لجهات التصديق على التوقيع الالكتروني، للباحثة آلاء أحمد محمد حاج علي، أطروحة ماجيستير تخصص قانون الخاص، جامعة النجاح الوطنية نابلس فلسطين، 2013، ودراسة لسامر عبد الجواد مضحي رشق بعنوان النظام القانوني لتوثيق التوقيع الالكتروني رسالة ماجيستير في القانون التجاري كلية الدراسات العليا، الجامعة العربية الامريكية، فلسطين 2019.

إن الدراسات السابقة التي تم ذكرها على سبيل المثال لا الحصر أبرزت أهمية التوقيع الالكتروني في مختلف المعاملات والتعاقدات التي باتت تتم وفقا لمحررات الكترونية كنتيجة حتمية للتطورات التكنولوجية والمعلوماتية وما نتج عنها من جرائم وسعي المشرع الوطني والدولي لمواجهة هذا النوع من الجرائم والوقاية منها، وذلك بإيجاد الاحكام التي تتلاءم وطبيعة هذه الجرائم

ومن هنا يمكن طرح الإشكالية التالية **إلى أي مدى وفق المشرع الجزائري في تكريس الحماية الجنائية للتوقيع الالكتروني**؟ وتتفرع عنها مجموعة من التساؤلات:

- ما المقصود بالتوقيع الالكتروني وماهي أهم أشكاله وصوره؟
- ماهي الجرائم المتعلقة بالتوقيع الالكتروني؟
- كيف يتم اثبات الجرائم الواقعة على التوقيع الالكتروني؟
- ما مدى اختصاص القضاء الجزائري في التعامل معها،
- كيف يساهم التعاون الدولي في تعزيز مكافحة جرائم التوقيع الالكتروني؟

ولمعالجة الإشكاليات تم الاعتماد أولا على المنهج الوصفي حيث سيتم من خلاله سرد وبيان النصوص التشريعية والدراسات ذات الصلة بموضوع المذكرة حيث نحتاج في كثيرا من الأحيان لوضع وصف لبعض الجرائم المتعلقة بالتوقيع الالكتروني، والطرق التي تتم بها هذه الجرائم، وهو ما يؤدي بنا بالضرورة الى المنهج التحليلي والذي يعتمد على تحليل الظواهر من خلال الوقوف على مدى فعالية النصوص التشريعية المكرسة لمكافحة هذا النوع من الجرائم. بالإضافة الى المنهج المقارن من خلال المقارنة بين القوانين الأجنبية (الفرنسي، الأمريكي .....) والقوانين العربية مثل القانون المصري مع التركيز على ما جاء به المشرع الجزائري.

وللإجابة على الإشكالية المطروحة وفقا للمنهج المتبع تم تقسيم الدراسة الى فصلين:

الفصل الأول: الأحكام الموضوعية لمكافحة جرائم التوقيع الالكتروني في التشريع الجزائري

الفصل الثاني: الاحكام الإجرائية لمكافحة جرائم التوقيع الالكتروني في التشريع الجزائري.

وفي الأخير نختم بخاتمة نبين من خلالها أهم النتائج التي تم التوصل اليها


الفصل الأول

لقد أنتجت العقود الأخيرة ثورة من نوع آخر تتعلق بوسائل الاتصال والمعلومات، وذلك بسبب التطور الذي تجسد بشكل رئيسي في انتشار أجهزة الكمبيوتر المتطورة باستمرار، والبرامج المتقدمة، وشبكات الاتصالات التي قربت بين الملايين من الافراد، وأتاحت فرصا جديدة لتطور المعلومات وتبادلها، وحتى التفاوض وإبرام العقود المختلفة، وخاصة عبر الإنترنت، فضلا عن إصدار المحررات الإلكترونية.، الأمر الذي استوجب بالضرورة التوقيع والمصادقة عليها الكترونيا،

لقد أحدث انتشار التقنيات الحديثة وتطبيقاتها، التي أثرت على جميع مناحي الحياة، تحولاتٍ ومتغيراتٍ عديدة، إيجابيةً وسلبية. ولا شك أن ثورة المعلومات، بفضل التقنيات المتطورة التي تستخدمها، والمتمثلة في استخدام الحاسوب والإنترنت، قد أحدثت آثارًا إيجابية، ومثلت نقلةً نوعيةً في حياة الأفراد والدول، بفضل سرعة ودقة أنظمة المعلومات هذه في تخزين المعلومات وجمعها وتبادلها. إلا أن هذه التقنية خلّفت أيضًا العديد من السلبيات، أهمها صعوبة ضمان أمن المعلومات نظرًا لسهولة الوصول إليها، والهجمات، والاعتداء على حرية المعلومات.

أدى التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة إلى ظهور أشكال جديدة من الجرائم، تُعرف عادةً بالجرائم السيبرانية، والتي تُمسّ الوثائق الإلكترونية من خلال المساس بالتوقيعات الإلكترونية. وقد دفع هذا المشرع الجزائري إلى التدخل لمكافحة هذه الجريمة وضمان الحماية الجنائية لأنظمة المعلومات. وقد تحقق ذلك من خلال تعديل قانون العقوبات لمواكبة التطورات الجنائية في مجال تكنولوجيا المعلومات والاتصالات، وسنّ قوانين جديدة تضمن الحماية الجنائية للتوقيعات الإلكترونية.

لذا، كان لا بد للتشريع الجزائري من مواكبة هذا التطور الملحوظ في الجرائم المتعلقة بالتوقيعات الإلكترونية. ولا بد من مواجهة تشريعية شاملة لمعالجة هذا الأمر، من خلال وضع قواعد قانونية غير تقليدية لمواجهة هذا النوع من الجرائم المستحدثة،

من خلال الفصل الاول حاولنا التعرف على التوقيع و التصديق الالكترونيين و كذا الجرائم الماسة بالتوقيع الالكتروني . حيث قسمناه إلى مبحثين:

المبحث الأول: مقتضيات التوقيع الالكتروني كمحل للحماية الجنائية

المبحث الثاني: الجرائم الماسة بالتوقيع الالكتروني

المبحث الأول: مقتضيات التوقيع الالكتروني كمحل للحماية الجنائية

كان التوقيع التقليدي الوسيلة المعتمدة الوحيدة المستعملة في القرون الماضية للمصادقة وإمضاء المحررات، ومع التطور التقني لوسائل الاتصال الحديثة وتقنيات المعلومات، اتاح التعامل بنوع جديد من المعاملات ،فالعالم اليوم تطور في شتى المجالات بفضل الثورة المعلوماتية وابتكار شبكات وسائل التواصل عن بعد المحلية والعالمية ، التي ازالت مختلف العوائق وأصبح العالم قربة صغيرة، حيث أصبح من الضروري ابتكار بدائل للمحررات الورقية بمحررات الكرتونية لتسهيل عملية بالتوقيع و التصديق عليها عبر وسائط إلكترونية من خلال التوقيع الإلكتروني. من خلال هذا المبحث سنحاول تقديم مفهوم للتوقيع الالكتروني من خلال (**المطلب الأول**) و كذا مفهوم التصديق الالكتروني من خلال (**المطلب الثاني**).

المطلب الأول: مفهوم التوقيع الالكتروني

حظيت التوقيعات الإلكترونية باهتمام كبير كبديل للتوقيعات التقليدية. وقد تنوعت التشريعات المتعلقة بها، قانونيًا وتشريعيًا. في فهم هذا النمط الجديد وتحديد مفهومه. وقد عرفته المنظمات الدولية أولًا من خلال التجارة الإلكترونية. لذلك، سعى فقهاء القانون إلى توضيح المقصود بالتوقيع الإلكتروني، وقد لاقى اهتمامًا بالغًا من معظم التشريعات الحديثة، إذ وضع إطارًا قانونيًا وتنظيميًا يغطي جميع المسائل والأحكام المتعلقة به. من خلال هذا المطلب حاولنا تحديد مفهوم للتوقيع الالكتروني و ذلك بتقسيمه الى أربعة فروع الاول خصصناه لتعريف التوقيع الالكتروني، الفرع الثاني متعلق بخصائص التوقيع الالكتروني ، الفرع الثالث تم من خلاله التمييز بين التوقيع الالكتروني و التوقيع التقليدي و خصصنا الفرع الرابع تم تخصيصه لصور التوقيع الالكتروني

الفرع الأول: تعريف التوقيع الالكتروني

تختلف تعريفات التوقيعات الإلكترونية باختلاف المنظور المُتّبع. فبعضها يُعرّفها بناءً على طريقة تطبيقها، بينما يُعرّفها آخرون بناءً على وظائفها أو تطبيقاتها العملية. ونجد على مستوى التشريعات العالمية فقد عرفته المادة 2 الفقرة أ من قانون الأمم المتحدة للتوقيعات الالكترونية لعام 2001 بأنه" **البيانات في شكل إلكتروني المضمنة في رسالة البيانات أو المضافة إليها أو المرتبطة منطقياً بها والتي يمكن استخدامها لتحديد هوية الشخص الموقع على رسالة البيانات والإشارة إلى مو افقته على المعلومات الواردة في رسالة البيانات.**"

عند استقراء المادة 7 من قانون الاونسترال يتضح أن القانون النموذجي قد ركز على ضرورة قيام التوقيع الالكتروني بوظائف التوقيع التقليدي حيث نصت المادة 07 من الفصل الثاني [1]-تطبيق المقتضيات القانونية على رسائل البيانات- وبالتالي لم يقدم تعريفا صريحا وانما اكتفى بتقديم

[1] - https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook_1.pdf تاريخ الاطلاع 2025/02/06 الساعة 22:43

الوظائف والشروط الواجب توفرها فيه كما ورد في الفقرة 1، "عندما يشترط القانون توقيع شخص يستوفي هذا الشرط فيما يتعلق برسالة بيانات، إذا:

(أ) استُخدمت طريقة لتحديد هوية ذلك الشخص من خلال المعلومات الواردة في رسالة البيانات

(ب) كانت تلك الطريقة موثوقة بالقدر المناسب للغرض الذي تم من أجله إنشاء أو إرسال رسالة البيانات، في ضوء جميع الظروف، بما في ذلك الاتفاق ذي الصلة.

وفي قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية لعام 2001، طرحت لجنة الأمم المتحدة للقانون التجاري الدولي تعريفا للتوقيع الإلكتروني في المادة 2، الفقرة (أ): "البيانات في شكل إلكتروني المضمنة في رسالة البيانات أو الملحقة بها أو المرتبطة منطقياً بها يجوز استخدامها لتحديد هوية الموقع فيما يتعلق برسالة البيانات والإشارة إلى موافقته على المعلومات الواردة في رسالة البيانات[1]".

من خلال هذا التعرف الأمم يظهر لنا أنها طرحته بشكل موسع، فهي لم تقم بتحديد طريقة اعتماده، حيث تركت الأمر بذلك للدول والأفراد في إصدار التشريعات الخاصة من خلال تحديد نوع التوقيع الإلكتروني واختيار الطريقة التي يتم إنشاؤها بها، طالما تسمح تلك الطريقة بتحديد هوية صاحب التوقيع وموافقته على المعلومات الواردة في الرسالة، مما قد يمكن الأفراد من فهم أي تقنية تظهر في المستقبل تختص بإنشاء توقيع إلكتروني.

طرح الاتحاد الأوروبي، كغيره من المنظمات، تعريفًا للتوقيعات الإلكترونية. حيث وضع نوعين من التوقيعات، وحدد لكل منهما تعريفا:

1. **التوقيع الإلكتروني البسيط** (SES) : "مجموعة من معلومات على شكل إلكتروني متعلقة بمعلومات إلكترونية أخرى ومرتبطة بها ارتباطا وثيقا ويستخدم أداة للتوثيق[2]".
2. **التوقيع الإلكتروني المعزز(المتقدم)** (SEA): "هو توقيع إلكتروني ويشترط أن يكون:
   - **أ.** له القدرة على تحديد شخصية الموقع ومميزا له عن غيره من الأشخاص.
   - **ب.** أن ينشأ باستخدام وسائل تقنية تقع تحت سيطرة الموقع[3] بحيث يضمن لصاحبه السرية التامة.

---

[1]- نفس المرجع

[2]- art 2-1 de la Directive : " la signature électronique une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ".

https://eur-lex.europa.eu/FR/legal-content/summary/esignature-in-the-eu.html تاريخ الاطلاع 2025/02/08 الساعة 11:46

[3]-عصام عبد الفتاح مطر، **التحكيم الالكتروني (ماهيته، اجراءاته، وآلياته في تسوية منازعات التجارة الالكترونية والعلامات التجارية وحقوق الملكية الفكرية**، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009، ص105-106.

ت. يتعلق بالمعلومات الموجودة في الرسالة-المحرر الالكتروني- لأنه يكشف عن كل تغييرات في المعلومات"[1]

وعلى الرغم من التقسيم الذي اعتمدته دول الاتحاد الأوروبي والذي تناول نوعين من التوقيعات الإلكترونية، إلا أن هذين التعريفين لم يخرجا عن التعريفات الأخرى التي تناولت التوقيعات الإلكترونية.

إلى جانب هذه التعاريف التي قدمت ، نجد كذلك بعض التشريعات الدولية والعربية المقارنة التي أعطت تعريفا للتوقيع الإلكتروني.

- عمل المشرّع الفرنسي على تعديل بعض أحكام القانون المدني لتتماشى مع التوقيع على المستندات والعقود الإلكترونية، وعرّفه بأنه "التوقيع اللازم لإتمام العمل القانوني، والذي يُعرّف الشخص الذي يُحتج به ضده، ويُعبّر رسميًا عن رضاء الطرفين بالالتزامات الناشئة عن هذا العمل. وعند إنشاء توقيع إلكتروني، يجب استخدام وسيلة آمنة لتحديد هوية الشخص لضمان ارتباطه بالعمل الذي وقّعه".[2]
- أما الولايات المتحدة الأمريكية عرف القانون الفيدرالي التوقع الإلكتروني " أي رمز أو وسيلة بصرف النظر عن التقنية المستخدمة إذا ما تم نسبته إلى شخص يرغب في توقيع محرر الكتروني"[3]
- كما تم تعريفه من خلال نص المادة الثانية من القانون الفيدرالي السويسري عام 2004 الخاص بتقديم خدمات الشهادات في مجال التوقيع الإلكتروني بأنه" معطيات إلكترونية مجتمعة [4] أو مرتبطة منطقياً بمعطيات إلكترونية أخرى وتستخدم في التحقق من مصداقيته"
- و جاء تعريف التوقيع الإلكتروني في قانون التجارة الإلكترونية رقم 2 لسنة 2002 الصادر في إمارة دبي أول دولة عربية تطبق الحكومة الإلكترونية[5] - بأنه "كل توقيع يتكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة في شكل إلكتروني، مرفق أو مرتبط برسالة إلكترونية مختومة بقصد المصادقة على تلك الرسالة أو الموافقة عليها".

---

[1]- علاء محمد نصيرات، **حجية التوقيع الإلكتروني في الاثبات**، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2005، ص24.

[2] -https://www.lita-lb.org/archive/50-signature-%C3%A9lectronique-les-questions-juridiques-ar.html تاريخ الاطلاع 2025/05/03 على الساعة 12:04

[3] -خالد ممدوح ابراهيم، **إبرام العقد الالكتروني**، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2011،ص 245 .

[4] - عصام عبد الفتاح مطر ،المرجع سابق ،ص 106.

[5] - منير الجنبهي، ممدوح الجنبهي، **الشركات الالكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2008، ص138.

- أما المشرع المصري عرف التوقيع الإلكتروني[1] في المادة الأولى من القانون رقم15 لسنة 2004 التوقيع الالكتروني على أنه "**ما يتم وضعه على محررإلكتروني ويتخذ شكل حروف أو أرقام أورموزأو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره**"
- كما كان للانتقال من الكتابة التقليدية إلى الكتابة الإلكترونية، ومن التوقيعات في شكلها التقليدي إلى التوقيعات في شكلها الإلكتروني، أثر على التشريع الجزائري، وكذلك على التشريعات الأخرى، حيث اعترف المشرع الجزائري صراحة بالقضيتين لأول مرة من خلال التعديل الذي أجراه على القانون المدني بموجب القانون رقم 10-05 المتضمن القانون المدني المعدل والمكمل.[2]، ومن خلال نص المادتين 44 و46، بإضافة المواد 323 مكرر و323 مكرر 1 والمادة 327، تنص المادة 323 مكرر المستحدثة على ما يلي: "**تنشأ الإثبات الكتابي عن سلسلة من الحروف أو الأوصاف أو الأرقام أو أي إشارات أورموزذات معنى مفهوم، مهما كانت الوسيلة التي تحتويها أو طريقة إرسالها**".[3]"

كما تنص المادة 323 مكرر 1 من القانون نفسه على أن: "يُعتبر الدليل الكتابي الإلكتروني في حكم الدليل الورقي، شريطة التحقق من هوية مُصدره، وإعداده وحفظه في ظروف تضمن سلامته". ووفقاً للمادة 327، الفقرة 2، التي تنص على: "يكون التوقيع الإلكتروني صحيحاً وفقاً للشروط المنصوص عليها في المادة 323 مكرر 1".

لذلك، نجد أن المشرع لم يُعرِّف التوقيع الإلكتروني، بل حدد الأشكال التي يجوز أن يظهر بها. كما اكتفى بالإشارة إلى أن التوقيع الإلكتروني يُعترف به بشروط، وهي إمكانية التحقق من هوية المُوقِّع، وإمكانية تعديله وحفظه في ضمن شروط تحقق سلامته

كما تدخل المشرع الجزائري و تدارك الأمر. حيث أصدر المرسوم التنفيذي 07-162[4]، يعدل و يتمم المرسوم التنفيذي رقم 01-123 لذي عرف صراحة التوقيع الإلكتروني من خلال نص المادة الثالثة منه بقولها :" **التوقيع الإلكتروني هو معطى ينجم عن المحددة استخدام أسلوب عمل** يستجيب للشروط في المادتين 323 مكرر و323 مكرر 1 ومن الامر رقم 75-58 المتضمن القانون المدني .

---

[1] - صفاء فتوح جمعة، **العقد الإداري الالكتروني**، بدون طبعة ، دار الفكر والقانون، المنصورة، ، 2018، ص116.

[2] - القانون 05-10 المؤرخ في 10 يونيو 2005 يعدل ويتمم الأمر رقم -75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم، الجريدة الرسمية ، العدد 44، سنة 2005،ص 17

[3] - نفس المرجع ،ص 24

[4] -المرسوم التنفيذي رقم 07-162 المؤرخ في 30ماي 2007،يعدل ويتمم المرسوم التنفيذي رقم 01-123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية والاسلكية، الجريدة الرسمية ، العدد 37، سنة 2007

في الفقرة الثانية من المادة 3 من المرسوم نفسه، نجد أن المشرع أدرج توقيعًا آمنًا وعرّفه بأنه: "توقيع إلكتروني يستوفي الشروط التالية:

- أن يكون خاصًا بصاحب التوقيع
- أن يُنشأ بوسائل تقع تحت السيطرة الحصرية للموقع .
- أن يرتبط بالعمل المرتبط به-بيانات المحرر- بحيث يكون أي تعديل لاحق عليه قابلاً للكشف.

مما سبق، يتضح أن المشرع الجزائري ترك المسألة غامضة بعض الشيء عندما عرّف التوقيع الإلكتروني بأنه "بيانات ناتجة عن استخدام أسلوب عمل يستوفي الشروط المذكورة في المادتين المشار إليهما أعلاه". ولم يكشف عن نوع وشكل أسلوب العمل هذا الذي يستوفي تلك الشروط .كما نجده تطرق إلى تعريف التوقيع الإلكتروني صراحة في القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين،[1] وهو أول قانون جاء منظما للتوقيع الالكتروني[2] أين ميز بين نوعين من التوقيعات الإلكترونية وهما:

النوع الأول: التوقيع الإلكتروني العادي حيث عرفه في المادة الثانية الفقرة 1 من الباب الأول الفصل الثاني بأنه: "بيانات إلكترونية في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق"

كما تناول المشرع الجزائري في الفقرة الثالثة من نفس المادة إلى تعريف بيانات إنشاء التوقيع الإلكتروني بأنه: "البيانات الفريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني".

النوع الثاني: ويمثله التوقيع الإلكتروني الموصوف والذي عرفه في المادة 7ب: "التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي يلبي المتطلبات التالية[3]:

1. يجب أن يُنشأ بناءً على شهادة مصادقة إلكترونية موصوفة.
2. يجب أن يكون مرتبطًا حصريًا بالموقع الإلكتروني.
3. يجب أن يسمح بالتعرف على الموقع الإلكتروني.
4. يجب أن يُصمم باستخدام آلية إنشاء توقيع إلكتروني آمنة.
5. يجب أن يُنشأ بوسائل خاضعة لسيطرة الموقع الإلكتروني الحصرية.
6. يجب أن يكون مرتبطًا ببياناته، بحيث يمكن اكتشاف أي تعديل لاحق لهذه البيانات.

---

[1] - القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، سنة 2015

[2] - سعدي ربيع، **حجية التوقيع الالكتروني في التشريع الجزائري**، أطروحة دكتوراه في القانون، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة 01 ،2017، ص32

[3] -المادة 07 من القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، سنة 2015

ومنه المشرع الجزائري لم يحصر التوقيع الإلكتروني في شكل واحد، بل جعله عاماً وشاملاً، يمتد إلى كل اكتشاف علمي قد يظهر مستقبلاً، كما هو الحال بالنسبة للكتابة الإلكترونية.

هذا ما يمكن استنتاجه من عبارة **"مهما كانت الوسيلة التي تتضمنها"** مما يفتح المجال واسعا لأي توقيع جديد ينتجه التطور التقني [1].

كما نلاحظ أن المشرع الجزائري لم يختلف كثيرًا عما قدمته التشريعات الأخرى، سواء العربية أو الغربية، وقدم تعريفًا قريبًا من تعريفاتها.

من جميع التعريفات السابقة للتوقيعات الإلكترونية، يتضح وجود تقارب في التعريف المقدم من كل دولة. علاوة على ذلك، لا يوجد تعريف شامل للتوقيعات الإلكترونية. ولعل ذلك يعود إلى التطور السريع لوسائل الاتصال، والذي أدى بالضرورة إلى تطور التعريفات. ومع ذلك، فإن ما يميز التوقيعات الإلكترونية هو اختلافها عن التوقيعات التقليدية في عدة جوانب.

مما سبق نستنتج أن التوقيع الإلكتروني يتميز بعدة خصائص، عن التوقيع العادي (التقليدي) .

الفرع الثاني: خصائص التوقيع الالكتروني

ومن خلال التعريفات السابقة يمكننا استنتاج خصائص وميزات التوقيع الإلكتروني بعد أن اتفقت معظم التعريفات على أن التوقيع الإلكتروني يتكون عناصر وميزات فريدة خاصة بالموقع تأخذ شكل أرقام وحروف وعلامات ورموز وما إلى ذلك[2]:

1. فهو يحدد شخصية الموقع ويميزه عن غيره.
2. يعبر عن رضا الموقع بما ورد في محتوى المحرر.
3. التوقيع الإلكتروني هو عبارة عن رسالة إلكترونية-محرر الكتروني- ، هي المعلومات التي تم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسائل إلكترونية. [3].
4. يحقق التوقيع الإلكتروني أغراض التوقيع التقليدي طالما كان صالحًا ويمكن إثبات نسبته إلى الموقع.
5. يضمن هذا النظام أمن وسرية وخصوصية[4] جميع مستخدمي الموقع، بمن فيهم مستخدمو الإنترنت والعقود التجارية الدولية. ويساعد تحديد هوية المُوقِّعين على حماية المؤسسات من تزوير التوقيعات.

---

[1] - زروق يوسف، **حجية وسائل الاثبات الحديثة**، أطروحة دكتوراه في القانون الخاص،كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2013، ص223

[2] -عبد الرحمان الخلفان الحارثي، **حجية التوقيع الالكتروني في الاثبات** دراسة مقارنة، الطبعة الأولى، مركز بحوث شرطة الشارقة، الامارات العربية المتحدة، 2019، ص38

[3] -مسعودي سوسف،أرجيلوس رحاب، **مدى حجية التوقيع الالكتروني في التشريع الجزائري (دراسة على ضوء أحكام القانون 15-04)**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنغاست، العدد 11، سنة 2017، ص84

[4] -لالوش راضية، **أمن التوقيع الالكتروني**، رسالة ماجستير في القانون تخصص القانون الدولي للاعمال، جامعة مولود معمري تيزي وزو،2012، ص 37

الفرع الثالث : التمييز بين التوقيع الالكتروني والتوقيع التقليدي

لعلّ الاختلاف الرئيسي بين التوقيع التقليدي والتوقيع الإلكتروني يكمن في أن الأخير يُنشأ بالاعتماد على دعامات ووسائط الكترونية[1]. فبدون هذه الوسائط، يصبح ذلك مستحيلًا. كما يُنشأ التوقيع العادي على الورق، ويتبعه توقيع تقليدي، مكتوبًا كان أو بخط اليد. ما يميز التوقيع الإلكتروني عن التوقيع التقليدي هو أن الأخير غالبًا ما يُمثل بالتوقيع في بعض التشريعات، أو ببصمة أو ختم أو إصبع في تشريعات أخرى.

لا تُحدد التشريعات المتعلقة بالتوقيعات الإلكترونية شكلًا محددًا؛ فقد تكون حروفًا أو أرقامًا أو رموزًا أو إشارات أو أشكالًا أخرى، شريطة أن تسمح طريقة الإنشاء بتحديد هوية المُوقّع وتمييزه عن الآخرين. في هذه الحالة، لا يُمكن تصور توقيع ببصمة أو ختم في هذا النوع من التوقيعات، وهو التوقيع الإلكتروني.

يختلف التوقيع الإلكتروني عن التوقيع التقليدي في قدرته على استخلاص محتوى الوثيقة الإلكترونية وحمايتها من التعديل بالإضافة أو الحذف، وذلك بربطها بالتوقيع الإلكتروني، بحيث يتطلب أي تعديل لاحق توقيعًا جديدًا. كما يتميز التوقيع الإلكتروني بأنه يُضفي على الوثيقة صفة الوثيقة الأصلية، مما يجعلها دليلًا مُعدًّا مسبقًا للإثبات قبل نشوء أي نزاع بين الطرفين.

يرتبط التوقيع الكتابي أيضًا بمدى حرية الشخص في اختيار توقيعه وشكله، إذ قد يتخذه وسيلةً للتصديق على المستندات، أو يعتمد بصمة الإصبع، سواءً أكانت ختمًا أم إصبعًا - وفقًا لبعض التشريعات التي تُجيز إمكانية التوقيع باليد أو بالختم أو ببصمة الإصبع - دون الحاجة إلى ترخيص من أي جهة. بخلاف التوقيع الإلكتروني، إذ يجب استخدام تقنية آمنة تُمكّن من تحديد هوية المُوقّع، وضمان سلامة المستند من العبث أو التشويه. وهذا يتطلب تدخل طرف ثالث لضمان صحة التوقيع، وعند الضرورة، تحديد هوية صاحبه.[2]، يتم تنفيذ هذه المهمة من قبل أي كيان قانوني معتمد من قبل السلطة المختصة للموافقة على التوقيعات الإلكترونية.، ويُعرف بمقدمي خدمات المصادقة الإلكترونية المعتمدين. وهم وحدهم، وحصراً، مخولون بإصدار وتسليم شهادات إلكترونية آمنة، وتقديم الخدمات ذات الصلة، وفقاً للشروط المحددة في هذا القانون والنصوص الصادرة تنفيذاً له. وهذا يُظهر لنا مدى الفرق بين التوقيع الكتابي والتوقيع الإلكتروني، فالتوقيع الإلكتروني مصطلح تقني عام يشمل جميع الطرق التي تُمكّن الشخص من توقيع مستند إلكتروني. ويعود سبب تعدد هذه الطرق إلى الإجراءات المتبعة لإنشائه.[3]، وخاصة أنها مرتبطة بتطور وسائل الاتصال، وبالتالي فإن التوقيع الإلكتروني ليس صورة واحدة، بل صور متعددة.

---

[1] - ثروت عبد الحميد، **التوقيع الالكتروني « ماهيته- مخاطره، وكيفية مواجهتها مدى حجيته في الاثبات»**، المرجع سابق، ص52

[2]- ثروت عبد الحميد، ، نفس المرجع، ص52.

[3] - نبيل بوحميدي، **الثورة التقنية ومسوغات التعديلات القانونية "التوقيع الإلكتروني نموذجا"**، مجلة محاكمة، العدد 4، 2008ص 175.

ومنه يتضح أن التوقيع الالكتروني و إن كان لا يناظر التوقيع الخطي التقليدي من حيث الشكل إلا أنه يناظره من حيث الوظيفة والهدف و الحجية ويبقى الاختلاف الجوهري بينهما يكمن في الوسيلة المستخدمة[1].

الفرع الرابع: صور التوقيع الالكتروني وشروطه

تتخذ التوقيعات الإلكترونية أشكالاً عديدة اعتمادًا على الطريقة المستخدمة، وتختلف هذه الصور أيضًا في درجة الثقة[2] ومستوى الضمانات التي توفرها، وذلك وفقًا للإجراءات المتبعة لإصدارها وتأمينها، والتقنيات التي توفرها. ومما لا شك فيه ونظرا للتطور التكنولوجي فان هذه التقنيات هي الأخرى في تطور مستمر.

أولا: صور التوقيع الإلكتروني

1. التوقيع بالقلم الالكتروني Pen-Op

هذه الصورة من أكثر صور التوقيع الإلكتروني شيوعاً، يتم نقل التوقيع المكتوب بخط اليد على المستند إلى الملف الذي سيتم نقل المستند إليه باستخدام جهاز الماسح الضوئي[3](Scanner) وإيصال هذا التوقيع مع المحرر وإرساله مع المحرر إلى الشخص الآخر عبر الإنترنت.

تم تطوير هذه الصورة من التوقيع لاحقاً باستخدام قلم إلكتروني يمكنه الكتابة على شاشة الكومبيوتر عن طريق استخدام برنامج خاص بذلك يقوم بالتقاط التوقيع والتحقق من صحته، وقبوله إذا كان صحيحاً، ورفضه إذا كان غير ذلك.

هذه الطريقة تمتاز بالمرونة والسهولة[4] في الاستعمال مع ذلك، فإن إمكانية تحويل التوقيع التقليدي إلى صيغة إلكترونية قد تؤدي إلى فقدان الثقة، إذ يمكن للمتلقي الاحتفاظ بهذا التوقيع ولصقه على مستندات أخرى، كما فعل مع المستند المُرسِل. كما يستحيل ضمان أن المُوقِّع هو نفسه الموجود على المستند، إذ يمكن لأي شخص - إن حصل عليه بأي وسيلة - لصق هذا التوقيع على أي مستند وإرساله إلى من يشاء، مما يُضعف الثقة في المستندات الموقعة إلكترونيًا، وبالتالي يُقلل من صحة التوقيع الإلكتروني[5].

2. التوقيع باستخدام الخواص الذاتية Biometric Singature

يعتمد هذا النوع على الخصائص الكيميائية والطبيعية للأفراد[6]:

---

[1]- خالد ممدوح ابراهيم ، المرجع السابق، ص 248

[2] - ثروت عبد الحميد، ، المرجع السابق، ص54.

[3] - خالد ممدوح ابراهيم ، المرجع السابق، ص 255

[4] - ثروت عبد الحميد، المرجع سابق، ص54.

[5] - منير محمد الجنبيهي ،ممدوح الجنبيهي ،**تزوير التوقيع الإلكتروني**،دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2008،ص45

[6] - محمد عبيد الكعبي ،**الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة)**،دار النهضة العربية، القاهرة مصر،2009 ، ص292-293.

- البصمة الشخصية
- مسح العين البشرية
- التعرف على الوجه البشري
- خواص اليد البشرية
- التحقق من نبرة الصوت
- التوقيع الشخصي

عند استخدام أي من هذه الميزات، يتم أولاً الحصول على صورة للشكل وتخزينها في الكمبيوتر حتى يمكن الرجوع إليها عند الحاجة[1].

3. التوقيع الرقمي Signature numerique

ويقصد به منظومة بيانات في صورة شفرة بحيث يكون بإمكان المرسل اليه التأكد من مصدرها ومضمونها. واكثر هذه التوقيعات الرقمية شيوعا هي تلك التي تقوم على ترميز المفاتيح[2]،المفاتيح العمومية(Public Keys) ، والمفاتيح الخاصة (Private Keys).

تتيح المفاتيح العامة لأي شخص مهتم قراءة الرسالة دون الحاجة إلى إجراء أي تعديلات. إذا وافق على محتواها ورغب في قبولها، فإنه يوقعها باستخدام مفتاحه الخاص، ثم تُعاد إلى المُرسِل بتوقيعه[3].

4. التوقيع بالبطاقات الممغنطة (التوقيع بالرقم السري)

يعرف كذلك باسم التوقيع الكودي، ويعد أول شكل أبرزته التقنيات التكنولوجية للتوقيع الالكتروني وهو الاكثر شيوعا واستعمالا، وهذه الصورة من التوقيعات الالكترونية ابتكرتها التقنيات التي استعملت من أجل الاسراع في إنجاز المعاملات البنكية[4]، فهو غالبا ما يرتبط بالبطاقات البلاستيكية والبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة إلكترونية.

---

[1] -دهليس عادل، كاسحي موسى، **دوروأهمية التوقيع الالكتروني في تسهيل المعاملات التجارية والمالية**، مداخلة مقدمة في الملتقى الوطني حول الإصلاحات المالية والمصرفية –الواقع والمأمول- جامعة وهران 2 محمد بن أحمد، 2022

https://www.univ-emir-constantine.edu.dz/download/somairesemexterne/chaira-eco/moussa-kashi/moussa-kashi-oran.pdf

تاريخ الاطلاع 2025/05/03 على الساعة 20:27

[2] -منير الجنبهي، ممدوح الجنبهي، ، المرجع السابق، ص 142.

[3] - نفس المرجع، ص 142.

[4] - عيسى غسان ريضي، **القواعد الخاصة بالتوقيع الالكتروني**، الطبعة أولى، دار الثقافة للنشر والتوزيع، عمان، الاردن،2009، ص58

وتيسيرا لانعقاد العمليات التجارية والحصول على المال في أي وقت منحت البنوك بطاقات ائتمان ممغنطة مصحوبة برقم سري لعملائها، لا يعلمه الا صاحب البطاقة، حيث تستعمل هذه البطاقات كوسيلة لايداع أو سحب النقود أو لسداد ثمن السلع والخدمات فهذه البطاقات تتضمن على بيانات شخص ذاك الشخص إما صاحبها أو العميل، وتلك البيانات تكون موجودة في دائرة إلكترونية مغلقة مثبتة على البطاقة، يتم إدخال البطاقة داخل الصراف الالي، وحتى تؤدي هذا الدور كان لزاما إدخال البطاقة بالوضع السليم داخل الجهاز المخصص لتنفيذ العملية، ثم يقوم بإدخال رقمه الكودي الخاص، وفي الاخير يتم الضغط على الاختيار الخاص لانهاء العملية، فتعتبر كل هذه الاجراءات تعبيرا عن إرادة صاحبه برغبته في الالتزام بمحتوى العقد المبرم[1]

ثانيا: شروط التوقيع الإلكتروني[2]

يتضح من قراءة القانون 15-04 أن المشرع الجزائري قد عرّف نوعين من التوقيعات الإلكترونية: التوقيع الإلكتروني البسيط والتوقيع الإلكتروني الموصوف[3]. ووضع شروطًا محددة لكل نوع. أما النوع الأول، وهو التوقيع الإلكتروني البسيط، فلم يُعرّف تعريفًا دقيقًا، واقتصر على الإشارة إلى استخدامه كوسيلة لإثبات هوية المُوقّع، وله قوة ثبوتية لإثبات قبوله لمضمون الكتابة الإلكترونية، وفقًا للمادة 2 من القانون.

تجدر الإشارة إلى أن المشرع أعاد التأكيد على هذا الشرط في شروط التوقيع الإلكتروني الواردة في المادة 7 من القانون رقم 15-04، حيث اشترط أن يكون التوقيع الإلكتروني موصوفًا، وأن يرتبط بالموقع فقط، وأن يسمح بتحديد هويته. وبالتالي، فإن الشروط العامة التي يجب أن يستوفيها التوقيع الإلكتروني لإضفاء قيمة إثباتية عليه هي:

1. أن ينشأ على أساس شهادة تصديق الكتروني موصوفة

لضمان سلامة المعاملات الإلكترونية عمومًا، والمعاملات التجارية الإلكترونية خصوصًا، يُصادق على التوقيع الإلكتروني من قِبل جهة أو إدارة، عامة أو خاصة، مُخوّلة بالتحقق من صحة التوقيعات وإصدار شهادة تصديق، وذلك لمنع الغش أو التزوير. وقد نصّ المشرّع الجزائري على أن يُنشأ التوقيع

[1] - سعيد السيد قنديل، **التوقيع الإلكتروني: (ماهيته، صوره، حجيته في الإثبات بين التدويل و الاقتباس)**، الطبعة الثانية، دار الجامعة الجديد للنشر، مصر،2006،ص66

[2] - القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، سنة 2015

[3] -بولافة سامية،غيلاني الطاهر، **التوقيع الالكتروني في ظل القانون 15-04**، المجلة الجزائرية للامن الانساني، المجلد 5 العدد 01، جامعة باتنة 1 الجزائر،2020، ص120

الإلكتروني الموصوف بناءً على شهادة تصديق إلكتروني موصوفة[1]، صادرة عن جهة خارجية موثوقة أو عن مُقدّم خدمات التصديق الإلكتروني.

2. أن تمنح للموقع دون سواه

وتتحقق سيطرة الموقع على التوقيع الإلكتروني إذا استطاع التحكم في الوسيلة الإلكترونية التي تحتوي على ذلك التوقيع، بما يضمن أن يكون مالك التوقيع هو الوحيد الذي يملك السيطرة عليه، سواء أثناء التوقيع أو في استخدامه بأية طريقة[2].

3. أن يمكن من تحديد هوية الموقع

بحسب المادة 07 الفقرة 03 ، فإن الهدف الأساسي من التوقيع هو تحديد هوية شخص الموقع وتمييزها عن الغير، خاصة في ظل البيئة الرقمية التي تتميز بتعدد الوسائط الالكترونية، واعتمادها على شبكة الانترنيت بشكل عام، وحتى يقوم التوقيع الالكتروني بوظيفته في الإثبات ينبغي أن يكون دالا على شخصية صاحبه ومميزا عن غيره.[3]

4. أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني

وفقًا للمادة 7، الفقرة 4، تُعرّف آلية إنشاء التوقيع الإلكتروني بأنها برنامج حاسوبي أو جهاز مصمم لتنفيذ البيانات اللازمة لإنشاء توقيع إلكتروني. وقد عرّف المشرع الجزائري هذه الآلية في المادة 2، الفقرة 3، بأنها "جهاز حاسوبي أو برنامج مصمم لتنفيذ إنشاء توقيع إلكتروني". ويجب أن تكون هذه الآلية موثوقة وتفي بمتطلبات إضافية تعزز أمنها، وفقًا لمتطلبات القانون الجزائري. وتنص المادة 10 من قانون التوقيع والتصديق الإلكتروني على ما يلي:" **يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوفة آمنة.**[4]."

5. يتم إنشاؤه بوسائل تقع تحت السيطرة الحصرية للموقع

جاء في نص المادة 11 الفقرة 05،هذا الشرط يرتبط ارتباطا وثيقا بالشرط السابق الذي يوجب أن ترتبط معطيات التوقيع بالموقع وحده، فسيطرة [5]شخص واحد فقط على وسيلة إنشاء التوقيع يؤدي إلى أن تكون البيانات الناتجة عن هذه الوسيلة مرتبطة فقط بهذا الشخص وخاصة به، وتوجد عدة وسائل تمكن الموقع من ذلك، كاستعمال تقنية نظام التشفير " CRYPTOLOGIE " الذي يتميز

---

[1] - القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، السالف الذكر.

[2] -فطيمة الزهراء مصدق، **التصديق الالكتروني كوسيلة لحماية التوقيع الالكتروني**، مجلة الدراسات والبحوث القانونية، المجلد 5العدد01، جامعة محمد بوضياف المسيلة ، 2020، ص34

[3] -زكرياء مسعودي،جقريف الزهرة، التوقيع الالكتروني وحمايته لعملية الدفع الالكتروني، المجلة الدولية للبحوث القانونية والسياسية، جامعة الشهيد حمه لخضر الوادي، العدد 03، 2017،ص 166

[4] -حواس فتيحة، **التوقيع الالكتروني (الخصوصيات والتطبيقات)**، مجلة الدراسات القانونية المقارنة، المجلد 7 العدد01، جامعة حسيبة بن بوعلي الشلف الجزائر، 2021، ص2997

[5] -بودراع فايزة، بليمان يمينة، **القوة الثبوتية للتوقيع الالكتروني**، مجلة المعيار، المجلد 26 العدد (5 رت 67) ،جامعة قسنطينة، 2022، ص343

بأنه يوفر للرقابة الحصرية لصاحبه على توقيعه حيث يعتبر الأكثر استخداما نظرا لطابع الأمان والثقة التي يوفرهما[1].

6. أن يكون مرتبطا بالبيانات الخاصة به

حسب نص المادة11 الفقرة 05،من القانون 15-04 سالف الذكر ،بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات[2]، يهدف التوقيع الالكتروني إلى تأكيد الصلة بين صاحبه وبين المعلومات الواردة فيه، هذا يعني انه لابد أن يكون التوقيع متصلا اتصالا ماديا ومباشرا بالبيانات وبالمحرر حتى يكون دليلا على إقرار الموقع بما ورد في المحرر.[3]

المطلب الثاني: مفهوم التصديق الالكتروني

قد أثارت مشكلة التحقق من هوية المتعاقدين في التعاقد الإلكتروني وأهليتهم، أحد المعضلات التي تحول دون انتشار التعاملات بالمحررات الإلكترونية ورواجها بين الناس، ذلك أن عدم الثقة بين أطراف التعاقد، لا سيما في ظل التباعد المكاني بين الطرفين، أدى إلى ظهور تخوفات حول مدى سلامة الأشياء محل التعاقد من ناحية، وتخوفات أخرى بمدى أهلية المتعاقدين وقدرتهم على تحمل الوفاء بالالتزامات التي تنشأ عن هذه التعاقدات، وكما كان التوقيع الإلكتروني، أحد الوسائل الهامة لحل هذه المشكلات، إلا أن مشكلة عدم الثقة تبقى قائمة، ولعل ذلك هو ما جعل المشرع في العديد من التشريعات تتطلب في كثير من الأحيان، أن يتم توثيق التوقيع الإلكتروني نفسه من خلال جهات تصديق وتوثيق إلكتروني مختصة.

من خلال هذا المطلب الذي ارتأينا الى تقسيمه الى ثلاثة فروع الاول خاص بتعريف التصديق الالكتروني و الفرع الثاني تناولنا من خلاله الجهات المختصة بالتصديق الالكتروني و الفرع الثالث خاص بسلطات التصديق الالكتروني .

الفرع الأول: تعريف التصديق الالكتروني

المصادقة الإلكترونية هي "وسيلة تقنية آمنة للتحقق من صحة التوقيع الإلكتروني أو الوثيقة الإلكترونية، بحيث يمكن نسبها إلى شخص أو جهة محددة. تصدرها جهة موثوقة أو طرف محايد يُسمى مُقدم خدمات التصديق". وتُعرف أيضًا بأنها "مجموعة من العناصر أو االاشياء، حسب الغرض من المصادقة"[4].

---

[1] - لالوش راضية، **أمن التوقيع الالكتروني**، المرجع السابق،ص 39

[2] - لالوش راضية، **أمن التوقيع الالكتروني**، المرجع السابق،ص 37

[3] -فاطمة الزهراء تبوب، **التوقيع والتصديق الالكترونيين في ظل القانون رقم 15-04المؤرخ في أول فبراير** 2015، حوليات جامعة الجزائر 1، العدد 29، الجزء الثاني، الجزائر، 2016،ص317

[4] -حرشاو مفتاح، **التصديق الالكتروني ضمان لأمن المعاملات الالكترونية**، مجلة أبحاث ودراسات التنمية، المجلد 10 ، العدد 01،جامعة برج بوعريريج، ، 2023، ص232.

وُضع تعريف آخر: يشير التصديق أو التوثيق الإلكتروني إلى عملية التحقق من صحة المستندات والتوقيعات الإلكترونية. ويتولى هذه العملية طرف محايد، مستقل عن أطراف العقد الإلكتروني. ويمكن أن يكون هذا الطرف شخصًا طبيعيًا أو شركة أو كيانًا محددًا، ويُطلق عليه "مقدم خدمات التصديق" أو "جهة التصديق[1]".

تختلف تسمياتها من تشريع لآخر. دور الموثق أو المُصدِّق الإلكتروني هو توثيق معاملات الأفراد الإلكترونية، ومنحهم الثقة بوثائقهم لإثبات تصرفاتهم القانونية. وقد أُطلق عليهم اسم" وكلاء الإثبات."

وحتى نستطيع البحث عن المقصود بالتصديق الالكتروني فانه يجب أولا البحث عن التعريفات التي وضعتها القوانين ما تعلق بالتصديق الالكتروني أو بجهة التصديق الالكتروني[2]. سواء قانون الاونسترال (أولا) أو التشريع الأوروبي أو الفرنسي (ثانيا) والتشريعات العربية المصري (ثالثا) والجزائري (رابعا).

أولا: قانون الاونسترال النموذجي بشأن التجارة الالكترونية:

عند استقراء المادة 2 الفقرة (ه) من قانون الاونسترال يتضح أن القانون النموذجي لم يقدم تعريفا للتصديق الالكتروني بل ركز على جهة التصديق الالكتروني حيث عرف مقدم خدمات التصديق على وبدلاً من ذلك، ركزت على هيئة التصديق الإلكتروني، حيث حددت تعريفا لمزود خدمة التصديق على النحو التالي " **الشخص الذي يصدر الشهادات وقد يقدم خدمات أخرى متعلقة بالتوقيعات الإلكترونية.** "[3]

ثانيا: التوجه الأوروبي[4]

أما التوجيه الأوروبي 99-93 المتعلق بالتوقيعات الالكترونية ومن خلال المادة 02-10 فقد عرف[5] شهادة التصديق الالكتروني بأنها " شهادة الكترونية تربط بين بيانات التحقق من التوقيع الالكتروني الخاص بالموقع بما يثبت هويته بصورة قاطعة حيث تصدرها الجهة

---

[1] - إلياس ناصيف، **العقود الدولية العقد الإلكتروني في القانون المقارن**، الطبعة الاولى ، منشورات الحلبي الحقوقية، لبنان،2009، ص25 .

[2] - سامح عبد الواحد التهامي، **التعاقد عبر الانترنت دراسة مقارنة**، دار الكتب القانونية ، دار شتات للنشر و البرمجيات، مصر، 2008،ص 411.

[3] - قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية مع دليل الاشتراع 2001،

https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-elecsig-a.pdf تاريخ الاطلاع 2025/02/13 على الساعة 19:15

[4] - **تشريع وفق نظام القوانين في الاتحاد الأوروبي**

[5] -دحماني سمير،**دراسة مقارنة بين التوجه الاوروبي 93/99 المتعلق بالتوقيعات الالكترونية والقانون رقم 15-04المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين**، مجلة العلوم الانسانية ،العدد 01، المركز الجامعي تندوف، 2017، ص181

المسؤولة في الدولة ويوضح فيها أنه عند مراجعة السندات الالكترونية يحدد شخصية مصدره ويستوفي الشروط اللازمة للثقة فيه واداءه و لوظيفته.[1]

يُعرّف بعض القانونيين هيئات التصديق الإلكتروني بأنها شركات أو أفراد أو منظمات مستقلة ومحايدة تعمل كوسيط بين المستخدمين لتوثيق معاملاتهم الإلكترونية بإصدار شهادات التصديق اللازمة لهم. وتُسمى هذه الجهة مزود(مقدم) خدمات التصديق[2].

ثالثا: المشرع المصري

بالإشارة إلى القانون المصري الخاص بتنظيم التوقيع الالكتروني، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ،لم يحدد أي تعريف لجهة التصديق على التوقيع الإلكتروني[3]، إلا أن اللائحة التنفيذية لهذا القانون من خلال المادة 6/1 عرفت جهات التصديق على التوقيع الإلكتروني بأنها "الجهات المرخص لها بإصدار شهادة التصديق الالكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني"[4]

يترتب على تعريف هيئات التصديق الإلكتروني في اللائحة أن تقديم خدمات التصديق الإلكتروني يقتصر على الكيانات القانونية دون الأشخاص الطبيعيين، وذلك باستخدام مصطلح "الجهات"، دون الإشارة إلى إمكانية قيام أشخاص طبيعيين بهذه المهام، مما يحصر تقديم هذه الخدمات بالجهات القانونية دون الأشخاص الطبيعيين. علاوة على ذلك، لا يقتصر هذا التعريف على إصدار شهادات التصديق الإلكتروني، بل يوسع نطاق نشاطها ليشمل جميع الخدمات الأخرى المتعلقة بالتوقيعات الإلكترونية.

رابعا : المشرع الجزائري

المصادقة الإلكترونية، والمعروفة أيضًا بالمصادقة الرقمية أو التصديق الإلكتروني، هي عملية مصممة لضمان قانونية وسلامة وأمان المعلومات المنقولة أو المخزنة إلكترونيًا. تعتمد على استخدام مفاتيح التشفير (المفاتيح العامة والخاصة) لتأمين البيانات والمعاملات عبر الإنترنت. تُستخدم المصادقة الإلكترونية عادةً لضمان هوية الأطراف المشاركة في المعاملات الإلكترونية، ولضمان عدم تغيير البيانات أثناء النقل[5].

---

[1] - وسن قاسم الخفاجي وعلاء كاظم حسين, **الحجية القانونية لشهادات تصديق التوقيع الالكتروني** (دراسة مقارنة)، مجلة المحقق الحلي للعلوم القانونية والسياسية, ، العدد الرابع, السنة الثامنة, جامعة بابل العراق,2016 ص.296

[2] - إبراهيم خالد ممدوح ،**التوقيع الالكتروني** ،بدون طبعة ،الدار الجامعية ،الإسكندرية ،2010 ،ص 63.

[3]- خالد ممدوح ابراهيم، **إبرام العقد الالكتروني**، المرجع السابق، ص 251 .

[4] -آلاء أحمد محمد حاج علي، **التنظيم القانوني لجهات التصديق على التوقيع الالكتروني**، أطروحة ماجيستير تخصص قانون الخاص، جامعة النجاح الوطنية نابلس فلسطين، 2013، ص 58.

[5] - https://www.mpt.gov.dz/%d8%a7%d9%84%d8%aa%d9%88%d9%82%d9%8a%d8%b9-%d9%88%d8%a7%d9%84%d8%aa%d8%b5%d8%af%d9%8a%d9%82-%d8%a7%d9%84%d8%a7%d9%84%d9%83%d8%aa%d8%b1%d9%88%d9%86%d9%8a%d9%8a%d9%86/ تاريخ الاطلاع 2025/05/04 على الساعة 19:29

على المستوى الوطني، يخضع التصديق الإلكتروني للقانون رقم 15-04 الصادر في 11 ربيع الثاني 1436 الموافق 1 فبراير 2015، والذي يحدد القواعد العامة المتعلقة بالتوقيعات والتصديق الإلكتروني. وبموجب هذا القانون، يرتكز النظام الوطني للتصديق والتوقيع الإلكتروني على ثلاث هيئات متكاملة:

1. **السلطة الوطنية للتصديق الإلكتروني(ANCE)** : تحت سلطة الوزير الاول، تلعب الهيئة دوراً محورياً في تعزيز وتطوير استخدام التوقيعات والشهادات الإلكترونية وضمان موثوقيتها.
2. **السلطة الحكومية للتصديق الإلكتروني(AGCE)** : الخاضعة لإشراف وزير البريد والمواصالات السلكية واللاسلكية، مسؤولة عن مراقبة ومراقبة نشاط التصديق الإلكتروني لأطراف ثالثة موثوقة، فضلاً عن تقديم خدمات التصديق الإلكتروني لأصحاب المصلحة في الفرع الحكومي.
3. **السلطة الاقتصادية للتصديق الإلكتروني(AECE)** : التابعة لسلطة ضبط البريد والاتصالات الالكترونية(ARPCE) ، مسؤولة عن متابعة ومراقبة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لصالح الجمهور.

الهدف الرئيسي من هذا الهيكل لنظام التصديق الوطني والتوقيع الإلكتروني هو الحصول على الاعتراف الدولي، وضمان التوافق مع هيئات التصديق الأخرى في العالم.

الفرع الثاني: الجهات المختصة بالتصديق الالكتروني

الثقة والأمان هما جوهر الضمانات التي يسعى إليها العملاء، وهما أساسيان لازدهار وتطوير المعاملات الإلكترونية. تتم هذه المعاملات بين أطراف متباعدة جغرافيًا، وغالبًا ما لا يعرف بعضهم البعض. يتطلب هذا الوضع تطبيق ضمانات وآليات تقنية لتحديد هوية الأطراف والتحقق من حقيقة المعاملة ومضمونها. في هذه الحالة، يجب على طرف ثالث محايد وموثوق التحقق من صحة النية التعاقدية التي يعرب عنها الطرف الآخر، وجديتها، وخلوها من الغش والخداع. كما يجب عليه تحديد مضمونها بدقة، مما يسمح للعميل بالاعتماد عليها أثناء المعاملة، وإلزامه (سواءً كان شخصًا طبيعيًا أو اعتباريًا) بتوقيعه[1].

تتنوع مسميات الجهات المسؤولة عن تصديق التوقيعات الإلكترونية، بدءًا من سلطة التصديق وصولًا إلى مؤدي خدمات التصديق أو سلطة تصديق التوقيعات الإلكترونية. ويرى البعض أن مصطلح "الموثق الإلكتروني أو الكاتب العدل الالكتروني" هو الأكثر موثوقية، نظرًا لدوره كجهة تقنية محايدة. ، ومصادقته على المحررات الكتابية الاعتيادية سواء قام بإجراءات التوثيق أو الضمان،

[1] - عبد الفتاح بيومي حجازي ، **حماية المستهلك عبر شبكة الانترنت** ، دار الكتب القانونية ، مصر ، 2008 ، ص 102 .

وهذا يعادل تقريباً ضمانات الموثق الإلكتروني، خاصة فيما يتعلق باحتفاظ الموثق الإلكتروني بنسخة من الوثائق الإلكترونية وهوية أصحابها وبصماتهم الإلكترونية.[1].

فيما يتعلق بالموقف الفرنسي فنلاحظ أن المشرع عرف جهة التصديق الالكتروني "بمقدم خدمة التصديق :- كل شخص يقدم شهادات التصديق أو خدمات أخرى متعلقة التوقيع الالكتروني[2] " .
لكي تعمل هيئة التصديق الإلكتروني، يجب عليها الحصول على ترخيص من الجهة المُحددة قانونًا. ووفقًا لقانون التوقيعات والمعاملات الإلكترونية العراقي، فإن الجهة المُصدرة للترخيص هي الشركة العامة لخدمات شبكات المعلومات الدولية التابعة لوزارة الاتصالات. وقد حددت المادة السادسة من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012[3] مهام هذه الشركة، والتي تنص على أن تلتزم الشركة بما يلي[4]:

1. منح التراخيص لإصدار شهادات التصديق بعد اعتمادها من الوزير، وفقًا للقانون.
2. تحديد المعايير الفنية لأنظمة التوقيع الإلكتروني وتحديد مواصفاتها الفنية.
3. مراقبة أداء الجهات العامة في إصدار شهادات التصديق وتقييم أدائها.
4. النظر في الشكاوى المتعلقة بأنشطة التوقيع الإلكتروني وتصديق الشهادات والمعاملات الإلكترونية، واتخاذ القرارات المناسبة بشأنها وفقًا للقانون.
5. تقديم المشورة الفنية للجهات العاملة في مجال التوقيع الإلكتروني وتصديق الشهادات.
6. تنظيم دورات تدريبية للمتخصصين في مجال التوقيع الإلكتروني وتصديق الشهادات، وتنظيم ندوات ومؤتمرات حول هذا الموضوع.

كما اشترط المشرع على الشركة عند مزاولة نشاط منح الترخيص بإصدار شهادة التصديق توافر عدة شروط أدرجها في المادة (8) [5] من قانون التوقيع الإلكتروني والمعاملات الإلكترونية حيث نصت

---

[1] - عباس العبودي ، **تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها** ، الطبعة الاولى ،منشورات الحلبي الحقوقية ، بيروت – لبنان ، 2010 ، ص 230.

[2] - المادة (1 / 11) من المرسوم رقم 272 لسنة 2001 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000404810/ تاريخ الاطلاع 2025/04/18 على الساعة 18:29

[3] - https://maryco.net/wp-content/uploads/2022/07/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%B1%D9%82%D9%85-78-%D9%84%D8%B3%D9%86%D8%A9-2012.pdf تاريخ الاطلاع 2025/06/07 على الساعة 21:29

[4] - نجلاء عبد حسن، عبد الرسول عبد الرضا، **تطور موقف المشرع العراقي في قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012**، مجلة العلوم الإنسانية،العدد 2، جامعة بابل ،العراق،2013، ص347

[5] -المادة 8 من المرسوم 272 لسنة 2001 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000404810/ تاريخ الاطلاع 2025/04/18 على الساعة 18:29.

هذه المادة على: "يجب على الشركة عند منح الترخيص لمزاولة نشاط إصدار شهادة التصديق أن تراعي الشروط الآتية:

1. ضمان المنافسة والشفافية في اختيار حامل الترخيص.
2. تحديد مدة مناسبة لسريان الترخيص .
3. تحديد وسائل الرقابة والمتابعة الفنية والمالية لضمان حسن أداء الجهات المعتمدة.
4. لا يجوز التوقف عن ممارسة النشاط المرخص له أو الاندماج مع جهات أخرى أو تحويل الترخيص كلياً أو جزئياً إلى طرف ثالث خلال مدة سريانه إلا بعد الحصول على موافقة الشركة ووفقاً للقانون.
5. ويجب أن يتمتع حاملها بالمؤهلات البشرية والمادية اللازمة لممارسة مهنة التصديق على التوقيع الإلكتروني.
6. تقديم ضمانات لسداد الغرامات والتعويضات أو الالتزامات المالية الأخرى، على أن يستمر هذا الضمان ساريًا طوال مدة الترخيص.
7. أن يكون لديه مقر عمل ثابت ومعروف لمزاولة النشاط المتعلق بالترخيص.
8. تأكيد من الجهات المختصة بعدم وجود عوائق أمنية تحول دون إصدار الترخيص.

أما بالنسبة لموقف المشرع الفرنسي، فقد اعتمد المبدأ المنصوص عليه في المادة (2/3) من التوجيه الأوروبي رقم 93 لسنة 1999 بشأن التوقيعات الإلكترونية، والذي يُلزم الدول الأعضاء بعدم فرض قيود على إنشاء جهات التصديق أو اشتراط الحصول على ترخيص مسبق. وطبقًا لهذا المبدأ، فإن نشاط إصدار شهادات التصديق الإلكترونية حر، حيث يحق لأي جهة ممارسة هذا النشاط دون الحاجة إلى الحصول على ترخيص مسبق من السلطات الفرنسية. وقد كرس المشرع الفرنسي هذا المبدأ في المرسوم رقم 272 لسنة 2001. ومن ناحية أخرى، فقد سمح التوجيه الأوروبي المذكور للدول الأعضاء بإنشاء أنظمة اعتماد وهيئات تصديق إلكترونية. وبالفعل، أنشأ المشرع الفرنسي نظامًا لاعتماد جهات التصديق، إلا أن هذا النظام طوعي، مما يعني أن لجهة التصديق الإلكتروني الحق في ممارسة أنشطتها دون الحاجة إلى الحصول على اعتماد من الجهة التي تنشئها الدولة. في المقابل، يحق لها تقديم طلب اعتماد، شريطة استيفائها للشروط المنصوص عليها في القانون. مع ذلك، تجدر الإشارة إلى أن الواقع العملي يفرض على جهات التصديق تقديم طلب اعتماد. في الواقع، ينص القانون الفرنسي على أنه لكي يكون التوقيع الإلكتروني صحيحًا، يجب التحقق من صحته باستخدام شهادة تصديق إلكترونية معتمدة (أي صادرة عن جهة معتمدة). لذلك، يربط القانون الفرنسي صحة التوقيع الإلكتروني باعتماد جهة التصديق[1] .

[1] - سامح عبد الواحد التهامي، **التعاقد عبر الانترنت**، دار الكتب القانونية، مصر، 2009 ، ص416،417.

أما عن موقف المشرع المصري فنلاحظ أنه أوكل مهمة منح إصدار شهادات التصديق الإلكتروني إلى هيئة تنمية صناعة تكنولوجيا المعلومات وحدد اختصاصاتها في المادة الرابعة من قانون التوقيع الإلكتروني المصري.[1] .

يُشار إلى أن المشرع المصري لم يُشر إلى مهام جهات التصديق الإلكتروني في قانون التوقيع الإلكتروني أو لائحته التنفيذية، بل تركها لهيئة صناعة تكنولوجيا المعلومات، التي أدرجتها في الترخيص رقم 2006/103 الصادر عنها، والذي مُنح بموجبه تراخيص لجهات التصديق الإلكتروني لمزاولة نشاطها بتقديم خدمات التوقيع الإلكتروني. وقد حددت المادة 45 من الترخيص مجموعة من الخدمات التي يجب على جهة التصديق تقديمها، ولا يجوز تقديم خدمات أخرى إلا بإذن كتابي مسبق من الهيئة. وتتمثل هذه الخدمات في تسجيل وإصدار شهادات التصديق الإلكتروني، بالإضافة إلى توفير أدوات إنشاء وتثبيت التوقيعات الإلكترونية.

مما سبق، نلاحظ أن الهيئة فرضت على جهة التصديق توفير أدوات لإنشاء وتثبيت التوقيعات الإلكترونية. وتتمثل هذه الخدمة في إصدار البطاقة الذكية وجهاز القراءة. وتُعرّف المادة (15/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري البطاقة الذكية بأنها "وسيلة إلكترونية آمنة تُستخدم لإنشاء وتثبيت التوقيع الإلكتروني على مستند إلكتروني. وتحتوي على شريحة إلكترونية مزودة بمعالج وعناصر تخزين وبرنامج تشغيل. وتشمل بطاقات ذكية وشرائح إلكترونية منفصلة أو متشابهة، تتيح أداء الوظائف المطلوبة وفقًا للمعايير الفنية المحددة في هذه اللائحة".[2]

من جانب المشرع الجزائري، تم اعتماد مصطلح "مقدم خدمات التصديق الإلكتروني" لأول مرة في المرسوم التنفيذي رقم 07-162 المؤرخ 30 مايو 2007، المتعلق بأنواع الشبكات والاتصالات السلكية واللاسلكية[3] ، حيث تم تعريفه في نص المادة 3 على النحو التالي: "كل شخص وفقًا للمادة 8-8 من القانون رقم 2000-03 المؤرخ 5 أغسطس 2000، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، والذي يصدر شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيعات الإلكترونية".

---

[1] -كبير آمنة، **التصديق الالكتروني (دراسة مقارنة)**، مجلة القانون و المجتمع، العدد 6، جامعة أحمد درارية ،ادرار،2018، ص155،131.

[2] -قرار رقم 109 لسنة 2005 بتاريخ 2005/5/15 بإصدار اللائحة التنفيذية لقانون التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

[3] - المرسوم التنفيذي رقم 07-162 المؤرخ في 30ماي 2007،يعدل ويتمم المرسوم التنفيذي رقم 01-123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشيكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية والاسلكية، الجريدة الرسمية ، العدد 37، سنة 2007

فيما يتعلق بالمادة 8-8 من القانون رقم 2000-03 المؤرخ 5 أغسطس 2000، الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية ، استخدم المشرع الجزائري مصطلح "مزود-موفر- الخدمة"، حيث عرفه على أنه: "كل شخص طبيعي أو معنوي يقدم خدمات باستخدام وسائل المواصلات السلكية واللاسلكية [1] ".

يُعرَّف مزود الخدمة في المادة 2 من القانون 09-04، الذي يتضمن قواعد خاصة للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال ومكافحتها، على أنه: "كل كيان عام أو خاص يوفر لمستخدمي خدماته إمكانية الاتصال عبر نظام معلومات و/أو نظام اتصالات - وكل كيان آخر يقوم بمعالجة أو تخزين البيانات المعلوماتية لصالح خدمة الاتصال المذكورة أو مستخدميها"[2].

وفقًا للمادة 2 من القانون رقم 15-04 المؤرخ 1 فبراير 2015 بشأن النظام العام للتوقيعات والشهادات الإلكترونية، عرّف المشرع الجزائري "مقدم خدمات التصديق الإلكتروني" على النحو التالي: "الشخص الطبيعي أو المعنوي الذي يصدر شهادات التصديق الإلكتروني المقررة ويمكنه تقديم خدمات أخرى في مجال التصديق الإلكتروني". بهذا التعريف، تناول المشرع الجزائري لأول مرة شهادة التصديق الإلكتروني المقررة، المحددة في المادة 15 من القانون المذكور.

كما حدد المشرع الجزائري شروط وكيفية ممارسة نشاط التصديق الإلكتروني في المواد من 33 إلى 40 من القانون رقم 15-04 بشأن التوقيعات والشهادات الإلكترونية، ولا سيما شروط ممارسة نشاط تقديم خدمات التصديق الإلكتروني، وكذلك إجراءات الحصول على الموافقة الصادرة عن الهيئة الاقتصادية للتصديق الإلكتروني.

الفرع الثالث: سلطات التصديق الالكتروني

نظّم المشرّع الجزائري هيئات التصديق الإلكتروني في الفصل الثاني من الباب الثالث من القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق 1 فبراير 2015[3]، والذي يُحدّد القواعد العامة المتعلقة بالتوقيعات والتصديق الإلكتروني. كما منح هذه الهيئة صلاحية مراجعة التراخيص ومنحها وتجديدها وسحبها وإلغائها. وتتمثّل هذه الهيئات، أولاً، بالهيئة الوطنية للتصديق الإلكتروني، وثانياً بالهيئة الحكومية للتصديق الإلكتروني، وثالثاً بالهيئة الاقتصادية للتصديق الإلكتروني.

أولا: السلطة الوطنية للتصديق الالكتروني

تتضمن المواد من 16 إلى 25 من القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 (الموافق 1 فبراير 2015)، الذي يحدد القواعد العامة للتوقيعات والتصديق الإلكتروني، أحكام هذه السلطة.

---

[1] - المادة 8-8 من القانون 2000-03 ،السالف الذكر.

[2] - القانون رقم 09-04 المؤرخ في 05 أغسطس 2009: المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية، العدد07 المؤرخة في 2009/08/16

[3] - القانون رقم 15-04 ، سالف الذكر.

ووفقًا للمادة 16، الفقرة 1، فإن الهيئة الوطنية للتصديق الإلكتروني هي سلطة إدارية تتمتع بالشخصية المعنوية والذمة المالية المستقلة. وهي تخضع لسلطة الوزير الاول، وتتولى مسؤولية الترويج والترقية للتوقيعات والتصديق الإلكتروني واستخدامهما، وتطويرهما، وضمان موثوقيتهما. وهذا ما نصت عليه المادة 18، الفقرة 1، من القانون 15-04. كما تضطلع الهيئة الوطنية للتصديق الإلكتروني بعدة مهام، وفقًا للمادة 18، الفقرة 1، من القانون 15-04، منها:

- - وضع سياسات التصديق الإلكتروني وضمان تنفيذها؛
- - إقرار سياسات التصديق الإلكتروني الصادرة عن الجهات الحكومية والاقتصادية؛
- إبرام اتفاقيات الاعتراف المتبادل الدولي؛
- اقتراح مشاريع أولية للنصوص التشريعية أو التنظيمية المتعلقة بالتوقيعات الإلكترونية أو التصديق الإلكتروني على الوزير الأول؛

إجراء عمليات تدقيق على الجهات الحكومية والاقتصادية بشأن التصديق الإلكتروني، من خلال هيئة التدقيق الحكومية

وبالإضافة إلى هذه المهام، نلاحظ أن المشرع قد عهد إلى الهيئة الوطنية للتصديق الإلكتروني بمهمة استشارية، حيث يتم استشارتها أثناء إعداد أي مشروع نص تشريعي أو تنظيمي يتعلق بالتوقيع أو التصديق الإلكتروني.

ثانيا: السلطات الحكومية للتصديق الالكتروني [1]

تخضع هذه الهيئة لإشراف الوزير المسؤول عن البريد وتكنولوجيا المعلومات والاتصالات. وتتمتع بالشخصية القانونية والاستقلال المالي، وفقًا للمادة 26 من القانون رقم 15-04 المتعلق بالقواعد العامة المتعلقة بالتوقيعات والتصديق الإلكتروني.

ووفقًا للمادة 28، الفقرة 1، من القانون رقم 15-04، تُشرف هيئة التصديق الإلكتروني الحكومية على أنشطة التصديق الإلكتروني للجهات الخارجية الموثوقة وتُراقبها، وتُقدم خدمات التصديق الإلكتروني للجهات الحكومية.

وبناءً على ذلك، وفي السياق نفسه، تُنفذ هذه الهيئة، وفقًا لنص المادة 28، الفقرة 2، من القانون رقم 15-04، المهام التالية[2]:

[1] - موقع وزارة البريد والمواصلات السلكية واللاسلكية الجزائرية ، HTTPS://WWW.AGCE.DZ/AR/PRESENTATION-DE-LAGCE/ تاريخ الاطلاع 18-05-2025 على الساعة 00:44

[2] - القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سالف الذكر.

- وضع سياسة التصديق الإلكتروني الخاصة بها، ورفعها إلى الهيئة للموافقة عليها، وضمان تنفيذها؛
- اعتماد سياسات التصديق الإلكتروني الصادرة عن جهات خارجية موثوقة، وضمان تنفيذها؛
- الاحتفاظ بشهادات التصديق الإلكتروني منتهية الصلاحية، والبيانات المتعلقة بإصدارها من قبل الجهة الخارجية الموثوقة، لإحالتها إلى الجهات القضائية المختصة عند الاقتضاء؛
- نشر شهادة التصديق الإلكتروني للمفتاح العام الخاصة بالهيئة؛
- تزويد الهيئة، بشكل دوري أو بناءً على طلبها، بجميع المعلومات المتعلقة بنشاط التصديق الإلكتروني؛
- إجراء عمليات تدقيق على الجهة الخارجية الموثوقة، من خلال الجهة الحكومية المسؤولة عن التدقيق، وفقًا لسياسات التصديق.

ثالثا: السلطة الاقتصادية للتصديق الالكتروني[1]

هذه هي السلطة الثالثة التي ينظمها المشرع الجزائري في المادتين 29 و30 من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيعات والتصديقات الإلكترونية. وتتمثل أحكام هذه السلطة فيما يلي: عُيّنت السلطة المسؤولة عن تنظيم البريد والاتصالات السلكية واللاسلكية جهةً اقتصاديةً للتصديق الإلكتروني، وذلك وفقًا للمادة 29 من القانون رقم 15-04.

وقد أوكل إليها المشرع الجزائري مهمة مراقبة ومراقبة مقدمي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لعملائهم، وذلك وفقًا للمادة 90، الفقرة 1، من القانون رقم 15-04.

ولأداء هذه المهمة، تمارس المهام التالية، وفقًا للمادة 30، الفقرة 2[2]

- وضع سياسة التصديق الإلكتروني الخاصة بها، ورفعها إلى الهيئة لاعتمادها، وضمان تنفيذها؛
- منح التراخيص لمقدمي خدمات التصديق الإلكتروني بعد اعتمادها من الهيئة؛
- اعتماد سياسات التصديق الصادرة عن مقدمي خدمات التصديق الإلكتروني، وضمان تنفيذها؛

[1] - موقع وزارة البريد والمواصلات السلكية واللاسلكية الجزائرية، HTTPS://AECE.DZ/AR/A_PROPOS/ تاريخ الاطلاع 2025/05/18 على الساعة 00:51

[2] - القانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، سالف الذكر.

- الاحتفاظ بشهادات التصديق الإلكتروني منتهية الصلاحية، والبيانات المتعلقة بإصدارها من مقدمي خدمات التصديق الإلكتروني، لإحالتها إلى الجهات القضائية المختصة عند الاقتضاء؛
- نشر شهادات التصديق الإلكتروني[1] ذات المفتاح العام الصادرة عن الهيئة؛
- اتخاذ التدابير اللازمة لضمان استمرارية الخدمة في حال عدم تمكن مقدم خدمات التصديق الإلكتروني من تقديم خدماته؛
- تزويد الهيئة، دوريًا أو بناءً على طلبها، بأي معلومات تتعلق بأنشطة التصديق الإلكتروني؛
- التحقق من امتثال طالبي الاعتماد لسياسة التصديق الإلكتروني، سواءً شخصيًا أو من خلال مكاتب تدقيق معتمدة؛
- ضمان المنافسة الفعالة والعادلة باتخاذ جميع التدابير اللازمة لتعزيز أو استعادة المنافسة بين مقدمي خدمات التصديق الإلكتروني؛
- طلب أي وثيقة أو معلومات من مقدمي خدمات التصديق الإلكتروني أو أي طرف مهتم تفيد الهيئة في أداء مهامها؛
- إعداد المواصفات التي تحدد الشروط العامة لتقديم خدمات التصديق الإلكتروني، وتقديمها إلى الهيئة للموافقة عليها؛
- القيام بجميع أعمال المراقبة وفقًا لسياسة التصديق الإلكتروني والمواصفات التي تحدد الشروط العامة لتقديم خدمات التصديق الإلكتروني؛
- نشر التقارير والإحصاءات العامة، وإعداد تقرير سنوي يصف أنشطتها، مع الالتزام بمبدأ السرية.

بالإضافة إلى هذه الوظائف، فإن هيئة التصديق الاقتصادي الإلكتروني مسؤولة عن الإبلاغ إلى النيابة العامة عن أي فعل إجرامي تكتشفه أثناء ممارسة وظائفها.

[1] موقع -سلطة ضبط البريد و الاتصالات الالكترونية، https://www.arpce.dz/ar/about تاريخ الاطلاع 2025/04/18 الساعة 19:45

المبحث الثاني: الجرائم الماسة بالتوقيع الالكتروني

اكتسبت الجريمة بُعدًا جديدًا، متأثرةً بالعوامل الاقتصادية والصناعية التي شهدها العالم، لا سيما مع ظهور الحاسوب والإنترنت. ونتيجةً لذلك، تطوّر مفهوم الجريمة من مفهوم تقليدي وخطير إلى مفهوم معلوماتي أكثر خطورة. لذا، يُعتبر تزوير التوقيعات الإلكترونية جريمة معلوماتية، وقد توسّع ليشمل التزوير التقليدي المتأثر بالتكنولوجيا، سنحاول تقديم مفهوم لجرائم التوقيع الالكتروني من خلال **(المطلب الاول)**، **والانشطة محل جرائم التوقيع الالكتروني والجزاء المترتب عن قيامها من خلال (المطلب الثاني).**

المطلب الأول: مفهوم جرائم التوقيع الإلكتروني

التوقيع الإلكتروني وانطلاقا من أنه مجموعة من البيانات في شكل إلكتروني، فإنه توجد خطورة الاعتداء عليه بجرائم تأخذ أشكالا وصورا متعددة، ونظرا لهذه الخطورة وضعت مختلف التشريعات الدولية والوطنية وسائل حماية جنائية للتوقيع الإلكتروني. حيث اعتمدنا في هذا المطلب على إعطاء تعريف لجرائم التوقيع الالكتروني في **(الفرع الاول)** وخصائص هذا النوع من الجرائم في **(الفرع الثاني)**.

الفرع الأول: تعريف الجرائم الواقعة على التوقيع الالكتروني

يتطلب النشاط أو السلوك البدني في الجرائم الإلكترونية بيئة رقمية واتصالاً بالإنترنت. كما يلزم معرفة بداية هذا النشاط ونهايته، بالإضافة إلى نتائجه. على سبيل المثال، يُجهّز مرتكب الجريمة جهاز الكمبيوتر لارتكاب الجريمة، إما بتثبيت برامج اختراق أو إعدادها بنفسه. وقد يُنشئ وينشر صفحات تحتوي على مواد مُخلة بالآداب العامة. وقد يُرتكب أيضًا جريمة إعداد فيروسات للتوزيع. لا تتطلب جميع الجرائم أعمالًا تحضيرية، ويصعب تمييز هذا العمل عن بداية النشاط الإجرامي في جرائم الحاسوب والإنترنت.[1]

تُشبه الجريمة الإلكترونية الجريمة التقليدية من حيث عناصرها: المجرم ذو الدافع، والضحية، سواءً كانت مادية أو معنوية، والأداة المستخدمة. في الجريمة الإلكترونية، تُعدّ الأداة نتاجًا للتكنولوجيا، وكذلك مسرح الجريمة، الذي يسهل على الجاني الوصول إليه، مما يُسهّل عملية الجريمة الإلكترونية. في العديد من هذه الجرائم، تُرتكب الجريمة عن بُعد، باستخدام خطوط وشبكات اتصال بين الجاني ومسرح الجريمة"[2]

[1] - حسنين شفيق، **الإعلام الجديد والجريمة الإلكترونية**، الطبعة الاولى، دار فكر وفن للطباعة و النشر والتوزيع ،مدينة السادس من أكتوبر 2015، ص 215-216.

[2] - حسنين شفيق ، نفس المرجع ، ص 201.

الفرع الثاني: خصائص الجرائم الواقعة على التوقيع الالكتروني

وتعتبر الجرائم ضد التوقيعات الإلكترونية جزءاً من الجرائم الإلكتروني و التي تتميز بخصائص تجعلها مختلفة عن الجريمة الواقعة على التوقيع العادي بحكم البيئة الافتراضية التي تتم فيها، والوسائل التي يرتكب بها هذا النوع من الجرائم، مما يجعل هذه الاخيرة تتميز بطبيعة مختلفة عن الجريمة الواقعة على التوقيع العادي، إن هذه الخصائص والمتمثلة في :

أولا : ترتكب من مجرم غير تقليدي:

حيث يمتاز المجرم بمهارات تقنية عالية[1]،وخبرة فنية عالية حتى ان المحقق العادي يجد صعوبة في كشفها.

ثانيا: صعوبة اكتشاف الجرائم الواقعة على التوقيع الإلكتروني :

حيث توصف الجرائم الإلكترونية بأنها خفية[2] ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة،

ثالثا: الجرائم الواقعة على التوقيع الالكتروني جريمة ناعمة ومغرية للمجرمين

في حين أن الجرائم التقليدية، كالقتل والاغتصاب، غالبًا ما تتطلب جهدًا بدنيًا، فإن الجرائم الإلكترونية لا تتطلب ذلك. بل تعتمد على بصيرة فكرية وتفكير متأنٍّ، قائم على إتقان تكنولوجيا الحاسوب. ولا تتطلب أي درجة من القرب أو التلامس الجسدي بين الجاني والضحية، وبالتالي فهي أقل عنفًا ووحشية من الجرائم التقليدية.[3]

رابعا: تعتبر الجرائم الواقعة على التوقيع الالكتروني من الجرائم العابرة للحدود

لقد أدت قدرة تكنولوجيا المعلومات على تقصير المسافات وتعزيز الاتصالات بين مختلف أنحاء العالم إلى التأمل في طبيعة الأعمال الإجرامية، حيث يستخدم المجرمون هذه التقنيات لخرق القانون، بمعنى أن مسرح الجريمة الإلكترونية لم يعد محلياً بل أصبح عالمياً[4].

---

[1] - خالد حسن أحمد لطفي. **الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية**. دار الفكر الجامعي، الاسكندرية: سنة 2020، ص36.

[2] -نعيمة دوادي، **الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)**، مجلة معهد اللغات، العدد01،جامعة حسيبة بن بوعلي الشلف، الجزائر، سنة 2020، ص 48.

[3]- أدهم باسم نمر بغدادي، **وسائل البحث والتحري عن الجرائم الإلكترونية**، ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص:11-12.

https://repository.najah.edu/server/api/core/bitstreams/93d6f55d-024e-4b67-bc6f-5ca764bca2a0/content تاريخ الاطلاع 2025/05/03 على الساعة 21:04

[4] -محمد خليفة، **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**،مجلة دراسات و أبحات، العدد 01، جامعة زيان عاشور الجلفة، 2009، ص370.

خامسا: الجرائم الواقعة على التوقيع الالكتروني فادحة الاضرار:

أكدت دراسات الشركة العالمية المتخصصة في تقنيات حماية وآمن المعلومات " إنتل سكيور يتي" أن الخسائر التي كبدتها الجرائم الإلكترونية ضخمة، لاسيما أن الاعتماد على الحاسب الآلي في مختلف مجالات الحياة[1].

المطلب الثاني: الأنشطة محل جرائم التوقيع الالكتروني والجزاء المترتب عن قيامها

إن الانشطة التي تندرج ضمن جرائم التوقيع الالكتروني والتي تشمل مجموعة من الافعال و التصرفات غير المشروعة والتي تستهدف التوقيع الالكتروني بغرض استخدامه لغرض اجرامي، حيث تمثل هذه الانشطة صورا لمختلف وابرز الجرائم التي يمكن ارتكابها. قسمنا هذا المطلب الى فرعين **الأول** خصصناه لأشكال الجرائم المتصلة بالتوقيع الالكتروني و **الفرع الثاني** الجزاءات المترتبة على قيام جرام التوقيع الإلكتروني

الفرع الأول: صور الجرائم المتصلة بالتوقيع الالكتروني

من خلال هذا الفرع سوف نتناول أشكال (صور) الجرائم المتصلة بالتوقيع الالكتروني، والتي من بينها –على سبيل المثال لا الحصر- الدخول والبقاء غير المصرح به الى قاعدة بيانات تتعلق بالتوقيع الالكتروني ، الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية (النصب)، جريمة اتلاف التوقيع الالكتروني، و جريمة تزوير التوقيع الالكتروني

أولا: الدخول والبقاء غير المصرح به الى قاعدة بيانات تتعلق بالتوقيع الالكتروني

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

اكتسبت الجريمة بُعدًا جديدًا، متأثرةً بالعوامل الاقتصادية والصناعية التي شهدها العالم، لا سيما مع ظهور الحاسوب والإنترنت. ونتيجةً لذلك، تطوّر مفهوم الجريمة من مفهوم تقليدي وخطير إلى مفهوم معلوماتي أكثر خطورة. لذا، يُعتبر تزوير التوقيعات الإلكترونية جريمة معلوماتية، وقد توسّع ليشمل التزوير التقليدي المتأثر بالتكنولوجيا.

يستفاد من هذه المادة أنّه يقصد بجريمة الدخول غير المصرح به الدخول غير المشروع – وهو ما عبّر عنه المشرع بالغش – إلى منظومة المعالجة الآلية للمعطيات، أي أن يكون الدخول إلى نظام

[1] -محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري والمقارن**، درا الجامعة الجديدة، الاسكندرية،2007، ص79

المعلومات بدون وجه حق، فمناط عدم المشروعية هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك.

ومن الحالات التي يكون الدخول غير مصرح به في النظام المعلوماتي، دخول الفاعل إلى النظام دون تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له .

1 الركن المادي

يتكون الركن المادي لهذه الجريمة" من نشاط إجرامي يتمثل في فعل الدخول(للدخول معنيان، أحدهما مادي كالدخول مثلا إلى محل أو غرفة معينة و آخر معنوي و هو المقصود في هذه الحالة.) غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه أو البقاء غير المصرح به"[1]، و"دائما ما يثار التساؤل بشأن هذا الفعل وكيف يمكن تحديد ما إذا كان الفعل الذي ارتكبه الجاني هو ذاته الفعل المؤثم قانونا؟".

جريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني فإنه" لقيام هذه الجريمة لابد وأن الركن المادي المتمثّل في الدخول غير المشروع قد وقع على أنظمة معلوماتية أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني"، كما أن هذه الجريمة تّصنّف من جرائم الخطر، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه".[2]

ويقصد به التواجد داخل نظام المواقع الالكترونية ضد إرادة من له الحق في السيطرة على هذا النظام , وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ لكن المتدخل لم ينسحب و بقي رغم ذلك . فيعاقب في هذه الحالة على جريمة البقاء غير المشروع إذا توافر ركنها المعنوي.[3]

---

[1] - صالح شنين ،**الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة**، أطروحة دكتوراه، تخصص القانون الخاص،.جامعة تلمسان ،2013، ص72.

[2]-علي عبد القادر قهوجي ،**الحماية الجنائية لبرامج الكمبيوتر**، المكتبة القانونية، القاهرة،سنة ،1999 ص.133

[3] - فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري** ،بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا،ليبيا،أكتوبر،2009.

https://docs.google.com/viewerng/viewer?url=https://ebook.univeyes.com/?download_books%3D43202-445b500d608a82d57fa9d2cc2152b3c3&hl=ar تاريخ الاطلاع 2025/05/03 الساعة 21:13

ويعتبر البقاء أيضا جريمة في الحالة التي يستمر فيها الجاني داخل النظام بعد المدة المحددة له للبقاء داخله , أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها برؤيتها والاطلاع عليها فقط.[1]

وقد يجتمع الدخول مع البقاء غير المصرح بهما معا، وذلك في الحالة التي لا يكون فيها للجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك , وقد ثار تساؤل بين الفقه فيما إذا كان فعل الدخول غير المشروع إلى لنظام المعلوماتي أو البقاء فيه بدون إذن يشكل تعدد مادي للجرائم أم أنه جريمة واحدة ذهب البعض إلى القول بأننا أمام جريمة واحدة , لان الجاني قصد بالدخول البقاء داخل. النظام , بينما ذهب البعض الآخر إلى تحقق الاجتماع المادي بين الجريمتين وهو الراجح في التشريع الجزائري على حسب ما نصت عليه المادة 394 مكرر من قانون العقوبات[2].

2 الركن المعنوي

جريمة الدخول أو البقاء داخل مواقع التجارة الالكترونية جريمة عمدية لابد فيها من توافر القصد الجنائي بعنصريه العلم والارادة , فيلزم أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء في مواقع التجارة الالكترونية , وأن يعلم أنه ليس له الحق في الدخول إلى الموقع أو البقاء فيه. [3]

ومن ثمة فلا يتوافر القصد الجنائي إذا كان دخول الجاني داخل النظام مسموح به أي مشروع أو إذا وقع في خطأ كأن يجهل وجود حظر للدخول أو البقاء، ويكفي فيها توافر القصد الجنائي العام، ولا يشترط أيضا توافر قصد جنائي خاص.

3 العقوبة

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

فقد جاء في المادة السادسة من الفصل الثاني من القانون العربي النموذجي الموحد[4] لمكافحة جرائم إساءة استعمال أنظمة تقنية المعلومات على" أن كل من توصّل بطريق غير مشروع لإختراق نظام

---

[1] - سي مرابط زينب، غلام الله بنت الشيخ، **الحماية القانونية للعقد المبرم عبر الانترنت**، مذكرة ماستر في الحقوق تخصص علاقات مهنية، جامعة ابن خلدون تيارت، 2017، ص63.

[2] -فليح نور الدين ،**الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، جامعة مولاي الطاهر سعيدة، 2019،ص27.

[3] -إيمان بغدادي، **أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية**، مجلة آفاق للبحوث والدراسات، العدد الرابع، المركز الجامعي إليزي، جوان 2019،ص186.

[4] -الاتفاقية العربية الموحدة لمكافحة جرائم تقنية المعلومات، https://esttf.motrans.gov.iq/wp-content/uploads/2016/04/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D9%80%D8%A7%D9%82%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-

المعالجة الآلية للبيانات، يعاقب بالحبس والغرامة (تترك لتقدير لكل دولة)، وإذا نتج عن هذا الفعل محو أو تعديل البيانات المخزنة بالحاسب الآلي أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غيره من الأساليب المعلوماتية، تكون عقوبته الحبس الذي لا تزيد مدته (تترك لتقدير لكل دولة) والغ ارمة (تترك لتقدير لكل دولة)...

كما تضيف المادة نفسها: إذا ضُبط الشخص داخل نظام المعالجة الآلية للبيانات دون وجه حق يعاقب بالحبس والغرامة (تترك لتقدير كل دولة)، وإذا ترتب على الفعل انتهاك لسرية البيانات المخزنة بالحاسب يعاقب بالحبس الذي لا تقل مدته عن (تترك لتقدير كل دولة)، والغ ارمة (تترك لتقدير كل دولة).

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

حيث نصّت هذه المادة على« عقاب الدخول أو البقاء بطريقة ما كليا أو جزئيا داخل نظام لمعالجة المعلومات، يعاقب بالحبس الذي لا يقل عن شهرين والغرامة التي لا تزيد عن خمسين ألف يورو أو بإحدى العقوبتين، وإذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل في المعطيات المخزنة في النظام سواءً بالإتلاف أو غيره تكون العقوبة الحبس الذي لا يقل عن شهرين ولا يزيد عن سنتين، والغ ارمة التي لا تقل عن عشرة آلاف يورو ولا تزيد عن مائة ألف يورو» [1]

كما نصت المادة 394 مكرر من قانون العقوبات الجزائري[2] على أنه "يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أ يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

وعليه تقوم جريمة الدخول أو البقاء داخل النظام من خلال نص المادة 394 مكرر من ق ع شأنها في ذلك شأن أي جريمة أخرى، على ركن مادي وآخر معنوي.

من خلال ما سبق نستخلص أن مختلف التشريعات تعتبر الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني جريمةً يعاقب عليها القانون كونها تشتمل على فعل الدخول غير المرخّص لشخص الجاني، وبقائه في نظام المعلومات بشكل غير مشروع من جهة، وقد يحصل وأن ينتج عن هذا الدخول غير المشروع إلى إتلاف بيانات نظام المعلومات أو تحريفها أو سرقتها، مما يتسبب إما في

%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf تاريخ الاطلاع 2025/04/21 على الساعة 22:48

[1] -ياسمينة كواشي، **الحماية الجنائية للتوقيع والتصديق الالكترونيين في ظل القانون**، مذكرة ماستر تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، 2017، ص54.

[2] - القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية رقم 71، سنة 2004.

تعطيل هذا النظام عن تأدية وظائفه، أو في إلحاق ضرر بصاحب هذه البيانات سواءً كان شخصا طبيعيا أو معنويا.

نلاحظ أنّ المشرع الجزائري جرّم مجرّد الدخول أو البقاء غير المشروع داخل النظام المعلوماتي حتى ولو لم ينجم عن هذا الفعل ضرر بالنظام المعلوماتي، وشدّد العقوبة إذا ترتب على جريمة الدخول والبقاء غير المصرح بهما حذف أو تغيير لمعطيات المنظومة.

ثانيا: الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية (النصب)

بعد الوقوف على جريمة الدخول غير المشروع لقاعدة بيانات تتعلق بالتوقيع الإلكتروني، هناك جريمة أخرى لا تقل خطورة عن هذه الأخيرة متمثلة في الحصول على التوقيع الإلكتروني بالطرق والوسائل الاحتيالية.

حيث يعد "الاحتيال في مجال نظم معلومات التوقيع الإلكتروني من أخطر الجرائم التي يمكن أن تقع على التوقيع الإلكتروني وتسبب خسائر اقتصادية فادحة، نظرا للتطور المذهل في مجال التعامل واختزان التوقيعات الإلكترونية في حاسبات آلية موصولة بشبكة الأنترنيت"[1].

1 الركن المادي:

يتمثّل الركن المادي لجريمة الاحتيال الإلكتروني في: "التلاعب [2]في معلومات وبيانات لها قيمة مالية بطرق احتيالية، قد لا تكون محصورة تماشيا مع طبيعة الاحتيال المعلوماتي، فالجريمة المعلوماتية بصفة عامة جريمة متطورة ومتجددة لارتباطها بتكنولوجيا المعلومات".

ولدراسة أعمق للركن المادي في جرائم الاحتيال وهو من الجرائم ذات النتيجة لدا يتكون عنصرها المادي من ثلاث عناصر السلوك، النتيجة والعلاقة السببية[3]

سلوك احتيالي (الاجرامي): يتمثل في ارسال رسائل مزيفة عبر البريد الالكتروني او الرسائل النصية أو أي وسيلة الكترونية ،عادة تتضمن الرسائل روابط أو مستندات مزيفة تطلب توقيع الضحية الكترونيا[4].

- **الوسائل الاحتيالية:**

[1] - ياسمينة كواشي، **الحماية الجنائية للتوقيع والتصديق الالكترونيين في ظل القانون**، المرجع السابق، ص 54

[2] -بشان عبد النور، **الجوانب الموضوعية لمعالجة الجريمة المعلوماتية**، أطروحة دكتوراه، تخصص قانون جنائي والعلوم الجنائية، جامعة الجزائر 1 ،2018،ص 163.

[3] -عبد القادر عميمر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (مقارنة دراسة**)، تخصص قانون جنائي، أطروحة دكتوراه، جامعة الجزائر 1 ،2020،ص 111. والعلوم الجنائية،

[4] -بن عزة محمد حمزة، **حماية المستهلك الالكتروني من مخاطر البريد الدعائي (دراسة مقارنة)**،مجلة المنار للبحوث والدراسات القانونية والسياسية، العدد03،جامعة عمر الثليجي الاغواط، ا 2003، ص258.

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

وعلى أساس هذا الخلاف الفقهي، تنوعت الوسائل الاحتيالية[1] المستخدمة من قبل مرتكبي الجرائم المعلوماتية بتطور استخدامات الحواسيب، كما يمكن أن تقع جريمة الاحتيال في بيئة التوقيع الإلكتروني "باتخاذ اسم كاذب أو صفة غير صحيحة ومن ذلك الدخول إلى نظام معلومات التوقيع الإلكتروني باستخدام أسماء وشفرات مستخدميه الشرعيين بقصد الاستيلاء على التوقيعات، ومن ثم الأموال"

- **النتيجة الجرمية:**

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

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

- **العلاقة السببية**

لا يكفي لقيام جريمة الاحتيال التامة أن يصدر من الجاني فعل الاحتيال، وأن يسلم المجني عليه الشيء المملوك له إلى هذا الجاني، بل يلزم أن تتوفر صلة ما بين فعل الاحتيال وتسليم الشيء المملوك وأن يكون الثاني ثمرة أو نتيجة للأول"، بمعنى لابد من توافر علاقة سببية ما بين فعل الاحتيال وفعل التسليم[2].

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

---

[1] -براهمي حنان، **جريمة التزوير الوثيقة الإدارية الرسمية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه، تخصص قانون جنائي، جامعة محمد خيضر بسكرة،2015، ص250.

[2] -نائل طه ،**جريمة الاحتيال (دراسة مقارنة)**، أطروحة ماجستير، تخصص قانون عام، جامعة النجاح الوطنية، نابلس، فلسطين،2008، ص57.

https://repository.najah.edu/server/api/core/bitstreams/2445285c-21ff-4103-bc7a-443e3c74ebb1/content تاريخ الاطلاع 2025/05/03 على الساعة 21:16

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

2 الركن المعنوي

باعتبار الاحتيال في مجال التوقيع الإلكتروني جريمة عمدية[1] فهو يستلزم توافر القصد الجنائي بنوعيه أي القصد العام والقصد الخاص.

- يقوم القصد الجنائي العام على عنصريْ العلم والارادة[2] ،"إذ ينبغي أن يعلم الجاني أن التوقيعات الإلكترونية التي يستولي عليها مملوكة للغير بأنها مملوكة للمجني عليه أو لغيره، كما ورد بالمذكرة التفسيرية للاتفاقية الأوروبية لمكافحة جرائم المعلوماتية[3] بشأن المادة (8/ب) أن الجريمة يجب أن تُرتكب عمدا، ويتمثّل العنصر العام للقصد في التلاعب أو التدخل المعلوماتي الذي يسبّب ضرار ماديا للغير".
- يقوم القصد الخاص في جريمة الاحتيال[4] "اتجاه نية الجاني إلى تملك الشيء الذي تسلمه من المجني عليه، ويباشر مظاهر السيطرة التي ينطوي عليها حق الملكية وأن يحرم المجني عليه من مباشرتها، ولنية التملك في الاحتيال ذات مدلولها في جريمة السرقة، فإذا لم تتوافر لدى الجاني نية تملك الشيء الذي تسلمه فإن القصد الخاص لا يتوافر لديه"

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

إذا في إطار معلومات التوقيع الإلكتروني، فإنه "يجب أن تتجه إرادة الجاني إلى تحقيق ربح غير مشروع له أو لغيره، وهو ما فسرته المذكرة التفسيرية لاتفاقية بودابست الموقعة في 23 -11 -2001 بأن جريمة الاحتيال في مجال المعلومات تتطلب بالإضافة للقصد العام قصدا خاصا يتمثل في نية

---

[1] - نائل طه ،جريمة الاحتيال (دراسة مفارنة)،نفس المرجع،ص14.

[2] -معاشي سميرة، **آليات مكافحة الجريمة المعلوماتية (دراسة مقارنة)**،أطروحة دكتوراه تخصص قانون أعمال،جامعة محمد خيضر بسكرة،2020، ص154.

[3] -[1]المجلس الاوروبي، **اتفاقية بشأن الجرائم الالكترونية**، رقم 185، https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf تاريخ الاطلاع 2025/04/22

[4] -عبد المهيمن بكر، **قانون العقوبات القسم الخاص**، دار النهضة العربية، القاهرة، 1974، ص840.

الغش أو نية الغش خاصة، أو بتعبير آخر نية غير آمنة أو غير شريفة بغرض الحصول على منفعة اقتصادية لشخص الجاني أو لغيره".

3 العقوبة

تعاقب المادة 394 مكرر 2 من ق ع ج على هذه الجريمة بالحبس من شهرين إلى03 سنوات وبالغرامة من مليون (1000000) إلى خمسة ملايين (5000000) دينار جزائري.

كما يعاقب عليها بالعقوبة التكميلية المقررة على كل الجرائم السابقة.

ثالثا: جريمة اتلاف التوقيع الالكتروني

يمكن تعريف الإتلاف الإلكتروني بأنه: "إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواءً استيلاء على أموال أو إطلاع على معلومات، ولكن إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته"

وعرف جانب من الفقه الإتلاف على أنه: "محو المعلومات أو البرامج كليةً أو تدميرها إلكترونيا أو أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال.

ويعرّف إتلاف التوقيع الإلكتروني بأنه: "استخدام أي من الوسائل التكنولوجية أو البرامج لإحداث تعديل أو محو أو تدمير لنظم معلومات التوقيع الإلكتروني أو أي من مكوناتها المنطقية للإضرار بالمؤسسة أو الشخص صاحب التوقيع الإلكتروني بقصد جعل النظام المعلوماتي غير صالح للاستخدام.

1 الركن المادي:

يتمثّل الركن المادي لهذه الجريمة "في الأفعال المادية التي يتكون منها السلوك المجرّم، وهذه الأفعال تتمثّل في إتلاف أو تعييب التوقيع الإلكتروني ويتحقق فعل الإتلاف بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني قدرته على العمل عن طريق نشر فيروس معلوماتي أو سكب سائل على الوسيط الإلكتروني المحفوظ عليه ،ويحدث تعييب التوقيع الإلكتروني كذلك بذات الوسيلة على نحو يفقده القدرة على العمل أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوها أو غير واضح"

وقد "يقع الإتلاف على المعلومات المنسوخة على شرائط أو دعامات[1]، وقد يقع أيضا على المكوّنات المادية والأجهزة المستخدمة في عمل التوقيع الإلكتروني مثل شاشات العرض والأشرطة والأسطوانات والكابلات والمفاتيح و الاقراص الممغنطة، وغيرها من المكونات المادية سواءً كانت تحوي بيانات أو برامج أو مجرد أوعية فارغة، بشرط أن يؤدي الإتلاف أو التخريب إلى التقليل من قيمتها الاقتصادية أو يؤدي إلى تعطيلها أو عدم صلاحيتها للاستخدام"

[1] -رامي حليم، **جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات**، مجلة دراسات وأبحات، جامعة زيان عاشور الجلفة، العدد 01، 2009، ص339.

ويتطلب لقيام هذه الجريمة "ضرو رة توافر الضرر، فالضرر هو النتيجة الاجرامية الناتجة عن الاعتداء وترتبط بالفعل برابطة سببية قانونية حال توافر أركان الجريمة، ويستوي أن يكون الضرر ضرار ماديا أو معنويا".

كما أن "العقاب على الجريمة هو عقاب على السلوك والقصد الاجرامي وليس على مدى الضرر المتحقق من هذا السلوك"

2 الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصرْيْه العلم والإ اردة ،"يتمثل الأول في علم مرتكب الواقعة (الجاني) بأن فعل الإتلاف أو التعييب للتوقيع الإلكتروني محظور ومعاقب عليه قانونا، وأن تتجه إ اردته للفعل المجرّم، أما إذا كان الإتلاف أو التعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه، فلا تقوم هذه الجريمة"

مع الإشارة إلى أن "هذه الجريمة لا تتطلب قصدا جنائيا خاصا، وإنما يكفي وجود القصد الجنائي العام بعنصريه الإ اردة والعلم، فتقوم بذلك الجريمة بتوافر الركن المادي والقصد الجنائي العام"

العقوبة

نصت المادة 394 مكرر 1 من قانون العقوبات على التوالي يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000دج إلى 2000000دج كلّ من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أ ازل أو عدّل بطريق الغش المعطيات التي يتضمنها".

يتبن من هذه المادة أن المشرع الجزائري حصر في الاولى صور الاعتداء على المعطيات في ثلاثة صور تتمثل في إدخال معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها آليا، ومحو و إزالة معطيات كانت موجودة، أو تعديل وتغيير المعطيات واستبدلها بأخرى من خلال برامج معيّنة تعمل على إتلاف ال معطيات. إذن، يعد مقترفا لجريمة الاعتداء على المعطيات كلّ من ارتكب أحد صور الاعتداء السابقة. وهي جريمة مستقلة عن جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة، لأنه يمكن حصول الاعتداء عن بعد دون الدّخول أو البقاء في النّظام عن طريق استخدام برامج الفيروسات.

رابعا: جريمة تزوير التوقيع الالكتروني

يعرف التزوير لغةً على أنه "إصلاح الكلام وتهيئته، وهي كلمة مشتقة من الزور ويعني الكذب والباطل فيقال كلام مزور ومموه بالكذب، أما في الفقه فيعرف على أنه كل وسيلة يستعملها شخص ليغش بها آخر.

أما التزوير قانونا فهو"عملية مادية وصورة من صور الكذب التي يقوم بها الشخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو رسمي بإحدى الطرق المحددة في القانون، ومن شأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الإدعاء بالتزوير.

والتزوير في مجال الأنظمة المعلوماتية، يعرف على أنه: "التلاعب في المعلومات المخزّنة في أجهزة الحاسب المرتبطة بالشبكة أو اعتراض المعلومات بقصد تحريفها وتزويرها.[1]

أما في إطار جرائم الاعتداء على التوقيع الإلكتروني، فقد عرّفه قانون التوقيع الإلكتروني المصري رقم 51 لسنة 2004 على أنه: "تغيير الحقيقة في محرر أو توقيع أو وسيط إلكتروني بإحدى الطرق التي حددها قانون العقوبات، مما يؤدي للإضرار بالغير بنية استعماله فيما زوّر من أجله.[2]

عرف الفقه التزوير الإلكتروني (المعلوماتي) بأنه: تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها كما عرفه بأنه: تغيير الحقيقة بأي وسيلة كانت سواءً كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة

وعرف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلي لعام 1994 في مقرراته وتوصياته بشأن جرائم الكومبيوتر والتزوير الإلكتروني بأنه: "المجرى الطبيعي لمعالجة البيانات التي ترتكب باستخدام الكومبيوتر، وتعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني[3]"

كما عُرّف التزوير المعلوماتي بأنه: »تغيير الحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب

كما عُرّف التزوير المعلوماتي بأنه: »تغيير الحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب

يعني الإتلاف: »تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كليا أو جزئيا

بالنسبة للمشرع الجزائر لم يحدد تعريفا لجريمة تزوير التوقيع الالكتروني ، هذا لا يمنع من أنه يمكن استنتاج موقف المشرع بالرجوع الى النصوص المتعلقة بالتزوير بشكل عام.

---

[1] -رابحي أحسن، **الجريمة الالكترونية:النقطة المظلمة بالنسبة للتكنولوجية المعلوماتية**، مجلة العلوم القانونية الاقتصادية والسياسية، العدد 01 ، جامعة الجزائر، سنة 2011

[2] -رامي بن الصديق، **تزوير المحررات الإلكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07 العدد02 ، جامعة تنغاست، سنة 2018 ص200

[3] - ليندة شرابشة، **السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية**، مجلة دراسات وابحاث، العدد 1، جامعة زيان عاشور الجلفة، 2009، ص245

وفقًا للقانون رقم 24-02 المؤرخ في 26 فبراير 2024 المتعلق بمكافحة التزوير واستعمال المزور[1] ، يُعرف التزوير بأنه :"كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون، بأي وسيلة، من شأنه إحداث ضرر، ويهدف أو من شأنه أن يترتب عليه إقرار حق أو صفة أو واقعة ترتب آثارًا قانونية ". ويشمل هذا التعريف التزوير في المحررات الإلكترونية، بما في ذلك التوقيع الإلكتروني .

العقوبات المقررة لتزوير المحررات الإلكترونية، كما نصت المادة 31 من نفس القانون على العقوبات المقررة لتزوير المحررات العمومية أو الرسمية، والتي تشمل : السجن من 10 إلى 20 سنة. غرامة من 1.000.000 دج إلى 2.000.000 دج .

حيث تنطبق هذه العقوبات على من ارتكب تزويرًا في المحررات الإلكترونية الرسمية أو العمومية، بما في ذلك التوقيع الإلكتروني .

الفرع الثاني: الجزاءات المترتبة على قيام جرائم التوقيع الإلكتروني

إن الجرائم المتصلة بالتوقيع الالكتروني تعد من الجرائم الالكترونية الحديثة والتي يترتب عليها آثار قانونية و تقنية واقتصادية و أمنية بالغة الخطورة

أولا : عقوبات مطبقة على شخص طبيعي

لقد أورد المشرع الجزائري جملة من الجزاءات على الشخص الطبيعي والتي تختلف باختلاف الفعل المرتكب.

حيث اقر المشرع عقوبات تكميلية التي تطبق على كافة صور المساس بأنظمة المعالجة الآلية للمعطيات[2] وهي العقوبات المنصوص عليها بالمادة 394 مكررة على النحو التالي مع الاحتفاظ بحقوق الغير حسن النية بحكم مصادرة أجهزة والب ارمج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة

على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت يعلم مالكها ومن نص هذه المادة يمكن حصر العقوبات التكميلية في:

1- المصادرة : كما عرفتها المادة 15 فقرتها الأولى من قانون العقوبات هي: الأيلولة النهائية إلى الدولة المال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء وتشمل المصادرة فيما يتعلق بهذه الجرائم أجهزة والب ارمج والوسائل المستعملة في ارتكاب الجريمة مع مراعاة حقوق الغير حسن النية، ولا تكون المصادرة بالنسبة لهذه الجرائم عقوبة وجوبية. المادة 394 مكرر 2 ،ف 2 ، من الأمر66- 156 ، السابق الذكر.

[1] - القانون رقم 24-02 المؤرخ في 16 شعبان 1445 الموافق ل26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور. الجريدة الرسمية ، العدد 15،سنة 2024

[2] - غنية باطلي، **الجريمة الالكترونية، دراسة مقارنة**، الدار الجزائرية للنشر والتوزيع، االجزائر،2015، ص 221

2- **إغلاق الموقع** :يتعلق الأمر بالواقع التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

3- **إغلاق المحل أو مكان الاستغلال** شرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي سمح من خلاله بالدخول عبر المصرح به لمختلف الأنظمة وسمح بالتلاعب بالمعطيات مثل مقاهي الانترنت وهنا وجب التأكد واثبات ركن العلم لدى الأخير اذ يمكن أن يكون غير مرتكب الجريمة وعليه لا تطبق عليه العقوبة التكميلية بعد إدانة الجاني وبالنسبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من ق ع ج، وعليه يمكن أن تكون مؤيدة أو مؤقتة .[2]

وفيما يخص العقوبات التكميلية الخاصة بالجريمة التزوير للمثل في حرمان مرتكب التزوير من تولي بعض الوظائف وغيرها من العقوبات المذكورة في المادة 394 مكرر ومكرر1 من الأمر66-156 المتضمن قانون العقوبات المعدل والمتمم، أما فيما يخص تطبيق عقوبة المصادرة على هذا النوع من الجرائم فتتم بالمصادرة الأجهزة التي استعملت في ارتكاب جريمة التزوير كجهاز الحاسب الآلي وغيره من المعدات المستعملة في الجريمة أو كانت معدة للاستعمال وذا ما ذكرته المادة 394 مكرر.

ثانيا: عقوبات مطبقة على شخص معنوي

نص المشرع الجزائري على مسألة الشخص المعنوي وتطبيق عقوبات خاصة به تطبيقا التوصية الواردة بالمادة 12 والتي نصت على وجوب أن يسال الشخص المعنوي عن هذه الجرائم سواء بصفه فاعلا أصليا أو شريكا أو متدخلا، كما يسال عن الجريمة العامة أو الشروع فيها شرط أن تكون الجريمة في ارتكبت الحساب الشخص المعنوي وبواسطة أحد أعضائه أو ممثليها.

1. **العقوبات الأصلية**

أخذ المشرع الجزائري بمبدأ مسؤولية الشخص المعنوي عامة مستقلة عن مسؤولية الشخص الطبيعي بعد تعديل قانون العقوبات بموجب القانون 06-23 المؤرخ في 2006/12/20 في المادة 18 مكرر، والتي تنص فيها على العقوبات المطبقة على الشخص المعنوي فيما يخص الجنايات والجنح وهي كالآتي[3]:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.

---

[1] - غنية باطلي، نفس المرجع، ص 222

[2] - فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري** ،بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا،ليبيا،أكتوبر،2009.

https://docs.google.com/viewerng/viewer?url=https://ebook.univeyes.com/?download_books%3D43202-445b500d608a82d57fa9d2cc2152b3c3&hl=ar تاريخ الاطلاع 2025/05/03 الساعة 21:13

[3] - قرفي ادريس، **الجزاءات الجنائية الموقعة على الشخص المعنوي**، مجلة الحقوق والعلوم الانسانية، جامعة زيان عاشور الجلفة، العدد 06، 2010، ص151.

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر المدة 5 سن وات.
- مصادره الشيء المستعمل في ارتكاب الجريمة.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.
- وبالنسبة للعقوبات المطبقة على الشخص المعنوي في حال ارتكابه أحد الجرائم الماسة أنظمة المعالجة الآلية للمعطيات فقد نصت عليها المادة 394 مكرر4 من ق ع ج على النحو الآتي :
- يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغ ارمة تعادل خمس مرات الحد الأقصى للغ ارمة المقررة لشخص الطبيعي.
- ويشترط تبعا لذلك التقرير مسؤولية الشخص المعنوي ثلاث شروط:
- يشترط في الشخص المعنوي أن يكون عاما أو خاصا باستثناء الدولة.
- يجب أن ترتكب الجريمة لصالح الشخص المعنوي.
- يجب أن ترتكب الجريمة من طرف أجهزة أو ممثل الشخص المعنوي دون أن تؤثر على مسؤولية الشخص الطبيعي[1] بالإضافة إلى هاته العقوبات هناك عقوبات أخرى مقررة في حالة الاعتداء على الجهات العامة والتي نصت عليها المادة 394 مكرر3 من ق ع ج والتي تنص تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق العقوبات أشد[2].

2. العقوبات التكميلية

وهي نفس العقوبات التكميلية المطبقة على الشخص الطبيعي والمنصوص عليها بالمادة 394 مكرر المطبقة على الشخص الطبيعي، مع الاحتفاظ بحقوق الغير حسن النية [3]بحكم بمصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة فقد ارتكبت بعلم مالك كما أنه لابد من الإشارة إلى عقوبة الشروع والاشت ارك في الجريمة الالكترونية

[1] -مزاولي محمد، **المسؤولية الجنائية للأشخاص المعنوية عن الجر ائم الالكترونية في القانون الجز ائري**، العدد 01، مجلة دراسات وابحاث، جامعة الجلفة، 2009، 279.

[2] -ترجمان نسيمة، **الحماية الجنائية للتوقيع الالكتروني، دراسة مقارنة**، أطروحة دكتوراه، تخصص التجريم في قانون الاعمال، جامعة ابن خلدون تيارت،2021، ص95 .

[3] -المادة 394 مكرر 6 من القانون رقم 04-15 ،سالف الذكر.

باعتبار أن المشرع يعاقب على الاشت ارك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة في عقوبة الجريمة الأشد.[1] وفق المادة 394 مكرر5 من قانون العقوبات نصت على شروط للعقاب على **الاتفاق الجنائي** وهي كالأتي:

- مجموعة أو اتفاق.
- يهدف لتحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.
- القصد الجنائي.

من خلال استقراء المادة السابقة فان المشرع لم يخرج عن القواعد العامة لمعاقبة الشريك، حيث رصد لها نفس عقوبة الفاعل الأصلي، لك ان ج ارئم الاعتداء على نظم المعالجة الآلية المعطيات عليها لتم في شكل جماعات، وان كان لم يسبق اتفاق بينها على ارتكاب هذه الجريمة، ولكن نتيجة الجريمة من اتفاق ضمني بين أفراد المجموعة، إلا أن هذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص لآخر وان لم يكن هناك بينهما معرفة سابقة، كما يستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية.

أما عن **عقوبة الشروع** فقد نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع في المادة 394 مكرر 7 من قانون العقوبات يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة لجنحة ذاته[2].

مما سبق يمكن القول أن الجرائم الواقعة على التوقيع الالكتروني تتميز بخصوصية أنها صعبة الكشف عن التحايل والغش الذي وقع فيها ، حيث تستعمل فيها أساليب تقنية دقيقة مقارنة بتزوير التوقيع التقليدي وتتميز هذه الجرائم كذالك بتعدد صورها، وبذلك فالمشرع الجزائري

---

[1] -امال قارة ، **الجريمة المعلوماتية**، رسالة ماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر،2012، ص 131 .

[2] - فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجز ائري** ،بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا،ليبيا،أكتوبر،2009.

https://docs.google.com/viewerng/viewer?url=https://ebook.univeyes.com/?download_books%3D43202-445b500d608a82d57fa9d2cc2152b3c3&hl=ar تاريخ الاطلاع 2025/05/03 الساعة 21:13

أصدر قوانين صارمة في حق الشخص الطبيعي أو المعنوي لردعهم على ارتكاب الجرائم الماسة بالتوقيع الالكتروني ومختلف الالكترونية الالكترونية .

في نهاية هذا الفصل، نخلص إلى أن القانون الجزائري قد أقرّ تنظيم التوقيعات الإلكترونية، واشترط مجموعة من الشروط القانونية لضمان صحة التوقيع الإلكتروني. أهمها أن يُصمّم باستخدام آلية إنشاء آمنة خاصة بالتوقيع الإلكتروني الموصوف، وأن يكون التوقيع مرتبطًا بالموقع دون غيره.

وله خصائص التي يتميز بها باعتباره يقوم على دعامة الكترونية، أما عن صوره فقد تعددت واختلفت باختلاف وسائل إنشائه، وبالنسبة للمشرع الجزائري فقد حدد صورتين أطلق عليهما التوقيع الالكتروني الموصوف والتوقيع الالكتروني غير المؤمن.

وينص القانون أيضاً على أن آلية إنشاء التوقيع الإلكتروني يجب أن تتضمن الوسائل التقنية الكفيلة بحماية التوقيع من أي اعتداء أو تزوير، وحماية البيانات المرتبطة بالتوقيع الإلكتروني، مع ضمان سريتها بكل الوسائل المتاحة

كما اعتبر المشرع أن التوقيع الالكتروني الموصوف مماثلا للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي، إضافة إلى أن التمسك بالتوقيع الالكتروني البسيط يعد مقبولا أمام القضاء كوسيلة إثبات.

كما تم تسليط الضوء في هذا الفصل على جهات التصديق الالكتروني التي تم استحداثها بموجب القانون رقم 05-14، باعتبارها الطرف الثالث المحايد، فقمنا ببيان مفهومها، مهامها، ومسؤولياتها، فهي تمثل حلقة الوصل بين المتعاملين الكترونيا الذين يبرمون تعاملاتهم على أساس الثقة والأمان التي توفرها هذه الجهات عبر الانترنت في بيئة الكترونية لمنة للتعامل، فضلا على شهادة التصديق والتعرف على بياناتها وأنواعها، إضافة إلى الحماية القانونية للتوقيع الالكتروني.

و من خلال تعداد مختلف الجرائم الواقعة على التوقيع الالكتروني في ضوء قانون العقوبات والوقوف على صور الحماية الجزائية الخاصة في قانون15 -04 للتوقيع و التصديق الالكترونيين ومن ثم تعداد هذه الجرائم في ظل التشريع الجزائري الذي تصدى لحماية التوقيع الالكتروني في أول الأمر من خلال قانون العقوبات، وفي مرحلة لاحقة في قانون خاص للتوقيع والتصديق الالكترونيين، ويشكل توفير المشرع الجزائري لوسائل الحماية الجزائية للتوقيع والتصديق الالكترونيين في قانون خاص بهما ،توجها نحو مسايرة التغيرات التي تشهدها بيئة التعاملات الالكترونية على الصعيد الدولي والعمل على خلق بيئة إلكترونية آمنة وموثوقة تعزيزا لاستعمال الوسائل التكنولوجية المعاصرة وتوجيهها نحو المساهمة الفعالة في ترقية التجارة الالكترونية، لكن بالرغم مما جاء به قانون 15-04حول التوقيع والتصديق الالكترونيين فهو لا يخلو حسب عدة قانونيين وباحثين من بعض السلبيات .حيث تقول عزيزة لرقط (2017) في هذا الصدد:" أن هذا القانون على حسب أنه قانون خاص بالتوقيع والتصديق الالكترونيين إلا أنه لم يتناول كافة الاعتداءات التي قد تلحق بهما خاصة المتعلقة بالإتلاف والتزوير والدخول أو البقاء غير المصرح بهما مما يستدعي الرجوع إلى القواعد العامة لقانون العقوبات والتي بدورها لم تتصدى لحماية التوقيع الالكتروني.


الفصل الثاني

إن دراسة الحماية الجنائية الموضوعية لمكافحة جرائم التوقيع الإلكتروني لا تكتمل إلا بالنظر إلى الجانب الإجرائي، الذي يُعد مكملًا لتلك الحماية وداعمًا لفعاليتها. فالجوانب الإجرائية تمثل الوسيلة التي تنتقل من خلالها نصوص التجريم من حالة الجمود إلى حيز التنفيذ والتطبيق العملي. وعند تفعيل الحماية الجنائية في إطار جرائم التوقيع الالكتروني، تبرز عدة تحديات عملية تبدأ منذ المراحل الأولى للتحقيق وجمع الأدلة.

وقد أفرزت طبيعة جرائم الاعتداء على التوقيع الالكتروني جملة من المشكلات، منها صعوبة السيطرة على الأدلة غير المادية، وغموض مسرح الجريمة الافتراضي، ما انعكس سلبًا على أدوات ووسائل التحقيق والإثبات. وعليه، فإن دراسة هذه الجوانب الإجرائية تكتسب أهمية خاصة كونها تُسلّط الضوء على العقبات الواقعية التي تعترض السلطات المختصة في مواجهة هذا النوع من الجرائم.

وبناءً على ما تقدم، سيتم تقسيم هذا الفصل إلى مبحثين رئيسيين:

المبحث الأول: السياسة الإجرائية لمكافحة جرائم التوقيع الإلكتروني

المبحث الثاني: التعاون القضائي الدولي في مكافحة جرائم التوقيع الإلكتروني

المبحث الأول: السياسة الإجرائية لمكافحة جرائم التوقيع الإلكتروني

أسهم التطور الهائل في تقنيات الحاسب الآلي في كسر الحواجز الجغرافية، حيث ظهرت جرائم جديدة تتطلب نوعًا خاصًا من الأدلة، يُعرف بالأدلة الرقمية أو الإلكترونية، والتي تتماشى مع طبيعة البيئة الافتراضية التي ارتُكبت فيها الجريمة. وقد واجه المشرّع الجزائري تحديًا مزدوجًا، تمثل في ضرورة تحديد هذه الأفعال بدقة، من جهة، والعمل على إيجاد حلول قانونية وإجرائية لمشكلات الإثبات، من جهة أخرى، خاصة فيما يتعلق بوسائل جمع الأدلة الرقمية، وإجراءات الحصول عليها سواءاً كانت تقليدية أم حديثة، وفي ظل هذا الواقع المستجد , حيث بات من الممكن ارتكاب أفعال النسخ أو البحث غير المشروع من دولة معينة، في حين يكون الفاعل متواجدًا في دولة أخرى تمامًا. وقد ترتب على هذا الواقع تعقيدات قانونية تتعلق بتحديد الجهة القضائية المختصة بالنظر في مثل هذه الجرائم، ولا سيما تلك المتعلقة بالاعتداء على التوقيع الإلكتروني، مما جعل مسألة تحديد الاختصاص القضائي من أبرز التحديات التي فرضها التعامل التقني عن بُعد. وانطلاقًا من هذا الإطار، سيتناول هذا المبحث محورين أساسيين:

المطلب الأول: إجراءات الإثبات الجنائي في جرائم التوقيع الإلكتروني.

المطلب الثاني: مسألة الاختصاص القضائي في جرائم التوقيع الإلكتروني

المطلب الأول: إجراءات الإثبات الجنائي في جرائم التوقيع الإلكتروني

ظهرت جرائم جديدة ناتجة عن استخدام شبكة الإنترنت، تطلبت نوعًا خاصًا من الأدلة يُعرف بالأدلة الرقمية، والتي تتناسب مع طبيعة الوسط الافتراضي. وقد واجه كل من المشرع الجزائري والمشرع المقارن تحديات في تحديد هذه الأفعال بدقة، وإيجاد حلول للمشكلات المرتبطة بجمع الأدلة الرقمية وإجراءات الحصول عليها، سواءاً كانت تقليدية أو حديثة. حيث تناولنا في الفرع الأول الإجراءات التقليدية في جرائم التوقيع الإلكترونية أما في الفرع الثاني الإجراءات المستحدثة في جرائم التوقيع الإلكتروني.

الفرع الأول: الإجراءات التقليدية في جرائم التوقيع الإلكترونية

الكشف عن جرائم الاعتداء على التوقيع الإلكتروني يتطلب استراتيجيات خاصة، تشمل تأهيل القائمين على جمع الأدلة بمهارات تقنية تواكب تطور تقنيات الحاسب الآلي والشبكات. فهذه الجرائم تستخدم وسائل معقدة ومتنوعة، وتتعدد أدلتها، ومنها الأدلة التقليدية حيث سنتطرق (أولا) التبليغات والشكاوى (ثانيا) التفتيش في جرائم التوقيع الالكتروني (ثالثا) الانتقال و المعاينة في جرائم التوقيع الالكتروني (رابعا) الخبرة التقنية في جرائم الاعتداء على التوقيع الالكتروني

أولا: تلقي التبليغات والشكاوى في جرائم الاعتداء على التوقيع الإلكتروني

أدى التطور في تكنولوجيا الإعلام والاتصال إلى ظهور أنماط إجرامية جديدة، مما دفع المجلس الأوروبي إلى تبني إجراءات خاصة بمكافحة جرائم التوقيع الإلكتروني، أبرزها استقبال الشكاوى والتبليغات عبر الإنترنت. تشمل هذه الإجراءات مراحل تبدأ باستقبال الشكاوى، ثم التحري والتحقيق، وصولًا إلى اتخاذ التدابير القانونية المناسبة. وتقوم الجهات المختصة بتحليل المعطيات وتوظيفها قانونيًا، مع تنظيم سجلات تشمل البيانات والمرفقات الخاصة بكل بلاغ.[1]

كما تم إنشاء نظام توثيق إلكتروني لتسجيل جميع الشكاوى والبلاغات، مع إعداد تقارير دورية تتضمن نتائج دراستها، مقترحات التعامل معها، والإجراءات التي تم اتخاذها بشأنه.[2]

1- تعريف إجراء تلقي التبليغات والشكاوى

يقصد بها مجموعة الإجراءات والمراحل التي تتم في دائرة البلاغات والشكاوى وتمر خلالها البلاغات والشكاوى بداية من استقبالها مرورا بدراستها والتحري حولها والتصرف فيها وفقا للتشريعات النافذة للتأكد من صحتها وتباشر الهيئات متلقية البلاغات والشكاوى من تلقاء نفسها التحري والتحقيق في جرائم الاعتداء على منظومة التوقيع الإلكتروني وتحليل مرافقاتها وإعطاء التوظيف القانوني لما تتلقاه من بلاغات وشكاوى وإعداد السجلات والاستمارات المنظمة لعملية تلقي البلاغات والشكاوى متضمنة البيانات لكل منها شاملا مرفقاتها[3].

إضافة إلى ذلك إعداد نظام توثيق إلكتروني لكافة البلاغات والشكاوى الواردة ، وإعداد تقارير دورية عن البلاغات والشكاوى التي تلقتها الإدارة متبوعة بنتائج دراستها ومقترحات التعامل معها وانتهاء الإجراءات التي تمت بشأنها، وفي هذا الإطار[4]

البلاغات هي الإخبارات التي تصل إلى ضباط الشرطة القضائية حول وقوع جريمة، سواء كانت هذه الإخبارات شفهية أو مكتوبة. ببساطة، هي نقل المعلومة عن وقوع حادث أو جريمة إلى الجهة المسؤولة بناءً على أسباب منطقية.[5]

2- الجهة المختصة بتلقي الشكاوى والتبليغات

---

[1]-Christiane féralschuhl , **cyber droit, le droit à l'épreuve de l'internet**, édition dalloz, 2009.P358

[2] - فهد عبد الله العبيد العازمي، **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، مصر، 2016، ص 160.

[3] - فهد عبد الله العبيد العازمي، المرجع نفسه، ص 160.

[4] - حسام محمد نبيل الشرافي، **جرائم الاعتداء على التوقيع الإلكتروني**، دار الكتب القانونية، مصر، 2013، ص 337.

[5]- يزيد بوحليط، المرجع نفسه ، ص59

.المادة 18 من قانون الإجراءات الجزائية الجزائري، المحدد بالأمر 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم.

أدى تطور تكنولوجيا الاتصال إلى بروز جرائم إلكترونية جديدة، كجرائم التوقيع الإلكتروني، ما دفع المجلس الأوروبي إلى اعتماد إجراءات خاصة، منها استقبال الشكاوى عبر الإنترنت، والتحقيق فيها تلقائيًا وتحليل المعطيات المرتبطة بها قانونيًا.

وتخول قوانين الإجراءات الجنائية، مثل المادة 17 من قانون الإجراءات الجزائية الجزائري، لضباط الضبط القضائي صلاحية تلقي الشكاوى بجميع أشكالها، سواء من المتضرر أو محاميه،

دون تقييد بشكل معين، مع توثيقها إلكترونيًا، وإعداد تقارير دورية، واتخاذ ما يلزم لحفظ الأدلة[1]

كما نصت المادة 18 من ق.إ. ج. ج على أنه:"يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم"[2]

لم يفرض القانون الجزائري طريقة معينة لتقديم الشكاوى، وهذا يسمح باستخدام الوسائل الحديثة مثل الإنترنت والهاتف. وقد أطلقت قيادة الدرك الوطني خدمة "الشكوى المسبقة والاستعلام عن بعد" في جميع الولايات لتسهيل تقديم المواطنين لشكواهم عبر الإنترنت. هذه الخدمة تهدف إلى تسريع عمليات البحث والتحقيق في الجرائم الإلكترونية وتوفير وقت عناصر الضبطية القضائية.

3- مراحل حسب آلية تلقي التبليغات والشكاوى:

ويتضح من المهام السابقة أن آلية تلقي البلاغات والشكاوى تتكون من المراحل التالية:

- مرحلة الاستقبال والتوثيق بمحضر التحري.
- مرحلة جمع المعلومات والأدلة.
- إحالة البلاغات والشكاوى إلى وكالات تطبيق القانون أو فرق العمل الخاصة المحلية أو الدولية. وينبغي التنويه ألا تشمل الإجراءات تجاه البلاغات والشكاوى، فهذه الإجراءات متنوعة بحسب نوع الشكوى أو البلاغ، كما أنها متعددة منها جمع المعلومات وإجراء التحريات

[1]- يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة**، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص58.

[2]- قانون رقم 06 22- مؤرخ في 29 ذي القعدة عام 1427 الوافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر رقم 155-66 المؤرخ في 18 صفر عام 1386الوافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءا الإجراءات الجزائية، الجريدة الرسمية، العدد 84، 2006

ومنها التحقيق ومتابعة الإجراءات والجهات القضائية بعد انتهائها من التحقيق فيها، كما أن جرائم الاعتداء على التوقيع الإلكتروني ليست بمقدور أي شخص الإبلاغ عنها ما لم تتوافر لديه القدرة على التعامل مع الجهاز الآلي أو نظم تقنية المعلومات[1]

فالبلاغ عن جرائم الانترنت قد يكون جواز على أي شخص علم بوقوع الجريمة أن يبلغ أولا مأموري الضبط القضائي سواء كان له مصلحة في ذلك أو لا، بعكس الشكوى التي يجب أن تصدر من المتضرر أو من وكيله خاصة وان هناك جهات تحجم من الإعلان والبلاغ عن هذه الجرائم خاصة البنوك والمؤسسات المالية خوفا من تزعزع ثقة العملاء بها أو قد يكون واجبا وهذا ما أقرته لجنة خبراء مجلس أوروبا الإلزام بإبلاغ جهة خاصة، والإلزام بإبلاغ سلطات إشرافية، وتشكيل جهاز خاص لتبادل المعلومات وكذا إصدار شهادة امن خاصة.[2]

4- العناصر الأساسية للتحقيق في جرائم الاعتداء على التوقيع الإلكتروني

يجب أن تتوافر في البلاغ والشكوى العناصر الأساسية اللازمة للتحقيق في الجريمة، كما يجب على المحقق أن يستظهر ما يلي:

- **إظهار الركن المادي:** النشاط أو السلوك المادي في جرائم منظومة التوقيعات الإلكترونية ومعرفة هذا النشاط والشروع فيه ونتيجته.
- **إظهار الركن المعنوي:** إظهار الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة و شخصية الجاني.
- **تحديد وقت ومكان ارتكاب الجريمة:** تتميز مسألة النتيجة الإجرامية في الجرائم الإلكترونية مشاكل متعددة بخصوص مكان وزمان تحقق النتيجة الإجرامية وتثير أيضا إشكاليات القانون الواجب التطبيق لوجود عدة دول في هذا المجال، ذلك أن جرائم التوقيع الإلكتروني من الجرائم العابرة للحدود.[3]
- **يجب على المحقق الجنائي أثناء القيام بالتحقيق مراعاة مايلي:**
- توفير معلومات مسبقة عن مكان وقوع الجريمة، ومن المالك لهذا المكان، ونوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها وتحديد إمكانية التعامل معها فنيا.
- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.[4]

5- أجهزة تلقي التبليغات والشكاوى:

---

[1]- فهد عبد الله العبيد العازمي، المرجع السابق، ص 162.

[2]- فهد عبدالله العبيد العازمي ،المرجع نفسه، ص127.

[3]- خالد ممدوح إبراهيم، **التوقيع الالكتروني** ،الدار الجامعية، الطبعة الاولى، الاسكندرية ، مصر ، 2000، ص 218.

[4]-فهد عبد الله العبيد العازمي، المرجع السابق، ص166.

تتلقى الشكاوى والبلاغات بواسطة شبكة الانترنت واتخاذ الإجراءات اللازمة للكشف عن الجريمة وملاحقة مرتكبيها، ومن هذه المواقع نجد وزارة العدل الأمريكية usdoj-go وموقع المباحث الفيدرالي bi go وموقع منظمة الانتربول interpol.int والمجلس الأوروبي col.gov وأيضا موقع البلاغات للمخابرات المركزية الأمريكية cia وكذلك منظمة الانترنت الأمنيةIFCC.[1] وفي فرنسا يتم الإبلاغ عن الجرائم الإلكترونية عبر الموقع الإلكتروني لجهاز الشرطة الفرنسي Judiciaire gendarmerie défense باعتباره الجهة المختصة بالتحقيق والتحري عن تلك الجرائم وموقع جمعية مزود الدخول وخدمات الانترنت.contact.net AFAhttp//www.pointide

وفي مصر يتم الإبلاغ عن الجرائم الإلكترونية عبر المواقع الإلكترونية عبر شبكة الانترنت www.moiegypt.gov-eg

ثانيا: التفتيش في جر ائم الاعتداء على التوقيع الإلكتروني

إن التفتيش غرضه ضبط الأدلة المادية للكشف عن الجريمة ومرتكبها، فكل ما يضبط بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فيعرف التفتيش بأنه: "ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، الغرض منه البحث عن الأدلة المتعلقة بالجريمة للوصول إلى الحقيقة في متابعة أي شخص يشتبه في انه ارتكب الجريمة ويكون على المكونات المادية بأشكالها أي شيء يتصل بجريمة معلوماتية يمكن الكشف عنها وعن مرتكبيها".

يدخل في نطاق التفتيش التقليدي وفقا لقانون الإجراءات الجزائية الجزائري والمعمول بها إلا أن هناك حالات خاصة للتفتيش في هذه المكونات والمتمثلة في:

- إذا وُجدت مكونات الجريمة الإلكترونية في مكان خاص كمسكن المتهم أو ملحقاته، فإنها تخضع لنفس الأحكام والضمانات القانونية المقررة لتفتيش المساكن.
- إذا كانت المكونات الحاسوبية منفصلة عن باقي أجهزتها وفي مكان آخر غير مسكن المتهم، فإن إجراءات التعامل معها تختلف عن تفتيش المساكن.[2]

1- القواعد الإجر ائية للتفتيش:

بما أن التفتيش هو إجراء من إجراءات التحقيق يهدف إلى ضبط أدلة الجريمة موضع التحقيق وكل ما يفيد في الكشف عن الحقيقة، وذلك وفقا لقواعد إجرائية تتلخص فيما يلي:

---

[1] -IFCC:والذي أسسه مكتب التحقيقات الفيدرالي (FBI) (والمركز الوطني لجرائم الياقات البيضاء (NW3C) في فرجينيا الغربية بالولايات المتحدة الأمريكية من اجل مكافحة ظاهرة الاحتيال عبر الانترنت , ولاحقا تغير اسمه الى IC3 : INTERNET CRIME COMPLINT CENTER وظيفته الأساسية استقبال الشكاوى المتعلقة بجرائم الانترنت , مثل : جرائم التوقيع الالكتروني , الاحتيال المالي , سرقة الهوية , الابتزاز و الهجمات السيبرانية .

[2]- عبد القادر عدو، **الجريمة الإلكترونية إجر ائيا**، الطبعة الثانية، دار هومة، الجزائر، 2016، ص 80.

أ- **إجراء الإذن:**

كقاعدة عامة، لا يشترط القانون الجزائري الحصول على إذن لتفتيش المنظومة المعلوماتية. ومع ذلك، عند الانتقال إلى منزل المشتبه به لتفتيش منظومة معلوماتية، تطبق قواعد تفتيش المنازل والأماكن الخاصة، مما يستلزم الحصول على إذن مكتوب من وكيل الجمهورية المختص، وإلا اعتبر التفتيش تعسفيًا،[1] ويمكن التفرقة بين حالتين:

1- تفتيش منظومة معلوماتية في الأماكن الخاصة (كالمنازل): يتطلب إذنًا مكتوبًا.

2- التفتيش في الأماكن العامة (كمقهى أو ساحة): يخضع لقواعد تفتيش الأماكن العامة ولا يتطلب إذنًا .وقد نصت المادة 44 من قانون الإجراءات الجزائية على ضرورة وجود إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق لدخول الأماكن الخاصة، ويجب إبراز هذا الإذن عند الدخول ويتضمن وصفًا للجريمة وموضوع البحث عن الأدلة وحضور الشخص المعني. وبناءً عليه، يجب الانتقال إلى مكان وجود جهاز الحاسوب ومكوناته وملحقاته و حجزها..[2]

ب- **إجراء التفتيش بحضور أشخاص معينين قانونا:**

من بين الأشخاص المعنيين بالتفتيش: المشتبه فيه المتهم، ضابط الشرطة القضائية القائم بالتفتيش، وشاهدين. والقاعدة العامة في التفتيش تقتضي حضور هؤلاء الأشخاص، خاصة المتهم أو من يمثله. إلا أن المشرع الجزائري استثنى الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من هذه القاعدة بموجب المادة 45 من قانون الإجراءات الجزائية، حيث يجوز تفتيش المنظومة المعلوماتية بدون حضور المتهم أو الشاهدين.[3]

ج-مواعيد التفتيش :

كقاعدة عامة في الجرائم التقليدية، لا يجوز تفتيش الأماكن الخاصة إلا بين الساعة الخامسة صباحًا والثامنة مساءً، ويُعتد بوقت الدخول ما لم يطلب صاحب المنزل خلاف ذلك. لكن تفتيش المنظومة المعلوماتية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يستثنى من هذه القاعدة، حيث يمكن إجراؤه في أي ساعة من الليل أو النهار بإذن مسبق من وكيل الجمهورية المختص[4].

---

[1]- عبد القادرعدو، المرجع السابق، ص 86.

[2]- المادة 44 من ق.إ.ج.ج.م.

[3]- ناصر جوادي ،**إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري**، الطبعة الثالثة، دار العلوم ،الجزائر، 2011 ص 417.

[4]- ناصر جوادي، المرجع السابق ص 48 .أنظر المادة 7ف 3 من ق.إ.ج.

وفقًا للمادة 47/ف3 من قانون الإجراءات الجزائية. ويعود هذا الاستثناء إلى طبيعة الأدلة الإلكترونية التي يمكن إخفاؤها أو تغييرها أو تدميرها أو التلاعب بها بسرعة، مما يستدعي إمكانية التفتيش في أي وقت للحفاظ عليها وتسهيل التحقيق..[1]

د/ تحرير محاضر التفتيش:

المحاضر هي تلخيص شامل ومبسط للواقعة، تتضمن إثبات جميع الإجراءات القانونية والفنية التي قام بها المحقق لكشف ملابسات القضية وجمع الأدلة.[2]

المحاضر هي تلخيص شامل ومبسط للواقعة، تتضمن إثبات جميع الإجراءات القانونية والفنية التي قام بها المحقق لكشف ملابسات القضية وجمع الأدلة.

يُكلف القائم بالتفتيش باصطحاب كاتب من أعوان الضبط القضائي لتحرير محضر خاص بالتفتيش، سواء أسفر عن نتائج إيجابية أو سلبية. ويتم في المحضر تسجيل جميع وقائع التحقيق والتفاصيل، وذكر البيانات والأشياء والوثائق المضبوطة بدقة وأمانة.[3]

يلزم القانون المحقق والكاتب بالتوقيع على المحاضر، ويجب التوقيع على كل صفحة في نهايتها لمنع أي تزوير. ويكفي توقيع الكاتب مع المحقق في نهاية محضر التحقيق، لأن حجية المحضر مستمدة من توقيع النيابة العامة

2- القواعد الموضوعية للتفتيش:

يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة وهي كالآتي:

1- سبب التفتيش في المجال الإلكتروني:

يتطلب تفتيش الأنظمة المعلوماتية وجود جريمة تتعلق بالتوقيعات الإلكترونية، أي فعل مرتبط باستخدام الحاسوب لتحقيق أهداف غير قانونية تمس هذه التوقيعات، وتورط شخص أو أكثر في ارتكابها أو الاشتراك فيها، بالإضافة إلى توفر أدلة أو قرائن قوية تساعد في الكشف عن مرتكب الجريمة المعلوماتية.[4]

---

[1]- معمش زهية، غائم نسيمة، **الإثبات الجنائي ف الجرائم المعلوماتية**، مذكرة تخرج لنيل شهادة الماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق، جامعة عبد الرحمن ميرة، بجاية، 2011/2012، ص 25.

[2]- ابتسام بغو، **إجراءات المتابعة الجزائية في الجريمة المعلوماتية**، مذكرة تخرج لنيل شهادة الماستر في القانون الجنائي الأعمال، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، 2015/2014، ص 16.

[3]- غرداين حسام، **الجريمة الإلكترونية وإجراءات التصدي لها**، مذكرة تخرج لنيل شهادة الماستر،كلية الحقوق، جامعة الجزائر، 2015/2014، ص 87.

[4]- حسام نبيل الشراقي، المرجع السابق، ص465.

أما بالنسبة لاتهام شخص أو مجموعة أشخاص بارتكاب الجريمة أو المشاركة فيها، فيجب توفر دلائل كافية تدعو للاعتقاد بمساهمة الشخص المراد تفتيشه في الجريمة، سواء كان فاعلًا أصليًا أو شريكًا.[1]

2- محل التفتيش:

محل التفتيش في الجريمة الإلكترونية هو الحاسب الآلي ونظم معلوماته ومكوناته سواء المادية أو المعنوية، بالإضافة للأشخاص الذين يستخدمونه وقد سبق وأن أشرنا إلى مكونات الحاسب الآلي المادية والمعنوية. ك الكومبيوتر و ملحقاته و برامجه , الهاتف الذكي و شبكات الاتصال عن بعد , كما نشير استثناءا الى بعض الأشخاص و الأماكن من التفتيش مثل أعضاء السلك الدبلوماسي و أعضاء المجالس النيابية , ومكاتب المحامين لتمتعهم بالحصانة , وعليه فأي تفتيش لها يعد منافيا للقانون و مأله البطلان[2]

3- السلطة المختصة بالتفتيش

بما أن التفتيش إجراء من إجراءات التحقيق الابتدائي ومن أخطر الإجراءات التي تمس بحقوق وحريات الأشخاص، عمدت معظم التشريعات بالاستناد إلى جهة خاصة لكي يتم وفق إجراءات محددة قانونا.

أما بخصوص المشرع الجزائري فنجده حدد بوضوح الجهة المختصة سواء في مجال الإذن بوضع ترتيبات المراقبة الإلكترونية أو في مجال الدخول بغرض تفتيش منظومة المعلوماتية أو جزء منها، فنجد نص المادة 1/4 من القانون 09-04: "إذ يختص النائب العام لدى مجلس قضاء الجزائر يمنح ضباط الشرطة القضائية المتبنى للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته المنصوص عليها بموجب المادة 13 من نفس القانون إذن بتفتيش لمدة 6 أشهر قابلة للتجديد التي تسمح باللجوء إلى المراقبة الإلكترونية"[3].

فيما عدا هذه الحالة الخاصة وبموجب نص المادة 05 من القانون 09-04: "يجوز للسلطات القضائية المختصة وكذا الشرطة القضائية ... الدخول بغرض التفتيش"، إذ يتعين الرجوع إلى المادة 37 من ق.إ.ج. ج سواء بالنسبة لوكيل الجمهورية أو قاضي التحقيق بموجب المادة 40اللتان تنصان

[1] فهد عبد الله العبيد العازمي، المرجع السابق، ص 262.

[2] - أنظر جمال براهيمي , **التحقيق الجنائي في الجرائم الالكترونية** , أطروحة دكتوراه في القانون , كلية الحقوق و العلوم السياسية , جامعة مولود معمري , تيزي وزو , الجزائر, 2018 , ص58.

[3] - القانون رقم 09-04 المؤرخ في 05 أغسطس 2009: المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية، العدد07 المؤرخة في 2009/08/16.

على تجديد الاختصاص لكل من وكيل الجمهورية أو قاضي التحقيق في جرائم محددة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

4- ضبط الأدلة في مجال الاعتداء على التوقيع الإلكتروني:

عقب التوصل للأدلة الإلكترونية في مسرح الجريمة الإلكترونية، يجب أن يتم جمع تلك الأدلة بشكل كافي وفق نظم معينة حتى تكون لها حجية أمام القضاء وتتم عملية الضبط وفق مجموعة من المراحل:

- **مرحلة جمع الدليل:**

تعتبر هذه المرحلة من أهم المراحل التي تلجأ إليها جهات التحقيق للكشف عن الحقيقة حيث يتم إتباع الإجراءات التالية من خلالها:

- تسجيل كل ما يتم من إجراءات في الملاحظات.
- مراقبة الشاشة وتحديد ما إذا كانت معلقة أو مطفأة.
- تسجيل الموديل والرقم المتسلسل للجهاز.
- إزالة أعلى أقراص مدمجة موجودة لتجنب تلف الأدلة.
- تسجيل كل الأفعال المرتبطة بالتلاعب بالجهاز لحفظ الموثوقية في المعلومات ومثال هذه الأجهزة تسجيل الصوت، أجهزة الرد الآلي.

- **مرحلة نقل وتخزين الأدلة:**

في هذا السياق، نص المشرع الجزائري في المادة 6 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على ما يلي: "عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية على معطيات مخزنة يتم نسخ كل المعطيات اللازمة لفهمها على دعامة التخزين الإلكترونية تكون قابلة للحجز والوضع في أقراص وفقا للقواعد المقررة في ق.إ.ج. ج وفي جميع الأحوال على السلطة القائمة بالتفتيش والحجز أن تحرص على سلامة المعطيات الموجودة في المنظومة المعلوماتية." وهذا ما أكدته المادة 27 من قانون الإجراءات الجزائية تحت عنوان "ضبط المعلومات المخزنة" والتي تنص على: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط المعلومات التقنية وعمل نسخة من المعلومات التقنية وكذا الحفاظ على سلامة تقنية للمعلومات، وأيضا إعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص المادة 6/3 من ق.إ.ج.ج وهذا تحت طائلة العقوبات وفقا للمادة

[1]- ق.إ.ج. ج من الأمر 66-155 المؤرخ 23 يونيو 1966 جريدة رسمية العدد 84 المتضمن من ق.إ.ج.ج. المعدل والمتمم بالقانون 17/07 المؤرخ في 27 مارس 2017.

85 من ق.إ.ج. ج، بالإضافة إلى وضع تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواد التي تكون محلا للجريمة.[1]

ثالثا: الانتقال والمعاينة في جر ائم التوقيع الإلكتروني.

المعاينة هي إجراء أساسي في بداية التحقيق، حيث ينتقل المحقق إلى مسرح الجريمة لفحص الأشياء والأشخاص المتعلقين بها بهدف إثبات الحالة والحفاظ على الآثار التي قد تكشف الحقيقة.

1-معاينة مسرح جريمة التوقيع الإلكتروني:

تم معاينة الجرائم الإلكترونية بالانتقال إلى مكان وقوعها، ولكن هذا الانتقال يختلف حسب طبيعة الجريمة. يجب التمييز بين:

-معاينة الجرائم الواقعة على المكونات المادية للجهاز وتشمل فحص الأجزاء الملموسة للحاسوب مثل الشاشة والمفاتيح والأقراص، وهي لا تثير صعوبات ويمكن لضابط الشرطة القضائية معاينتها والتحفظ عليها كأدلة مادية.[2]

-معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها وتشمل البرامج والبيانات، وتثير صعوبات بسبب قلة الآثار المادية وتردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة قد تكون طويلة بين ارتكاب الجريمة واكتشافها.[3]

2 -الإجراءات القانونية المتبعة لمعاينة مسرح جريمة التوقيع الالكتروني:

هي جملة من الإجراءات المطبقة في كافة الجرائم، لكن القانون الجزائري يفرض قواعد إلزامية للقيام بها، فهي جائزة في الجنح وواجبة في الجنايات. وقد تجرى في مكان عام، وفي هذه الحالة لا يحتاج ضابط الشرطة القضائية إلى إذن من سلطة التحقيق. أما إذا كانت في مكان خاص، فتتطلب شروطًا خاصة.

أ - إخطاروكيل الجمهورية:

لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضابط الشرطة القضائية، وهذا ما نصت عليه المادة 42من ق.إ. ج. ج.[4]

---

[1]- يزيد بوحليط، المرجع السابق، ص 489-488.

[2]- أحمد حزيط، الوجيز في الإجراءات الجزائية، الطبعة الثانية، دارهومة، الجزائر، 2015، ص38.

[3]- أحمد حزيط، المرجع نفسه، ص 39.

[4]- أنظر:المادة 42 من ق.إ.ج.ج، السالف الذكر.

وعملا بنص المواد ،18 ،32 ،42، 63 من ق. إ. ج. بالإضافة إلى المادتين 42 و 49 من قانون القضاء العسكري، يلتزم ضباط الشرطة القضائية بإبلاغ وكيل الجمهورية المختص (مدنيًا أو عسكريًا) فور علمهم بأي جريمة. يجب أن يسبق هذا الإبلاغ تأكد الضباط من وقوع الجريمة بالفعل، ويتم الإبلاغ باستخدام أي وسيلة متاحة كالكتابة أو الهاتف أو الفاكس.

ب- أوقات المعاينة:

أوجب القانون الجزائري على ضباط الشرطة الحصول على إذن من وكيل الجمهورية المختص لدخول منازل الأشخاص بغرض التفتيش والمعاينة، وتسري هذه القواعد عند معاينة الجرائم الإلكترونية.[1]

ومع ذلك، أجازت المادة 47 من قانون الإجراءات الجزائية إجراء المعاينة والتفتيش والحجز في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في أي وقت وفي أي مكان (سكني أو غير سكني) دون تأخير، بناءً على إذن مسبق من وكيل الجمهورية المختص. كما يحق لضابط الشرطة القضائية الاستعانة بأشخاص مؤهلين للقيام بذلك.[2]

ج- رضا المشتبه فيه بالتفتيش:

لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المشتبه فيها إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، أو يجب أن يكون هذا الرضا صريحا وكذلك الشأن بخصوص الجرائم الواقعة على النظم المعلوماتية وهذا ما نص عليه المشرع الجزائري في نص المادة64 من ق.إ. ج.ج.[3]

لا يجوز تفتيش مسكن المتهم أو حجز متعلقاته إلا بموافقته الصريحة والمكتوبة، أو بمساعدة شخص يختاره هو ويثبت ذلك في المحضر في حال عجزه عن الكتابة. لكن في جرائم الأنظمة المعلوماتية، تطبق أحكام المادة 47 مكرر من قانون الإجراءات الجزائية. وتوضح المادة 45 كيفية إجراء التفتيش وفقًا للمادة 44:

---

[1]- أحمد حزيط ، المرجع السابق، ص 39.

[2]- المادتان 47 و49 من ق.إ. ج.ج، السالف الذكر.

[3]- المادة 64 من ق.إ.ج. ج تنص على ما يلي: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه."

- عند تفتيش مسكن شخص يشتبه في مساهمته في جناية، يجب أن يتم التفتيش بحضوره. إذا تعذر ذلك، يكلفه ضابط الشرطة القضائية بتعيين ممثل له، وإذا امتنع أو كان هاربًا، يستدعي الضابط شاهدين من غير موظفيه لحضور التفتيش.[1]

رابعا: الخبرة التقنية في جرائم الاعتداء على التوقيع الإلكتروني.

يستعين المحقق الجنائي في جرائم الاعتداء على التوقيع الإلكتروني بخبراء متخصصين، نظرًا للطبيعة الفنية الخاصة لهذه الجرائم، مما يجعل الاستعانة بهم ضرورة حتمية في عملية التحقيق . تعرف الخبرة بأنها إبداء رأي فني من شخص مختص في شان واقعة ذات أهمية في الدعوى الجنائية".[2]

وبمعنى آخر هي: "تنقيب وبحث يرتبط بمادة لتطلب معارف علمية أو فنية خاصة لا تتوافر لدى المحقق أو القاضي"[3]

تعيين الخبير وفي هذا الإطار نجد نص المادة 92 من قانون الإجراءات الجزائية الإماراتي يقولها " إن اقتضى التحقيق الاستعانة بطبيب أو غيره من الخبراء ....[4]

أما المشرع المصري فقد نص صراحة من خلال المادة 1/85 من قانون إجراءات الجزائية المصري بقولها " إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من هذا الخبراء[5]

بالنسبة للمشرع الجزائري، فقد أجاز لجهات التحقيق والمحكمة تعيين خبراء سواء بمبادرة منها أو بناءً على طلب أحد الأطراف. و تنص المادة 143 من قانون الإجراءات الجزائية الجزائري على أنه عندما تُعرض على جهات التحقيق أو الحكم مسألة ذات طابع فني، يجوز لها أن تأمر بندب خبير سواء بطلب من النيابة أو بمبادرة منها أو بناءً على طلب الخصوم.

1- **أداء اليمين:** حيث جل التشريعات المقارنة وقبل قيام الخبير التقني بأعماله أداء اليمين نظرا بخطورة مهامه في إطار المنظومة الالكترونية وفي هذا السياق نجد المشرع الجزائري اوجب لضمان صحة تقرير الخبير ونيل وثقة أطراف الدعوى أن يقوم الخبير بحلف اليمين."[6]

---

[1]- أنظر المادة 47 مكرر والمادتان 44، 45 من ق.إ.ج.ج، السالف الذكر.

[2]- داود سليمان علي الحمادي ، **أحكام جريمة التزوير الالكترونية** , دار النهضة العربية , القاهرة , مصر , 2008، ص 174.

[3]- يزيد بوحليط، المرجع السابق، ص 329.

[4]- داود سليمان علي الحمادي ، المرجع السابق ، ص188.

[5]- حسام محمد نبيل الشرقاني ، المرجع السابق، ص 440.

[6]- حيث تنص المادة 145 من (ق.ا.ج.ج) على " يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلكم المجلس ...."

2- **الخضوع لرقابة القضائية :** عندما يباشر الخبير مهمته فهو تحت رقابة قاضي التحقيق أو القاضي الذي أمره بإجراء الخبرة.

3- **انجاز الخبير لأعمال الخبرة بنفسه:** لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر وحكم الندب وان يستجيب لطلبات التي يقدمها أطراف الخصومة مثل سماع أي شخص قادرا على إعطاء معلومات فنية.

4- **إبداع الخبرة التقنية:** بعد انتهاء الخبير من أعماله التي كلف بها يقوم بإيداع الخبرة التقنية خلال المدة المحددة وتقديم ما توصل إليه خبرته من نتائج إلى القاضي المختص[1]

5- **موقف المشرع الجزائري بالنسبة للخبرة التقنية:**

لقد وضع المشرع الجزائري تنظيمًا لإجراء الخبرة الرقمية يراعي خصوصية الجرائم الإلكترونية وصعوبة التحقيق فيها، وذلك من خلال نصوص قانونية تسهل إجراء هذه الخبرة على عدة مستويات:

أ/ على مستوى تعيين الخبراء: بالإضافة إلى المادة 144 من قانون الإجراءات الجزائية التي تحدد كيفية اختيار الخبراء بشكل عام، نجد المادة 05 من القانون رقم 09-04 تجيز للسلطات المكلفة بالتفتيش تسخير أي شخص لديه خبرة بعمل المنظومة المعلوماتية.

ب/ على مستوى الهيئات: أنشأ المشرع الجزائري هيئات مزودة بكوادر مؤهلة لإجراء الخبرة الرقمية، مثل:

-المعهد الوطني للبحث في علم التحقيق الجنائي.

-المركز الوطني لمكافحة الجريمة المعلوماتية التابع لقيادة الدرك الوطني.

المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، والذي يهدف إلى توفير الوسائل الحديثة في مجال تكنولوجيا الإعلام والاتصال.[2]

الفرع الثاني: الإجراءات المستحدثة في جرائم التوقيع الإلكتروني

تُعد الإجراءات التقليدية للحصول على الدليل الإلكتروني غير كافية، ما يخلق صعوبات في كشف الجرائم الإلكترونية ويتيح للمجرمين فرصة الإفلات من العقاب. لذلك، بات من الضروري أن

---

[1]- يزيد بوحليط ، المرجع السابق ، ص283 .

[2]- في إطار المجهودات المبذولة من طرف السلطة القضائية بالجزائر بخصوص تدريب وتكوين ضباط الشرطة القضائية والقضاة في مجال البحث والتحري عن الجرائم الإلكترونية أشرف خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفدرالي على تكوين ورشات حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة تهدف إلى اطلاعهم على آخر التكنولوجيا لمحاربة الجريمة.

مقال منشور على الموقع الرسمي http//www.djazzairess.com/alkhabar :اطلع عليه على الساعة 9:24 بتاريخ 16 أفريل2025.

تواكب التشريعات طبيعة هذه الجرائم المستحدثة، من خلال اعتماد وسائل تقنية متطورة تسهّل الكشف عن الجريمة وضبط مرتكبيها. وقد تم في هذا الإطار استحداث إجراءات جديدة، أبرزها اعتراض المراسلات، وتسجيل الأصوات والتقاط الصور كوسائل إثبات حديثة, حيث سنتطرق الى اعتراض المراسلات (أولا) و تسجيل الأصوات و التقاط الصور(ثانيا)

أولا : اعتراض المراسلات في جر ائم الاعتداء و التوقيع الالكتروني

لا يجوز اعتراض محتوى المستندات أو السجلات الإلكترونية إلا باتخاذ تدابير تقنية معينة، تسهّل جمع المعلومات أو تسجيلها أو التحقق منها. وقد نصّت المادة 21 من اتفاقية بودابست على التدابير التي يمكن لسلطة التحقيق استخدامها عند اعتراض محتوى البيانات الإلكترونية، لضمان مشروعية الدليل وفعالية الإجراءات.

1/تجميع أو تسجيل البيانات من خلال تطبيق واستخدام الوسائل الفنية على أراضي تلك الدولة التي تكون طرف في الاتفاقية.

2/ألزم جهاز تقديم الخدمة المعلوماتية في حدود قدرته الفنية بما يلي:

تجميعها أو تسجيلها خلال تطبيق واستخدام الوسائل الفنية والتعاون ومساعدة السلطات المختصة في تجميع أو تسجيل مضمون البيانات، يجب على تلك السلطة أن تتوخى السرية التامة عن اعتراض من مضمون البيان الإلكتروني وذلك حفاظا على سرية البيانات التي تم اعتراضها ومؤدى كل ذلك أن الإفصاح عن تلك البيانات لا يكون إلا عندما تكون الجريمة الاعتداء على التوقيع الإلكتروني.[1]

أ/ السلطة المختصة في إصدار إذن الاعتراض:

تختص السلطة القضائية عمومًا بإصدار إذن اعتراض الاتصالات، كضمانة لحماية الحياة الخاصة من تدخل أجهزة الدولة، وفقًا للقانون المصري. ولا يُشترط تنفيذ الإذن من قبل قاضي التحقيق أو النيابة، إذ يجوز إسناده لضباط الضبط القضائي. أما في القانون الجزائري، فقد خالف المشرع هذا المبدأ، إذ أجاز لوكيل الجمهورية المختص أن يصدر بنفسه إذنًا باعتراض المراسلات عبر وسائل الاتصال، وذلك بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

ب/مدة الاعتراض:

[1]- هلالي عبد الله احمد، **جر ائم المعلوماتية التقليدية و المستحدثة و تطبيقها في النظام البحريني**، دار النهضة العربية ،القاهرة ، 2013، ص 182.

حرصت التشريعات الحديثة على تحديد مدة زمنية للاعتراض على الاتصالات، كضمانة ضد التعسف وسوء استعمال السلطة. في القانون المصري، حُددت المدة بـ 30 يومًا قابلة للتجديد لمدة مماثلة، وفقًا للمادتين 90 و206 من قانون الإجراءات الجنائية. أما في التشريع الجزائري، فقد نصت المادة 65 مكرر 5 من قانون الإجراءات الجزائية على مدة أقصاها 4 أشهر، قابلة للتجديد بحسب مقتضيات التحري أو التحقيق.[1]

ت- موقف المشرع الجزائري من اعتراض المراسلات الإلكترونية:

لقد أغفل المشرع الجزائري تعريف اعتراض المراسلات ولكنه بالمقابل اكتفى بتنظيم هذه العملية بموجب المادة 65 مكرر 05 من ق.إ. ج. ج "إذ اقتضت ضروريات التحري على الجريمة المتلبس بها أو التحقيق الابتدائي... في الجرائم الآلية للمعطيات ... يجوز لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية دون الموافقة العينية من أجل التقاط وتكتب وتبث وتسجيل الكلام أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص"[2]

أما بالرجوع إلى نص المادة 47 من التعديل الدستوري 2020 والتي تنص على: "**لكل شخص الحق في حماية حياته الخاصة ، لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت , لا مساس بالحقوق و المذكورة في الفقرتين الأولى و الثانية إلا بأمر معلل من السلطة القضائية حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي يعاقب القانون على كل انتهاك لهذه الحقوق**" .

كما نص أيضا على سرية البيانات المتعلقة بالتصديق الإلكتروني بنص المادتين 42 و43 من القانون رقم 15-04 [3]المؤرخ في 2015/02/01 يحدد القواعد العامة لتوقيع والتصديق الإلكتروني على مؤدى خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.

ثانيا: تسجيل الأصوات والتقاط الصور

يتم تسجيل الأصوات عن طريق وضع أجهزة تنصت في أمكنة أو مركبات خاصة أو عمومية وإخفائها لتلقى أحاديث يمكن أن تفيد في التعرف على الحقيقة وتسجيلها، أما التقاط الصورة فيقصد

---

[1]- أيمن رمضان محمد أحمد،**الحماية الجنائية للتوقيع الإلكتروني،رسالة دكتوراه**، كلية الحقوق، جامعة عين شمس،القاهرة،2010 ، ص 190.

[2]- المادة 65 مكرر 05 من ق.إ. ج.ج، السالف الذكر.

[3]- المادتين 42، 43 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.، السالف الذكر.

به تثبيت صورة شخص على مادة خاصة مما يسهل الاطلاع عليها ونسخها وذلك باستخدام الوسائل التقنية المخصصة و المعدة لذلك[1]

أ/ تسجيل الأصوات:

يُقصد بتسجيل المحادثات نقل الموجات الصوتية من مصدرها بنبراتها وخصائصها الفردية، بما فيها عيوب النطق، وحفظها على شريط يسجل الإشارات الكهربائية بشكل يسمح بإعادة سماعها وفهم محتواها. ويشمل ذلك المحادثات الشفوية التي تدور بشكل سري أو خاص في أماكن عامة أو خاصة، باستخدام جهاز معد لتسجيلها والاستماع إليها لاحقًا.[2]

وفي هذا الإطار نجد أن المشرع الجزائري نص من خلال نص المادة 65 مكرر 05 من ق.إ.ج. ج السابقة الذكر على تسجيل أحاديث المتهم.[3]

حيث أجاز المشرع وضع ترتيبات تقنية دون علم وموافقة المعنيين من أجل تسجيل الأحاديث في الأماكن العامة أو الخاصة، حيث أن أخذ المشرع الجزائري بالمذاهب الموضوعية،

حيث طبيعة الحديث أساس الحماية الجنائية بغض النظر على المكان الذي أجري فيه وهو المعيار الذي أخذ به المشرع الفرنسي أيضا، بما أن المشرع المصري تأثر بالقانون الفرنسي وأصدر القانون رقم 37 لسنة 1982 بمقتضاه أضيفت المواد 309 مكرر التي اعتنق من خلالها معيار المكان الخاص لتحديد طبيعة الحديث وإضفاء حماية عن المحادثات الخاصة، ذلك أنه يضع حماية على المحادثات التي تدور في أماكن خاصة، ويتطلب شروط وإجراءات خاصة للاعتداد بالدليل المستمد من التسجيل، لذلك من الأفضل تعديل هاتين المادتين على نحو يكفل الأخذ بطبيعة الحديث وبمكان صدور وسبب وطبيعة الحديث فقط، كالنهج الذي أخذ به المشرعين الفرنسي والأمريكي.

يتم تسجيل الأصوات عن طريق أجهزة التسجيل السلكية واللاسلكية بإخفاء ميكروفون في المكان المستهدف وتوصيله بأسلاك دقيقة، ويُسند تنفيذ العملية للأعوان المختصين ومصالح الاتصالات السلكية واللاسلكية، سواء العمومية أو الخاصة، وفقًا للمادة 65 مكرر 8 من قانون الإجراءات الجزائية الجزائري. وتُعد التسجيلات الصوتية الحديثة دليلًا قويًا في الإثبات الجنائي، نظرًا لدقة تقنياتها وصعوبة التلاعب بها، إذ يمكن للخبراء كشف أي تعديل بفضل تقنيات عالية الكفاءة.

ب- التقاط الصور:

---

[1] - شنتير خضرة, **الأليات القانونية لمكافحة الجريمة الالكترونية،دراسة مقارانة** ،ابن النديم للنشر و التوزيع، وهران ، 2022 ، ص 140.

[2]- ياسرمحمد الكومي ،**الحماية الجنائية والامنية لتوقيع الالكترونية** ،**دراسة مقارنة**،رسالة دكتوراه في القانون الجنائي ،جامعة حلوان ،مصر،ص 250.

[3]- المادة 65 من ق.إ.ج.ج.السالف الذكر.

لم يشر المشرع الجزائري إلى مفهوم التقاط الصور بل اكتفى بالإشارة إليه في نص المادة 65 مكرر9 من قانون الإجراءات الجزائية بمصطلح " الالتقاط" , في حين عرفها جانب من الفقه الجنائي الصورة بأنها امتداد ضوئي لحجم الإنسان وهي لسبب لها فكرة أو دلالة الإشارة إلى شخصية صاحبها[1] حيث أن التصوير المرئي يعتمد على توثيق مشاهد متحركة، ويقوم هذا الإجراء أساسا على استخدام الكاميرات أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير ....

- أجهزة التصوير المرئي التي تستخدم في تسجيل الأحداث والجرائم:

- التصوير المرئي بكاميرات السينما والتلفاز.
- التصوير المرئي بكاميرات الفيديو.
- التصوير المرئي بالكاميرات الرقمية وهو ما يسمى بكاميرات الديجتال.
- التصوير المرئي بكاميرات الهاتف الخلوي.
- التصوير المرئي عن طريق أجهزة مراقبة وكاميرات خاصة.
- التصوير المرئي بالكاميرات السرية.
- التصوير عن طريق القرصنة الإلكترونية[2].

المطلب الثاني: مسألة الاختصاص القضائي في جرائم التوقيع الإلكتروني

بما أنه لا يوجد اختصاص تشريعي في الجزائر، سوف نتناول الاختصاص بالنظر في جرائم الاعتداء على التوقيع الإلكتروني، فتحديد القضاء المختص بالنظر في جرائم الاعتداء على التوقيع الإلكتروني من أهم الصعوبات الحديثة التي أسفر عنها التعامل التقني للحاسب الإلكتروني عن بعد، مما يؤدي إلى صعوبة تحديد ا محكمة المختصة، وأن دراسة لسلطة القاضي في قبول الدليل الإلكتروني، وهذا ما سنتناوله في الفرع الأول الاختصاص القضائي للنظر في جرائم الاعتداء على التوقيع الإلكتروني أما في الفرع الثاني تطرقنا ل سلطة القاضي في قبول الدليل الإلكتروني

الفرع الأول: الاختصاص القضائي للنظر في جرائم الاعتداء على التوقيع الإلكتروني

اثار حلاف فقهي وقضائي كبير حول تحديد المحكمة المختصة في الجرائم بمنظومة التوقيعات الإلكترونية، ولكننا سنتطرق للنصوص القانونية الجزائرية التي استحدثها المشرع الجزائري

[2] أنظر 303 و 303 مكرر و 303 مكرر1 من قانون العقوبات الجزائري القانون رقم 24-06 المؤرخ في 28 أبريل سنة 2024

خاصة بالقواعد الإجرائية قصد مكافحة الجرائم المعلوماتية سواء في قانون الإجراءات الجزائية أم ضمن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .[1]

فنجد المشرع الجزائري نص على ثلاث معاير تحكم الاختصاص المحلي وهي المحكمة التي ارتكبت الجريمة ف نطاق إقليمها أو المحكمة التي يقبض على المتهم في نطاقها أو المحكمة التي يقيم المتهم دائرتهما فالمشرع الجزائري قام بتوسيع الاختصاص لكل من الضبطية القضائية ثم وكيل الجمهورية وقاضي التحقيق[2].

أولا: الاختصاص المحلي بالجهات القضائية على جر ائم التوقيع الالكتروني

يُعد تحديد الاختصاص المحلي لكل من الضبطية القضائية ووكيل الجمهورية وقاضي التحقيق مسألة جوهرية في معالجة جرائم التوقيع الإلكتروني، وذلك بالنظر إلى طبيعتها غير المادية التي تجعلها تمتد عبر نطاقات إقليمية مختلفة، متجاوزة الحدود الجغرافية التقليدية. فبينما كانت قواعد الاختصاص المحلي في الجرائم التقليدية تستند إلى موقع ارتكاب الجريمة أو محل إقامة المتهم، فإن الجرائم الرقمية تفرض واقعًا جديدًا يستلزم إعادة النظر في هذه القواعد لضمان تحقيق العدالة الفعالة.

1- الضبطية القضائية:

في العديد من المرات ما تفتح الإجراءات الجزائية في الدعوى العمومية بمحطة التحري و البحث أي خطوة جمع الدلائل التي تشرف عليها الضبطية أو بالأحرى الشرطة القضائية ، بحيث نص قانون الإجراءات الجزائية الجزائري على أحكام الضبط القضائي في المواد 12 و 28 و 42 و 55 و 63 و 65 و تحدد الضبطية القضائية ضباط الشرطة القضائية وأعوانه ، وكدا بعض الموظفين الذين يناط بهم بعض مهام الشرطة القضائية ، وتجسيد السياسية الإجرائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية ، خاصة في مجال البحث والتحري[3] ، كما نص صراحة في المادة 16 فقرة 07 على تمديد اختصاصات ضباط الشرطة القضائية ، إذ نجد أنه بإمكانهم القيام بعمليات البحث والمعاينة على كافة إقليم التراب الوطني ، ويكون ذلك تحت سلطة النائب العام لدى المجلس القضائي المختص محليا وإشرافه ، كما يشترط علم وكيل

[1]- القانون رقم 09-04 المؤرخ في 05 أغسطس 2009: المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ج.رج ج، العدد07،المؤرخة في 2009/08/16.

[2]- نجاة بن مكي، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، مذكرة تخرج لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية؛ كلية الحقوق والعلوم السياسية جامعة عباس لغرور خنشلة، 2012/2013، ص 231.

[3]- يزيد بوحليط،المرجع السابق؛ ص 394.

الجمهورية لدى المحكمة المختصة اقليميا[1] ، بالإضافة إلى أن صلاحيات الضبط القضائي تشمل تقديم الدعم و المساعدة ، وفقا لما جاء في نص المادة 20 من قانون الإجراءات الجزائية الجزائري ، والتي بدورها تحدد دور أعوان الضبط القضائي ، كما جاء في نص المادة 19[2] من نفس القانون

ومن جهة ثانية ، يسمح لضباط وأعوان الشرطة القضائية ، في حال عدم اعتراض وكيل الجمهورية بعد إعلامه ، يتم تمديد عمليات مراقبة الأشخاص الذين تتوفر ضدهم مبررات قانونية تستوجب الاشتباه فيهم ، وذلك وفقا لما أشارت إليه المادة 16 مكرر من قانون الإجراءات الجزائية الجزائري[3] ، والتي تتيح إمكانية توسيع نطاق المراقبة عبر كامل الإقليم الوطني ، شريطة أن يكون هناك مبرر قانوني واضح يستدعي ذلك.

2- وكيل الجمهورية:

لقد حددت المادة 37 من ق.إ. ج. ج الاختصاص المحلي لوكيل الجمهورية بصفة واضحة وموضوعية ويعرف الاختصاص المحلي بأنه : "تلك الدائرة القضائية التي يستطيع فيها وكيل الجمهورية مباشرة وظيفته بصفة مباشرة طبقا لقانون الإجراءات الجزائية[4].

فيتحدد الاختصاص المحلي لوكيل الجمهورية حسب [5]المادة 37 من ق.إ. ج. ج بمكان وقوع الجريمة، ومحل إقامة أحد الأشخاص من المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم القبض على هؤلاء الأشخاص[6] ، ولكن بالنظر إلى طبيعة جرائم التوقيع الإلكتروني وإمكانية ارتكابها عبر مناطق متعددة وتجاوزها للحدود، استثنى المشرع الجزائري من مبدأ الاختصاص المحلي. فبموجب المادة 2/37 من قانون الإجراءات الجزائية، يجوز تمديد الاختصاص المحلي لوكيل الجمهورية ليشمل كامل التراب الوطني. وقد صدر المرسوم التنفيذي رقم 348/06 بتاريخ 2006/10/15 الخاص بالتنظيم القضائي المعدل بموجب المرسوم التنفيدي رقم: 267/16 المؤرخ في 2016/10/17 ج ر رقم:62 الذي حدد هذه المحاكم , ولتحديد المحاكم ووكلاء الجمهورية وقضاة التحقيق الذين يمتد اختصاصهم

---

[1]- قانون رقم 06 22- مؤرخ في 29 ذي القعدة عام 1427 الوافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر رقم 155-66 السالف الذكر.

[2]- المادة 19 من ق.إ. ج. ج المعدلة عدلت بالأمر رقم 10/95 المؤرخ في 25/02/1995، الجريدة الرسمية، العدد 11نصت على أنه "يعد من أعوان الضبط القضائي موظفو مصالح الشرطة وذو الرتب في الدرك الوطني ورجال الدرك، ومستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية".

[3]- مولاي ملياني بغدادي، **الإجراءات الجزائية في التشريع الجزائري**، المؤسسة الوطنية للكتاب، الجزائر،1992، ص 139

[4]- المادة1/37 من ق.إ.ج.ج

[5] - المرسوم التنفيذي المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق رقم 63 المؤرخة في 2006/10/08 .

المحلي.المادة 2/37 من قانون الإجراءات الجزائية: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات... الصرف، وتجدر الإشارة إلى أن المحاكم التي تم تمديد اختصاصها اصطلح على تسميتها بالأقطاب الجزائية أو محكمة القطب المتخصص. ومن ناحية أخرى نجد أن المشرع وتحسبا لهذا النوع من الجرائم نص على مجموعة على من الإجراءات لتسهيل عملية البحث والتحري عن هذه الجرائم فنصت المادة توسيعه للاختصاص المحلي للنيابة العامة في مجال الجرائم الإلكترونية وأجبرها أن تباشر إجراءات المتابعة تلقائيا.[1]

3- قاضي التحقيق:

ويُقصد بالاختصاص المحلي لقاضي التحقيق النطاق الذي يمارس فيه مهامه. ووفقًا للمادة 40 من قانون الإجراءات الجزائية، يتحدد هذا الاختصاص بناءً على أحد المعايير التالية: مكان وقوع الجريمة، أو محل إقامة أحد المشتبه بهم، أو مكان القبض على أحدهم حتى لو كان القبض لسبب آخر.[2].

وبموجب الفقرة 2 المادة 40 وسع المشرع الاختصاص المحلي لقاضي التحقيق كلما تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبالتالي يصبح لقاضي التحقيق التابع لهذه المحكمة اختصاص إقليمي يتجاوز اختصاصه العادي ويمكنه التنقل أو انتداب أي ضابط شرطة قضائية للقيام بمهام تتعلق بالتحقيق القضائي في الجرائم الخطيرة الماسة بأنظمة المعالجة الآلية للمعطيات[3]

بما سبق يتبين أن المشرع الجزائري بموجب التعديل الوارد بالأمر04- 14 المؤرخ في 10 نوفمبر 2004 الذي يتعلق بتوسيع الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق إلى محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه ترك تحديد كيفية تطبيق تلك الإجراءات.

للتنظيم، كما يتبين من خلال استقراء نص المادتين 37 و 40 من ق.إ.ج. ج أن الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق يعتبر واحدا.[4]

كما تجدر الإشارة للاختصاص القضائي بالنسبة للجرائم العابرة للحدود (الأجنبي) حسب المادة المادة 15 من القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من

---

[1]- المادتان 144 مكرر و144 مكرر 2 من قانون العقوبات الجزائري، السالف الذكر.

[2]- المادة 40 من ق.إ. ج.ج، السالف الذكر.

[3]- المادة 2/40الجرائم المذكورة سالفا.

[4]- نجاة بن مكي، المرجع السابق، ص.215.

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من النصوص القانونية الأساسية التي تنظم مسألة الاختصاص القضائي في الجرائم الإلكترونية ذات الطابع الدولي.

وقد نصت المادة 15 على ما يلي:

"تختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا القانون، ولو ارتكبها أجنبي خارج الإقليم الوطني، إذا كان لها مساس بمصالح الدولة أو بأمن النظام المعلوماتي الوطني".

يُفهم من هذه المادة أن المشرع الجزائري تبنى مبدأ "الاختصاص القضائي الموسع"، الذي يُمكّن القضاء الوطني من تتبع مرتكبي الجرائم الإلكترونية حتى خارج الحدود الجغرافية للدولة، متى كان للفعل أثر مباشر على أمن أو مصالح الجزائر.

ثانيا : الاختصاص النوعي للمحاكم بالنظرفي جرائم الاعتداء على التوقيع الإلكتروني

يتحدد الاختصاص النوعي للمحاكم بحسب طبيعة الجريمة المطروحة أمامها، إذ تعود الصلاحية لمحكمة الجنايات للفصل في القضايا المتعلقة بالجنايات وكذا الأفعال الموصوفة بالإرهاب أو التخريب، إضافة إلى بعض الجنح والمخالفات المرتبطة بها، والتي تُحال إليها بموجب قرار صادر عن غرفة الاتهام، وذلك تطبيقا لما تنص عليه المادة 248 من قانون الإجراءات الجزائية الجزائري.

حيث يوجد على مستوى كل مجلس قضائي محكمة جنايات ابتدائية وأخرى استئنافية ، في حين يُعهد إلى قسم الجنح والمخالفات على مستوى المحاكم الابتدائية بالنظر في الجرائم المصنفة ضمن هذين النوعين، عملاً بالمادة 328 من نفس القانون.

غير أنّ القانون أجاز، في حالات محددة، توسيع اختصاص بعض المحاكم للنظر في فئات معينة من الجرائم، كالجرائم المتعلقة بالاتجار غير المشروع بالمخدرات، والجرائم المنظمة عبر الحدود، وتبييض الأموال، والأعمال الإرهابية، وكذا الجرائم المرتبطة بتشريع الصرف والاعتداءات على أنظمة الإعلام الآلي. وقد ورد هذا التوسيع في المادة 329 من قانون الإجراءات الجزائية، التي أُدخلت عليها تعديلات بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، والتي فُصلت أحكامها التنظيمية في المرسوم التنفيذي رقم 06-348 الخاص بالتنظيم القضائي المعدل بموجب المرسوم التنفيذي رقم: 16-267 المؤرخ في 2016/10/17 ج ر رقم:62 الذي حدد هذه المحاكم[1].

ويختلف الاختصاص النوعي بالنظر في هذه الجرائم حسب درجة خطورتها حيث تخضع للتقسيم التالي :

[1] - المرسوم التنفيذي رقم 16- 267 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، الصادر بتاريخ 17 /2016/10، الجريدة الرسمية ،العدد 62، 2016

1- المحكمة الابتدائية (محكمة الجنح):

إذا كانت الجريمة تُصنف ضمن الجنح (مثلا، تزوير توقيع إلكتروني بسيط، أو استعمال توقيع دون إذن)، تكون محكمة الجنح أو القسم الجزائي بالمحكمة الابتدائية هي الجهة المختصة بالنظر فيها. فالعقوبة في هذا النوع من الجرائم غالبًا تكون بالغرامة أو الحبس.

2- محكمة الجنايات:

إذا كان الاعتداء على التوقيع الإلكتروني يشكل جريمة خطيرة (مثلا: تزوير توقيع إلكتروني لاستيلاء على أموال طائلة أو ارتكاب جريمة منظمة)، فإن الجريمة قد ترتقي إلى جناية. وبالتالي تختص محكمة الجنايات بالنظر فيها، لخطورتها وشدة العقوبات[1].

كما أن بعض المحاكم الجزائرية أنشأت أقسامًا متخصصة في الجرائم السيبرانية للنظر في هذا النوع من القضايا، تطبيقًا للمنشور الوزاري المشترك رقم 05 المؤرخ في 4 أكتوبر 2020، المتعلق بتنظيم النيابات المتخصصة في مكافحة الجريمة السيبرانية[2].

و بذلك فإن المشرع الجزائري لم ينص على محكمة خاصة بالتوقيع الإلكتروني، وإنما تُوزع القضايا حسب طبيعتها بين المحاكم العادية مع الاستعانة أحيانًا بأقسام متخصصة داخلها[3].

كما تنص المادة 15 من القانون 09-04 على انه "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[4].

3- **القطب الجزائي:** هو هيئة قضائية متخصصة تهدف إلى معالجة الجرائم المعقدة، خصوصًا الجرائم الإلكترونية والمالية، بفعالية وسرعة أكبر. يعتمد على فرق قضائية ذات خبرة لضمان تحقيق العدالة الجنائية بطرق دقيقة وشفافة، مع مراعاة حقوق الأفراد والمؤسسات.

- **الاختصاص الإقليمي للقطب الجزائي الوطني:**

---

[1] - القانون رقم 18-04 المؤرخ في 10 ماي 2018، والمتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية ، العدد 27، ا 2018.

[2] - المنشور الوزاري المشترك رقم 05 المؤرخ في 4 أكتوبر 2020، المتعلق بتنظيم النيابات المتخصصة في مكافحة الجريمة السيبرانية، الصادر عن وزارة العدل ووزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الجريدة الرسمية ة، العدد 61، الصادرة في 7 أكتوبر 2020، ص 12.

[3] - محمد عصفور، **الوجيز في شرح قانون الإجراءات الجزائية**، دار الجامعة الجديدة، الإسكندرية، 2016، ص 89.

[4]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريد الرسمية ، العدد 07، 2009.

وفي هذا الاطار تنص المادة 329 فقرة 1 من قانون الإجراءات الجزائية تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محكمة القامة أحد المتهمين أو شركاتهم أو محل القبض عليهم ، ولو كان هذا القبض لسبب آخر"

غير أن الفقرة 5 من المادة 329 جاءت باستثناء بقولها " يجوز المديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والارهاب والجرائم المتعلقة بالتشريع الخاص بالصرف , حيث المحمد ذلك من خلال المرسوم التنفيذي رقم 06-348 مؤرخ في 05-10-2006 توجيه تم التحديد أربعة محاكم على المستوى الوطني وتوسيع اختصاصها الإقليمي . تجدر الاشارة أن الاختصاص الاقليمي للقطب الجزائي يشمل كافة مراحل الدعوى العمومية إلى غاية صدور الحكم ليشمل دوائر اختصاص محاكم أخرى موزعة عبر الوطن :

- محكمة سيدي محمد – محكمة قسنطينة – محكمة وهران – محكمة ورقلة

وفقا للمواد 3-4-5 من المرسوم التنفيذي رقم 06-348 المذكور اعلاه ، يمتد اختصاص هذه المحاكم إلى المجالس القضائية حس التقسيم الجهوي هذا كله الموجهة الاجرام المنظم من خلال اختراق الاجرام عن طريق التسرب، والتنصت واعتراض الاتصالات والنقاط الصور، غير أن معيار الاختصاص الإقليمي التقليدي لا يسري على الجرائم السيرانية، وذلك ما أكدته المادة 211 مكرر 23 من الأمر 21-11- بقولها يمارس وكيل الجمهورية لدى القطب الجزائي الوطني المختص المكافحة الجرائم المتصلة بتكنولوجيات

الإعلام والاتصال، وكذا قاضي التحقيق وليس ذات القطب صلاحياتهم في كامل الاقليم الوطني

وهذا يكون القطب الجزائي الوطني المختص بمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، يتمتع باختصاص وطني في ممارسة صلاحياته وهذا كاستثناء من القاعدة العامة أن الاختصاص يكون محليا هذا من جهة بالإضافة إلى تفرغ القطب الجزائي وحده بالجرائم المستحدثة التي تتميز بالتعقيد والخطورة[1]

- **الاختصاص النوعي للقطب الجزائي الوطني :**
- يتعين نتاجا من خلال الجرائم التي أشار إليها المشرع الجزائري حصرا في المادة 211 مكرر 22 من قانون .....أنه ينعقد على مستوى محكمة مقر مجلس قضاء الجزائر ، قطب جزائي وطني متخصص في إجراءات المتابعة والتحقيق في الجرائم المتعلقة بتكنولوجيات

[1]-المرسوم التنفيذي رقم 06-348 مؤرخ في 05/10/2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رعدد 63، العدل بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 17/10/2016، عدد 62.

الإعلام و الاتصال وما يدخل ضمنها ، كما يؤول الاختصاص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تمثل جنحة ، أما تعلق بالمادة 211 مكرر 24 من الأمر 21 /11 ، حيث أشار فيها المشرع الجزائري إلى ما يلي :" مع مراعاة أحكام الفقرة 02 من المادة 211 مكرر 22 أعلاه ، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، وقاضي التحقيق ، ورئيس ذات القطب حصريا بالمتابعة والتحقيق ، والتحكم في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[1] المذكورة أدناه ، وكدا الجرائم المرتبطة مثل :

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.
- زيادة على ما تم الإشارة إليه من الجرائم المحددة في المادة 211 مكرر 24 المذكورة أعلاه ، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وكذا قاضي التحقيق ، ورئيس ذات القطب حصريا بالمتابعة والتحقيق و الحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المتصلة بها ، والتي يقصد بها الجريمة التي ينظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية مكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار الناشئة عنها ، أو طابعها المنظم العابر للحدود الوطنية أو مساسها بالنظام العام والأمن العموميين ، حيث تتطلب استعمال وسائل تحري خاصة ، أو خبرة فنية متخصصة ،أو حتى اللجوء إلى تعاون قضائي دولي. "

الفرع الثاني: سلطة القاضي في قبول الدليل الإلكتروني

تُعد مرحلة قبول الدليل الجنائي، سواء كان تقليديًا أو إلكترونيًا، الخطوة الإجرائية الأولى للقاضي. يهدف القاضي في هذه المرحلة إلى التحقق من مدى احترام الدليل الإلكتروني لمبدأ الشرعية الإجرائية قبل الشروع في تقديره. فإذا لم يستوفِ الدليل شروط الشرعية، فإنه يكون باطلًا ولا يمكن الاستناد إليه قانونًا. حيث سنتناول أساس قبول الدليل الالكتروني في الإثبات الجنائي (أولا) , ثم ضوابط الدليل الإلكتروني وأثره على اقتناع القاضي (ثانيا).

أولا: أساس قبول الدليل الإلكتروني في الإثبات الجنائي.

يختلف موقف القوانين بشأن سلطة القاضي الجنائي في قبول الدليل الإلكتروني في جرائم التوقيع الإلكتروني تبعًا لنظام الإثبات المتبع في الدولة. ويمكن تقسيم الدول في هذا الصدد إلى ثلاث فئات:

[1]-الأمر رقم 21-11 مؤرخ في 25 أوت 2021، يتمم الأمر رقم 155-66، المؤرخة في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد65 ، 2021

- وهي القوانين اللاتينية والتي تبنت مبدأ حرية الإثبات ومنها سلطة القاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستعيد المشرع بعضها صراحة.[1]
- وهي القوانين **الأنجلوسكسونية** حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، وغما في مرحلة تحديد العقوبة فيسود مبدأ حرية الإثبات.[2]
- تأخذ بنظام الأدلة القانونية، بحيث تحدد الأدلة التي يجوز للقاضي الجنائي قبوله كالقانون الهولندي 339ق. إ الجنائية والقانون الألماني الذي يحدد على سبيل الحصر وسائل الإثبات
- الذي يتعين على القاضي قبولها.[3]

1- مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني:

تتبنى الدول التي تتأثر قوانينها بالصياغة اللاتينية في مجال الاثبات الجنائي مبدأ حرية الاثبات ومنها سلطة القاضي في قبول جميع الأدلة ,حيث يمثل هذا المبدأ نظام الإثبات الحر[4]، المستمد من التأثير اللاتيني، تمنح القاضي سلطة واسعة في قبول الأدلة، بما في ذلك الأدلة الإلكترونية في جرائم التوقيع الإلكتروني. فالمعيار الأساسي هو اقتناع القاضي بصحة الدليل وملاءمته لإظهار الحقيقة، بغض النظر عن نوع الوسيلة التي تم الحصول عليها بها.[5] فقد أقر قانون الإجراءات الفرنسي مبدأ حرية الإثبات الجنائي صراحة بمقتضى المادة 427 بحيث يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخص. كما أقر المشرع المصري هذا المبدأ بموجب المادة 1/302 من قانون الإجراءات الجنائية.[6]

نجد أن المشرع الجزائري قد تبنى أيضًا مبدأ حرية الإثبات الجنائي في المادة 212 من قانون الإجراءات الجزائية، والتي تنص على أنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي نص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعًا للاقتناع الشخصي". وتكمن الأسباب التي تستدعي تطبيق مبدأ حرية الإثبات في نطاق نظرية الإثبات الجنائي فيما يلي:

- حرية الإثبات هي نتيجة لمبدأ اقتناع القاضي الحر، إذ تمكّنه من استخدام كل وسائل الإثبات التي يطمئن إليها لتحقيق العدالة بين الخصوم.

1- أحمد عصام عجيلة، **الحماية الجنائية للمحررات الإلكترونية**، دار النهضة العربية، القاهرة،2014، ص 480.

2- أحمد عوض بلال، **قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة**، الطبعة الثانية، دار النهضة العربية القاهرة، 2006، ص14.

3- سعيد السيد قنديل، **التوقيع الالكتروني** ، دار الجامع الجديدة ، الاسكندرية ،مصر ، 2006، ص 194 .

4 سعيد السيد قنديل المرجع نفسه , ص 194.

5- أحمد عصام عجيلة، المرجع السابق، ص 486.

6- المادة 1/302 من ق.إ.ج المصري: "يحكم القاضي في الدعوى حسب العقيدة التي تكون لديه بكامل حريته."

- إن الإثبات في الدعوى الجنائية يرد على وقائع قانونية، مادية أو نفسية يصعب بل يستحيل الحصول على دليل مسبق لها.

- الإثبات في الدعوى الجنائية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك للمحكمة أن تستدعي بكل الوسائل الممكنة كي يعتد لها رواية ما حدث.

- من المسلم به أن قرينة الإثبات تلقي عبء الإثبات كلية على عاتق سلطة الاتهام، مما جعلت مهمة هذه الأخيرة جد صعبة.[1]

- تختلف طبيعة المصلحة في الدعوى الجنائية عن الدعوى المدنية، وقد أقرّ المشرع بمبدأ حرية الإثبات لعدم كفاية الأدلة التقليدية في مواجهة الجرائم المستحدثة مثل الجرائم الإلكترونية.

ثانيا: ضوابط الدليل الإلكتروني و أثره على اقتناع القاضي

ضوابط الدليل الإلكتروني وأثره على اقتناع القاضي يتمتع القاضي الجنائي بسلطة تقديرية واسعة في تقييم الأدلة، بما في ذلك الأدلة الإلكترونية، حيث منح له المشرع حرية البحث عن الحقيقة باستخدام مختلف وسائل الإثبات، دون التقيد بقيمة مسبقة لأي دليل، حتى وإن كان علميًا مثل الدليل الإلكتروني.

1- الضوابط المتعلقة بمصدر الاقتناع:

يخضع اقتناع القاضي بالأدلة الإلكترونية لشروط قبولها، إذ يقتصر حريته على الأدلة التي تم الحصول عليها بطريقة مشروعة، ويستبعد الأدلة غير المقبولة احترامًا لمبدأ الشرعية الإجرائية،[2] وعليه لا يجوز للقاضي الاستناد إلى دليل استمد من إجراءات باطلة لان ما بني على باطل فهو باطل.

من القواعد الأساسية في الإجراءات الجنائية أن القاضي لا يجوز أن يبني حكمه على دليل لم يُطرح للمناقشة أمام الخصوم، إذ يجب أن يكون للدليل أصل في أوراق الدعوى وأن يُتاح للخصوم الاطلاع عليه ومناقشته، تطبيقًا لمبدأي الشفوية والمواجهة اللذين أقرهما المشرع الجزائري بموجب نص المواد: 300.304.353 من ق.إ.ج.ج،[3] و مبدأ العلنية بحسب المواد . 285.342.355.399 من نفس القانون إذ ينبغي القاضي أن يطرح كل دليل مقدم في دعوى المناقشة أمام الخصوم في الجلسة حتى يكونوا على بينة مما يقدم ضدهم من أدلة.

---

[1]- سعيد السيد قنديل، المرجع السابق، ص 198.

[2]- محمد زكي أبو عامر، **القيود القضائية على حرية القاضي الجنائي في الاقتناع** ،مجلة القانون والاقتصاد، العدد 51،جامعة القاهرة ، مصر، 1991، ص 139.

[3]- نص المادة 212/فـ2 من ق .إ .ج. ج: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا.

يتطلب مبدأ المواجهة ضمانات منها: مواجهة المتهم بالتهمة ومنحه وقتًا كافيًا لإعداد دفاعه مع توفير مترجم عند الحاجة، والسماح لكل طرف بتقديم مستنداته وسؤال الشهود وإثارة الدفوع. كما يشترط وجود أصل للدليل الإلكتروني ضمن أوراق الدعوى، عبر إعداد محضر الجلسة لإثبات الوقائع والأدلة، ضمانًا لتحقيق العدالة وتمكين المحكمة من مراجعة الحكم[1].

2- تو افق الاقتناع القضائي مع مقتضيات العقل والمنطق:

يجب أن يكون استخلاص محكمة الموضوع للوقائع معقولًا، بحيث يكون الاقتناع بالأدلة، بما في ذلك الأدلة الرقمية، منطقيًا وغير متعسف في الاستنتاج. كما يجب أن يتفق مع مقتضيات العقل والمنطق ولا يتعارض معها .[2]

المبحث الثاني: التعاون الدولي لمكافحة جر ائم التوقيع الإلكتروني

يُعد التعاون الدولي في مكافحة جرائم التوقيع الإلكتروني آلية أساسية لمنع إفلات المجرمين من العقاب، نظرًا لطبيعة هذه الجرائم العابرة للحدود. رغم أهميته، يواجه التعاون الدولي عدة إشكالات، ويأخذ صورًا متعددة كالتعاون الشرطي خلال جمع الاستدلالات، والمساعدة القضائية أثناء المحاكمة، وتسليم المجرمين. وسيتم تناول هذا الموضوع من خلال مطلبين: الأول عن التعاون الأمني الدولي بإنشاء هيئات متخصصة في مكافحة جرائم التوقيع الالكتروني ، والثاني عن التعاون القضائي الدولي لمكافحة هذه الجرائم.

المطلب الأول: التعاون الأمني الدولي بإنشاء هيئات متخصصة في مكافحة جر ائم التوقيع الإلكتروني.

تتسم جرائم التوقيع الإلكتروني بالنظر إلى طبيعتها بطابع دولي، ولا تستطيع الدول بجهودها المنفردة القضاء على هذه الجريمة، لذا من الضروري أن تساعد الدول بعضها البعض في الأدلة على أن يكون المحققون والنواب العامون على دراية بآليات متبعة للحصول على هذه المعلومات ويتحقق هذا التعاون بعقد اتفاقيات دولية، وتدعيم التعاون مع البوليس الدولي، أما على المستوى الوطني لابد من خلق أجهزة اتصال متطورة تتماشى وطبيعة الجرائم والقبض على المجرمين، بالإضافة إلى تنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وتقديم المعونة ف مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء، وتتمثل الإجراءات الجنائية

في إجراءات ضبط مرتكبيها من قبض وتفتيش وتسليم لتصبح منطقة قضائية واحدة، و من ثم يم تقسيم هذا المطلب إلى فرعين نتعرض في الفرع الأول الى **التعاون الشرطي الدولي لمكافحة جر ائم**

[1]- محمود نجيب حسني،**شرح قانون الإجراءات الجنائية**، الطبعة الثالثة، دار النهضة العربية،القاهرة،1988 ، ص 210.

[2]- يزيد بوحليط، المرجع السابق، ص416.

الاعتداء على التوقيع الإلكتروني، ونتعرض في الفرع الثاني الى مهام ودور الانتربول في التعاون مع المنظمات الشرطية الإقليمية (الأفريبول) (اليورو بول)

الفرع الأول: التعاون الشرطي الدولي لمكافحة جر ائم الاعتداء على التوقيع الإلكتروني .

تمثل المساعدة البوليسية بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم المعلوماتية بصفة عامة، وجرائم التوقيع الإلكتروني بصفة خاصة، أحد أهم هذه الجرائم، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، فتوقيع العقاب يستلزم تعاون دولي شرطي لذلك أنشأت العديد من منظمات الشرطة على الصعيد الدولي وأنشأت مكاتب شرطة الانترنت لمكافحة جرائم الاعتداء على التوقيع الإلكتروني[1]. حيث قسمنا هذا الفرع إلى أولا تعريف المنظمة الدولية للشرطة الجنائية (الإنتربول) واجهزتها. ثانيا مهام و دور الانتربول في التعاون مع المنظمات الشرطية الإقليمية (الأفريبول – اليوروبول)

أولا: تعريف المنظمة الدولية للشرطة الجنائية (الإنتربول)

هناك مجموعة من التعاريف الخاصة بالانتربول و المتمثلة فيما يلي:

- فالمنظمة الدولية للشرطة الجنائية (الانتربول) هي منظمة حكومية تعمل في إطار الإعلان العالمي لحقوق الإنسان وتقدم مساعدة مشتركة لسلطات الشرطة الجنائية طبقا للقوانين الداخلية لكل دولة وهي منظمة تكافح الجريمة وتساهم في تدبير وسائل لمكافحة الجريمة وكيفية تتبع مرتكبي الجرائم والقبض عليهم "[2]
- وتعد المنظمة الدولية للشرطة الجنائية international criminel police organisation)) إحدى المنظمات الحكومية التي أوكل إليها المجتمع الدولي مهمة التنسيق والبحث والتقصي - وتقديم الإرشادات في ميدان مكافحة الإجرام عموما ، وجريمة غسل الأموال على وجه الخصوص[3]."

الانتربول هو الشرطة الجنائية الدولية ، وقد تم إنشائه عام 1923 بمدينة "ليون" بفرنسا، وهو منظمة دولية تسعى لتحقيق التعاون الأمني بين الدول"[4]. ويعرفها الدكتور منتصر سعيد حمودة بأنها : الانتربول هو الاسم الدال على المنظمة الدولية للشرطة الجنائية، والتي تتخذ من مدينة ليون

---

[1]- علاء الدين شحاتة، **التعاون الدولي لمكافحة الجريمة**، دراسة الإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، الطبعة الأولى،إشراك للنشر والتوزيع، مصر، 2000، ص18.

[2]. فيصل عبد الله طلافحة ، ملاك تامر ميخائيل ، **إجراءات القبض والتقديم أمام المحكمة الجنائية الدولية** ، الطبعة الاولى ، مركز الكتاب الأكاديمي الأردن 2016 ، ص199

[3]-محمد إبراهيم خيري الوكيل، **مكافحة جريمة غسيل الأموال في المملكة العربية السعودية** ، الطبعة الاولى، مكتبة القانون والاقتصاد للنشر و التوزيع، السعودية.2016،ص

[4]- صلاح رزق عبد الغفار يونس ، **جر ائم الاستغلال الاقتصادي للأطفال** ، الطبعة الاولى، دار الفكر والقانون ، مصر ، 2015 ، ص 77.

الفرنسية مقرا لها. إن هذه المنظمة الدولية هي من قبيل المنظمات الدولية المتخصصة التي تهتم بالتعاون الدولي بين الدول الأعضاء فيها في مجال مكافحة الجريمة وتعقب المجرمين الذين يستطيعون تجاوز حدود الدولة التي ارتكبوا فيها جرائمهم وهربوا إلى دولة أخرى"[1].

ثانيا: أجهزة المنظمة الدولية للشرطة الجنائية (إنتربول)

تطورت جهود الإنتربول عبر إنشاء مراكز اتصالات إقليمية في عدة دول لتسهيل تبادل المعلومات بين أجهزة الشرطة، مع اعتماد نظامين للاتصال،[2] حسب طبيعة الدول: مركزي ولا مركزي. كما أنشأ المجلس الأوروبي سنة 1991 الشرطة الأوروبية لتنسيق جهود الدول الأعضاء في مكافحة الجرائم العابرة للحدود، بما فيها الجرائم المعلوماتية. وعلى المستوى العربي، أنشأ مجلس وزراء الداخلية العرب المكتب العربي للشرطة الجنائية لتعزيز التعاون الأمني وملاحقة المجرمين ودعم أجهزة الشرطة في الدول الأعضاء.[3]

أ- تبادل المعاونة لمواجهة الكوارث والأزمات والمو اقف الحرجة:

تواجه جميع دول العالم احتمالات وقوع كوارث ضخمة ومفاجئة يصعب التنبؤ بها أو التعامل معها بالإمكانات المحلية فقط، مما يجعل التعاون الدولي أمرًا ضروريًا، خاصة مع أهمية عنصر السرعة في المواجهة. ويزداد هذا التحدي بسبب تفاوت جاهزية أجهزة العدالة الجزائية بين الدول، حيث تتمتع بعض الدول بتقدم تقني كبير في مكافحة الجرائم المعلوماتية، بينما تفتقر أخرى لذلك.[4]

ب- القيام ببعض العمليات الشرطية والأمنية المشتركة:

يتطلب تعقب مجرمي المعلوماتية والأدلة الرقمية وتنفيذ التفتيش العابر للحدود عمليات شرطية وفنية مشتركة، مما يعزز مهارات مكافحة الجرائم المعلوماتية.[5]

انضمت الجزائر إلى الإنتربول في 1963، حيث يعمل المكتب المركزي الوطني تحت إشراف الشرطة القضائية ويخضع للتشريعات الوطنية. يتولى هذا المكتب مهامه وفقًا لاستراتيجية واضحة تتماشى مع احتياجات الأمن الوطني. وتقدم الإنتربول خدمات تشمل الاتصالات الشرطية العالمية،

---

[1] منتصر سعيد حمودة ، **المنظمة الدولية للشرطة الجنائية " الانتربول "** . الطبعة الاولى ، دار الفكر الجامعي ، مصر، 2008، ص 11

[2]-Malcon Anderson, policing the word, **interpole the politics of international police**, Co, oxford, 1989, P168, 185.

[3]- نجاة بن مكي، المرجع السابق، ص 150.

[4]- حسين بن سعيد بن سيف الغافري، **السياسة الجنائية في مواجهة جرائم الانترنت " دراسة مقارنة "**،دار النهضة العربية ، القاهرة، مصر ، 2009 ، ص220 -ص221.

[5]- علاء الدين شحاتة، المرجع السابق، ص 116.

قواعد بيانات، التدريب، وإعداد القضاة والخبراء القضائيين للتحقيق في الجرائم الإلكترونية. دول مثل كندا وفرنسا وإنجلترا نظمت دورات تدريبية لرجال الشرطة والخبراء القضائيين في هذا المجال[1]

الفرع الثاني: مهام و دور الانتربول في التعاون مع المنظمات الشرطية الإقليمية (الأفريبول – اليوروبول)

أولا : مهام المنظمة الدولية للشرطة الجنائية (الإنتربول)

للمنظمة الدولية للشرطة الجنائية (الإنتربول) عدة مهام كونها من أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم، فقد وجدت الإنتربول لتحقيق عدة أمور منها:

- التعاون الدولي لمواجهة الإجرام المتزايد باستمرار.
- تأمين الاتصال الرسمي بين رجال الشرطة في مختلف أرجاء العالم، بغية تبادل الخبرات والأفكار والمناهج وأساليب العمل في مجالات الأمن المختلفة منذ وجدت الدول القومية (الوطنية) التي تفصل بينها الحدود الجغرافية والصناعية، وارتباط الظاهرة الإجرامية برغبة المجرم للانتقال من مكان إلى آخر، ابتعاداً عن مسرح جريمته، واختفائه عن نظر السلطات الأمنية، و لأجل تحقيق أهدافها تقوم الإنتربول بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، من مختلف المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، حيث تقوم المنظمة بعد تجميعها للبيانات والمعلومات بتنظيمها لتكون بها أرشيفاً متكاملاً يمكن الرجوع إليه عند الحاجة[2].

ومن المهام التي يقوم بها الإنتربول فيما يخص الجريمة الإلكترونية تعقب مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود المكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية[3]

ثانيا: دور الانتربول في التعاون مع المنظمات الشرطية (الأفريبول – اليوروبول)

إنَّ الإنتربول، بوصفه أداةً مركزية للتعاون الشرطي الدولي، يعمل على تسهيل تبادل المعلومات بين أجهزة الشرطة في الدول الأعضاء، وتقديم الدعم الفني واللوجستي لملاحقة المجرمين الفارين، خاصة في ظل التحديات التي تفرضها الجرائم السيبرانية، وتمويل الإرهاب، وجرائم الاتجار بالبشر [4]. كما

---

[1]- علاء الدين شحاتة، المرجع نفسه، ص 117.

[2] - مجاهدي خديجة، **إستراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة**، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس المدية الجزائر، المجلد الثاني، العدد الثاني، جوان 2015، ص 102

[3] - حسين بن سعيد بن سيف الغافري، المرجع السابق , ص 507.

[4]- طارق المجالي، **الجريمة المنظمة والتعاون الأمني الدولي**، الطبعة الاولى، دار الحامد، عمان، 2018، ص 77.

توجد منظمات شرطية إقليمية مثل اليوروبول (Europol) في الاتحاد الأوروبي، والأفريبول (Afripol) في إفريقيا، تسهم في بناء شبكات أمنية متكاملة لمواجهة الجرائم ذات الطابع الإقليمي[1].

ومن ثمّ، فإن دراسة مهام ودور الإنتربول والمنظمات الشرطية الدولية الأخرى تُعدّ ضرورة علمية وأمنية لفهم آليات التعاون الدولي في مجال مكافحة الجريمة، خاصة في ظل ما يشهده العالم من تزايد الترابط بين التهديدات الأمنية.

1- دور الإنتربول في التعاون مع الأفريبول

الأفريبول هو الجهاز الشرطي الإفريقي الذي يهدف إلى تعزيز التعاون بين الدول الإفريقية في مكافحة الجريمة المنظمة والإرهاب، وهي جرائم تؤثر مباشرة على المجتمعات الضعيفة والفئات الهشة، خاصة في القارة الإفريقية. حيث يعمل الإنتربول جنبًا إلى جنب مع الأفريبول من خلال:

-تبادل المعلومات الاستخباراتية حول الشبكات الإجرامية العابرة للحدود.

- ينظم دورات تدريبية لضباط الشرطة الأفارقة لتعزيز مهاراتهم في التحقيقات الجنائية الرقمية.

-دعم العمليات المشتركة لمكافحة الجرائم مثل الاتجار بالبشر، تهريب المخدرات، والجرائم السيبرانية، وهي أنشطة تُهدد كرامة الإنسان وحريته وتستهدف الضعفاء[2].

2- دور الإنتربول في التعاون مع اليوروبول

اليوروبول هو الجهاز الأمني الأوروبي المسؤول عن تنسيق جهود الدول الأعضاء في الاتحاد الأوروبي لمكافحة الجريمة المنظمة. يتعاون الإنتربول مع اليوروبول من خلال:

-إنشاء قواعد بيانات مشتركة تتيح تبادل المعلومات حول المجرمين الدوليين.

-تنسيق التحقيقات الدولية في قضايا مثل الإرهاب، غسل الأموال، والجرائم الإلكترونية التي تُهدد الاستقرار الاجتماعي والحقوق الأساسية.

-تعزيز التعاون في مجال تسليم المجرمين بين الدول الأوروبية والدول الأعضاء في الإنتربول، بهدف تحقيق العدالة وعدم الإفلات من العقاب، بما يضمن حق الضحايا في الإنصاف[3]

3- أهمية التعاون بين الإنتربول والمنظمات الشرطية الإقليمية

يساهم هذا التعاون في تحقيق عدة أهداف إنسانية جوهرية، منها:

- تعزيز الامن الدولي من خلال مكافحة الجرائم التي تهدد استقرار المجتمع وتمس بحقه الأساسي في الحياة

---

[1] عبد الله أبو رمان، **دور الإنتربول في مكافحة الجريمة الدولية**، مجلة العلوم القانونية، العدد 2، 2020، ص 105.

-2 لموقع الرسمي https://www.interpol.int/en : تاريخ الاطلاع 2جوان 2025 على الساعة 11:00

[3] الموقع الرسمي https://www.europol.europa.eu : تم الدخول إليه بتاريخ 2جوان 2025 على الساعة 11:15

-رفع كفاءة الأجهزة الشرطية عبر تبادل الخبرات والتدريب المشترك، مما يضمن حماية الحقوق في مختلف المناطق.

-تحسين سرعة الاستجابة للتهديدات الأمنية من خلال التنسيق الفوري بين الدول، وتفادي الكوارث التي تُخلِّف ضحايا أبرياء[1].

المطلب الثاني: التعاون القضائي الدولي في مكافحة جر ائم التوقيع الإلكتروني.

تعد إشكالية الاختصاص القضائي في الجرائم الإلكترونية معقدة، مما يتطلب تعزيز التعاون الشرطي والقضائي الدولي لملاحقة الجناة ومنع إفلاتهم، عبر تسهيل الاتصال بين أجهزة الشرطة وإنشاء مكاتب متخصصة. ولا يتحقق ذلك إلا بتفعيل دور الإنتربول وتسريع اتفاقات التعاون الدولي، وقد قُسم إلى فرعين: التعاون الأمني الدولي القضائي الفرع الثاني العقبات التي تواجه التعاون القضائي الدولي في جرائم التوقيع الالكتروني

الفرع الأول: التعاون الأمني الدولي القضائي.

يشكل التعاون القضائي الدولي أداة أساسية في مكافحة جرائم الاعتداء على المواقع الإلكترونية، خاصة خلال مرحلتي التحقيق والمحاكمة ونظرًا للطبيعة العابرة للحدود لهذه الجرائم، لم يعد بالإمكان الاعتماد فقط على الإمكانيات الوطنية لملاحقة مرتكبيها، بل أصبح من الضروري تفعيل آليات التعاون بين الدول عبر تبادل المعلومات ، وتسليم المجرمين، وتقديم المساعدة القانونية المتبادلة[2].

ويتجلى هذا التعاون في عدة صور أبرزها:

حيث سنتطرق الى المساعدة القضائية الدولية في الكشف عن جرائم الاعتداء على التوقيع الإلكتروني (أولا) , ثم الإجراءات القانونية المتبعة في تسليم المجرمين (ثانيا) .

أولا: المساعدة القضائية الدولية في الكشف عن جر ائم الاعتداء على التوقيع الإلكتروني

تعني كل إجراء قضائي تتخذه دولة لدعم محاكمة جريمة في دولة أخرى. وقد أكدت عدة اتفاقيات دولية على أهميتها، أبرزها.[3]

---

[1] INTERPOL-Europol. Coordination Framework and Reports. Official Documents Archive, 2022. tps://www.europol.europa.eu
على الساعة 202511:30 الدخول إليه تم بتاريخ 02 جوان

[2]- عبد القادر بوعرفة، **التعاون الدولي في مكافحة الجر ائم الإلكترونية**، دار الجامعة الجديدة، الإسكندرية، 2017، ص. 89.

[3]- محمد مدحت المراسي، **أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة** ،مجلة مركز بحوث الشرطة، العدد22،أكاديمية الشرطة، سنة 2002، ص 127.

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية (باليرمو 2000): نصت في المواد 18، 19، و20 على التعاون عبر المساعدة القانونية المتبادلة، التحقيقات المشتركة، وأساليب التحري الخاصة اتفاقية بودابست لجرائم الحاسب الآلي: شددت في المادة 27 على أهمية المساعدة القضائية حتى بين الدول غير الأطراف.
- اتفاقية باليرمو: أكدت في المادة 18 على التزام الدول بتقديم المساعدة القانونية المتبادلة في التحقيقات والملاحقات القضائية.

تظهر هذه الاتفاقيات أهمية المساعدة القضائية كآلية ضرورية للتصدي للجرائم الإلكترونية والجريمة المنظمة العابرة للحدود.[1] و تتمثل هذه المساعدة فيما يلي:

1- تبادل المعلومات في جرائم التوقيع الإلكتروني

تشمل المساعدة القضائية تقديم المعلومات والوثائق والأدلة التي تطلبها سلطة قضائية أجنبية بخصوص جريمة معينة، بالإضافة إلى تبادل السوابق القضائية للجناة بهدف معرفة ماضيهم الجنائي، مما يساعد في تشديد العقوبات عند تكرار الجريمة. وتُقيّد بعض الدول مثل فرنسا تبادل هذه المعلومات بشروط خاصة واتفاقيات تعاون، ويتم كل ذلك عبر تعزيز الاتصال بين سلطات الدول المختصة بمكافحة الجرائم الإلكتروني.[2]

ومن أجل تسيير تبادل المعلومات بصورة مأمونة وسريعة بشأن كل ما يتعلق بتلك الجرائم:

- هوية الأشخاص المشتبه فيهم في تلك الجرائم وأماكن وجودهم وأنشطتهم وأماكن الأشخاص الآخرين المعنيين.
- حركة عائدات الجرائم أو الممتلكات المتأتية من ارتكاب الجرائم.
- تبادل المعلومات عبر الوسائل والأساليب المحددة.

يمكن للجهات المختصة في دولة ما إرسال بيانات حول الأحكام القضائية النهائية الصادرة ضد مواطنيها أو المقيمين في إقليمها إلى الجهة المختصة في دولة أخرى، وذلك في سياق التحقيقات أو الملاحقات الجنائية المتعلقة بجريمة معينة.[3]

وتؤكد المادة 26 من اتفاقية بودابست على ضرورة مساعدة الدول التي تمتلك معلومات هامة لتسهيل التحقيقات وتداول القضايا الجنائية، ولا يتم تقديم طلب للمساعدة المتبادلة في حال وجود هذه المعلومات.[4]

---

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 407.

[2]- المادة 05 اتفاقية الرياض العربية للتعاون القضائي اتفاقية الرياض العربية للتعاون القضائي 1983.

[3]- محمد كمال محمود الدوسقي، المرجع السابق، ص 148.

[4]- إيهاب محمد يوسف، **إتفاقيات تسليم المجرمين**،رسالة دكتوراه،كلية الدراسات العليا بأكديمية الشرطة،دبي 2003 ، ص 23.

كما تنص المادة 66 من قانون رومانيا 203/2004 على حق السلطات الرومانية المختصة في أن ترسل تلقائيا إلى السلطات الأجنبية المختصة المعلومات والبيانات الضرورية التي تسمح باكتشاف الجرائم المرتكبة بواسطة جهاز الحاسوب، أو يحل القضايا المتعلقة بتلك الجرائم.[1] نظرًا لما تثيره مسألة المساعدة القضائية بين الدول من حساسية تتعلق بسيادة الدولة من جهة وطبيعة جرائم الحاسوب من جهة أخرى، فقد وضع المشرع الجزائري شروطًا خاصة لذلك في المادة 17 من القانون 09-04، التي تتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. تنص هذه المادة على ضرورة استجابة الدولة لطلبات المساعدة الخاصة بتبادل المعلومات أو اتخاذ إجراءات تحفظية وفقًا للاتفاقيات الثنائية والدولية المعتمدة، وبمبدأ المعاملة بالمثل. كما أكدت المادة 04 من نفس القانون على ضرورة احترام السيادة الإقليمية وعدم التدخل في الشؤون الداخلية للدول الأخرى. هذه الشروط وضعت لحماية السيادة الوطنية وحماية المعطيات الشخصية للأفراد نظرًا لحساسية هذه المعلومات وأثرها على سلامة الأفراد والدولة.[2]

2- نقل الإجراءات في جرائم التوقيع الإلكتروني

يقصد بالمساعدة القضائية في هذه الحالة قيام دولة باتخاذ إجراءات جنائية بناءً على اتفاقية أو معاهدة، لصالح دولة أخرى في جريمة ارتكبت في إقليمها، بشرط توافر شروط معينة، أبرزها التجريم المزدوج، أي أن يكون الفعل المنسوب إلى الجاني مجرمًا في كلا البلدين، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها في الدولة المطلوبة. ومع ذلك، فإن الاعتماد على الآليات التقليدية للتعاون القضائي عبر القنوات الدبلوماسية يؤدي إلى بطء الإجراءات، وهو ما يتعارض مع طبيعة الجرائم الإلكترونية التي تتطلب استجابة سريعة. ولهذا تم إبرام اتفاقيات جديدة تسهل الوقت والإجراءات عبر الاتصال المباشر بين السلطات المعنية، مثل الاتفاقية بين الولايات المتحدة وكندا التي تسمح بتبادل المعلومات شفوياً في حالات الاستعجال..[3]

3- الإنابة القضائية في جرائم التوقيع الإلكتروني:

الإنابة القضائية هي طلب من دولة إلى أخرى لتنفيذ إجراء قضائي في قضية جنائية دولية معلوماتية نيابة عن الدولة الطالبة. ويتم ذلك عندما تكون الدولة الطالبة قادرة على القيام بالإجراء بنفسها، ولكن تطلب المساعدة من الدولة الأخرى لتنفيذه على أراضيها..[4]

---

[1] Art 66 of Romania law, N°161, 2003 , on measures to ensure transparency in the exercise of public dignities , public position and in the business environment , and for preventing and sanctioning , corruption published in the official gazette , n°: 279 , April 21, 2003.

[2]- يزيد بوحليط، المرجع السابق، ص 516-517.

[3]- سالم محمد سليمان الأوحلي، **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية دراسة مقارنة**، رسالة دكتوراه، جامعة عين شمس، مصر، 1998، ص 428.

[4]- د. طارق , ابراهيم الدسوقي, **الأمن المعلوماتي , النظام القانوني للحماية المعلوماتية** ,دار الجامعة الجديدة , الاسكندرية , 2009, ص 601

الإنابة القضائية تسهم في تسهيل الإجراءات الجنائية بين الدول، مما يسمح بتنفيذ التحقيقات الضرورية وتقديم المتهمين للمحاكمة. تساعد هذه الآلية على تجاوز عقبة السيادة الإقليمية التي قد تمنع دولة من القيام ببعض الأعمال القضائية داخل أراضي دولة أخرى، مثل سماع الشهود أو تنفيذ التفتيش والحجز. تم إبرام العديد من الاتفاقيات في هذا المجال، مثل تلك الموقعة بين فرنسا والجزائر في 1962، وبين الجزائر وألمانيا في 1984، وبين مصر ودول أخرى مثل الكويت 1988، إلى جانب الاتفاقيات الأوروبية والعربية التي تعزز التعاون القضائي في المواد الجنائية.[1]

ثانيا: الإجراءات القانونية المتبعة في مجال تسليم المجرمين:

تسليم المجرمين، حسب المحكمة العليا الأمريكية، هو إجراء قانوني يعتمد على معاهدة، معاملة بالمثل، أو قانون وطني، حيث تقوم دولة ما بتسليم شخص متهم أو مرتكب جريمة جنائية إلى دولة أخرى بناءً على مخالفة القوانين الخاصة بالدولة الطالبة أو مخالفة القانون الجنائي الدولي، والتي يعاقب عليها في الدولة الطالبة. وتتنوع مصادر تسليم المجرمين إلى مصادر أصلية تشمل المعاهدات والاتفاقيات الثنائية التي تتم بين دولتين وفقًا لشروط وضوابط متفق عليها، كما توجد اتفاقيات تسليم متعددة الأطراف التي تشمل عدة دول، مثل اتفاقية جامعة الدول العربية لتسليم المجرمين عام 1953 والاتفاقية الأوروبية الدولية لتسليم المجرمين 1957. بالإضافة إلى ذلك، تشمل المصادر الأصلية أيضًا القوانين الداخلية الدولية والعرف. أما المصادر الاحتياطية فتتمثل في قواعد الأخلاق والمعاملة بالمثل بين الدول.

I. شروط تسليم المجرمين في جر ائم الاعتداء على التوقيع الإلكتروني.

لقد وضعت الاتفاقيات الدولية عدة شروط لتسليم المجرمين وهي:

1- عدم جواز تسليم الرعايا:

من المبادئ الدولية المعتمدة في معظم التشريعات الوطنية والاتفاقيات الدولية هو مبدأ عدم جواز تسليم الرعايا الذين ارتكبوا جرائم في دول أخرى. هذا المبدأ منصوص عليه في قوانين دول مثل فرنسا ومصر، حيث ينص الدستور المصري على أنه "لا يجوز إبعاد مواطن عن البلاد". وتتبنى نفس القاعدة دول أخرى مثل سويسرا وألمانيا، وفي معاهدات مثل معاهدة تسليم المجرمين بين العراق والسعودية. ومع ذلك، بعض الدول تفرض قيودًا على تسليم رعاياها. مثلًا، في القانون الفرنسي، يمكن تسليم شخص فرنسي اكتسب الجنسية بعد ارتكاب جريمة، ولا يمنع القانون الفرنسي مرور شخص فرنسي عبر أراضيها لتسليمه .

[1]- فهد عبد الله العبيد العازمي، المرجع السابق، ص 494

2-عدم التسليم في الجرائم السياسية

لا يجوز تسليم الأفراد في الجرائم السياسية، حيث أن التسليم قد يكون هدفه اتخاذ إجراءات انتقامية ضد الشخص المطلوب تسليمه، وهو أمر لا يجوز أن تشارك فيه الدولة المطلوبة. وقد أكدت اتفاقية باليرمو بشأن جرائم الكمبيوتر في البند العاشر من المادة 16 أن الدولة التي ترفض طلب التسليم ملزمة بمعاقبة المتهم. كما نصت الاتفاقية العربية لمكافحة الجريمة في المادة 6/ف1 على أنه لا يجوز التسليم إذا كانت الجريمة الموجهة ضد الشخص تُعد جريمة سياسية وفقًا لقوانين الدولة المتعاقدة. نفس المبدأ موجود في معاهدة الأمم المتحدة النموذجية لعام 1950 واتفاقية جامعة الدول العربية لتسليم المجرمين لعام 1952، بالإضافة إلى المادة 20 من الاتفاقية الأمنية لدول مجلس التعاون الخليجي.

3-عدم جواز التسليم في الجرائم العسكرية:

تنص المادة 06 من الاتفاقية العربية لمكافحة الجرائم على أنه لا يجوز تسليم الشخص إذا كانت الجريمة المطلوب تسليمه من أجلها تتعلق بالإخلال بالواجبات العسكرية. كما لا يجوز التسليم إذا كان الشخص قد تمت محاكمته بالفعل عن الجريمة المطلوبة، أو تم معاقبته بشأنها. بالإضافة إلى ذلك، لا يجوز التسليم إذا كان الشخص قيد التحقيق أو المحاكمة عن نفس الفعل المطلوب تسليمه من أجله[1].

4- عدم انقضاء الدعوى العمومية أو العقوبة:

يشترط بجواز التسليم ألا تكون الدعوى العمومية أو حكم القاضي يفرض العقوبة قد انقضى بأحد أساليب الانقضاء المحددة في التشريعات الوطنية للدولة طالبة التسليم والمطلوب إليها التسليم أو الدولة التي ارتكبت الجريمة على أراضيها"[2].

II. إجراءات تسليم المجرمين في جرائم الاعتداء على التوقيع الإلكتروني.

تتمثل القواعد الإجرائية التي تتبعها الدول الأطراف في عملية التسليم في مراعاة التوازن بين حماية حقوق الإنسان وحريته وبين ضمان تحقيق التعاون الدولي لمكافحة الجريمة. تهدف هذه القواعد إلى التأكد من أن المجرمين لا يفلتون من العقاب، مع مراعاة ضمانات حقوق الإنسان في كافة مراحل عملية التسليم وفقاً لقوانين الدول المعنية

-مراحل طلب التسليم: يمر طلب التسليم بثلاث مراحل:

[1] محمد كمال محمود الدوسوقي، **الحماية الجنائية السرية المعلومات الالكترونية** ،دار الفكر والقانون ، المصورة مصر 2010 ص 185

[2] ياسر محمد الكومي محمود أبو حطب، **الحماية الجنائية والأمنية التوقيع الالكتروني, دراسة مقرانة**, رسالة دكتوراه في القانون الخاص ، جامعة حلوان ،مصر ، 2014 ،ص 360 .

أ-المرحلة الأولى: تتمثل في تلقي الطلب واتخاذ إجراءات التحري وجمع الاستدلالات والقبض على الشخص المطلوب وهي من اختصاص الشرطة.

ب-المرحلة الثانية: استجواب المقبوض عليه وحبسه احتياطيا، أو إطلاق سراحه بكفالة أو بدونها، أو كمنعه من مغادرة الأراضي الإقليمية إلا أن يتم الفصل ي الطلب الوارد بشأن وهيمن اختصاص الادعاء العام.

ج-المرحلة الثالثة: وهي فحص الطلب من قبل الحكمة المختصة والبت فيه بالقبول أو بالرفض مع توافر الشروط الشكلية.[1]

III. القيود الواردة في تسليم المجرمين.

عند تسليم المجرمين أحد أهم صور التعاون القضائي الدولي، إلا أن القانون الجزائري قد وضع جملة من القيود والضمانات التي تحول دون التسليم في بعض الحالات، وذلك حمايةً لحقوق الأفراد واحترامًا للسيادة الوطنية. وقد نص قانون الإجراءات الجزائية، في المواد من 702 إلى 713، على الضوابط العامة المتعلقة بآليات التسليم، وبيّن الحالات التي لا يجوز فيها التسليم[2]

ومن بين أبرز هذه القيود ما يلي:

- عدم جواز تسليم المواطن الجزائري، حيث تنص المادة 711 من قانون الإجراءات الجزائية على أنه لا يجوز تسليم أي شخص يحمل الجنسية الجزائرية، حتى لو ارتكب الجريمة في الخارج، بل يُمكن أن يُحاكم أمام القضاء الوطني.
- الطبيعة السياسية للجريمة، حيث يُرفض تسليم الشخص إذا كانت الجريمة المطلوب من أجلها التسليم ذات طابع سياسي، وفقًا لما تقرره السلطات الجزائرية.
- الجرائم العسكرية الخالصة، لا يجوز التسليم إذا كانت الأفعال تدخل ضمن اختصاص القضاء العسكري المحض.
- غياب مبدأ التجريم المزدوج، أي إذا كان الفعل المطلوب بشأنه التسليم لا يُشكل جريمة في القانون الجزائري.
- احتمال التعرض للاضطهاد أو المعاملة غير الإنسانية، إذ يُمنع التسليم إذا وُجدت مؤشرات قوية على تعرض المطلوب للتعذيب أو الاضطهاد أو محاكمة غير عادلة في الدولة الطالبة.

---

[1]- سليمان أحمد فضل , **المواجهة التشريعية و الأمينة للجر ائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)** ، دار النهضة العربية، القاهرة ، مصر ، 2008، ص 421.

[2] -

- العفو أو سقوط الجريمة بالتقادم، في حال كانت الجريمة مشمولة بالعفو أو سقطت بالتقادم حسب القانون الجزائري.

الفرع الثاني: العقبات التي تواجه التعاون القضائي الدولي في الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من التحديات الكبرى التي تواجه الأنظمة القضائية في ظل التطور التكنولوجي السريع والاعتماد المتزايد على الإنترنت. تشمل هذه الجرائم تهديدات مثل القرصنة، الاحتيال الإلكتروني، وسرقة البيانات الشخصية، مما يزيد من صعوبة التعاون القضائي الدولي لمكافحتها بفعالية،حيث قسمنا هذا الفرع الى تباين و اختلاف التشريعات الوطنية وتطبيق القواعد التقليدية في الجرائم الإلكترونية (أولا) , و اختلاف النظم القانونية الإجرائية الجنائية(ثانيا) , ثم الصعوبات المتعلقة بالمساعدات القضائية الدولية في مكافحة جرائم التوقيع الالكتروني (ثالثاً).

أولًا :تباين و اختلاف التشريعات الوطنية وتطبيق القواعد التقليدية في الجرائم الإلكترونية

يؤثر اختلاف النظم القانونية والتشريعات العقابية بشكل كبير على تحقيق التعاون الدولي في مكافحة الجرائم الإلكترونية. أحد العوامل الرئيسية في هذا السياق هو اشتراط تجريم الفعل ذاته في التشريعات الوطنية، خصوصًا في قضايا تسليم المجرمين. العديد من الدول لم تصدر تشريعات خاصة بالجرائم الإلكترونية أو لم تضع آليات مناسبة لمواجهتها. كما أن تطبيق القواعد التقليدية الإجرائية والعقابية على الجرائم الإلكترونية يظهر فجوات كبيرة بين الأنظمة القانونية المختلفة. فبعض الأفعال التي تعتبر مشروعة في بعض الأنظمة قد تكون مجرمة في أنظمة أخرى، ويرجع ذلك إلى الاختلافات الثقافية والدينية والعادات والتقاليد بين الدول، مما يساهم في تنوع السياسات التشريعية من مجتمع إلى آخر[1].

ثانيًا- اختلاف النظم القانونية الإجرائية الجنائية

بسبب تنوع النظم القانونية الإجرائية واختلافها، تتباين طرق التحري والتحقيق والمحاكمة من دولة إلى أخرى، مما يجعل بعض الإجراءات فعّالة في دولة ما ولكن غير قابلة للتطبيق في دولة أخرى. على سبيل المثال، تقنيات مثل المراقبة الإلكترونية، التسليم المراقب، والعمليات المستترة قد تكون مشروعة في بعض الدول، بينما تُعتبر غير قانونية في دول أخرى. وبالتالي، إذا اعتُبرت طريقة جمع الأدلة قانونية في دولة ما، فقد تكون غير مشروعة في دولة أخرى، مما يؤدي إلى عدم القدرة على استخدام هذه الأدلة في الدولة الثانية. هذا الاختلاف يمكن أن يسبب خيبة أمل للسلطات القضائية

[1] - السيد عبد الفتاح على، **مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل**، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية ،2017م، ص447.

في الدولة الأولى، حيث لا تتمكن من استخدام الأدوات التي تعتبرها فعّالة لجمع الأدلة، حتى وإن كانت هذه الأدلة قد تم جمعها بشكل قانوني في اختصاص قضائي.[1]

نظرًا لاختلاف التشريعات فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود، يتطلب الأمر إعادة صياغة أطر التعاون القضائي بين الدول. منذ عام 1993، أدرك المجلس الأوروبي التحديات التي تثيرها الشبكة المعلوماتية في الإجراءات الجنائية. ولتحسين التعاون، يُقترح أن تتعاون دول مثل الإمارات ومصر من خلال تبادل الإنابة القضائية الدولية، التي تسمح لدولة ما بطلب إجراءات تحقيق من دولة أخرى نيابة عنها، مثل التفتيش أو سماع الشهود أو مراقبة الشبكة المعلوماتية2.

ثالثاً: الصعوبات المتعلقة بالمساعدات القضائية الدولية في مكافحة جر ائم التوقيع الالكتروني

تُعد الإنابة القضائية الدولية من أبرز صور المساعدات القضائية في المجال الجنائي، حيث تعتمد الدول عليها لضمان تنفيذ إجراءات التحقيق والمحاكمة عبر الحدود. غير أن الأسلوب التقليدي لتقديم طلبات الإنابة عبر القنوات الدبلوماسية غالبًا ما يؤدي إلى بطء في الإجراءات وتعقيد في التنفيذ، وهو ما يتعارض مع طبيعة الجرائم الإلكترونية التي تتميز بالسرعة [3]، مما قد يُضعف فعالية الملاحقة القانونية للمجرمين الرقميين.

ومن بين التحديات الكبرى التي تواجه المساعدات القضائية الدولية، التباطؤ في الاستجابة للطلبات المقدمة، حيث تواجه الدول المتلقية لهذه الطلبات عقبات متعددة، مثل نقص الموظفين المؤهلين في التحقيقات الإلكترونية، والصعوبات اللغوية التي تعرقل تحليل البيانات والمعلومات الواردة، فضلاً عن الفوارق في النظم القانونية والإجرائية بين الدول، مما يجعل التعامل مع القضايا العابرة للحدود أكثر تعقيدًا.

هذا التأخير قد يؤدي إلى إغلاق بعض القضايا بسبب عدم تلقي الردود في الوقت المناسب[4]، وهو ما يمثل تحديًا خطيرًا، خاصة في الجرائم الإلكترونية التي تعتمد على البيانات الرقمية كأدلة رئيسية. فمع مرور الوقت، قد تتعرض هذه البيانات للتلاعب أو الحذف، ما يُضعف حجية الأدلة الجنائية ويُعقد مسألة تقديم الجناة للعدالة[5].لذلك، أصبح من الضروري تطوير آليات تعاون قضائي أكثر سرعة وفعالية، مثل تبني بروتوكولات رقمية لتبادل المعلومات، وإنشاء منصات أمنية تُسهّل التنسيق

[1]- السيد عبد الفتاح على، المرجع السابق، ص448.

[2]- سعيد علي بحبوح النقبي ،**المواجهة الجنائية للإرهاب، في ضوء الأحكام الموضوعية والإجر ائية للقانون الدولي والداخلي، دارسة مقارنة**، الطبعة الأولى ، دار النهضة العربية، القاهرة ،2011، ص815.

[3]- السيد عبد الفتاح على, المرجع سابق، ص450.

[4] -خالد ممدوح إبراهيم, المرجع سابق، ص414-415.

[5] د. طارق إبراهيم الدسوقي, المرجع سابق، ص602

بين الدول، مما يُعزز القدرة على تعقب الجرائم الإلكترونية ومحاسبة مرتكبيها بفعالية أكبر، مع ضمان حماية الحقوق القانونية للأفراد في البيئة الرقمية.

وفي نهاية هذا الفصل يمكن القول أن الأحكام الإجرائية لمكافحة جريمة التوقيع الإلكتروني جزءاً محورياً من المنظومة القانونية الحديثة التي تهدف إلى حماية التعاملات الرقمية وضمان مصداقيتها. وتشمل هذه الأحكام مجموعة من الإجراءات القانونية التي تنظم كيفية التحقيق في الجرائم المرتبطة بالتوقيع الإلكتروني، من جمع الأدلة الرقمية، والتحقق من صحة التوقيع، إلى ضمان موثوقية وسائل الإثبات الإلكترونية. وتحرص التشريعات على مراعاة التوازن بين حماية الحق في الخصوصية وضمان النزاهة في الإثبات، حيث يُشترط في كثير من الأنظمة أن يكون التوقيع الإلكتروني مُعترفاً به قانوناً ومصحوباً بشهادة رقمية صادرة من جهة معتمدة. كما تُمنح السلطات القضائية صلاحيات خاصة للتعامل مع هذا النوع من الجرائم، بما يشمل الاستعانة بخبراء تقنيين، وضمان سرية البيانات أثناء التحقيق، بالإضافة إلى وضع عقوبات رادعة لكل من يثبت تورطه في تزوير أو استخدام توقيع إلكتروني بطريقة غير مشروعة. وبهذا تسهم هذه الأحكام في تعزيز الثقة في البيئة الرقمية، وتوفير حماية قانونية فعالة للأطراف المتعاملة إلكترونياً.

حيث تتمثل الأحكام الإجرائية لمكافحة جريمة التوقيع الإلكتروني في مجموعة من القواعد القانونية التي تنظم كيفية تعقب هذه الجريمة والتحقيق فيها ومقاضاة مرتكبيها، بما يضمن حماية المعاملات الإلكترونية وسلامتها. وتشمل هذه الإجراءات تحديد الجهة المختصة بالتحقيق، واعتماد وسائل الإثبات الرقمية كالدلائل المستخرجة من الأجهزة الإلكترونية، وإخضاع التوقيعات الإلكترونية للفحص الفني من قبل خبراء مختصين للتأكد من صحتها. كما تنص القوانين على ضمان حقوق المتهم أثناء التحقيق، مثل سرية البيانات وحق الدفاع، بالإضافة إلى تنظيم إجراءات تفتيش الأجهزة ومصادرتها بإذن قضائي. وتهدف هذه الأحكام إلى تحقيق التوازن بين مكافحة الجريمة وحماية الحقوق والحريات في البيئة الرقمية.

لقد بدأ المشرع الجزائري بمعالجة الجرائم الواقعة على التوقيع الإلكتروني من خلال إجراءات تقليدية بسيطة وذات طابع كلاسيكي، تعكس في بدايتها محدودية الإطار القانوني في مواجهة جرائم التوقيع الإلكتروني المتطورة. غير أن التطور السريع في وسائل التقنية الرقمية، وازدياد التهديدات المرتبطة بها، دفع بالمشرع إلى تطوير منظومته القانونية والإجرائية، ويمنحه الحماية القانونية اللازمة بموجب التشريعات الخاصة كالقانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين. وفي هذا الإطار، تم اعتماد إجراءات دقيقة على المستويين الفني والقانوني لضبط هذه الجرائم وملاحقة مرتكبيها، منها تعزيز آليات التبليغ عن جرائم التوقيع الإلكتروني، وإتاحة إمكانية تقديم الشكاوى المتعلقة بالجرائم الماسة بالتوقيع الإلكتروني، إضافة إلى السماح باعتراض المراسلات ذات الصلة،

وتسجيل الأصوات والتقاط الصور عند الاقتضاء، وذلك ضمن ضوابط قانونية تكفل احترام الحقوق والحريات الفردية، وتراعي مبدأ الشرعية الإجرائية.

كما أن الشرطة الجنائية الدولية (الإنتربول) تلعب دورًا محوريًا في مكافحة جرائم التوقيع الإلكتروني من خلال تنسيق الجهود بين الدول وتبادل المعلومات التقنية. تساهم في تطوير أدوات التحقيق الرقمية وتدريب كوادر إنفاذ القانون على تتبع الجرائم السيبرانية. كما يُعزز التعاون القضائي الدولي عبر الاتفاقيات وآليات تسليم المجرمين لضمان ملاحقة الجناة العابرين للحدود.


خاتمة

بعد تطرقنا لموضوع " الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري،" تبيّن أن هذا الأخير بات يشكل عنصرًا جوهريًا لضمان أمن المعاملات الإلكترونية، مما استدعى ضرورة توفير حماية جنائية فعالة له .وقد سعى المشرع الجزائري، من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، إلى وضع إطار قانوني ينظم هذه العمليات ويحدد العقوبات اللازمة لمواجهة إساءة استخدام هذه التقنية .كما جاء القانون رقم 18-05 المتعلق بالتجارة الالكترونية لتعزيز هذا الإطار، حيث تضمن تعديلات وإضافات تدعم الموثوقية القانونية للتعاملات الإلكترونية وتكرّس مبادئ الأمن المعلوماتي.

وفي هذا السياق، تم التطرق إلى مقتضيات التوقيع الإلكتروني كمحل للحماية الجنائية، حيث ناقشنا مفهومه وأهميته القانونية في ضمان مصداقية المستندات الإلكترونية .كما سلطنا الضوء على الجرائم التي تهدد سلامة التوقيع الإلكتروني، من تزوير البيانات إلى استخدامه في أنشطة غير مشروعة، مع بيان العقوبات المنصوص عليها لمكافحة هذه الأفعال.

أما من حيث الجانب الإجرائي، فقد تناول البحث السياسة المعتمدة في مكافحة جرائم التوقيع الإلكتروني، لا سيما ما يتعلق بإجراءات الإثبات التي تمزج بين الأدلة التقليدية والحديثة لضمان فعالية التحقيقات .كما تطرقنا إلى إشكالية الاختصاص القضائي، نظرًا للطابع العابر للحدود لهذه الجرائم، وهو ما يستلزم تعاونًا دوليًا فعالًا في تبادل المعلومات والملاحقة القضائية للجناة.

ويُعد التعاون الأمني والقضائي الدولي ركيزة أساسية لمكافحة هذه الجرائم، حيث يتيح التنسيق وتبادل الخبرات وإنشاء هيئات متخصصة لمعالجة التحديات التقنية والقانونية، ما يسهم في تعزيز فعالية إنفاذ القانون وضمان عدم الإفلات من العقاب.

وفي الختام، يمكن القول إن الإطار القانوني الجزائري، رغم ما شهده من تطور بفضل القانونين 15-04 و 18-05 ، لا يزال بحاجة إلى تحديث مستمر لمواكبة التقدم التكنولوجي، وتعزيز آليات التعاون الدولي، بما يضمن حماية جنائية أكثر فاعلية للتوقيع الإلكتروني ويوفر بيئة قانونية آمنة للتعاملات الرقمية.

الإطار القانوني الجزائري يوفر حماية جنائية للتوقيع الإلكتروني من خلال قانون رقم15-04 ، إلا أن فعالية. هذه الحماية تتوقف على التطبيق العملي ومدى القدرة على ضبط الجرائم الرقمية.

استناداً إلى ما تم التوصل إليه من خلال هذه الدراسة، يُمكن تلخيص النتائج على الوجه الآتي :

1. أول ما يمكن استنتاجه هو عدم وجود تعريف جامع مانع لبعض الأفعال المجرمة المرتبطة بالتوقيع الإلكتروني، مما نتج عنه الإختلاف المتباين في الأفعال التي تعد من قبيل جرائم التوقيع الإلكتروني، وقد يكون سبب ذلك الطبيعة المتسارعة والتطور الكبير الذي تشهده هذه الجريمة الخطيرة وعدم قدرة التشريع على مجاراتها .
2. - قيام حماية جزائية للتوقيع الإلكتروني، حيث أن تم تجريم بعض الأفعال المتعلقة باستعمال التوقيع الإلكتروني، مثل تزوير التوقيع الإلكتروني. واستعمال توقيع إلكتروني مزور. وكذا استعمال غير المشروع لشهادة تصديق إلكترونية. أن هذه الجرائم تُعامل كجرائم التزوير والاحتيال ويُعاقب عليها في قانون العقوبات.
3. وجود الاعتراف القانوني بالتوقيع الإلكتروني ،حيث يعترف المشرّع الجزائري بالتوقيع الإلكتروني كوسيلة قانونية لإثبات التصرفات القانونية، وله حجية مماثلة للتوقيع الخطي التقليدي، إذا تم وفق الشروط القانونية
4. الاختصاص القضائي في الجرائم الإلكترونية يواجه تحديات نظرًا للطبيعة العابرة للحدود لهذه الجرائم، مما يستدعي وضع قواعد واضحة لمعالجة مسائل الاختصاص وملاحقة الجناة.
5. وجود قصور في الإجراءات التقنية والقضائية للتثبت من صحة التوقيع أو كشف التزوير.
6. التعاون الدولي يلعب دورًا محوريًا في مكافحة جريمة التوقيع الالكتروني على غرار باقي الجرائم الإلكترونية، حيث يُعدّ تبادل المعلومات بين الدول وإنشاء هيئات متخصصة أمرًا ضروريًا لضمان استجابة فعالة لهذه التحديات.
7. آليات المكافحة الحالية غير كافية لمجابهة جريمة التوقيع الإلكتروني، فلا يمكن لأي دولة مهما بلغ تطورها التكنولوجي والمعلوماتي أن تتصدي لهذه الجريمة العالمية بمفردها، فالمجرم الإلكتروني قد يكون في دولة ما وينفذ جريمته الإلكترونية في دولة ثانية، وبالإمكان أن تتحقق نتيجتها في دولة ثالثة، أو حتى في عدة دول مما يُصَعِب عملية متابعته خاصة في حالة عدم وجود اتفاقية بين الدولة التي يتواجد على أرضها والدولة المطالبة به، وعليه فإن آليات المكافحة المخصصة من طرف بعض الدول تعد غير كافية للتصدي للجريمة الإلكترونية

استنادًا إلى النتائج التي توصلت إليها هذه الدراسة، تقتضي الضرورة التشريعية، في إطار مكافحة الجرائم المرتبطة بالتوقيع الإلكتروني، اعتماد عدد من التوصيات، والتي يمكن تلخيصها على النحو التالي:

1- تحيين الإطار القانوني: مراجعة وتحيين القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني لمواكبة التطورات التكنولوجية والمعايير الدولية الحديثة (مثل اللائحة الأوروبية eIDAS)..

2- لابد من تفعيل آليات التعاون الدولي الذي يتسم بسرعة التنفيد حتى لا يترك للمجرم الإلكتروني ملاذا آمنا يلتجئ إليه, وتوسيع الإتفاقيات الدولية الثنائية و الجماعية لمكافحة الجرائم الإلكترونية.

3- تمكين سلطة التحقيق بنص قانوني حول اختراق نظام الحاسب و ضبط ما يحتويه لضرورة التحقيق لأجل ظهور الحقيقة و ضبط قواعد التفتيش و المعاينة و ضبط الأدلة في إطار المشروعية الإجرائية.

4- إعادة النظر في قواعد الإختصاص القضائي و المسلمات القانونية كمبدأ السيادة ' كون الجريمة الالكترونية عابرة للحدود وترتكب في عالم افتراضي غير ملموس ماديا.

5- توحيد مدى قبول الدليل الالكتروني على المستوى الدولي في اطار اتفاقية دولية تبرم لهذا الشأن.

6- إعتماد برامج وتطبيقات معلوماتية من طرف وزارة العدل يعد غير قابلة للطعن في موثوقيتها إلا بالدليل العلمي العكسي. تجربتها وتفحصها لإستعمالها كمراجع في إستخراج الأدلة الإلكترونية .

7- العمل على إنشاء وسائل وآليات التعاون الدولي لأجل تسريع الرقمية في آجال لازمة للتدخل من خلال وسائل الاتصالات الحديثة مثل البريد الالكتروني أو الإنضمام لشبكة التواصل بالجزائر بين الدول بإقتراح الانضمام لشبكة | لتكون كنقطة إتصال متاحة طوال 24 ساعة يوميا ولمدة سبعة أيام أسبوعيا وذلك لضمان توافر المساعدة الفورية لأغراض التحقيقات والإجراءات الخاصة بجمع الأدلة للجرائم في شكل إلكتروني.

8- إنشاء منصة Plate-forme لتبادل المنشورات الفنية والخبرات بين مصالح الضبطية المتخصصة داخليا ودوليا في إطار بروتوكولات و اتفاقات ثنائية .

9- يتعين على القائمين على الشؤون القانونية والقضائية الإهتمام بتكوين رجال البحث والتحري في الجرائم الإلكترونية تكويناً قانونياً، وتكوين رجال العدالة تكويناً تقنياً حتى يكون هناك تكامل وتنسيق فيما بينهم للوصول إلى أدلة إلكترونية صحيحة ومقبولة أمام الجهات المعنية.

10- إنشاء محكمة جنائية دولية تحت مظلة الأمم المتحدة يكون لها صلاحية النظر في القضايا التي تعنى بالجرائم الإلكترونية الخطيرة ذات الطابع الدولي.

قائمة المراجع

أولا: الكتب

1. إبراهيم خالد ممدوح ،التوقيع الالكتروني ،بدون طبعة ،الدار الجامعية ،الإسكندرية ،2010 ،ص 63.
2. أحمد حزيط، الوجيز في الإجراءات الجزائية، الطبعة الثانية، دارهومة، الجزائر، 2015.
3. أحمد عصام عجيلة، الحماية الجنائية للمحررات الإلكترونية، دار النهضة العربية، القاهرة،2014.
4. أحمد عوض، بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، الطبعة الثانية دار النهضة العربية القاهرة، 2006.
5. السيد عبد الفتاح على، مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية ،2017
6. إلياس ناصيف، العقود الدولية العقد الإلكتروني في القانون المقارن، الطبعة الاولى ، منشورات الحلبي الحقوقية، لبنان،2009
7. حسام محمد نبيل الشرافي، جرائم الاعتداء على التوقيع الإلكتروني، دار الكتب القانونية، مصر، 2013
8. حسنين شفيق، الإعلام الجديد والجريمة الإلكترونية، الطبعة الاولى، دار فكر وفن للطباعة و النشر والتوزيع ،مدينة السادس من أكتوبر 2015،
9. حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)،دار النهضة العربية ، القاهرة، مصر ، 2009 .
10. خالد حسن أحمد لطفي. الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية. دار الفكر الجامعي، الاسكندرية: سنة 2020،
11. خالد ممدوح ابراهيم، إبرام العقد الالكتروني، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2011
12. داود سليمان علي الحمادي ، أحكام جريمة التزوير الالكترونية , دار النهضة العربية , القاهرة , مصر , 2008.
13. سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دار الكتب القانونية، مصر، 2009 ،
14. سامح عبد الواحد التهامي، التعاقد عبر الانترنت دراسة مقارنة، دار الكتب القانونية ، دار شتات للنشر و البرمجيات، مصر، 2008
15. سعيد السيد قنديل، التوقيع الالكتروني ، دار الجامع الجديدة ، الاسكندرية ،مصر ، 2006.
16. سعيد علي بحبوح النقبي ،المواجهة الجنائية للإرهاب، في ضوء الأحكام الموضوعية والإجرائية للقانون الدولي والداخلي، دارسة مقارنة ، الطبعة الأولى، دار النهضة العربية، القاهرة،2011

17. سليمان أحمد فضل , المواجهة التشريعية و الأمينة للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) ، دار النهضة العربية، القاهرة ، مصر ، 2008
18. شنتير خضرة, الأليات القانونية لمكافحة الجريمة الالكترونية،دراسة مقارانة ،ابن النديم للنشر و التوزيع، وهران ، 2022 .
19. صفاء فتوح جمعة، العقد الإداري الالكتروني، بدون طبعة ، دار الفكر والقانون، المنصورة، ، 2018،
20. صلاح رزق عبد الغفار يونس ، جرائم الاستغلال الاقتصادي للأطفال ، الطبعة الاولى، دار الفكر والقانون ، مصر ، 2015 .
21. طارق , ابراهيم الدسوقي, الأمن المعلوماتي , النظام القانوني للحماية المعلوماتية ,دار الجامعة الجديدة , الاسكندرية , 2009.
22. طارق المجالي، الجريمة المنظمة والتعاون الأمني الدولي، الطبعة الاولى، دار الحامد، عمان، 2018.
23. عباس العبودي ، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها ، الطبعة الاولى ،منشورات الحلبي الحقوقية ، بيروت – لبنان ، 2010
24. عبد الرحمان الخلفان الحارثي، حجية التوقيع الالكتروني في الاثبات دراسة مقارنة، الطبعة الأولى، مركز بحوث شرطة الشارقة، الامارات العربية المتحدة، 2019، ص38
25. عبد الفتاح بيومي حجازي ، حماية المستهلك عبر شبكة الانترنت ، دار الكتب القانونية ، مصر ، 2008
26. عبد القادر بوعرفة، التعاون الدولي في مكافحة الجرائم الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2017
27. عبد القادر عدو، الجريمة الإلكترونية إجرائيا، الطبعة الثانية، دار هومة، الجزائر، 2016.
28. عبد المهيمن بكر، قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1974
29. عصام عبد الفتاح مطر، التحكيم الالكتروني (ماهيته، اجراءاته، وآلياته في تسوية منازعات التجارة الالكترونية والعلامات التجارية وحقوق الملكية الفكرية، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2009،
30. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة دراسة الإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات ،الطبعة الأولى، إشراك للنشر والتوزيع، مصر، 2000.
31. علاء محمد نصيرات، حجية التوقيع الإلكتروني في الاثبات، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2005،
32. علي عبد القادر قهوجي ،الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة،سنة 1999،

33. عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، الطبعة أولى، دار الثقافة للنشر والتوزيع، عمان، الاردن،2009
34. غرداين حسام، الجريمة الإلكترونية وإجراءات التصدي لها، مذكرة تخرج لنيل شهادة الماستر،كلية الحقوق، جامعة الجزائر، 2015/2014.
35. غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، االجزائر،2015،
36. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2016.
37. فيصل عبد الله طلافحة - ملاك تامر ميخائيل ، إجراءات القبض والتقديم أمام المحكمة الجنائية الدولية ،الطبعة الاولى، مركز الكتاب الأكاديمي الأردن 2016 .
38. محمد إبراهيم خيري الوكيل مكافحة جريمة غسيل الأموال في المملكة العربية السعودية ، الطبعة الاولى، مكتبة القانون والاقتصاد ، السعودية.1992
39. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري و المقارن، درا الجامعة الجديدة، الاسكتدرية،2007
40. محمد عبيد الكعبي ،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة)،دار النهضة العربية، القاهرة مصر،2009
41. محمد عصفور، الوجيز في شرح قانون الإجراءات الجزائية، دار الجامعة الجديدة، الإسكندرية، 2016.
42. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية،القاهرة،1988 .
43. منتصر سعيد حمودة ، المنظمة الدولية للشرطة الجنائية " الانتربول " الطبعة الاولى ، دار الفكر الجامعي ، مصر، 2008.
44. منير محمد الجنبيهي ،ممدوح الجنبيهي ،تزوير التوقيع الإلكتروني،دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2008
45. منير الجنبهي، ممدوح الجنبهي، الشركات الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2008
46. مولاي ملياني بغدادي، الإجراءات الجزائية في التشريع الجزائري، المؤسسة الوطنية للكتاب، الجزائر،1992
47. ناصر جوادي ،إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، الطبعة الثالثة، دار العلوم ،الجزائر، 2011
48. هلالي عبد الله احمد، جرائم المعلوماتية التقليدية و المستحدثة و تطبيقها في النظام البحريني، دار النهضة العربية ،القاهرة ، 2013.

49. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

ثانيا: الرسائل والمذكرات الجامعية

❖ **أطروحات الدكتوراه:**

1. براهمي حنان، جريمة التزوير الوثيقة الإدارية الرسمية ذات الطبيعة المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي، جامعة محمد خيضر بسكرة،2015،
2. بشان عبد النور، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي والعلوم الجنائية، جامعة الجزائر 1 ،2018،
3. ترجمان نسيمة، الحماية الجنائية للتوقيع الالكتروني، دراسة مقارنة، أطروحة دكتوراه، تخصص التجريم في قانون الاعمال، جامعة ابن خلدون تيارت،2021،
4. زروق يوسف، حجية وسائل الاثبات الحديثة، أطروحة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، 2013،
5. سعدي ربيع، حجية التوقيع الالكتروني في التشريع الجزائري، أطروحة دكتوراه في القانون، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة 01 ،2017
6. صالح شنين ،الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، أطروحة دكتوراه، تخصص القانون الخاص،.جامعة تلمسان ،2013،
7. عبد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري(دراسة مقارنة)،أطروحة دكتوراه، تخصص قانون جنائي والعلوم الجنائية، جامعة الجزائر 1 ،2020،
8. معاشي سميرة، آليات مكافحة الجريمة المعلوماتية (دراسة مقارنة)،أطروحة دكتوراه تخصص قانون أعمال،جامعة محمد خيضر بسكرة،2020،

❖ **رسائل ماجيستير**

9. أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018،
10. آلاء أحمد محمد حاج علي، التنظيم القانوني لجهات التصديق على التوقيع الالكتروني، أطروحة ماجيستير تخصص قانون الخاص، جامعة النجاح الوطنية نابلس فلسطين، 2013،
11. امال قارة، الجريمة المعلوماتية، رسالة ماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر،2012،

12. لالوش راضية، أمن التوقيع الالكتروني، رسالة ماجستير في القانون تخصص القانون الدولي للاعمال، جامعة مولود معمري تيزي وزو،2012،
13. نائل طه ،جريمة الاحتيال (دراسة مفارنة)، أطروحة ماجستير، تخصص قانون عام، جامعة النجاح الوطنية، نابلس، فلسطين،2008،

❖ مذكرات ماستر

1. بوحفص راوية، الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص قانون جنائي،جامعة محمد خيضر بسكرة،2018،
2. سي مرابط زينب، غلام الله بنت الشيخ، الحماية القانونية للعقد المبرم عبر الانترنت، مذكرة ماستر في الحقوق تخصص علاقات مهنية، جامعة ابن خلدون تيارت، 2017،
3. فليح نور الدين ،الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، جامعة مولاي الطاهر سعيدة، 2019،
4. ياسمينة كواشي، الحماية الجنائية للتوقيع والتصديق الالكترونيين في ظل القانون، مذكرة ماستر تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، 2017،

ثالثا: المقالات والأبحاث

1. إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية، مجلة آفاق للبحوث والدراسات، العدد الرابع، المركز الجامعي إليزي، جوان 2019،
2. بن عزة محمد حمزة، حماية المستهلك الالكتروني من مخاطر البريد الدعائي (دراسة مقارنة)،مجلة المنار للبحوث والدراسات القانونية والسياسية، العدد03،جامعة عمر الثليجي الاغواط، ا 2003،
3. بودراع فايزة، بليمان يمينة، القوة الثبوتية للتوقيع الالكتروني، مجلة المعيار، المجلد 26 العدد (5 رت 67) ،جامعة قسنطينة، 2022
4. بولافة سامية،غيلاني الطاهر، التوقيع الالكتروني في ظل القانون 15-04، المجلة الجزائرية للامن الانساني، المجلد 5 العدد 01، جامعة باتنة 1 الجزائر،2020،
5. حرشاو مفتاح، التصديق الالكتروني ضمان لأمن المعاملات الالكترونية، مجلة أبحاث ودراسات التنمية، المجلد 10 ، العدد 01،جامعة برج بوعريريج، ، 2023،
6. حواس فتيحة، التوقيع الالكتروني (الخصوصيات والتطبيقات)، مجلة الدراسات القانونية المقارنة، المجلد 7 العدد01، جامعة حسيبة بن بوعلي الشلف الجزائر، 2021،
7. دحماني سمير،دراسة مقارنة بين التوجه الاوروبي 93/99 المتعلق بالتوقيعات الالكترونية والقانون رقم 15-04المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مجلة العلوم الانسانية ،العدد 01، المركز الجامعي تندوف، 2017

8. دهليس عادل، كاسحي موسى، دور وأهمية التوقيع الالكتروني في تسهيل المعاملات التجارية والمالية، مداخلة مقدمة في الملتقى الوطني حول الإصلاحات المالية والمصرفية –الواقع والمأمول- جامعة وهران 2 محمد بن أحمد، 2022
9. رابحي أحسن، الجريمة الالكترونية:النقطة المظلمة بالنسبة للتكنولوجية المعلوماتية، مجلة العلوم القانونية الاقتصادية والسياسية، العدد 01 ، جامعة الجزائر، سنة 2011
10. رامي بن الصديق، تزوير المحررات الإلكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07 العدد02 ، جامعة تنغاست، سنة 2018
11. رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحات، جامعة زيان عاشور الجلفة، العدد 01، 2009،
12. زكرياء مسعودي،جقريف الزهرة، التوقيع الالكتروني وحمايته لعملية الدفع الالكتروني، المجلة الدولية للبحوث القانونية والسياسية، جامعة الشهيد حمه لخضر الوادي، العدد 03، 2017،
13. عبد الله أبو رمان، دور الإنتربول في مكافحة الجريمة الدولية، مجلة العلوم القانونية، العدد 2، 2020.
14. فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري ،بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية، أكاديمية الدراسات العليا،ليبيا،أكتوبر،2009.
15. فاطمة الزهراء تبوب، التوقيع والتصديق الالكترونيين في ظل القانون رقم 15-04المؤرخ في أول فبراير 2015، حوليات جامعة الجزائر 1، العدد 29، الجزء الثاني، الجزائر، 2016،
16. فطيمة الزهراء مصدق، التصديق الالكتروني كوسيلة لحماية التوقيع الالكتروني، مجلة الدراسات والبحوث القانونية، المجلد 5العدد01، جامعة محمد بوضياف المسيلة ، 2020
17. قرفي ادريس، الجزاءات الجنائية الموقعة على الشخص المعنوي، مجلة الحقوق والعلوم الانسانية، جامعة زيان عاشور الجلفة، العدد 06، 2010،
18. كبير آمنة، التصديق الالكتروني (دراسة مقارنة)، مجلة القانون و المجتمع، العدد 6، جامعة أحمد درارية ،ادرار،2018،
19. ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وابحاث، العدد 1، جامعة زيان عاشور الجلفة، 2009،
20. محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها،مجلة دراسات و أبحات، العدد 01، جامعة زيان عاشور الجلفة، 2009،

21. مجاهدي خديجة، إستراتيجية المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس المدية الجزائر، المجلد الثاني، العدد الثاني، جوان 2015
22. محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع مجلة القانون والاقتصاد، العدد 51،جامعة القاهرة ، مصر، 1991.
23. محمد مدحت المراسي،أوجه الاستفادة من المعطيات العلمية والتكنولوجية المعاصرة في مجال تطوير برامج تأهيل رجال الشرطة مجلة مركز بحوث الشرطة، العدد22،أكاديمية الشرطة، سنة 2002
24. مزاولي محمد، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الالكترونية في القانون الجزائري، العدد 01، مجلة دراسات وابحاث، جامعة الجلفة، 2009،
25. مسعودي سوسف،أرجيلوس رحاب، مدى حجية التوقيع الالكتروني في التشريع الجزائري (دراسة على ضوء أحكام القانون 15-04)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنغاست، العدد 11، سنة 2017،
26. نبيل بوحميدي، الثورة التقنية ومسوغات التعديلات القانونية "التوقيع الإلكتروني نموذجا"، مجلة محاكمة، العدد 4، 2008
27. نجلاء عبد حسن، عبد الرسول عبد الرضا، تطور موقف المشرع العراقي في قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012، مجلة العلوم الإنسانية،العدد 2، جامعة بابل ،العراق،2013،
28. نعيمة دوادي، الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)، مجلة معهد اللغات، العدد01،جامعة حسيبة بن بوعللي الشلف، الجزائر، سنة 2020،
29. وسن قاسم الخفاجي وعلاء كاظم حسين, الحجية القانونية لشهادات تصديق التوقيع الالكتروني (دراسة مقارنة)، مجلة المحقق الحلي للعلوم القانونية والسياسية, ، العدد الرابع, السنة الثامنة, جامعة بابل العراق,2016
30. ياسمينة بونعارة، الجريمة الالكترونية، مجلة المعيار، العدد 39، قسنطينة،2015

رابعا: النصوص القانونية

1. القانون 05-10 المؤرخ في 10 يونيو 2005 يعدل ويتمم الأمر رقم -75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم، الجريدة الرسمية ، العدد 44، سنة 2005،ص 17
2. المرسوم التنفيذي رقم 07-162 المؤرخ في 30ماي 2007،يعدل ويتمم المرسوم التنفيذي رقم 01-123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشيكات بما فيها اللاسلكية

الكهربائية وعلى مختلف خدمات المواصلات السلكية والاسلكية، الجريدة الرسمية ، العدد 37، سنة 2007

3. القانون رقم 2000-03 المؤرخ 05 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية،،الجريدة الرسمية، العدد 48، 2000
4. القانون رقم 24-02 المؤرخ في 16 شعبان 1445 الموافق ل26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور. الجريدة الرسمية ، العدد 15،سنة 2024
5. القانون رقم 09-04 المؤرخ في 05 أغسطس 2009: المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ج.رج ج، العدد07،المؤرخة في 2009/08/16.
6. المنشور الوزاري المشترك رقم 05 المؤرخ في 4 أكتوبر 2020، المتعلق بتنظيم النيابات المتخصصة في مكافحة الجريمة السيبرانية، الصادر عن وزارة العدل ووزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 61، الصادرة في 7 أكتوبر 2020
7. القانون رقم 18-04 المؤرخ في 10 ماي 2018، والمتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية ، العدد 27، المؤرخة في 13 ماي 2018.
8. قانون الإجراءات الجزائية الجزائري، المحدد بالأمر 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم.
9. المرسوم التنفيذي المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق رقم 63 المؤرخة في 2006/10/08
10. المرسوم التنفيذي رقم 06-348 مؤرخ في 05/10/2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رعدد 63، العدل بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 17/10/2016

خامسا: المواقع الالكترونية

1. موقع وزارة البريد والمواصلات السلكية واللاسلكية الجزائرية ، /HTTPS://WWW.AGCE.DZ/AR/PRESENTATION-DE-LAGCE
2. موقع سلطة ضبط البريد و الاتصالات الالكترونية،https://www.arpce.dz/ar/about
3. موقع -سلطة ضبط البريد و الاتصالات الالكترونية، https://www.arpce.dz/ar/about
4. الاتفاقية العربية الموحدة لمكافحة جرائم تقنية المعلومات، https://esttf.motrans.gov.iq/wp-content/uploads/2016/04/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D9%80%D8%A7%D9%82%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-

%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf

5. قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية مع دليل الاشتراع 2001،
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-elecsig-a.pdf تاريخ الاطلاع 2025/02/13


الفهرس

الفهرس

الفصل الثاني: الاحكام الإجرائية لمكافحة جرائم التوقيع الالكتروني في التشريع الجزائري

الملخص

تعتبر الجرائم الالكترونية خاصة ما تعلق منها بالتوقيع الالكتروني وما يتفرع عنها من مشكلات، مقارنة مع الجرائم الواقعة على التوقيع التقليدي من أخطر الجرائم التي أفرزتها الثورة المعلوماتية، ومن أكثر ما يؤرق الافراد والدول في هذا العصر الموصوف بعصر التكنولوجيا، وتحسبا للعواقب التي يمكن أن تنتج عن هذا النوع من الجرائم كان لزاما على الدول مجابهة ذلك، الامر الذي دفع بالمشرع الى سن واعتماد قوانين وسياسات جزائية حازمة من أجل ضمان مكافحة فعالة للجرائم الماسة بالتوقيع الالكتروني من جهة، وخلق وضمان الثقة في المعاملات الالكترونية التي استوجبت التوقيع عليها الكترونيا من جهة أخرى.

من خلال تجريم اشكال الاعتداء على التوقيع الالكتروني، نتيجة لما يتمتع به هذا النوع من الجرائم ،مع طرح بعض الاحكام الجزائية الخاصة بها، والجزاءات المترتبة عنها ومن الجانب الاجرائي تم إقرار واعداد خطط لمتابعتها على المستويين الوطني والدولي بهدف تحقيق الدفاع عن المحررات الالكترونية .

الكلمات المفتاحية : جرائم التوقيع الالكتروني، الجزاءات، الإجراءات الجنائية، التشـريع الجزائري، التعاون الدولي

ABSTRACT:

Cybercrimes, especially those related to electronic signatures and the problems that arise from them, are considered, compared to crimes against traditional signatures, to be among the most serious crimes resulting from the information revolution, and among the most troubling issues for individuals and countries in this era described as the age of technology. In anticipation of the consequences that could result from this type of crime, countries were obliged to confront it, which prompted the legislator to enact and adopt strict penal laws and policies in order to ensure effective combating of crimes affecting electronic signatures on the one hand, and to create and guarantee confidence in electronic transactions that require electronic signatures on the other hand. By criminalizing all forms of assault on electronic signatures, as a result of the nature of this type of crime, with the introduction of some penal provisions specific to it, and the penalties resulting from it, and from the procedural side, plans were approved and prepared to follow up on it at the national and international levels with the aim of achieving the defense of electronic documents.

Key words: Electronic signature crimes, Sanctions, Criminal Procedures, Algerian Legislation, International Cooperation