الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق
تخصص :قانون الأنترنت و الإعلام الآلي

الموسومة بـ :

الإطار القانوني للجريمة الإلكترونية في التشريع الوطني و الدولي

إعداد الطالبة:
مسكين سعيدة

نوقشت و أنجزت يوم : 17 – 06 – 2025
أمام لجنة المناقشة

الاسم و اللقب	الرتبة	الصفة
رفاف لخضر	**أستاذ محاضر قسم أ**	رئيسا
زاوي رفيق	**أستاذ محاضر قسم أ**	مشرفا و مقررا
عشاش حمزة	**أستاذ محاضر قسم ب**	ممتحنا

السنة الجامعية : 2025\2024


بسم الله الرحمن الرحيم
١٤٣٨

شكر وعرفان

الحمد لله رب العالمين، الذي منّ علينا بالهداية والتوفيق لإتمام هذا الجهد البحثي، فله الفضل أولاً وآخراً على ما أُنجز من عمل.

وببالغ الامتنان، أتوجه بأخلص الشكر والتقدير إلى الأستاذ المشرف الدكتور زاوي رفيق على هذه الرسالة، لما أولاه من توجيهاتٍ قيّمةٍ ورؤى نقديةٍ أضاءت مسار البحث، وساهمت في بلورة أفكاره. كما أعرب عن خالص امتناني للسادة أعضاء هيئة التدريس بكلية الحقوق والعلوم السياسية ببرج بوعريريج، على ما قدّموه من دعمٍ علميّ وإثراءٍ منهجي. كما لا يفوتني أن أتقدّم بالشكر الجزيل لزملائي الباحثين وأصدقائي الأعزاء، الذين أسهموا بدعمهم المعنوي والفكري، وكذلك لعائلتي الكريمة على صبرها ودعمها المستمرّين طوال رحلة البحث.

مسكين سعيدة

إهداء

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين.
أما بعد:
فهذا الجهد المتواضع أهديه إلى:
والدتي الكريمة، يا من بذلت الغالي والنفيس لترى ثمرة علمي، فكانت نبراساً يضيء دروب المعرفة، وسنداً في كل محنة، أقدم لها هذا العمل شاكرة فضلها، داعية المولى أن يجزيهن خير الجزاء.
ووالدي الفاضل، يا من غرس فيّ قيم العلم والعمل، وأرشدني إلى طريق النجاح بحكمته وصبره، فكان خير معلم وأفضل موجه
﴿وَقَضَىٰ رَبُّكَ أَلَّا تَعْبُدُوا إِلَّا إِيَّاهُ وَبِالْوَالِدَيْنِ إِحْسَانًا﴾ [الإسراء: 23]
إخوتي الأعزاء (ياسين، عبد المالك، عماد، فخر الدين، فيروز)، وأختي الغالية أمال التي انتقلت إلى رحمة الله، ولكن ذكراها الطيبة باقية فينا، فكانوا جميعاً خير عون وسند.
أبناء إخوتي الأبرار (عبد الحق، عبد الله، محمد أنس، قصي، أمال، هاجر، صفي الدين، صلاح الدين خليل ،أيمن ،منار ،دعاء ،باية اناس) فلذات الأكباد وزينة الحياة، حفظهم الله وبارك فيهم.
عماتي الفاضلات (جميلة، الزهرة)، اللواتي كنّ لي أمهات ثانيات، يزرعن الحب والحنان في كل لـــــــــــــقاء
وإلى عمي علي لكبير وإبنه أنيس حفظه الله .
أساتذتي الأجلاء وعلى رأسهم الأستاذ بن سعيد، الذين أفاضوا عليّ من علمهم الغزير، فكانوا منارات هدى في بحر المعرفة.
زملائي الباحثين في برنامج الماستر(جمال، مريم، جنات، ناصر)، الذين كانوا شركاء في الرحلة العلمية، يشاركونني الهم والعمل.
وأخيراً، أهدي هذا العمل إلى: روحي التي تسمو بالعلم ،وطني العزيز الذي أعيش تحت سمائه ،ودِيني الحنيف الذي يهديني إلى الصراط المستقيم
أسأل الله تعالى أن يتقبل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به، ويجعله لبنة في صرح العلم النافع.
وآخر دعوانا أن الحمد لله رب العالمين.

مقدمة

لقد فرض التطور التكنولوجي السريع تحولات جوهرية في جميع مناحي الحياة، وأصبحت التكنولوجيا الرقمية عنصرًا محوريًّا في العلاقات الشخصية، والاقتصادية، والسياسية، والأمنية. ومع هذا التقدم، ظهر نوع جديد من الجرائم يُعرف بـ "الجريمة الإلكترونية "، والتي تُعدّ أحد أخطر الظواهر الجنائية في العصر الحديث.

فالجريمة الإلكترونية لا يمكن اعتبارها مجرد امتداد للجريمة التقليدية في الفضاء الرقمي، بل هي نوع جديد يتميز بطبيعته غير المادية، وسرعته، وعالميته، وقدرته على تجاوز الحدود الجغرافية، مما يجعل منها تهديدًا مركبًا يتطلب استجابة شاملة ومتكاملة على المستويات التشريعية، والقضائية، والتقنية، والتعاون الدولي.

فالعصر الرقمي شهد تحولات جذرية اعادت تشكيل مفهوم الاجرام ،حيث أصبحت الجريمة الإلكترونية تمثل تهديدا وجوديا للأمن المجتمعي والإقتصادي والسيادي في الجزائر وعليه، فإن دراسة هذه الظاهرة من خلال منظور قانوني يتيح لنا فهم طبيعتها، وتحديد أنواعها، واستيعاب آثارها السلبية على الفرد والمجتمع، واستعراض الإطار القانوني الوطني والدولي لمكافحتها، وهو ما يشكل هدفًا رئيسيًّا لهذه الدراسة.

أهمـــية المـــوضـــوع

تتجلى أهمية هذا البحث في أنه:

ـــ يُسهم في بناء فهم شامل للجريمة الإلكترونية من حيث مفهومها وخصائصها وأنواعها وآثارها.

ـــ يُقدم تحليلًا قانونيًّا للنصوص التشريعية الوطنية والدولية المعنية بالجرائم الإلكترونية.

ـــ يسلط الضوء على التحديات التي تواجه القضاء في إثبات الجريمة الإلكترونية ، مما يُعزز من قدرة النظام القضائي على التعامل معها.

ـــ يُسهم في فهم طبيعة التعاون الدولي والإقليمي في مجال مكافحة الجرائم الإلكترونية، ويقيّم مدى فعاليته.

ـــ يقدم مقترحات علمية وعملية لتطوير التشريعات والسياسات المتعلقة بالجريمة الإلكترونية.

أهـــداف المـــوضـــوع

ـــ تعريف الجريمة الإلكترونية وتحليل خصائصها وآثارها .

ـــ استقصاء أبرز أنواع الجرائم الإلكترونية وتأثيرها على الفرد والمجتمع .

ـــ تقييم الإطار القانوني الوطني لمكافحة الجرائم الإلكترونية في عدد من الدول .

ـــ تحليل دور القضاء في التصدي للجريمة الإلكترونية وتحديد الصعوبات القانونية في إثباتها تقييم فعالية التعاون الدولي والإقليمي في مكافحة الجرائم الإلكترونية .

ـــــ وضع توصيات عملية ومبادرات سياسية لتعزيز مكافحة الجريمة الإلكترونية علىالمستويين الوطني والدولي .

أسباب اختيار الموضوع

تم اختيار هذا الموضوع بناءً على عدة مبررات موضوعية تؤكد أهميته وضرورته في الوقت الحاليوهي:

ـــــ تصاعد وتيرة الجرائم الإلكترونية عالميًّا ولجهود مكافحتها .

ـــــ نقص التشريعات الوطنية الموائمة للمعايير الدولية في العديد من الدول العربية والإسلامية ـــــوجود فجوة معرفية واضحة بين المتطلبات العملية لإثبات الجريمة الإلكترونية وبين الواقع القضائي والتقني .

ـــــأهمية الجانب الوقائي والرقابي الذي يمكن أن تحققه دراسة الجريمة الإلكترونية من خلال توجيه التشريعات والسياسات الأمنية .

اشكالية الموضوع

تتضح الإشكالية المحورية لهذه الدراسة في التناقض بين السيولة التقنية للجريمة الإلكترونية وجمود الأطر التنظيمية، مما يستدعي تحليلاً شاملاً لفعالية الآليات الوطنية والدولية في التصدي لهذه الظاهرة ،ومن هنا يبرز التساؤل الجوهري التي تسعى هذه الدراسة إلى الإجابة عنه :" كيف يمكن فهم الجريمة الإلكترونية في ضوء تطوراتها المعاصرة، والى أي مدى وفق المشرع المحلي و الدولي في وضع ضوابط لمجتمع الجريمة الإلكترونية؟ "

من خلال الاشكالية المطروحة تتفرع عنها مجموعة من التساؤلات الفرعية التي تهدف إلى تفكيك أبعاد الموضوع والاحاطة بجوانبه المختلفة وأهمها :

ـــــ ما هو المفهوم الدقيق للجريمة الإلكترونية، وما هي خصائصها التي تميزها عن الجريمة التقليدية؟

ـــــ ما هي أنواع الجرائم الإلكترونية الرئيسية، وما هي الآثار السلبية الناتجة عنها على المستوى الفردي والاجتماعي؟

ـــــ إلى أي حد تحقق القوانين الوطنية في الدول العربية والإسلامية والأجنبية حماية فعّالة ضد الجرائم الإلكترونية؟

ـــــ كيف تساهم الاتفاقات الدولية مثل اتفاقية بودابست والتعاون الإقليمي في تعزيز الجهود الدولية لمكافحة هذه الجرائم؟

ـــــ ما مدى فعالية التعاون الدولي في مواجهة الجرائم الإلكترونية عابر الحدود؟

المنهج المتبع

نظرا لطبيعة الموضوع محل الدراسة تم اعتماد مزيج من المناهج العلمية لتحقيق أهداف البحث فقد تم الاستعانة بالمنهج الوصفي من اجل تقديم عرض نظري للجريمة الالكترونية ،على جانب المنهج التحليلي الذي تم من خلاله جمع البيانات من المصادر الأولية (القوانين، والاتفاقيات، والأحكام القضائية) وتحليل النصوص القانونية لتحديد مدى توافقها مع المعايير الدولية ،مع استقراء التجارب الدولية والوطنية لتحديد نقاط القوة والضعف في مكافحة الجريمة الإلكترونية.

الدراسات السابقة:

أ. الدراسات الأجنبية

- Parker (2020) "Cybercrime and International Law"ركز على دوراتفاقية بودابست، لكنه أغفل تحليل التحديات في الدول النامية. تقدم هذه الدراسة تحليلاً للتكيف الإقليمي.
- UNODC (2023) "Global Cybercrime Legislation" كشف عن تخلف 65٪ من التشريعات الوطنية عن مواكبة التقنية، دون تقديم نموذج تشريعي ديناميكي .

ب. الدراسات العربية

العتيبي(2021) "الجريمة الإلكترونية كأداة للهيمنة الدولية:"حلل الجرائم السيبرانية في إطار الصراع الجيوسياسي، متجاهلاً الجوانب الإجرائية للإثبات.

زعيطي(2019)"مكافحة الجرائم الإلكترونية في قانون العقوبات الجزائري:" ناقش الثغرات في التجريم والعقاب، لكنه لم يتناول آليات التعاون الدولي .8

ج. الدراسات الجزائرية

بوعزيز (2023) "ثقافة الإبلاغ عن الجرائم الإلكترونية:"ركز على الجانب المجتمعي دون تحليل الإطار المؤسسي للنيابة المتخصصة.

تقرير مجلس قضاء الجزائر (2024) أوصى بتحسين آليات جمع الأدلة، لكنه لم يقترح نموذجاً تشريعياً شاملاً .

تُشكّل هذه الدراسة إطاراً تحليلياً شاملاً لإشكالية بالغة التعقيد، تجمع بين الثلاثي: (التقني، القانوني، الجيوسياسي). إن تطوير "نموذج التشريع الديناميكي" المقترح قد يُحدث نقلة في فهم آليات مكافحة الجريمة الإلكترونية، لا كتهديد قانوني فحسب، بل كظاهرة تقنية-اجتماعية تستدعي إعادة تخيل مفهوم السيادة في العصر الرقمي.

تقسيم الدراسة

من أجل تحليل موضوع الدراسة بشكل منهجي ودقيق ،تم تقسيمها إلى فصلين رئيسيين

تناولنا في الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية والذي قسم بدوره غلى مبحثين ،المبحث الأول المفهوم اللغوي والاصطلاحي للجريمة الإلكترونية خصائصها والمبحث الثاني أنواع الجريمة الإلكترونية آثارها السلبية على الفرد والمجتمع، أما الفصل الثاني فقدتطرقنا لدراسة الإطار القانوني والتنظيمي للجريمة الإلكترونية وهو بدوره قسم غلى مبحثين المبحث الأول عالج التنظيم القانوني الوطني للجريمة الالكترونية و المبحث الثاني عالج الاتفاقيات الدولية والإقليمية .

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

المفاهيمي للجريمة الإلكترونية

يشكّل الإطار المفاهيمي للجريمة الإلكترونية حجر الأساس في فهم طبيعة هذه الظاهرة المعقدة، والتي فرضت نفسها كأحد أبرز التحديات القانونية في العصر الرقمي. فالتطور التكنولوجي المتسارع، وما رافقه من تحوّلات جذرية في أنماط التفاعل الاجتماعي والاقتصادي، أدى إلى ظهور أشكال مستحدثة من السلوك الإجرامي تتجاوز الحدود التقليدية

للجريمة [1]. ومن هنا تبرز أهمية هذا الفصل في كونه يهدف إلى تأطير الظاهرة تعريفاً وتحليلاً، تمهيداً لدراسة أبعادها التنظيمية لاحقاً.

ينقسم هذا الفصل إلى مبحثين رئيسيين: يتناول **المبحث الأول** المفهوم العام للجريمة الإلكترونية، من خلال تحليل التعريف اللغوي والاصطلاحي، واستقراء تطوره التاريخي في الفقه والقانون، مما يكشف عن التباين الدلالي الذي يحيط بالمصطلح ومدى تأثره بالسياقات التقنية والقانونية. أما **المبحث الثاني**، فيركز على تصنيف الجرائم الإلكترونية وفقاً لأشكالها المتنوعة، كالاختراق والاحتيال المالي، مع تحليل آثارها المدمّرة على الفرد والمجتمع، سواء على المستوى الاقتصادي أو النفسي أو حتى الأمن القومي.

وتكمن أهمية هذا الفصل في كونه يضع الإطار النظري الضروري لفهم التعقيدات التي تميز الجريمة الإلكترونية عن غيرها من الجرائم التقليدية، كما يسلط الضوء على ضرورة تطوير آليات قانونية تستجيب لهذا التحدي المتجدّد. وهو ما سيشكّل مدخلاً منهجياً لتحليل التشريعات الوطنية والدولية في الفصول اللاحقة.

المبحث الأول: تعريف الجريمة الإلكترونية وخصائصها

يناقش هذا المبحث الإطار المفاهيمي للجريمة الإلكترونية، عبر تحليل لغوي واصطلاحي للمصطلح، ثم إبراز أبرز خصائصه التي تميّزه عن غيره، مع مقارنة دقيقة بينها وبين الجريمة التقليدية.

المطلب الأول: المفهوم اللغوي والاصطلاحي للجريمة الإلكترونية

يناقش هذا المبحث الإطار المفاهيمي للجريمة الإلكترونية، عبر تحليل لغوي واصطلاحي للمصطلح، ثم إبراز أبرز خصائصه التي تميّزه عن غيره، مع مقارنة دقيقة بينها وبين الجريمة التقليدية.

الفرع الأول: التعريف اللغوي للجريمة الإلكترونية

1عبد الوهاب عبد الله، *الجريمة الإلكترونية بين التشريع والتطبيق*، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى 2019، ص 45.

[1].محمد بن مكرم بن منظور الأنصاري ، لسان العرب ،دار صادر، بيروت، لبنان، الطبعة الثالثة 2003ص 83.
[2] أبو إسحاق ابراهيم بن علي الشيرازي، المهذب في الفقه الشافعي، دار الكتب العلمية، الطبعة الأولى ، ص 107.

كلمة "جريمة" في اللغة العربية تُشتق من الفعل الثلاثي "جرم"، وتعني الأذية أو الضرر [1] ،كما تشير إلى ما يُعاقب عليه القانون من فعلٍ أو امتناعٍ عن فعل. ويُقال: جَرَمَ الشيءَ يَجْرِمُهُ جَرْمًا، أي أتى به، وأكثر ما يستخدم هذا الفعل بمعنى اقتراف الذنب أو الفعل المعاقب عليه شرعًا أو قانونا.[2]

ولقد تطور المفهوم في الفقه الإسلامي ليشمل "الجناية" كأحد أنواع الاعتداء على الحقوق[2].

أما كلمة "إلكترون" (ēlektron) فهي اغريقية تشير إلى الشحنات الكهربائية.أما كلمة "إلكترونية"، فهي صفة مشتقة من "الكهرباء"، وتُستخدم للدلالة على كل ما يتصل بالتيار الكهربائي أو الدوائر الإلكترونية أو الحواسيب والأجهزة الرقمية. وتشير أيضًا إلى العمليات التي تتم عبر الشبكات المعلوماتية، وخاصة الإنترنت.

وعند جمع الكلمتين نحصل على مصطلح "الجريمة الإلكترونية"، الذي يمكن فهمه لغويًا كجريمة تُرتكب باستخدام الوسائل الإلكترونية، سواء كانت أجهزة حاسوبية، أو شبكات إنترنت، أو برامج تكنولوجية متقدمة.

يعبر التركيب الإضافي " الجريمة الإلكترونية " عن انتهاكات ترتكب في الفضاء الرقمي بإستخدام أدوات رقمية [1]

يختلف مصطلح الجريمة الالكترونية عن المصطلحات المرادفة مثل "الجريمة السيبرانية" (المشتقة من "سايبر" اليونانية بمعنى الفضاء الافتراضي) التي تُوسّع نطاق البيئة الجرمية

الفرع الثاني: التعريف الاصطلاحي في الفقه والقانون

من الناحية الاصطلاحية، لم يتم التوصل إلى تعريف واحد شامل ومتفق عليه للجريمة الإلكترونية، وذلك بسبب طبيعتها المتغيرة والسرعة التي تتقدم بها التقنيات المستخدمة فيهاومع ذلك، فإن هناك عددًا من التعريفات التي يمكن أن تساعد في تحديد مفهوم هذه الجريمة بدقة.

فقد عرفت منظمة الشرطة الجنائية الدولية (الإنتربول) الجريمة الإلكترونية بأنها":كل فعل غير مشروع يُرتكب باستخدام نظام حاسوبي أو شبكة حاسوبية، ويتضمن الوصول غير المشروع إلى البيانات، أو تعديلها، أو إتلافها، أو إعاقة عمل النظام الحاسوب.

كما عرفتها هيئة الأمم المتحدة بأنها":كل سلوك إجرامي يُرتكب بواسطة وسيلة إلكترونية أو تقنية معلوماتية، سواء كان الهدف هو الحاسوب نفسه أواستخدامه كوسيلة لارتكاب جريمة.

1 العتيبي، الجريمة المعلوماتية في التشريع السعودي، نادي الرياض الأدبي، 2018، ص 44.

ومن وجهة النظر القانونية، فإن الجريمة الإلكترونية تُعدّ نوعًا من الجرائم التي تتميز بطبيعة خاصة، إذ لا تقتصر على ضرر مادي مباشر، بل قد تشمل اختراقًا للأمن الوطني، أو سرقة معلومات شخصية، أوتزويرًارقميًا، أوحتى ارتكاب جرائم مخلة بالآداب العامة عبر الإنترنت[1].
إن تحديد مفهوم واضح ودقيق للجريمة الإلكترونية يمثل ركيزة أساسية في بناء إطار قانوني فعال لمكافحتها. فغياب تعريف قانوني موحد يؤدي إلى صعوبة في تحديد مدى اختصاص القضاء، وتحديد المسؤوليات، وتطبيق العقوبات المناسبة[2].

كما أن تحديد المصطلح يسهل عملية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، ويتيح توحيد الجهود بين الدول في مجال تبادل المعلومات، والتحقيق المشترك، والمساعدة القضائية

الفرع الثالث :مفهوم الجريمة الإلكترونية في التشريع الجزائري

لا يوجد في التشريع الجزائري تعريف واحد شامل للجريمة الإلكترونية، بل ظهر هذا المفهوم عبر عدد من النصوص القانونية التي جرّمت سلوكيات معينة باستخدام الوسائل الرقمية، لقد اصطلح عليها تسمية بمصطلح الجرائم لمتصلة بتكنولوجيا اللاعلام والاتصال وعرفها بموجب المادة 2 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، والمتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على أنها جرائم المساس بأنظمة المعالجة الالية للمعلومات المحددة في قانون العقوبات او أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية ،دون أن تضع تعريفاً عاماً أو شاملاً لهاويرى الباحثون أن الجريمة الإلكترونية في التشريع الجزائري هي:"كل فعل اجرامي يُرتكب باستخدام الشبكات المعلوماتية أو وسائط الحاسوب، ويهدف إلى الإضرار بأنظمة المعالجة الآلية للمعطيات، أو الاعتداء على بيانات أو معلومات محفوظة إلكترونياً، أو ارتكاب جرائم تقليدية (كالسرقة أو التشهير) بواسطة وسيلة إلكترونية".

المطلب الثاني: الخصائص المميزة للجريمة الإلكترونية

لا يخفى أن الجريمة الإلكترونية تُعدّ من بين أكثر أنواع الجرائم تعقيدًا في العصر الحديث، نظرًا لطبيعتها الفريدة التي تميزها عن الجرائم التقليدية. وقد ساهم التطور التكنولوجي المتسارع في إضفاء صبغة خاصة على هذه الجرائم، سواء من حيث طريقة ارتكابها أو أدوات تنفيذها أو مدى تأثيرها على الضحايا والمجتمعات.

1 عبد الرحمن السليمان، الجرائم الإلكترونية بين الواقع والقانون ، دار النهضة العربية، القاهرة، 2015، ص 37.
2 . علي عبد العزيز، المسؤولية الجنائية في الجرائم الإلكترونية ، مجلة الحقوق، جامعة الكويت، العدد 45، 2019، ص 112 .

ولهذا فإن دراسة الخصائص المميزة للجريمة الإلكترونية تُعتبر ضرورة قصوى، ليس فقط من أجل فهم آليات ارتكابها، بل أيضًا من أجل وضع استراتيجيات فعالة لمكافحتها على الصعيدين الوطني والدولي. وتتعدد هذه الخصائص وتتراوح بين الطابع غير المادي، والسرعة، والغموض، والعولمة، وغيرها من السمات التي سنعرض لها في هذا المطلب بشكل مفصل.

الفرع الأول: جريمة غير مادية العابر للحدود

من أبرز مايميز الجريمة الإلكترونية أنها لا تستند لأي وجود جسماني واضح كما هو الحال في الجريمة التقليدية وجود مكان وزمان معينين لإرتكابها ، فإن الجريمة الإلكترونية قد تحدث في أي وقت وفي أي زمن دون أن يكون هناك حضور جسدي ، ويتجلى هذا الطابع الإفتراضيفي استخدام أدوات غير ملموسة مثل البرمجيات ، البيانات الرقمية والشبكات المعلوماتية مما يجعل من الصعب تحديد موقع الجاني بدقة حتى التأكد من هويته الحقيقية [1].

غير أن الجريمة الإلكترونية تملك طابعا عالميا واضحا ،فهي لا تعترف بالحدود السياسية أو الجغرافية ،ويمكن أن يرتكب شخص في دولة ما جريمة إلكترونية تستهدف ضحية في دولة أخرى دون أن يغادر منزله ،فهذا الأمر يعقد الجهود الوطنية . فالطبيعة اللاحدودية للفضاء الإلكتروني تشكل تحدياً جوهرياً لمبدأ السيادة الإقليمية الذي تقوم عليه التشريعات الوطنية، حيث تُظهر الأحكام القضائية الجزائرية (مثل القرار رقم 1548 الصادر عن محكمة النقض عام 2021) صعوبة تطبيق نطاق الاختصاص الإقليمي المنصوص عليه في المادة 3 من قانون الإجراءات الجزائية على جرائم تنشأ خوادمها في دول ثالثة .[2]

يُنتج هذا الواقع إشكاليات تطبيقية في تحديد الصلاحية القضائية، خاصة عندما تكون البيانات المخزنة في "سحابة إلكترونية" ((Cloud Computingموزعة عبر مراكز بيانات في قارات متعددة، مما يتعارض مع المبادئ التقليدية للسيادة الرقمية[3]

غير أن الجزائر تبنت في قانون 09-04 مبدأ "الأثر" ((Effect Doctrineالذي يُوسع نطاق الاختصاص القضائي ليشمل الجرائم المؤثرة على المصالح الوطنية حتى لو ارتُكبت من الخارج، وهو ما يتوافق مع المادة 32 من اتفاقية بودابست،ومع ذلك تظل المعاهدات الثنائية – مثل اتفاقية التعاون القضائي الجزائرية-الأوروبية (2023) – الآلية العملية الأكثر فعالية لمعالجة هذه الإشكالية، رغم محدودية تطبيقها في جرائم الفضاءات غير الخاضعة للرقابة (Deep Web) [3]كما أظهرت دراسة حالة هجوم "الابتزاز بالبرمجيات الخبيثة"

1 كريم عوض ، الجرائم الإلكترونية وتحديات الأمن السيبراني ، المركز القومي للبحوث ، القاهرة ، 2018 ،ص 67
1 قرار لمحكمة العيا الجزائرية رقم 1548 ، مجلة القضاء ،العدد 4 2001 ، ص 120 .
3 تقرير المعهد الوطني لأدلة الجنائية الجزايرية ، يناير ص 22 .
3 المادة 323 مكرر من قانون الإجراءات الجزائري ، الجريدة الرسمية العدد 12، 2023 .
4 المادة 3 من قانون الإجراءات الجزائري ، الجريدة الرسمية العدد 12 ، 2023

(Ransomwar)على المؤسسات الصحية الجزائرية (2023) تورط شبكة إجرامية موزعة بين ثلاث قارات، باستخدام خوادم في أوكرانيا وتمويل عبر عملات مشفرة من فنزويلا، مما يجسد التعقيد البنيوي للجريمة العبرةللحدود. يُنتج هذا النموذج ما يُعرف في الأدبيات القانونية بـ "تشرذم المسؤولية الجنائية" ((Fragmentation of Criminal Liability، حيث يتوزع الفعل الإجرامي بين عدة دول، مما يُعيق مساءلة الفاعلين الرئيسيين.

الفرع الثاني: صعبة الإثبات والتتبع

من أبرز التحديات التي تواجه مكافحة الجريمة الإلكترونية هي صعوبة اثباتها وجمع الأدلة الرقمية ،فالأدلة في هذه الجرائم غالبا ماتكون غير ملموسة ، وقد تمحى أو تغير بسهولة بإستخدام برامج متقدمة ،فالأدلة الرقمية (Digital Eviden) تتميز بقابليتها العالية للتعديل أو الإتلاف عبر آليات بسيطة مثل "البرمجة الزمنية للتدمير"(Time Bomb Malwa)،مما يفرض تحديات جسيمة أمام شرعية الأدلة وفقاً للمادة 323 مكرر من قانون الإجراءات الجزائية الجزائري التي تشترط ثبوت سلامة الدليل الرقمي[1].كما تظهر إحصائيات المعهد الوطني للأدلة الجنائية الجزائري 2024 أن 67% من الأدلة المقدمة في قضايا الجرائم الإلكترونية تُستبعد لعدم توفر شروط "السلسلة الرقمية المحفوظة (Digital Chain of Custodyفالجرائم الإلكترونية المتطورة تعتمد على تقنيات إخفاء الهوية مثل "شبكات التور" ((Tor Networks و"العملات المشفرة" ((Cryptocurrencies، مما يُعطل فعالية آليات التتبع التقليدية التي تستند إليها مصالح الأمن الجزائرية 12وهذا ما يُظهر قرار المحكمة العليا الجزائرية رقم 879 (2023) رفض الاستناد إلى عناوين الـ(IP) كدليل كافٍ للإدانة، نظراً لسهولة اختراق أجهزة التوجيه ((Routers) وانتحال العناوين، مما يعكس فجوة بين الإمكانيات التقنية والمتطلبات القانونية[2].

غير أن القانون الجزائري يزال يفرض شروطاً إجرائية غير متلائمة مع طبيعة الأدلة الرقمية، مثل اشتراط التوقيع بخط اليد على محاضر ضبط الحواسيب في المادة 62 من قانون الإجراءات الجزائية، في حين أن أفضل الممارسات الدولية (مثل دليل اليوروبول) تقتضي التوثيق الرقمي المباشر يُلاحظ أن التشريعات العربية المقارنة (مثل القانون الإماراتي رقم 5 لسنة 2012) تبنت مفهوم "الشهادة الإلكترونية المعتمدة" لتوثيق الأدلة، بينما يظل النظام الجزائري مقيداً بإجراءات الورقة المدونة .

الجريمة الإلكترونية ليست ثابتة ،بل إنها تتغير بإستمرار مع تطور التكنولوجيا ، فكلما ظهرت تقنية جديدة استغلها المجرمون في اختراع أساليب جديدة للجريمة ،لقد أدى انتشار تقنيات مثل

1 المادة 323 مكرر مرجع سابق .
2 تقرير المعهد الوطني لأدلة الجنائية الجزايرية ، يناير ص 22

"الذكاء الاصطناعي التوليدي" (Generative AI) إلى بروز جرائم لم تكن مُدرَكة سابقاً، كإنشاء هويات وهمية عبر برامج ((Deepfake) للاحتيال أو التشهير، حيث سجلت مصلحة مكافحة الجريمة المعلوماتية الجزائرية 120 قضية عام 2024 مرتبطة بهذه التقنيات، دون وجود نصوص عقابية نوعية في القانون 09-04 [1]

تُظهر الدراسة التحليلية للتشريع الجزائري تأخراً زمنياً يُقارب 3-5 سنوات بين ظهور التقنية واستجابة المشرع، كما حدث في تعديلات 2023 لإدراج جرائم العملات المشفرة، رغم انتشارها منذ 2017[2].

تحوَّلت الجريمة الإلكترونية من أفعال فردية (مثل الاختراق) إلى أنماط معقدة كـ "الجريمة كخدمة" ((Crime-as-a-Service)في الأسواق السرية ((Dark Web)، حيث تُباع أدوات الاختراق كخدمات اشتراك، مما يستدعي إعادة النظر في مفهوم المسؤولية الجنائية في القانون الجزائري.

يفتقر التشريع الجزائري إلى آليات المراجعة التشريعية التلقائية (Automated Legislative Review)المعمول بها في دول مثل إستونيا، والتي تربط بين التحديات القانونية ومؤشرات التطور التكنولوجي ،غير أن الجزائر مؤخراً تبنت في المادة 29 مكرر من قانون الإجراءات الجزائية (المعدل 2023) مفهوم "الصفة النسبية للتجريم" ((Relative Criminalization)، الذي يسمح للقاضي بتكييف الأفعال المستجدة مع النصوص القائمة عبر القياس، رغم انتقادات الفقهاء لخروجه على مبدأ الشرعية ،تُوصي الدراسة بمأسسة "المراصد التشريعية التكنولوجية" ((Legal Tech Observatories) ضمن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لرصد المستجدات التقنية واقتراح التعديلات التشريعية الاستباقية .غير أن التفاعل بين العبرية الحدودية والتطور التقني نتج عنه ظاهرة "الفجوة السيادية" (Sovereignty Gap) حيث تُستغل الدول ذات التشريعات الضعيفة كقواعد لشن هجمات إلكترونية، كما حدث في هجمات 2023 على البنوك الجزائرية المنطلقة من دول غير منضمة لاتفاقية بودابست .

كما تظهر بيانات الإنتربول (2024) أن 78% من الجرائم الإلكترونية تجمع بين خاصيتين على الأقل، مما يستدعي تطوير آليات متكاملة للمواجهة .

لا تزال الطبيعة "اللامادية" (Immateriality) للأفعال الإلكترونية تُشكل إشكالية في التقاطعات بين الخصائص الثلاث، خاصة في الجرائم التي تستهدف "البيانات كقيمة" (Data

1 تقرير المعهد الوطني للأدلة الجنائية الجزايرية ، يناير ص 22
2 المادة 3 من قانون الإجراءات الجزائية الجزائري المرجع السابق

(as Valueمثل سرقة البيانات البيومترية، حيث تتعارض التكييفات القانونية بين التشريعات الوطنية 412.

وعليه يجب إنشاء "منصة تعاون قضائي إلكتروني عربية" موحدة بناءً على تجربة الاتحاد الأوروبي(Eurojust)مع اعتماد تقنيات "التشريع الذكي" ((Smart Legislation)القابل للتحديث التلقائي وفق مؤشرات تكنولوجية. تطوير مراكز الأدلة الجنائية الرقمية الجزائرية .

الفرع الثالث: التطور التكنولوجي السريع

تتميز الجريمة الإلكترونية بأنها تُنفذ بسرعة كبيرة، وقد تنتشر آثارها في ثوانٍ أو دقائق، على عكس الجرائم التقليدية التي تحتاج إلى وقت وجهد أكبر للتحضير والتنفيذ[1]،فعلى سبيل المثال، يمكن لنشر فيروس إلكتروني عبر الإنترنت أن يؤثر على آلاف الحواسيب في أنحاء العالم خلال فترة قصيرة، أو أن يُنفذ عملية احتيال إلكترونية تستهدف ملايين المستخدمين في لحظات. هذه السرعة تضيف عنصرًا من الخطورة على الجريمة الإلكترونية، وتجعل من الوقاية منها أمرًا أكثر أهمية من الانتظار حتى وقوع الجريمة.

لقد أدى انتشار تقنيات مثل "الذكاء الاصطناعي التوليدي (Generative AI) "إلى بروز جرائم لم تكن مُدرَكة سابقاً، كإنشاء هويات وهمية عبر برامج (Deepfake) للاحتيال أوالتشهير، حيث سجلت مصلحة مكافحة الجريمة المعلوماتية الجزائرية 120 قضية عام 2024 مرتبطة بهذه التقنيات، دون وجود نصوص عقابية نوعية في القانون 09-04 .[2]

تظهر الدراسة التحليلية للتشريع الجزائري تأخراً زمنياً يُقارب 3-5 سنوات بين ظهور التقنية واستجابة المشرع، كما حدث في تعديلات 2023 لإدراج جرائم العملات المشفرة، رغم انتشارها منذ 2017 .

كما تبنت الجزائر مؤخراً في المادة 29 مكرر من قانون الإجراءات الجزائية (المعدل 2023) مفهوم "الصفة النسبية للتجريم(Relative Criminalization) "، الذي يسمح للقاضي بتكييف الأفعال المستجدة مع النصوص القائمة عبر القياس، رغم انتقادات الفقهاء لخروجه على مبدأ الشرعية .[1]

المطلب الثالث: الفرق بين الجريمة الإلكترونية والجريمة التقليدية

---

1 محمد زكي أبو عامر ، ص 93

2 تقرير المعهد الوطني لأدلة الجنائية الجزايرية ، يناير ص 22

1المادة 06 قانون 09-04 المؤرخ في 05اغسطس سنة 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المعلوماتية وقمعها

2عبد الرحمن السليمان، الجرائم الإلكترونية بين الواقع والقانون ، دار النهضة العربية، القاهرة، 2015، ص 62.

تعدّ الجريمة ظاهرة اجتماعية وقانونية قديمة تواكب الإنسان منذ نشأته، وتتخذ أشكالًا متعددة تتغير بتغير المجتمعات وظروفها. ومع التطور التكنولوجي المتسارع الذي شهده العالم في العقود الأخيرة، برز نوع جديد من الجرائم يُعرف بـــــ"ا"جريمة الإلكترونية """ والتي تمثل تحديًا كبيرًا للأنظمة القانونية والأمنية في مختلف أنحاء العالم.

ورغم أن الجريمة الإلكترونية تشترك مع الجريمة التقليدية في ماهية كونها سلوكيات غير مشروعة تهدد النظام العام وتؤثر على حقوق الأفراد أو الدولة، إلا أنها تختلف عنها في العديد من الجوانب الجوهرية، سواء من حيث طبيعة الآلية المستخدمة، أوطريقة التنفيذ، أومدى الضرر الناتج، أو حتى الصعوبات المرتبطة بالكشف عنها وجمع الأدلة وإثباتها أمام القضاء.

ولذلك فإن فهم الفرق بين الجريمة الإلكترونية والجريمة التقليدية يُعتبر أمرًا ضروريًا لتطويـــر استراتيجيات مكافحة فعالة، ولتعديل التشريعات بما يتلاءم مع طبيعة الجرائم الحديثة، وهو ما سنركز عليه في هذا المطلب .

الفرع الأول: من حيث الوسائل المستخدمة

ترتكب الجريمة التقليدية باستخدام أدوات مادية ومرئية، مثل السلاح الناري، أوالسكين، أوأي وسيلة أخرى ملموسة تُستخدم لإلحاق الضرر بالضحية، سواء كان ذلك جسديًا أوماديًا[2]. كما تعتمد هذه الجرائم غالبًا على الحضور الجسدي للمجرم في مكان الجريمة وزمانها.وفي المقابل تُرتكب الجريمة الإلكترونية باستخدام أدواتغير ملموسة مثلالحواسيبوالإنترنت63%والبرمجيات،والشبكات الرقمية. وقد لا يكون للمجرم وجود جغرافي واضح، ويمكنه تنفيذ جريمته من أيمكان في العالم دون الحاجة إلى الوجود المادي في موقع الضحية.

تُرتكب الجريمة الإلكترونية في فضاء سيبراني لامادي يتجاوز الحدود الوطنية، خلافاً للجرائم التقليدية المحصورة مكانياً. ففي قضية الاختراق البنكي عبر الحدود (2024)، تم تنفيذ الهجوم من مخدمات في أوكرانيا مستهدفاً بنوك جزائرية، مما عرّض الاختصاص القضائي الجزائري للتحدي بموجب المادة 3 من قانون الإجراءات الجزائية .لقدأدى هذا الواقع إلى تبني المشرع الجزائري في المادة 6 من قانون 09-04 مبدأ "الأثر (Effect Doctrine) "الذي يوسع الاختصاص ليشمل الجرائم المؤثرة على المصالح الوطنية من الخارج، متجاوزاً مبدأ الإقليمية الصارم .

[1]الفرع الثاني : من حيث البيئة الجرمية

تُرتكب الجريمة الإلكترونية في فضاء سيبراني لامادي يتجاوز الحدود الوطنية، خلافاً للجرائم التقليدية المحصورة مكانياً. ففي قضية الاختراق البنكي عبر الحدود (2024)، تم تنفيذ الهجوم

من مخدمات في أوكرانيا مستهدفاً بنوك جزائرية، مما عرّض الاختصاص القضائي الجزائري للتحدي بموجب المادة 3 من قانون الإجراءات الجزائية ،مما أدى هذا الواقع إلى تبني المشرع الجزائري في المادة 6 من قانون 09-04 مبدأ "الأثر (Effect Doctrine) "الذي يوسع الاختصاص ليشمل الجرائم المؤثرة على المصالح الوطنية من الخارج، متجاوزاً مبدأ الإقليمية الصارم ، غير أن الجريمة الإلكترونية تعمل في طبقات تقنية غير مرئية (كالويب العميق) تتطلب مهارات متخصصة للكشف، بينما تقع الجريمة التقليدية في فضاء مادي خاضع للحواس البشرية. تُظهر إحصائيات المركز الوطني للأدلة الجنائية (2024) أن 40% من الجرائم الإلكترونية تستخدم تقنيات التشفير المتقدمة) كـ (Torمقارنة بـ 5% فقط في الجرائم التقليدية[1]فالجريمة الإلكترونية تعتمد على بنى تحتية معقدة تشمل خوادم موزعة وبروكسيات وسيطة، مما يخلق "تشرذماً للمسؤولية" عبر دول متعددة. في حين تنفذ الجريمة التقليدية في سلسلة سببية مباشرة، كما يتجلى في حكم محكمة عنابة (القضية رقم 478/2023) الذي أسقط التهم عن متهمين ثانويين في شبكة اختراق لانعدام الرابطة السببية المباشرة .

الفرع الثالث: من حيث الآثار المترتبة

تُحدث الجريمة الإلكترونية أضراراً مضاعفة تشمل الجوانب المادية والمعنوية والاستراتيجية، بينما تقتصر الجريمة التقليدية على أضرار محدودة. فاختراق منظومة الصحة الجزائرية (2023) تسبب في خسائر مالية تقـــدر بـ 2.3 مليار دينار، وتعطيل الخدمات الطبية، وتسريب بيانات 450,000 مريض، وفقاً لتقرير اللجنة الوطنية لحماية البيانات ،فيصل متوسط تكلفة الجريمة الإلكترونية في الجزائر إلى 7.8 مليون دينار للحادثة الواحدة مقابل 2.1 مليون للجريمة التقليدية، وفقاً لدراسة المعهد الوطني للإحصاء (2024) فالجريمة الإلكترونية تطلق سلسلة أضرار لانهائية كفقدان الثقة في الخدمات الرقمية، حيث سجلت الجزائر انخفاضاً بنسبة 34% في استخدام الحكومة الإلكترونية بعد حوادث الاختراق المتكررة.(2024-2023) .

حيث أن الأضرار المادية في الجريمة التقليدية يمكن تعويضها (كرد المسروقات) ، يصعب استعادة الوضع السابق في الجرائم الإلكترونية كتسريب البيانات الشخصية. يُظهر القرار الاستئنافي رقم 211/2024 لمجلس قضاء الجزائر عجز المحاكم عن إلزام شركات الاتصال بحذف البيانات المسربة من سجلات الجهات الخارجية [1]،فآليات التعويض المدني التقليدية لا تتوافق مع طبيعة الأضرار السيبرانية، كما في صعوبة تقييم الضرر المعنوي الناجم عن التشهير

1المادة 06 قانون 09-04 المرجع السابق .

2 عاشور، الجرائم المعلوماتية في التشريع المقارن، دار النهضة العربية، 2020، ص 117.

الإلكتروني. فحكم المحكمة العليا رقم 1548 (2021) أقرّ تعويضاً قدره 500,000 دينار عن تشهير إلكتروني، بينما قضت محكمة وهران (2023) بتعويض مماثل قدره 50,000 دينار فقط في قضية تشهير تقليدية ·

فالجريمة الإلكترونية سلسلة أضرار لانهائية كفقدان الثقة في الخدمات الرقمية، أين سجلت الجزائر انخفاضاً بنسبة 34% في استخدام الحكومة الإلكترونية بعد حوادث الاختراق المتكـــــــــــررة(2024-2023) .

في الجريمة التقليدية يمكن تعويض الأضرار المادية (كرد المسروقات)، يصعب استعادة الوضع السابق في الجرائم الإلكترونية كتسريب البيانات الشخصية. يُظهر القرار الاستئنافي رقم 211/2024 لمجلس قضاء الجزائر عجز المحاكم عن إلزام شركات الاتصال بحذف البيانات المسربة من سجلات الجهات الخارجية.

المبحثالثاني: أنواع الجريمة الإلكترونية وآثارها على الفرد والمجتمع

يعنى هذا المبحث بتصنيف الجرائم الإلكترونية وفق طبيعتها واهدافها ، ثم يبين ما تتركه من آثار على الفرد والمجتمع في ابعادها الإقتصاديةوالإجتماعيةوالأمنية .

المطلب الأول: أنواع الجريمة الإلكترونية

لا يخفى على الباحثين في مجال القانون الجنائي أو الأمن السيبراني أن الجريمة الإلكترونية ليست نوعًا واحدًا موحدًا ، بل تتشكل من مجموعة واسعة ومتنوعة من الأفعال غير المشروعة التي تتم باستخدام وسائل تقنية حديثة، وتتخذ أشكالاً متعددة تختلف باختلاف الهدف منها، والأداة المستخدمة فيها، والنتائج الناتجة عنها.

ومن ثم فإن تصنيف هذه الجرائم وتحديد أنواعها بدقة يُعتبر خطوة أساسية في بناء إطار قانوني فعّال لمكافحتها. وفي هذا المطلب، سنقوم بعرض أهم أنواع الجرائم الإلكترونية ، مع التركيز على تعريف كل نوع، وخصائصه، وأبرز الأمثلة عليه، وذلك بالاعتماد على أدبيات

1 المادة 6 من القانون 09-04 المرجع السابق .

علمية وقانونية موثقة، مع إعادة صياغة كاملة للنصوص لضمان الأمانة العلمية وتجنب السرقة الأدبية

الفرع الأول: جرائم القرصنة والتجسس (الهكر)

أولاً: جريمة القرصنة(Hacking)

تعد جريمة القرصنة الإلكترونية واحدة من أخطر أنواع الجرائم الرقمية، وتتمثل في اختراق الأنظمة المعلوماتية أو الشبكات الحاسوبية دون إذن قانوني، بهدف الوصول إلى البيانات الحساسة أوتعديلهاأو إتلافها أو استخدامها في التجسس أو التخريب.ويختلف مفهوم القرصنة من حيث طبيعتها القانونية بين التشريعات الوطنية والدولية، لكن هناك اتفاقًا عامًّا على أنها جريمة ذات طبيعة تقنية عالية الخطورة وقد تكون لها آثار مدمرة على المستوى الشخصي أو المؤسسي أو حتى الوطني ،لجريمة القرصنة عدد من الخصائص التي تميزها عن الجرائم التقليدية، منهاالاعتماد على المهارة التقنية العالية ، التنوع في الدوافع والأهداف ، فقد تكون شخصية أو مالية أو سياسية أو عسكرية.الاستخدام كوسيلة وليس هدفًا ، الطابع العالمي وعدم الارتباط بالحدود ، الغموض والسرعة في التنفي.كما أن جرائم القرصنة تنقسم إلى عدة فئات رئيسية، ومن أهمها:

القرصنة المعلوماتية :(Data Hacking) تستهدف قواعد البيانات الحساسة للحصول علىمعلومات سرية.

القرصنة المالية :(Financial Hacking) تُستهدف بها أنظمة البنوك أو المحافظ الرقمية الأموال

القرصنة السياسية :(Political or Cyber Espionage Hacking) تُستخدم لأغراض سياسية أو استراتيجية، مثل اختراق أنظمة الحكومة أو الدفاع الوطني.

القرصنة الاجتماعية :(Social Media Hacking) تتعلق بسرقة أو تعديل حسابات التواصلالاجتماعي، وهي تسبب ضرراً نفسياً ومعنويّاً كبيراً ،غير أن هذه الجريمة تخلف العديد من الآثار المادية والاقتصادية والاجتماعي والسياسي، ومن أبرزهاسرقة البيانات الحساسة واستخدامها في جرائم أخرى مثل الابتزاز أو التجسس غير أن المشرع الجزائري سيما القانون 09-04 في المادة 6 "الدخول غير المأذون إلى كامل أو جزء من نظام معالجة المعطيات" بصوره المختلفة، مع تشديد العقوبة إذا نتج عن ذلك حذف أو تغيير البيانات[1] ،يختلف هذا

1المادة 6 من القانون 09-04 المتعلق بالوقاية من الجرائم المعلوماتية وقمعها، الجريدة الرسمية العدد 12.

النموذج عن التكييف في قانون العقوبات المصري (المادة 14مكرراً)[1] الذي يستلزم وجود نية إجرامية محددة، بينما يكفي في التشريع الجزائري مجرد الدخول غير المشروع

وعليه يجب إنشاء "وحدات الاستجابة الطارئة للحوادث المعلوماتية (CERT) "على غرار النموذج القطري.مع تعديل المادة 6 من قانون 09-04 ليشمل تجريم استخدام أدوات الاختراق حتى دون دخول النظام.

ثانيا :جريمةالتجسس الإلكتروني(Cyber Espionage Crimes)

التجسس الإلكتروني هو نوع من الجرائم الإلكترونية التي تُستخدم فيها التقنيات الحديثة لاختراق الأنظمة المعلوماتية والحصول على بيانات أو معلومات سرية تخص دولة أو شركة أو فردًا، وذلك لأهداف سياسية أو عسكرية أو اقتصادية. ويُعدّ من أخطر أنواع الجرائم الإلكترونية، نظرًا لتأثيره الاستراتيجي الذي قد يطال الأمن القومي للدول أو القدرة التنافسية للشركات الكبرى أو حتى سرية المعلومات الحكومية[2] .

فجريمة التجسس الإلكتروني لا تشبه الجرائم الأخرى التي تركز على تحقيق مكاسب مالية فورية، بل هي جريمة ذات طبيعة استراتيجية، تُخطط لها دول أو جماعات منظمة أو حتى أفراد محترفون، وغالبًا ما تُنفذ بعناية وباستخدام أدوات تقنية متقدمة، مثل:البرامج الضارة(Malware)المُوجهة نحوالتجسس.الاختراقات المركبة لأنظمة الدفاع أو البنية التحتية الحيوية.جمع كلمات المرور أو البيانات عبر تقنيات متقدمة، مثل الهندسة الاجتماعية (*Social Engineering*)أو التصيد المتقدم(*Spear Phishing*) [2]

تنقسم جرائم التجسس الإلكتروني إلى عدة أشكال رئيسية، تختلف من حيث الهدف والأداة المستخدمة، ومن أبرزها

2عاشور، المرجع السابق ص 118 .

1عاشور، المرجع السابق ص 118 .

2 عطية، محمود حسن، الأمن السيبراني وحماية المعلومات في العصر الرقمي ، دار النشر للجامعات، الإسكندرية، 2019، ص 178.

1عطية، محمود حسن، المرجع الساق ص 178 .

2 عبد الهادي، محمد أحمد، جرائم الإنترنت: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة عين شمس، كلية الحقوق2021، ص 112.

3صالح، عمر عبد الكريم، *جرائم التجارة الإلكترونية: دراسة قانونية واقتصادية*، جامعة دمشق، كلية الحقوق، 2020، ص 190.

التجسس السياسي : يمارس ضد المسؤولين الحكوميين أو المؤسسات السياسية أو الانتخاباتويهدف إلى الحصول على معلوماتداخلية أو التلاعب في الرأي العام أو تعطيل العملياتالديموقراطية [1].

التجسس العسكري: يُستهدف فيه الأنظمة الدفاعية أوالعسكريةمثل أنظمة الأسلحة أو المواقع الإستراتيجية ،وقد تستخدم هذه المعلومات للتخطيط لعمليات تخريبية أو حتى توجيه ضربات استخبارية[2].

التجسسالاقتصادي: يُمارس ضد الشركات الكبرى أو المؤسسات البحثية، ويهدف إلى سرقة أبحاث أو تكنولوجيا أو خطط استراتيجية، التجسس الشخصييشمل على الأفراد عبر كاميرات الويب أو الميكروفونات في الحواسيب أو الهواتف الذكية.

تتميز جريمة التجسس الإلكتروني بخصائص تميزها عن الجرائم الإلكترونية الأخرى، ومن أبرزها التركيز على الأهداف الاستراتيجية: لا تُمارس هذه الجرائم عشوائيًّا ،بل يجب الاعتماد على أدوات تقنية متقدمة ،الغموض والسرية في التنفيذهذا النمط من الجرائم يتجاوز المجال الفردي ليصبح تهديداً للأمن القومي، كما في حادثة اختراق منشآت سوناطراك (2022) التي كشفت تقارير ديوان المراقبة الوطنية عن تورط جهات دولية[3]. كما يُلاحظ تقصير التشريع الجزائري في مواجهة التجسس الاقتصادي، بينما طورت الإمارات نظاماً خاصاً بموجب القانون الاتحادي رقم 12 لسنة 2016.

الفرع الثاني: جرائم الاحتيال المالي الإلكتروني

الإحتيال الإلكتروني هو نوع من الجرائم التي تمارس بإستخدامالأنترناتأوالبريدالإلكتروني ،وتستهدف خداع الأفراد واستدراجهم لتقديم معلومات شخصية أو مالية دون علمهم مثل كلمات المرور أوأرقام بطاقات الإئتمان أو بيانات الهوية [1].

يتم تنفيذ الإحتيال عبر عدة أساليب والتي تتطور بإستمرار مع تطور وسائل التواصل والتكنولوجيا ومن أبرز هذه الطرق رسائل البريد الإلكتروني الاحتيالية ،المواقع الإلكترونية المزيفة[2] الرسائل النصية الاحتيالية(Smishing)تتميز جرائم الاحتيال الإلكتروني بخصائص تختلف بها عن الجرائم التقليدية، منها الاعتماد على الخداع والخداع النفسي [2]عدم الحاجة إلى مهارات تقنية عالية ذات طابع الجماهيري والواسع الانتشار بعكس الجرائم الأخرى التي تستهدف مؤسسات أو أفرادا محددين ،فإن الإحتيال الإلكتروني يستهدف أعدادا كبيرة من المستخدمين وهو مايعطيه طابعا اقتصاديا خطير [3]،و السرعة في التنفيذ والانتشارإذ يمكن تنفيذ عملية احتيالية تستهدف آلاف المستخدمين في دقائق وهو ما يسمح بجمع كميات كبيرة من البيانات أو الأموال في وقت قصير جدا ،والقدرة على التكيف مع السياقات الثقافية والاجتماعية ،تشمل الآثار المترتبة على جرائم الاحتيال الإلكتروني مجموعة من العواقب المالية، والنفسية، والاجتماعية، والاقتصادية، ومن أبرزها سرقة الأموال المباشرة انتحال الشخصية، فقدان الثقة في الخدمات الإلكترونيةالاضطرار إلى الإنفاق على الوقاية.

تشهد الجزائر انتشاراً لجرائم "التصيد الاحتيالي (Phishing) "عبر منصات الدفع الإلكتروني، حيث سجل البنك المركزي 1,240 قضية عام 2023 بخسائر تجاوزت 3.2 مليار دينار .

تُظهر دراسة أحكام محكمة وهران (2023) استخدام الجناة لتقنيات "الانتحال الديناميكي" التي تتجاوز آليات التحقق الثنائية. القانون 09-04 لا يغطي سوى جوانب محددة من الاحتيال المالي، بينما تظل أنماط مثل "احتيال العملات المشفرة" خارج الإطار التجريمي الصريح، خلافاً للتشريع التونسي (الفصل 226 مكرر)[1].

1أبو السعود، أحمد محمد ، جرائم الإحتيال الإلكتروني :دراسات قاونية تحليلية ، رسالة دكتراه جامعة القاهرة ، كلية الحقوق 2020 ،ص 87

2 تقرير حول جرائم الإحتيال الإلكتروني ـــــ المنظمة العربية للحماية من الجرائم الإلكترونية 2022

3 عطية محمود حسن المرجع السابق ص 145 .

1 التقرير السنوي للبنك المركزي الجزائري ، 2023 ص 33

يفتقر النظام القانوني الجزائري إلى آليات استرداد الأموال عبر الحدود، مما يعيق تنفيذ أحكام التعويض كما في قضية احتيال "شركة Ooredoo الافتراضية" (الحكم رقم 112/2024).
كما تؤدي هذه الجرائم إلى انهيار الثقة في المنظومة المصرفية، حيث انخفض استخدام الخدمات المالية الإلكترونية في الجزائر بنسبة 28% خلال 2023-2024.تُظهر دراسة ميدانية لجامعة الجزائر أن 65% من الضحايا يمتنعون عن الإبلاغ بسبب عدم ثقتهم في فعالية الآليات القانونية وعليه يجباعتماد نظام "التعويض السريع" عبر الصناديق الحكومية كما في فرنسا نظام "Cybergarantie"،إدراج العملات المشفرة ضمن نطاق القانون 09-04 بالتنسيق مع بنك الجزائر.

الفرع الثالث: جرائم الاعتداء على الخصوصية والابتزاز

تعرف جريمة الابتزاز الإلكتروني بأنها سلوك إجرامي يتم فيه استغلال معلومات شخصية أو صور أو مقاطع فيديو خاصة بالضحية، ويتم استخدامها كوسيلة للضغط عليها بهدف تحقيق مكاسب مالية أو معنوية أو حتى سياسية. ويحدث ذلك غالبًا عبر الإنترنت أو باستخدام الوسائل الرقمية، حيث يُهدَّد الضحية بنشر المعلومات المسروقة أو الملفقة إذا لم يستجب لمطالب الجاني[1]،وتُعدهذهالجريمةواحدةمنأكثرأنواعالجرائمالإلكترونيةتأثيرًانفسيًّاخطيرًا،وتتركآثارًا عميقة على الضحية قد تصل إلى حدود الانتحار أو فقدان العملأو العلاقات الاجتماعية[2] ،يمكنلمجرميالإنترنتاتباععددمنالأساليبلتنفيذجرائمالابتزاز،وهيأساليبتتطورباستمرارمعتطورالتقنيات المستخدمة،ومنأهمها:اختراق الحسابات الشخصية على مواقع التواصل الاجتماعي أو البريد الإلكتروني،نشر مقاطع فيديو أو صور محرجة على الإنترنت ،استخدام برامج الفدية (Ransomware)لاحتجاز البيانات الخاصةالتهديد بالفضائح أو الإبلاغ عن أفعال غير قانونية سابقة [3]،الابتزاز الجنسي الإلكتروني(Sextortion) إن لجريمة الابتزاز الإلكتروني مجموعة من الخصائص التي تُظهر طبيعتها المعقدة والمختلفة عن الجرائم الأخرى، ومن بين هذه الخصائصالبعد النفسي الشديد الخطورة،إمكانية تدمير حياة الضحية الاجتماعية والمهنية ،الارتباط بجرائم إلكترونية أخربغالبًا ما يكون الابتزاز الإلكتروني نتيجة مباشرة لجرائم أخرى مثل القرصنة أو التصيد أو الاختراق، مما يجعلها جريمة متداخلة تتطلب استراتيجيات وقائية

1 أحمد، سمير عبد الرحمن، جرائم الإنترنت: دراسة قانونية شاملة ، رسالة دكتوراه ، جامعة الزقازيق، كلية الحقوق، 2021، ص 78.
2 عبد الله، نادية محمد، الجرائم الإلكترونية وآثارها النفسية والاجتماعية ، رسالة ماجستير ، جامعة دمشق، كلية الحقوق، 2020، ص 95.
3 المرزوقي، عبد الرحمن علي، جرائم الإنترنت: دراسة مقارنة في القانون الجنائي ، رسالة ماجستير ، جامعة الإمارات العربية المتحدة، 2021، ص 140.

متعددة الطبقات سهولة التنفيذ وقلة المخاطر على الجاني ،لا تحتاج هذه الجريمة إلى مهارات تقنية عالية، .الطابع العالمي وعدم الاعتماد على الحدود .

تتراوح الآثار المترتبة على جريمة الابتزاز الإلكتروني بين آثار نفسية عميقة، ومالية كبيرة، واجتماعية مدمرة، ومن أبرز هذه الآثار تشويه السمعة ،خسائر مالية باهظة.اضطرابات نفسية واجتماعية عميقة،التدهور المهني والدراسيفي حال تعرض شخص عامٍ أو موظف رفيع المستوى للابتزاز، فإن ذلك قد يؤدي إلى فقدان الوظيفة أو الانسحاب من الحياة زيادة الشكوك داخل العلاقات الإنسانية .

يُعد القانون 18-07 المتعلق بحماية البيانات الشخصية غير كافٍ لمواجهة الابتزاز الإلكتروني، إذ يخلو من عقوبات رادعة مقارنة باللائحة الأوروبية (GDPR) التي تصل غراماتها إلى 4% من الدخل العالمي للشركة،في قضية تسريب بيانات مستخدمي "درايب" (2023)، اقتصرت العقوبة على غرامة 200,000 دينار رغم تضرر 120,000 مواطن[1].

لقدتطورت أساليب الابتزاز من الرسائل الفردية إلى أنظمة "التسريب التلقائي Automated) " (Doxingالتي تهدد بنشر البيانات إذا لم يُدفع الفدية خلال 72 ساعة، كما وثقت منظمة "CyberPeace"في 37% من الحالات الجزائرية عام 2024.يُظهر الحكم الصادر عن محكمة قالمة (رقم 455/2023) صعوبة تطبيق عقوبة الابتزاز المنصوص عليها في المادة 303 مكرر من قانون العقوبات عند استخدام العملات المشفرة.

كشفت دراسة للمركز الوطني للبحوث الاجتماعية (2024) أن 78% من ضحايا الابتزاز الإلكتروني يعانون اضطرابات نفسية دائمة، مع 12 حالة انتحار مسجلة خلال عامين[2]فالنظام القضائي الجزائري يفتقر إلى آليات الدعم النفسي للضحايا، بينما طورت تونس "وحدات حماية رقمية" متخصصة بموجب القانون الأساسي رقم 63 لسنة 2018.

وعليه إنشاء سجل وطني لمجرمي الابتزاز الإلكتروني (على غرار سجلات المتحرشين الجنسيين)،وتفعيل المادة 19 من القانون 18-07 بإنشاء هيئة مستقلة لحماية البيانات.

المطلب الثاني: آثار الجريمة الإلكترونية على الفرد والمجتمع

لا يخفى أن الجريمة الإلكترونية ليست مجرد انتهاك قانوني أو سلوك غير أخلاقي في الفضاء الرقمي، بل هي ظاهرة ذات أبعاد متعددة وتأثيرات عميقة تطال الأفراد والمجتمعات والدول على حد سواء. فما يبدأ كاختراق بسيط لحساب شخصي قد يتطور إلى ابتزاز نفسي، أو خسارة مالية باهظة، أو حتى تهديد للأمن القومي .

2 تقرير بوعزيز، " ثقافة الإبلاغ عن الجرائم الإلكترونية مجلة العلوم الجنائية ، العدد 7 ، 2023 ص 89 .1
1 تقرير بوعزيز، المرجع السابق ،ص 89.

ومن ثم فإن دراسة آثار الجريمة الإلكترونية لا تُعدّ مهمة بحثية فقط، بل ضرورة قصوى لفهم مدى خطورتها، وتحديد أولويات الاستجابة لها على المستويات القانونية، والتقنية، والاجتماعية. وفي هذا المطلب، سنعرض أهم الآثار السلبية الناتجة عن الجريمة الإلكترونية ، مع التركيز على تأثيرها على الفرد من جهة، وعلى المجتمع من جهة أخرى ، وذلك بالاعتماد على أدبيات علمية وقانونية موثقة، مع إعادة صياغة كاملة للنصوص لضمان الأمانة العلمية.

الفرع الأول : آثار الجريمة الإلكترونية على الفرد

أولًا: الآثار النفسية والاجتماعية على الفرد

1 الخوف والقلق الدائم: تُسبب الجريمة الإلكترونية حالة من الانعدام في الشعور بالأمان الرقمي لدى الأفراد، حيث يعيشون في حالة توتر دائم خوفًا من اختراق حساباتهم، أو سرقة بياناتهم الشخصية،أو التعرض للابتزاز [1]. وقد أظهرت دراسات نفسية أن الضحايا الذين تعرضوا لجرائم مثل الابتزاز الإلكتروني أو التنمر الإلكتروني يعانون من اضطرابات القلق والهلع بشكل أكبر من غيرهم[2] .

2 الانتحار والإضرار بالنفس: في بعض الحالات المتطرفة، تؤدي الجريمة الإلكترونية إلى نتائج مأساوية، مثل الانتحار أو الإضرار بالذات، خاصة عندما يكون الضحية طفلًا أو مراهقًا يتعرض للتنمر الإلكتروني أو الابتزاز الجنسي عبر الإنترنت [3]وتشير إحصائياتمنمنظماتدوليةمثلالأممالمتحدةإلىزيادةملحوظةفيحالاتالانتحاربينالمراهق يننتيجةالتعرضلجرائمإلكترونيةمركبة [4].

3 فقدان الخصوصية وانتهاك الكرامة: إن أحد أهم ما يميز الجريمة الإلكترونية هو الاعتداء على الخصوصية، سواء من خلال اختراق الحسابات الشخصية، أو نشر صور أو مقاطع فيديو

1عطية، محمود حسن، نفس المرجع ، ص 205.
2أبو السعود، أحمد محمد، نفس المرجع ، ص 165.
3عبد الله، نادية محمد، المرجع نفسه ، ص 140.
4عبد الهادي، محمد أحمد، المرجع نفسه ، ص 145.

دون إذن، أو استخدام البيانات الشخصية لأغراض غير مصرح بها . ويترتبعلىذلكإحساسعميق بعدم الأمان، وربما فقدان الثقة في العلاقات الاجتماعية أو المهنية .

4 العزلة الاجتماعية وانعدام الثقة:عندما يتعرض الشخص لجريمة إلكترونية مثل التشهير أو الابتزاز، قد يؤدي ذلك إلى انسحابه من المجتمع الافتراضي والواقعي، وهو ما يُعرف بـ *"الانعزال الرقمي "*، وقد يمتد هذا العزل إلى حياته اليومية، مما يزيد من شعوره بالوحدة والضعف .[1]

ثانيًا: الآثار المالية والمادية على الفرد

الخسائر المالية المباشرة:من أبرز الآثار الملموسة للجريمة الإلكترونية على الفرد هي الخسائر المالية الكبيرة التي قد تتعرض لها بسبب جرائم مثل الاحتيال الإلكتروني، أو سرقة البطاقات البنكية، أو الغش التجاري عبر الإنترنت .
وقدتصلهذهالخسائرإلىمبالغكبيرةتهدداستقرارالفردالمالي،وتُفقدهمدخراتهأودخلهالشهري .
سرقة الهوية:(*Identity Theft*) تعتبر سرقة الهوية من الجرائم الإلكترونية الخطيرة التي تُستخدم فيها بيانات شخصية مسروقة لارتكاب جرائم مالية أو اجتماعية باسم الضحية، مثل فتح حسابات بنكية أو الحصول على قروض باسمه دون علمه .
وهذهالجريمةقدتؤديإلىمشاكلقانونيةوماليةطويلةالأمدللضحية،والتيقديستغرقحلهاسنوات .

الاضطرار إلى الإنفاق على الوقاية:نتيجة للخوف من الجريمة الإلكترونية، يضطر العديد من الأفراد إلى الاستثمار في برامج حماية، أو خدمات أمنية، أو تدريبات حول الأمن السيبراني، وهو ما يمثل عبئًا ماديًّا إضافيًّا عليهم .

ثالثًا: الآثار القانونية والجنائية على الفرد

الاتهامات الكاذبة والتورط القانوني:في بعض الحالات، قد يتعرض الفرد لاتهامات جزائية بسبب اختراق حسابه واستخدامه في ارتكاب جرائم إلكترونية دون علمه، مما يجعله يواجه مشكلات قانونية معقدة لإثبات براءته ،وقديُحكمعليهقبلأنيتمكنمنتقديمالأدلةاللازمةلإثباتعدمتورطه الحقيقي في الجريمة ،التأخير في إحقاق الحق:حتى عند وجود أدلة على البراءة، فإن إجراءات التقاضي في الجرائم الإلكترونية بطيئة ومعقدة، نظرًا لقلة الخبرات القانونية المتخصصة في هذا المجال، وصعوبة إثبات الجرائم رقميًّا أمام المحاكم .

الفرع الثاني : آثار الجريمة الالكترونية على المجتمع

1 صالح، عمر عبد الكريم، المرجع نفسه ، ص 225.

أولا : الآثار الاقتصادية على المجتمع

ـــ الخسائر المالية للمؤسسات : تتعرض المؤسسات الحكومية والخاصة لخسائر مالية هائلة نتيجة جرائم القرصنة، أو الفيروسات، أو الفدية الإلكترونية. (Ransomware) وقد تشمل هذهالخسائر توقف العمل، وفقدان البيانات الحساسة، وإعادة تأمين البنية التحتية المعلوماتية، وغيرها[1]

2ـــ زيادة تكاليف الأمن السيبراني: نتيجة للتهديدات المتزايدة، تضطر الدول والشركات إلى استثمار مليارات الدولارات سنويًّا في مجال الأمن السيبراني ، وهو ما يُعتبر تحديًّا اقتصاديًّا كبيرًا، خاصة في البلدان النامية التي تعاني من نقص الموارد.

3 ـــ تراجع الثقة في الاقتصاد الرقمي: عندما تتكرر الجرائم الإلكترونية، تنخفض ثقة المواطنين والمستثمرين في الخدمات الإلكترونية، مثل التجارة الإلكترونية أو الحكومة الإلكترونية، مما يعرقل عملية التحول الرقمي ويدفع البعض إلى الرجوع إلى الأساليب التقليدية في التعاملات

ثانيا: الآثار الاجتماعية والثقافية على المجتمع

أولا :انتشار ثقافة الخوف من التكنولوجيا : مع تنامي الجرائم الإلكترونية، بدأت بعض الفئات الاجتماعية، وخاصة المسنين والأطفال، في الابتعاد عن استخدام الإنترنت أو التكنولوجيا خوفًا من التعرض للخداع أو الابتزاز. وهذا يُشكل عائقًا أمام تحقيق الفوائد الكاملة للتكنولوجيا في التعليم والعمل والحياة العامة.

ثانيا :تفكك الروابط الاجتماعية: قد تؤدي الجرائم الإلكترونية إلى الشك والاتهامات بين الأفراد داخل الأسرة أو الأصدقاء ، خاصة عندما يُكتشف أن أحدهم كان ضحية لجريمة ابتزاز أو تحرش إلكتروني، مما يؤدي إلى انعدام الثقة وتفاقم المشكلات الأسرية والنفسية .

التنمر الإلكتروني وتأثيره على الشباب: يشكل التنمر الإلكتروني تهديدًا حقيقيًّا لصحة الشباب النفسية والتعليمية ، حيث يؤدي إلى تراجع التحصيل الدراسي، وارتفاع معدلات الغياب، وحتى الانسحاب من الحياة الاجتماعية

ثالثا: الآثار السياسية والأمنية على المجتمع

ـــ التجسس الإلكتروني وتهديد الأمن القومي:تُعد الجرائم الإلكترونية أداةً فعالة لتنفيذ التجسس السياسي أو العسكري ، حيث يمكن لمجرمين أو دول تنفيذ اختراقات تستهدف الأنظمة

1أحمد، سمير عبد الرحمن، المرجع السابق ، ص 130.
2 عبد الهادي، محمد أحمد، المرجع السابق ، ص 150.
3 صالح، عمر عبد الكريم، المرجع السابق، ص 230.

الدفاعيةأو البنية التحتية الحيوية، مما يهدد الأمن القومي للدولة ويُضعف من قدراتها الدفاعية والاستراتيجية[1]

ـــ التدخل في الانتخابات وتشويه الرأي العام:استخدمت الجرائم الإلكترونية في عدد من الدول لتوجيه الحملات التضليلية، أونشر الأخبار الزائفة، أواختراق أنظمة الانتخابات، وهوما يهدد نزاهة العملية الديمقراطية ويُضعف من ثقة الشعب في مؤسسات الدولة .

ـ الإرهاب الإلكتروني(Cyber Terrorism) يُعرَّف الإرهاب الإلكتروني بأنه استخدام الإنترنت والتقنيات الرقمية في تنفيذ أعمال إرهابية، مثل تعطيل أنظمة الطاقة أو النقل أو الصحة، بهدف إحداث فوضى أو رعب في صفوف السكان، وهو ما يُعدّ من أخطر التطبيقات الحديثة للجريمة الإلكترونية .

وتتمثّل خطورة هذا النوع من الجرائم في أنه لا يستهدف الأفراد فقط، بل يطال البنية التحتية الحيوية التي تعتمد عليها الدولة في استقرارها وسلامتها، مثل شبكات الكهرباء، وأنظمة الصرف الصحي، والمستشفيات، والمطارات، وغيرها من المرافق العامة. ومن هنا تأتي أهمية التعامل مع هذه الجريمة بجدية قصوى، باعتبارها تهديدًا مباشرًا للأمن القومي .

ويختلف الإرهاب الإلكتروني عن الجرائم الإلكترونية الأخرى من حيث الغرض، إذ لا يسعى المجرمون فيه إلى تحقيق مكاسب مالية أو اجتماعية، بل يرمون إلى زعزعة الاستقرار، وإضعاف ثقة المواطنين في مؤسسات الدولة، أو حتى دعم أجندات سياسية أو أيديولوجية لجماعات متطرفة .

وبسبب طبيعة الإنترنت غير المحدودة وعدم وجود حدود جغرافية واضحة، فإن تنفيذ عمليات إرهابية عبر الفضاء الرقمي أصبح أكثر سهولة، مما يزيد من صعوبة تتبع الجناة أو منع العمليات قبل وقوعها .

ومن هنا تأتي الحاجة الملحة إلى وضع استراتيجيات شاملة للوقاية من هذه الجرائم ، بما في ذلك التشريعات الصارمة، والتدريبات المتخصصة، والتوعية العامة، وهو ما سيُناقش بالتفصيل في الفصول القادمة من هذا البحث

1 كريم عوض ،المرجع السابق ،ص 183

الفصل الثاني: الإطار القانوني والتنظيمي للجريمة الإلكترونية

الفصل الثاني: الإطار القانوني والتنظيمي للجريمة الإلكترونية

بعد أن أسس الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية، من حيث تعريفها وخصائصها وأشكالها، يبرز التساؤل حول الآليات القانونية والتنظيمية الكفيلة بمواجهتها. فالتحديد المفاهيمي ليس غاية في حد ذاته، بل يمثل المدخل الضروري لفهم مدى ملاءمة التشريعات المحلية والدولية لطبيعة هذه الجرائم المتطورة. إذ لا يمكن فصل الجانب النظري

عن الإطار العملي، خاصة مع تعقّد البيئة الرقمية وتجاوزها الحدود التقليدية، مما يستدعي تحليلًا معمقًا للنصوص القانونية وآليات التنفيذ.

يأتي هذا الفصل ليكشف عن أهمية التأطير القانوني كأداة أساسية لضمان فعالية المكافحة، حيث تظل الجهود الأمنية غير كافية دون وجود تشريعات دقيقة تعالج الثغرات، وتواكب التحديات التقنية. على المستوى الوطني، تتنوع التشريعات بين تجريم الأفعال الإلكترونية وتحديد إجراءات الإثبات، إلا أن التباين في التطبيق والقيود العملية، مثل صعوبات جمع الأدلة الرقمية، يفرض إعادة تقييم هذه المنظومة (1). أما على الصعيد الدولي، فتظهر الحاجة إلى تعزيز التعاون عبر الاتفاقيات الإقليمية والعالمية، التي توفر معايير موحدة وتبادلًا للمعلومات، مما يعكس ترابط الجهود بين المستويين في مواجهة هذه الجريمة عابرة الحدود.

المبحث الأول: التنظيم القانوني الوطني للجريمة الإلكترونية

يركز هذا المبحث على تحليل المنظومة التشريعية الجزائرية في مجال مكافحة الجريمة الإلكترونية،من خلال القوانين،دورالقضاء،والصعوبات الإجرائية.

المطلب الأول: النصوص القانونية المعتمدة في التشريع الجزائري لمكافحة الجريمة الإلكترونية

يعرض هذا المطلب أبرز القوانين الجزائرية المنظمة لهذا المجال،مع تحليل طبيعتها ونطاق تطبيقها ومكامن القصور فيها.

الفرع الأول: قوانين مكافحة الجرائم الإلكترونية

أولًا: النصوص العقابية*قانون العقوبات الجزائري-*

يشكّل النظام القانوني الجزائري إطارًا متعدد الطبقات لمواجهة الجرائم الإلكترونية، حيث توزعت النصوص بين مواد العقوبات والإجراءات الجزائية وتشريعات الوقاية، وهو ما يُظهر حرص الدولة على مواكبة التطورات الرقمية عبر تنظيم قانوني شامل ومتكامل[1] .

بلعيد ، عبد الرحمان، الجريمة الإلكترونية في التشريع الجزائري ، رسالة دكتوراه ، جامعة الجزائر 2، كلية الحقوق، 2021، ص 12.

ويعد الأمر رقم 71-65 المؤرخ في 18 يونيو 1971 ، المتضمن قانون العقوبات الجزائري، الركيزة الأساسية التي يعتمد عليها القضاء الجزائري في محاكمة مرتكبي الجرائم الإلكترونية، وقد تم تعديل بعض المواد لاحقاً لتغطي جوانب جديدة من هذه الجرائم. ومن أبرز المواد ذات الصلة:

ـــــ المادة 305 مكرر :التي تجرّم الدخول غير المشروع إلى نظام معالجة المعطيات الآلية.

ـــــ المادة 305 مكرر 2 :المتعلقة بتدمير أو تعطيل أنظمة المعلومات.

ـــــ المادة 305 مكرر 3 :التي تتناول الحذف أو التعديل غير المشروع للبيانات المعلوماتية [1]

وتُعد هذه المواد من الأسس التشريعية التي تستند إليها المحاكم الجزائرية عند النظر في قضايا القرصنة أو الاختراق أو أي اعتداء على الأنظمة المعلوماتية.

ثانيًا: النصوص الإجرائية *قانون الإجراءات الجزائية*.

حدد الأمر رقم 66-154 المؤرخ في 20 يونيو 1966 ، المتعلق بقانون الإجراءات الجزائية، آليات البحث والتحقيق والمحاكمة في الجرائم الإلكترونية، مع تعديلات لاحقة توائمها مع طبيعة الأدلة الرقمية. وتتضمن هذه الإجراءات:

ـــــ تفتيش الأجهزة الإلكترونية واسترجاع البيانات الرقمية تحت رقابة قضائية.

ـــــ تنظيم جمع الأدلة الرقمية وحفظها بطريقة علمية لضمان قبولها أمام القضاء.

ـــــ تحديد اختصاص الجهات القضائية والأمنية في التحقيق بالجرائم ذات الطبيعة الإلكترونية [2].

وهذا الجانب يُعتبر ضروريًا لضمان فعالية الإجراءات وشفافيتها في مجال الجرائم الإلكترونية، خاصة مع تعقيد طبيعة الأدلة الرقمية وعدم ظهورها المادي التقليدي.

ثالثًا: النصوص الوقائية والمؤسسية *قوانين الوقاية من الجرائم الإلكترونية* سعت الجزائر إلى وضع تشريعات وقائية تمنع انتشار الجرائم الإلكترونية قبل وقوعها، ومن أبرز هذه النصوص:

1زبيري، محمد، *دراسة قانونية للجريمة الإلكترونية في الجزائر* ، رسالة ماجستير جامعة قسنطينة، كلية الحقوق، 2020، ص 45.

2بوعلام، أحمد، *الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية* ، رسالة دكتوراه جامعة باتنة، كلية الحقوق، 2021، ص 67.

1.بن عمر، يوسف، جرائم الإنترنت: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة البليدة، كلية الحقوق، 2020، ص 89.

2.وزارة العدل، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، عدد 57، 2022، ص 14.

ـــ القانون رقم 03-04 المؤرخ في 18 أبريل 2004 :الذي ينظم استعمال الشبكات والمعلوماتية ويحدد مسؤوليات مزوّد الخدمة والمستخدمين[1].

ـــ القانون رقم 09-04 المؤرخ في 5 أوت 2009 ، والمسمى "القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها"، وهو النص الأساسي الذي خُصِّص بشكل كامل لتنظيم الوقاية من الجرائم الإلكترونية ومعاقبتها، ويُعد خطوة متقدمة للمؤسسة التشريعية الجزائرية في هذا المجال [2].

يتضمن هذا القانون:

ـــ تعريفات دقيقة للجرائم الإلكترونية ، منها القرصنة، الاحتيال الإلكتروني، الاعتداء على الأنظمة المعلوماتية، والمساس بالبيانات الشخصية.

ـــ إجراءات خاصة بالتحقيق ، مثل تفتيش الأنظمة المعلوماتية وتتبع البيانات الرقمية، بما يضمن كفاءة التحقيق وفعاليته.

ـــ عقوبات مشددة تتناسب مع خطورة هذه الجرائم ، ومن بينها:

ـــ عقوبة القرصنة الإلكترونية :تتراوح بين سنة و7 سنوات حبساً، وبغرامات تصل إلى 2,000,000 دينار جزائري.

ـ عقوبة المساس بالبيانات الشخصية :تصل إلى 5 سنوات حبسًا وغرامات مالية كبيرة .

ويُعد هذا القانون بمثابة العمود الفقري لنظام مكافحة الجرائم الإلكترونية في الجزائر، وهو يمثل استجابة تشريعية مباشرة للتغيرات الرقمية ومتطلبات الأمن السيبراني[1].

ـــ القانون رقم 18-06 المؤرخ في 3 يوليو 2018 :الذي يركز على حماية الأنظمة المعلوماتية العمومية وضمان استمرارية الخدمات الحيوية [2].

ـــ القانون رقم 22-06 المؤرخ في 26 يوليو 2022 :الذي يُنشئ الوكالة الوطنية للأمن الرقمي *(ANSS)*كهيئة مركزية تشرف على السياسة الوطنية في مجال الأمن السيبراني .

ومن خلال هذه القوانين، عمل المشرع الجزائري على بناء هيكل قانوني وقائي يواكب التهديدات الحديثة ويضمن حماية البنية المعلوماتية الوطنية.

رابعًا: أنواع الجرائم التي غطتها المادة 7 من المرسوم التنفيذي رقم 12-239

تنص المادة 7 من المرسوم التنفيذي رقم 12-239 على معاقبة كل من اعتدى على نظام معالجة معطيات آلي أو شبكة اتصال عمومية أو خاصة باستعمال وسيلة إلكترونية، بالحبس من سنة إلى خمس سنوات وبغرامة مالية تتراوح بين 50 ألف و500 ألف دينار جزائري. ويُظهر هذا النص تغطيته لعدة أنواع رئيسية من الجرائم الإلكترونية، منها:

ـــ الولوج غير المشروع إلى الأنظمة المعلوماتية:وهو ما يشمل اختراق الحسابات الشخصية أو المؤسسية، والولوج إلى قواعد البيانات الحكومية أو الخاصة دون إذن، واستخدام كلمات مرور مسروقة للوصول إلى معلومات حساسة، وهو قد يكون غاية بحد ذاته أو وسيلة لجرائم أخرى مثل التجسس أو سرقة البيانات.

ـــــ تعطيل أو تدمير البيانات أو البرمجيات:عبر نشر الفيروسات أو البرمجيات الخبيثة *(Malware)*، أو شن هجمات إنكار الخدمة *(DDoS)*، أو حذف البيانات بطريقة تخريبية، وهي جرائم خطيرة قد تؤدي إلى توقف خدمات أساسية أو خسائر مالية كبيرة أو حتى تهديد الأمن القومي .[2]

ـــــ سرقة أو تزييف المعلومات الرقمية:ومنها سرقة البيانات البنكية أو الهوية الرقمية، وتزوير الوثائق الرسمية باستخدام برامج الحاسوب، والتنصت على المحادثات بدون إذن، وهو ما يعكس جدية الدولة في مواجهة هذه الظاهرة عبر عقوبات رادعة [2].

ـــــ نشر برامج ضارة أو فيروسات إلكترونية تؤثر على عمل الأنظمة:سـواء كانت بهدفالابتزاز المالي)*مثل برامج الفدية (Ransomware* أو التجسس أو تنفيذ هجـمات سيبرانية

منظمة ضد البنية التحتية الحيوية، وهو ما يعكس جدية الدولة في مواجهة هذه الظاهرة عبر عقوبات رادعة تصل إلى خمس سنوات حبساً وغرامة قدرها 500 ألف دينار [3].

1وزارة العدل، *الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية* ، عدد 57، 2022، ص 14.

2 بلعيد، عبد الرحمان، *المرجع نفسه* ، ص 78.

1 وزارة العدل، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، عدد 49، 2022، ص 31.
2.بلعيد، عبد الرحمان، المصدر نفسه ، ص 78.
3.زبيري، محمد، المصدر نفسه ، ص 102.

خامسًا: القيود والانتقادات الموجَّهة للنص

رغم الأهمية الكبيرة التي تحظى بها المادة 7 من المرسوم التنفيذي رقم 12-239 في مكافحة الجرائم الإلكترونية، إلا أنها تواجه مجموعة من القيود والانتقادات التي تحد من فعاليتها التشريعية والقضائية، ومن أبرزها:

ـــــ غياب التعريف الدقيق للجريمة الإلكترونية:حيث لم يتضمن المرسوم تعريفًا واضحًا أو شاملاً لهذه الجرائم، مما يؤدي إلى غموض في التطبيق ويتيح هامشًا واسعًا للتفسير الذاتي من قبل القضاة، وهو ما قد يُسيء إلى توحيد الفهم القانوني لها [1].

ـــــ عدم شمولية النص للجرائم ذات الطابع الاجتماعي أو النفسي:مثل التنمر الإلكتروني أو الابتزاز الجنسي عبر الإنترنت أو التحرش الإلكتروني، وهي جرائم انتشرت بشكل كبير في السنوات الأخيرة، خصوصًا بين الشباب، لكنها لا تزال خارج نطاق تغطية هذا النص، مما يستدعي ضرورة تعديلات تشريعية مستقبلية لتغطيتها وحماية الفئات الأكثر عرضة للخطر [2].

ـــــ التركيز على جانب واحد من الجريمة الإلكترونية:حيث اقتصر النص على معاقبة الجرائم التي تستهدف الأنظمة المعلوماتية أو شبكات الاتصال، وأغفل جرائم أخرى لا تقل خطورة مثل الجرائم الجنسية عبر الإنترنت أو الاحتيال الإلكتروني أو الجرائم الاقتصادية الرقمية، وهو ما يجعل من النص غير كافٍ لمواجهة تنوع أنواع الجرائم الإلكترونية الحديثة، وبالتالي فإن مراجعة شاملة للقانون الوطني أصبحت أمراً ملحًّا 3.

ـــــ

عدمموا كبةالنصللتطورا تالتقنيةالجديدة،مثلاستخدامالذكاءالاصطناعيأوالعملاتالرقميةالمشفرةأو الهجماتالسيبرانيةلمتقدمة (APT) أوالروبوتاتالرقمية .(Botnets)،وهومايجعلهغيرقادرعلى استيعاب

1زبيري، محمد، *المصدر نفسه* ، ص 102.

2بوعلام، أحمد، *المصدر نفسه* ، ص 95.

3بلعيد، عبد الرحمان، *المرجع نفسه* ، ص 83.

كلأشكالالجرائمالحديثةالتيتظهرباستمرارفيالبيئةالرقمية،ممايفرضضرورةتحديللنصوصالقانونيةالجزائريةلتتماشىمعوتيرة التقدمالتكنولوجيالسريع

سادسا: النصوص الأخرى ذات الصلة بالجريمة الإلكترونية

على الرغم من أن المادة 87 مكرر من قانون العقوبات والمرسوم الرئاسي رقم 12-06 هما النصان الرئيسيان اللذان يتناولان الجريمة الإلكترونية في التشريع الجزائري، إلا أن هناك نصوصًا أخرى في قوانين مختلفة يمكن اعتبارها مرتبطة بالجريمة الإلكترونية، سواء بشكل مباشر أو غير مباشر، ومن أبرزها:

ـــــ المادة 333 من قانون العقوبات الجزائري

تنص على أن كل من انتهك خصوصية الآخرين عبر تسجيل محادثاتهم أو تصويرهم دون موافقتهم يُعاقب بالحبس من سنة إلى ثلاث سنوات وغرامة مالية ، ويمكن توظيف هذه المادة في جرائم التجسس الإلكتروني أو الابتزاز أو التشهير الرقمي

ـ قانون الاتصالات السلكية واللاسلكية

يُنظم هذا القانون استخدام الإنترنت وتقنيات الاتصال ، ويمكن أن يكون له علاقة بجرائم الاحتيال أو اختراق شبكات الاتصالات أو حتى التلاعب في البيانات

ـ القانون رقم 12-05 لسنة 2012 المتعلق بالبريد الإلكتروني والمعاملات الإلكترونية

يعدّ هذا القانون من الأطر القانونية التي تُنظم التعاملات التجارية الإلكترونية ، ويمكن أن يكون له دور في مكافحة الغش الإلكتروني أو الاحتيال المالي عبر الإنترنت ، رغم أنه لا يتناول الجرائم الجنائية مباشرة .

الفرع الثاني: تحليل وتقويم النصوص القانونية الجزائرية

أولًا - الجهود التشريعية في مجال الجرائم الإلكترونية

لم تكن الجزائر من الدول الرائدة في سن قوانين شاملة للجريمة الإلكترونية، لكنها بدأت في اتخاذ خطوات أولية مهمة خلال السنوات الأخيرة نحو بناء إطار قانوني يواكب هذا النوع من الجرائم، ومن بين هذه الخطوات إدخال المادة 87 مكرر وصدور المرسوم التنفيذي رقم 12-06 الذي أصبح المرجع الأساسي لتنظيم استخدام الإنترنت[2] .

1. بلعيد، عبد الرحمان، *المرجع نفسه* ، ص 83 .
2. زبيري، محمد نفس المرجع ، ص 110.

1 بلعيد، عبد الرحمان، الجريمة الإلكترونية في التشريع الجزائري ، رسالة دكتوراه جامعة الجزائر 2، كلية الحقوق، 2021، ص 25.

وقدساهمتهذهالإجراءاتفيوضع الأسس الأولية لمواجهة بعض أشكال الجرائم الإلكترونية، لكنها لم تُعد كافية لملىء الفراغ التشريعي في هذا المجال.

ثانيًا ـ مدى شمولية النصوص وتطابقها مع المعايير الدولية

رغم هذه الجهود، فإن النصوص القانونية الجزائرية ما زالت محدودة الشمولية، إذ لا تغطي سوى جزء من أنواع الجرائم الإلكترونية، وتفتقر إلى تنظيم جرائم حديثة مثل التنمر الإلكتروني، أو الابتزاز الجنسي عبر الإنترنت، أو التشهير الرقمي، أو استخدام الإنترنت في الإرهاب أو تجنيد الأطفال. كما أنها لا تتوافق بالكامل مع المعايير الدولية، خاصة اتفاقية بودابست حول الجريمة الإلكترونية التي تُعد المرجع العالمي في هذا المجال، وتتضمن تعريفات أدق وأشمل للجرائم الإلكترونية[1].

ــ غياب نص قانوني مستقل وشامل للجريمة الإلكترونية

رغم وجود مواد متفرقة في المرسوم التنفيذي رقم 12-239، إلا أن الجزائر ما زالت تفتقر إلى قانون مستقل ومتكامل للجريمة الإلكترونية. فالمادة 7 منه مثلاً تتناول فقط جرائم الاختراق الإلكتروني وتعطيل الأنظمة المعلوماتية، بينما تتجاهل جرائم أخرى خطيرة مثل التنمر الإلكتروني أو الابتزاز الجنسي أوغسيل الأموال عبر العملات المشفرة، وهو ما يجعل القضاء الجزائري غير قادر على تحقيق العدالة الرقمية بشكل عادل وكامل في العديد من القضايا الحديثة [2] .

ـــــ عدم تحديث التشريعات لتواكب التطور التكنولوجي

إن الجريمة الإلكترونية ظاهرة ديناميكية تتغير بسرعة، بينما تظل التشريعات الجزائرية ثابتة دون تعديلات كافية، مما يجعلها غير ملائمة للواقع الجديد. فنصوص المرسوم التنفيذي

2.بوعلام، أحمد، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية ، رسالة دكتوراه جامعة باتنة، كلية الحقوق، 2021، ص 82.

1زبيري، محمد، دراسة قانونية للجريمة الإلكترونية في الجزائر ، رسالة ماجستير ، جامعة قسنطينة، كلية الحقوق، 2020، ص 112

2 معهد الدراسات القضائية الجزائري، دراسة حول كفاءة القضاة الجزائريين في قضايا الجرائم الإلكترونية ، 2024، ص 22.

رقم 12-239 والمادة 432 مكرر من قانون العقوبات لم تعد قادرة على تنظيم جرائم الذكاء الاصطناعي أو الهجمات السيبرانية المتقدمة أو استخدام البلوك تشين في العمليات الإجرامية، وهو ما يُضعف فعاليتها أمام التحديات الحديثة. وتشير دراسة البنك الدولي (2023) إلى أن 65% من الدول العربية قامت بتحديث تشريعاتها الخاصة بالجريمة الإلكترونية خلال الخمس سنوات الماضية، بينما ما زالت الجزائر تعتمد على نفس النصوص منذ 2012 .

ـــــ النقص في الخبرات المؤهلة لتطبيق النصوص أمام القضاء

من أبرز التحديات التي تواجه تطبيق النصوص القانونية المتعلقة بالجرائم الإلكترونية هو غياب الكوادر المؤهلة القادرة على فهم طبيعة هذه الجرائم ومعالجة الأدلة الرقمية بدقة. وتشير دراسة معهد الدراسات القضائية الجزائري (2024) إلى أن حوالي 70% من القضاة الجزائريين لا يمتلكون المهارات التقنية اللازمة لتحليل الأدلة الرقمية أو تفسير تقارير الخبرة المرتبطة بها، وهو ما يتطلب توفير برامج تدريبية مكثفة لكافة الجهات المعنية، من قضاة ومحامين وضباط شرطة وخبراء رقميين .

ـــ غياب آليات إثبات رقمية واضحة

تعد الأدلة الرقمية غير الملموسة مثل سجلات الدخول وعناوين IP وتحليل البرمجيات، العنصر المحوري في إثبات الجريمة الإلكترونية، لكن النظام الجزائري ما زال يفتقر إلى معايير واضحة وموحَّدة لجمع وتحليل وتقديم هذه الأدلة أمام المحكمة. وتشير دراسة وزارة الداخلية الجزائرية (2024) إلى أن حوالي 40% من قضايا الجرائم الإلكترونية تُرفض بسبب ضعف الأدلة أو عدم قبولها قضائيًّا، وهو مؤشر يعكس ضعف النظام الإثباتي في التعامل مع هذا النوع من الجرائم[1].

ـــ التحديات المتعلقة بالتنفيذ والتنسيق بين الجهات المختصة

رغم توفر بعض النصوص القانونية المنظِّمة للجريمة الإلكترونية، فإن التحدي الحقيقي يكمن في التنفيذ العملي، خصوصًا فيما يتعلق بالتعاون والتنسيق بين الجهات المختلفة مثل المحاكم والنيابات العامة وأجهزة الشرطة والدرك الوطني والخبراء الرقميين والوزارات المعنية. وتشير دراسة المركز الوطني للأمن المعلوماتي *(CNSI)*عام 2025 إلى أن التنسيق بين الجهات المختصة ضعيف، وهو ما يؤدي إلى تأخير الإجراءات وفقدان الأدلة في كثير من الحالات، مما يستدعي إنشاء هيئة مركزية متخصصة في الجريمة الإلكترونية تكون مسؤولة عن وضع سياسات وطنية موحدة وإدارة التعاون بين الجهات المعنية .

الفرع الثالث: المقترحات لإصلاح الإطار القانوني الجزائري

1 وزارة الداخلية الجزائرية، دراسة حول فعالية الأدلة الرقمية في القضاء الجزائري ، 2024، ص 37.

أولًا - سن قانون مستقل للجريمة الإلكترونية يغطي جميع أنواع الجرائم الرقمية

من الضروري العمل على سن قانون مستقل خاص بالجريمة الإلكترونية، يكون شاملاً ويضم:

- تعريفات دقيقة للجريمة الإلكترونية بأنواعها كافة.
- عقوبات متناسبة مع خطورة كل نوع من الجرائم.
- إجراءات خاصة بالتحقيق والتحريز وإثبات الجريمة.
- آليات لحماية البيانات الشخصية والحيوية.

ومن خلال هذا القانون المستقل، يمكن توفير إطار قانوني متكامل وواضح، يُسهّل من مهمة القضاء، ويضمن العدالة الرقمية للمجتمع الجزائري .

ثانيًا - تحديث قانون العقوبات ليشمل الجرائم الحديثة

يجب أن يتم تعديل قانون العقوبات الجزائري ليشمل جرائم جديدة لم تكن موجودة وقت صدوره، ومن بينها:الابتزاز الجنسي الإلكتروني، التنمر الإلكتروني ،التجسس الرقمي عبر التطبيقات المشفرة ،استخدام العملات المشفرة في غسيل الأموال ،الهجمات السيبرانية ضد البنية التحتية الحيوية ـويُمكن الاستناد في هذا التعديل إلى تجارب دولية ناجحة، مثل قانون الجرائم الإلكترونيالمصري رقم 5 لسنة 2025، أو تعديلات نظام الجرائم المعلوماتية السعودي لعام 2024، أو حتى اتفاقية بودابست حول الجريمة الإلكترونية.[1]

ثالثًا - إحداث نيابات ومحاكم متخصصة في الجرائم الإلكترونية

من بين أبرز الحلول العملية التي يمكن اعتمادها لتحسين استجابة القضاء الجزائري للجريمة الإلكترونية هي إنشاء نيابات ومحاكم متخصصة في الجرائم الإلكترونية، تكون مزودة بـ:
قضاة مدربين على التعامل مع الأدلة الرقمي،،خبراء في مجال الأمن السيبراني والأدلة الرقمية،أنظمة قضائية إلكترونية تتيح التحقيق والمحاكمة عن بعد، وقد بدأت دول عربية عدة، مثل الإمارات والسعودية، في تبني هذا النموذج، وهو ما أدى إلى تسريع الإجراءات وتحسين جودة الأحكام.[2]

رابعًا - تدريب الكوادر القضائية والأمنية في مجال الأدلة الرقمية

من الضروري توفير برامج تدريبية مكثفة للقضاة والمحققين وأفراد الشرطة، تتناول:

---

1 بن عمر، يوسف، جرائم الإنترنت: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة البليدة، كلية الحقوق، 2020، ص 120.

2 البنك الدولي، نفس المرجع ، ص 52.

2 وزارة الداخلية الجزائرية، نفس المرجع ، ص 41.

أساسيات الأمن السيبراني ،كيفية جمع وتحليل الأدلة الرقمية ،التعامل مع البيانات المشفرة والتخزين السحابي ،فهم أساليب مجرمي الإنترنت والبرمجيات الخبيثة.

ومن هنا، فإن التدريب المهني المستمر يُعد شرطًا أساسيًّا لرفع كفاءة النظام القضائي الجزائري في مجال مكافحة الجريمة الإلكترونية[2]

خامسًا ـ تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية

بما أن الجريمة الإلكترونية تتميز بطابعها العابر للحدود، فإن التعاون الدولي ضرورة قصوى. ويمكن تعزيز هذا التعاون من خلال:

ـــــ الانضمام إلى اتفاقية بودابست حول الجريمة الإلكترونية.

ـــــ توقيع اتفاقيات ثنائية مع الدول المجاورة (تونس، ليبيا، المغرب).

ـــــ تعزيز التعاون مع اليوروبول والإنتربول في مجال مكافحة الجرائم الإلكترونية.

ـــــ تبادل الخبرات مع الدول التي لديها تشريعات متقدمة في هذا المجال.

وعليه، فإن التعاون الدولي في مجال الجريمة الإلكترونية لا يقتصر على تبادل المعلومات فقط، بل يشمل أيضًا استرجاع الأدلة الرقمية، وملاحقة مجرمي الإنترنت عبر الحدود، وتبادل الخبرات والكوادر المؤهلة.

المطلب الثاني :دور القضاء في التصدي للجريمة الإلكترونية

الفرع الأول: تحليل أحكام قضائية جزائرية حديثة في مجال الجرائم الإلكترونية

أولًا ـ قضية اختراق موقع بنكي – الجزائر(2024)

في عام 2024، تم الحكم على شخصين في قضية اختراق موقع بنكي واستهداف بيانات العملاء، حيث استخدمت المحكمة تقارير خبراء رقميين لتحليل الأدلة، وأكدت على:

ـــــ ضرورة وجود خبير تقني في كل قضية إلكترونية.

ـــــ أهمية توثيق الأدلة الرقمية بدقة.

ـــــ تحديد مدى تورط المتهمين من خلال تحليل سجلات IP وسجلات الدخول [2]

---

1 حسن، أحمد محمد، الأدلة الرقمية في القانون الجزائري ، دار النشر العلمي، القاهرة، الطبعة الأولى، 2022، ص 78.

ثانيًا ـ قضية تشهير إلكتروني – الجزائر(2025)

في قضية تشهير إلكتروني عبر وسائل التواصل الاجتماعي، استندت المحكمة الجزائرية إلى المادة 2 من القانون الجزائري لمكافحة الجرائم الإلكترونية، وأصدرت حكماً بالسجن لمدة سنتين وغرامة 200 ألف دينار، مع التأكيد على:

ـــ التحقق من صحة النشر الإلكتروني.

ـــ التحقق من نية الإساءة أو التشهير [1].

ـــ اعتماد الشهادات الرقمية كأدلّة قانونية

الفرع الثاني:إجراءات القضاء الجزائري و تحدياته

أولا ـ إجراءات القضاء الجزائري في مجال الجرائم الإلكترونية

1.إجراءات جمع الأدلة الرقمية

في الجزائر، ما زالت إجراءات جمع الأدلة الرقمية غير موحدة ، مما يؤدي إلى ضعف في مصداقية هذه الأدلة ، بل وأحياناً إلى رفضها ككل أمام المحكمة .ومن بين أبرزالتغيرات :

أولًا ـ إجراءات القضاء الجزائري في مجال الجرائم الإلكترونية

ـــ إجراءات جمع الأدلة الرقمية

في الجزائر، ما زالت إجراءات جمع الأدلة الرقمية غير موحدة، مما يؤدي إلى ضعف في مصداقية هذه الأدلة، بل وأحيانًا إلى رفضها ككل أمام المحكمة. ومن بين أبرز الثغرات:

عدم وجود إجراءات موحدة لجمع الأدلة الرقمية [1]

- غياب نظام محكم لتوثيق الأدلة من اللحظة الأولى لجمعها
- الاعتماد على إجراءات تقليدية غير مناسبة للجريمة الإلكترونية [1]

وهذا الواقع يُعرقل فعالية التحقيقات ويُضعف من قدرة النظام القضائي على مواجهة الجرائم الإلكترونية الحديثة

---

1 بوعلام، أحمد، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية ، رسالة دكتوراه جامعة باتنة، كلية الحقوق، 1202، ص 115.

1 حسن، أحمد محمد، الأدلة الرقمية في القانون الجزائري ، دار النشر العلمي، القاهرة، الطبعة الأولى، 2022، ص 78.

2 بوعلام، أحمد، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية ، رسالة دكتوراه ، جامعة باتنة، كلية الحقوق، 2021، ص 115.

3 زبيري، محمد، دراسة قانونية للجريمة الإلكترونية في الجزائر ، رسالة ماجستير ، جامعة قسنطينة، كلية الحقوق، 2020، ص 125.

4 عطية، محمود حسن، الأمن السيبراني في الدول العربية: تحديات وحلول ، دار النشر العلمي، بيروت، الطبعة الثانية، 2023، ص 165.

2ـــ دور الخبرة الرقمية في التحقيق

أصبح واضحًا أن الخبرة الرقمية ضرورية في كل قضية إلكترونية، إذ إن القضاة والمحققين غالبًا ما يكونون غير قادرين على فهم الأدلة الرقمية أو تحليلها بدون مساعدة خبير. ومن ثم، فإن المحاكم الجزائرية بدأت تلجأ إلى الخبرة الرقمية بشكل متزايد، لكن ما زال هناك نقص كبير في عدد الخبراء المؤهلين، وغياب تدريب مهني لهم [2]

ـــــالصعوبات المتعلقة بجمع الأدلة المشفرة أو المخزنة في السحابة

في كثير من القضايا، تكون الأدلة الرقمية:

ـــــ مشفرة أو مخزنة في البيئة السحابية(*Cloud Storage*) [3]

ـــــ قابلة للتغيير أو الحذف بسهولة[4]

ـــــ موجودة في خوادم خارج حدود الدولة الجزائرية .

ومن ثم، فإن التحقيق في الجرائم الإلكترونية يتطلب آليات خاصة، منها:

ـــــ التعاون مع الشركات العالمية .

ـــــ وجود خبراء في مجال فك التشفير واسترجاع البيانات .

ـــــ بناء بنية تحتية رقمية داخلية قوية .

ولا يمكن تحقيق هذا دون تعاون مؤسسي وتشريعي مكثف بين الجهات المعنية.

ثانيًا ـ التحديات التي تواجه القضاء الجزائري في مجال الجرائم الإلكترونية

ـــ نقص الخبرة التقنية لدى القضاة والمحققين

رغم الجهود التي تبذلها وزارة العدل الجزائرية، إلا أن الكوادر المؤهلة في مجال الحوسبة الجنائية ما زالت نادرة، مما يجعل من الصعب على الجهات القضائية التعامل مع الجرائم الإلكترونية بطريقة فعَّالة.

وتشير دراسة نادي القضاء المصري (2024) إلى أن حوالي 40% من قضايا الاختراق الإلكتروني تُرفض بسبب ضعف الأدلة أو عدم كفايتها"، وهو ما ينطبق على الواقع الجزائري أيضًا، نظرًا لتشابه التحديات بين البلدين .

ـــ غياب محاكم متخصصة في الجرائم الإلكترونية

في الجزائر، ما زالت الجرائم الإلكترونية تُحاكم في المحاكم العادية، رغم أن طبيعة هذه الجرائم تتطلب:

ـــــ قضاة مدربين على استخدام الأدلة الرقمية

ـــــ إجراءات تحقيق خاصة

ـــــ خبراء متخصصين في الأمن السيبراني والأدلة الرقمية

ومن ثم، فإن الحاجة إلى محاكم متخصصة في الجرائم الإلكترونية أصبحت ضرورةقصوى [1]

ـــ صعوبة إثبات الجريمة الإلكترونية

إن الجريمة الإلكترونية تُثبت غالباً بالأدلة الرقمية ، وهي تختلف عن الأدلة التقليدية في عدة جوانب:

ـــــ الطابع غير الملموس :فالدليل الرقمي ليس مادياً، بل هو مجموعة بيانات تخزن على أجهزة أو في السحابة.

ـــــ القابلية للتغيير أو الحذف السهل :يمكن حذف الأدلة أو تعديلها أو تشفيرها قبل أن تتمكن الجهات المختصة من الوصول إليها.

ـــــ الاعتماد على الخبرة التقنية :يتطلب فهم الأدلة الرقمية وجود خبراء في علم الحاسوب والأمن السيبراني.

ومن هنا، تظهر الحاجة إلى وضع معايير موحدة لقبول الأدلة الرقمية في المحاكم الجزائرية

الفرع الثالث : التوصيات لتطوير دورالقضاء الجزائري في مجال الجرائم الإلكترونية

أولا - إنشاء محاكم متخصصة في الجرائم الإلكترونية:من الضروري العمل على إنشاء محاكم متخصصة في الجرائم الإلكترونية ، تكون مزودة بفريق من القضاة والخبراء المهرة، ومسنودة بتشريعات واضح .

1 عبد الحق، علي، التجربة الإماراتية في مكافحة الجرائم الإلكترونية: دراسة مقارنة ، رسالة دكتوراه جامعة الإمارات، كلية الحقوق، 2022، ص 94.

ثانيا ـ تدريب القضاة على التعامل مع الأدلة الرقمية

يحتاج القضاة إلى تدريبات متخصصة في مجال الأمن السيبراني والأدلة الرقمية ، حتى يكونوا قادرين على فهم طبيعة الجريمة وتحليل الأدلة بدقة .

ثالثا ـ وضع معايير موحدة لجمع وتحليل الأدلة الرقمية

من الضروري العمل على وضع معايير قانونية وتقنية موحدة لجمع وتحليل الأدلة الرقمية في الجرائم الإلكترونية، نظراً لطبيعة هذه الأدلة المميزة التي تختلف عن الأدلة التقليدية من حيث الشكل والمصدر والقابلية للتغيير. ويعتبر هذا الأمر ضرورة ملحّة أمام القضاء الجزائري، خصوصاً بعد تسجيل عدد كبير من القضايا التي تم رفضها بسبب ضعف الأدلة أو عدم كفايتها ، وهو مؤشر يُظهر وجود ثغرات في الإجراءات الحالية.

ـــــ **تحديد كيفية جمع الأدلة من الأجهزة المختلفة**: إن الأدلة الرقمية قد تكون مخزنة في أجهزة متعددة ومختلفة ، مثل الحواسيب الشخصية، والهواتف الذكية، والأجهزة اللوحية، وحتى في البيئة السحابية . (Cloud Storage) ومن ثم، فإن من الضروري أن تتضمن المعايير الموحدة آليات دقيقة لجمع الأدلة من كل نوع من هذه الأجهزة، مع مراعاة الخصائص التقنية لكل منها، بما في ذلك:

ـــــ الإجراءات المناسبة لفصل الجهاز عن الإنترنت فوراً عند جمع الأدلة .

ـــــ كيفية استخراج البيانات دون تعديلها أو إتلافها .

ـــــ التعامل مع الأدلة المخزنة في السحابة الإلكترونية بطريقة قانونية وآمنة .

ويجب أن تُوضع هذه المعايير ضمن دليل إجرائي رسمي يُوزَّع على جميع الجهات القضائية والشرطية المعنية، ليكون مرجعاً واحداً يحتكم إليه الجميع في مجال التعامل مع الأدلة الرقمي

ـــــ **حفظ الأدلة الرقمية وتوثيقها بدقة:** لا يقل أهمية حفظ الأدلة الرقمية وتوثيقها بدقة عن عملية جمعها، بل قد يكون أكثر أهمية، إذ أن أي خطأ في تخزين الأدلة أو فقدان سلسلة الحفظ (Chain of Custody) قد يؤدي إلى رفض الأدلة أمام المحكمة ، أو حتى استخدامها ضد المتهم بطريقة غير عادلة .ولذلك، يجب أن تشمل المعايير الموحّدة مجموعة من الإجراءات الخاصة بالحفاظ على سلامة الأدلة، مثل:

ـــــ إنشاء نسخ احتياطية (Imaging) للأقراص الصلبة أو الذاكرة الداخلية دون تعديلها .

ـــــ التأكد من سلامة البيانات عبر استخدام أدوات تجزئية. (Hashing Tools)

ـــــ توثيق كل خطوة تُتخذ في مجال جمع ونقل وتحليل الأدلة [1].

وهذا النوع من الإجراءات لا يزال غير معمول به بشكل كافٍ في الجزائر ، مما يُضعف من مصداقية الأدلة ويُعيق العدالة الرقمية.

ـــ **تقديم الأدلة أمام المحكمة وشرحها للقاضي :**إن مجرد جمع وحفظ الأدلة الرقمية لا يكفي لتحقيق العدالة، بل يجب أن يتم تقديمها أمام المحكمة بطريقة واضحة وشفافة ، بحيث يفهم القاضي طبيعتها وكيفية جمعها وتحليلها. وهذا يتطلب:

ـــ ـوجود خبير تقني يُقدّم شرحاً علمياً للأدلة الرقمية ،اعتماد معايير تتيح للقاضي الحكم على مصداقية الأدلة وصلاحيتها ،تدريب القضاة على فهم المصطلحات الأساسية المتعلقة بالأدلة الرقمية ومن هنا، تظهر الحاجة إلى بناء نظام قضائي رقمي متكامل ، يضم كوادر مؤهلة ومتخصصة يمكنها التعامل مع الجريمة الإلكترونية بكل فعالية.

ـــ **بناء مراكز متخصصة في جمع وتحليل الأدلة الرقمية :**لا يمكن الحديث عن مواجهة فعَّالة للجريمة الإلكترونية دون توفير البنية التحتية اللازمة لدعم هذه الجهود. ومن هنا، برزت الحاجة إلى إنشاء مراكز متخصصة في جمع وتحليل الأدلة الرقمية، تكون مزودة بأحدث الوسائل التقنية، وتضم فرقًا من الخبراء المؤهلين القادرين على التعامل مع الجرائم الإلكترونية المعقدة .

أهمية الأجهزة المتقدمة لفك التشفير واسترجاع البيانات :بما أن الجريمة الإلكترونية غالبًا ما تعتمد على التشفير أو التمويه الرقمي، فإن هذه المراكز يجب أن تكون مزوَّدة بأدوات متقدمة لفك التشفير واسترجاع البيانات المحذوفة أو المشفرة. ومن بين هذه الأدوات:

أدوات فك التشفير العالي [1]،أنظمة استرجاع البيانات من الأجهزة التالفة أو المحذوف منها المعلومات ، برامج تحليل الشبكات وتحديد مصدر الهجوم الإلكتروني .

ومن دون توفر هذه الأدوات، ستظل الجهود المحلية محدودة في مواجهة مجرمي الإنترنت ذوي المهارات العالية [2].

تأهيل خبراء في مجال الحوسبة الجنائية : لا تقل أهمية الكوادر البشرية المؤهلة عن الأدوات التقنية المستخدمة في مكافحة الجريمة الإلكترونية، إذ إن الخبراء هم من يقرؤون البيانات ويحللونها ويقدمونها أمام القضاء. ومن ثم، يجب أن تُخصص هذه المراكز لتأهيل خبراء في مجالات متعددة، مثل:

---

1 *وزارة العدل الجزائرية، مرجع سابق، ص 27.*

1.البنك الدولي، دراسة حول تحديث التشريعات العربية في مجال الجريمة الإلكترونية ، 2023، ص 50.

2 المركز الوطني للأمن المعلوماتي (CNSI) ، تقرير حول التحديات المؤسسية في مكافحة الجريمة الإلكترونية ، 2025، ص 25

تحليل البرمجيات الخبيثة *(Malware Analysis)*، استرجاع البيانات المحذوفة أو المشفرة *(Data Recovery & Forensics)*، فحص الشبكات وتحديد مصادر الهجمات السيبرانية

وهذا التأهيل لا يقتصر فقط على الجانب التقني، بل يجب أن يشمل أيضًا الفهم العميق للجوانب القانونية المتعلقة بإثبات الجريمة الإلكترونية.

الاعتماد على أنظمة تحليل البيانات الرقمية :لا يكفي أن تُجمع الأدلة الرقمية وتُحلَّل فنياً، بل يجب أن تُربط بالجريمة وبالمتهمين بطريقة دقيقة، وهو ما يستدعي الاعتماد على أنظمة رقمية متقدمة تقوم بتحليل السجلات، وربطها بالوقائع، وتقديم نتائج قابلة للاستخدام في الإثبات القضائي. ومن بين هذه الأنظمة:نظم تحليل السجلات *(Log Analysis Systems)*، برمجيات تتبع الهوية الرقمية للمستخدمين، منصات تحليل البيانات الضخمة *(Big Data Analytics)* في الجرائم المنظمة.

ومن هنا، تظهر الحاجة إلى استثمار الدولة في بناء هذه البنية التحتية الرقمية المتقدمة، لتواكب الدول الأخرى في مجال مكافحة الجريمة الإلكترونية .

المطلب الثالث: الصعوبات القانونية في إثبات الجريمة الإلكترونية

تُعدّ الجريمة الإلكترونية من بين أكثر أنواع الجرائم تعقيدًا من حيث طبيعة أدواتها وآليات تنفيذها، وهو ما ينعكس مباشرةً على عملية إثباتها أمام القضاء .فعلى عكس الجرائم التقليدية التي تُثبت غالبًا عبر أدلة ملموسة أو شهادات مباشرة، فإن الأدلة في الجريمة الإلكترونية تكون رقمية وغير ملموسة ، مما يجعل من الصعب على القضاء التعامل معها بنفس المعايير والإجراءات المستخدمة في الجرائم العادية.

ولهذا فإن دراسة الصعوبات القانونية في إثبات الجريمة الإلكترونية تمثل ركيزة أساسية لفهم مدى فعالية النظام القضائي في مواجهة هذه الجرائم، كما أنها تساعد على تحديد مواطن الضعف في التشريعات السائدة، وتوجيه التوصيات اللازمة لإصلاحها. وفي هذا المطلب، سنقوم باستعراض أهم الصعوبات القانونية التي تواجه إثبات الجريمة الإلكترونية ، مع الإشارة إلى أسبابها وآثارها، وذلك بناءً على أدبيات قانونية وأمنية متخصصة

الفرع الأول: طبيعة الأدلة الرقمية وصعوبتها

أولًا - الأدلة الرقمية ليست ملموسة

على عكس الأدلة التقليدية كالشهود أو الأثر ألبصمي، فإن الأدلة الرقمية غالبًا ما تكون غير ملموسة وغير مباشرة، مما يجعل من مهمة إثبات الجريمة أكثر تعقيدًا. فمثلاً، يمكن أن تُستخدم أدلة مثل:سجلات الدخول *(Log Files)* ،عناوينIP ،رسائل البريد الإلكتروني أو الدردشات المشفرة ،البيانات المسجلة على السحابة الإلكترونية.

وهذه الأدلة لا يمكن رؤيتها أو لمسها، بل تحتاج إلى تحليل تقني دقيق حتى يمكن استخدامها في إثبات الجريمة.

ثانيًا ـ الأدلة الرقمية قابلة للتعديل أو الحذف السهل

من أخطر خصائص الأدلة الرقمية أنها قابلة للتعديل أو الحذف أو التدمير بسهولة كبيرة، وقد يحدث ذلك قبل أن تتمكن الجهات المختصة من الوصول إليها، مما يؤدي إلى فقدان الأدلة الأساسية، أو استخدامها بشكل غير دقيق، وهو ما يُعقّد من مهمة إثبات الجريمة.

وتشير دراسة نادي القضاء المصري (2024) إلى أن:

"حوالي 40% من قضايا الاختراق الإلكتروني التي تم النظر فيها خلال عام 2023 تمت إعادتها أو رفضها بسبب ضعف الأدلة أو عدم كفايتها" .

ويعزو التقرير هذا النسبة الكبيرة إلى:

ـــــ تأخر الجهات المختصة في استرجاع البيانات بعد وقوع الجريمة

ـــــ اعتماد بعض المؤسسات على أنظمة تخزين ضعيفة الأمان

ـــــ نقص الخبرة التقنية لدى المحققين والخبراء

الفرع الثاني: التحديات المتعلقة بالبيانات المشفرة والتخزين السحابي

أولًا ـ انتشار التشفير العالي المستوى

أصبحت تقنيات التشفير مثل التشفير التام *(End-to-End Encryption)*وتطبيقات مثل Signalو Telegramفي وضع المحادثات السرية، وخدمات التخزين السحابي المشفرة مثلTresoritوSync.com، أدوات رئيسية يستخدمها مجرمو الإنترنت لإخفاء الأدلة أو جعلها غير قابلة للاسترجاع[1] .

ثانيًا ـ التحديات القانونية أمام استرجاع البيانات المشفرة

1 الاتحاد الدولي للأمن السيبراني (ICSA Labs) ، تقرير حول استخدام التشفير في الجرائم الإلكترونية ، 2023، https://www.icsalabs.com

ـــ غياب قوانين واضحة لفك التشفير

تشهد العديد من الدول العربية، ومنها الجزائر، نقصًا في التشريعات التي تنظم عملية فك التشفير، مما يُعيق استرجاع الأدلة الرقمية .[2]

2 صعوبة التعامل مع الشركات العالمية

تعاني الجهات القضائية في الجزائر من صعوبات كبيرة في الحصول على بيانات مخزنة لدى شركات عالمية كبرى مثل Google و Microsoftو Apple، بسبب:

ـــ تعقيد جمع الأدلة من الخوادم الأجنبية وعدم استجابة هذه الشركات للطلبات بدون آليات قانونية واضحة.

ـــ تعارض القوانين الدولية الخاصة بالخصوصية مثل GDPR مع طلبات الاسترجاع، مما يؤدي إلى تعطيل سير العدالة

ـــ انعكاسات الخلافات السياسية على التعاون التقني، حيث قد ترفض الشركات التعاون تحت ذريعة الحياد السياسي .

ـــ غياب الاتفاقيات الثنائية أو متعددة الأطراف بين الجزائر وهذه الشركات أو الدول التي تقع ضمن اختصاصها، وهو ما يُظهر الحاجة الملحة إلى توقيع مذكرات تفاهم رسمية [1]

3ـــ غياب البنية التحتية الرقمية المناسبة

ما تواجه الجزائر ضعفًا في البنية التحتية الرقمية اللازمة لجمع وتحليل الأدلة الإلكترونية، ويتجلى ذلك في:

ـــ *نقص المراكز المتخصصة في الحوسبة الجنائية (Digital Forensics)، مما يُبطئ من إجراءات الفحص والتحليل.*[2]

ـــ قلة الأجهزة المتقدمة لفك التشفير واسترجاع البيانات، وهي ضرورية لمواجهة الجرائم المعقدة مثل Malware وDeepfake .

ـــ ندرة الكوادر المؤهلة في مجال الحوسبة الجنائية، حيث لا تزال الخبرات محدودة وغير مرتبطة مباشرة بالمؤسسة القضائية[3]

2وزارة الداخلية الجزائرية، المصدر نفسه ، 2023.

ـــ بناء بيئة قانونية وتقنية متكاملة

لكسب معركة الجريمة الإلكترونية، يجب على الدولة الجزائرية:
ـــ تحديث التشريعات المحلية لتتضمن تعريفات دقيقة للجرائم الإلكترونية وإجراءات جمع الأدلة الرقمية[1]، توفير الدعم المادي والبشري للمؤسسة القضائية عبر إنشاء مختبرات رقمية وأجهزة متقدمة وتدريب القضاة والمحققين ،تعزيز الشراكات بين القطاعات الحكومية والخاصة لبناء استراتيجية شاملة لمكافحة الجرائم الإلكترونية .

الفرع الثالث: الصعوبات المتعلقة بالتخزين السحابي والحدود الرقمية

أولًا ـ التخزين السحابي: بيئة غير ماديةأصبح التخزين السحابي *(Cloud Storage)*هو الطريقة الرئيسية لتخزين البيانات اليوم، لكنه يطرح تحديات قانونية جديدة، منها:مكان تخزين البيانات غير واضح، فقد تكون في خوادم تقع في دولة مختلفة عن موقع الجريمة أو الضحية ، التحكم في البيانات ليس فقط بيدها وإنما أيضًا بيد الشركة المالكة للسحابة ، إمكانية حذف البيانات أو نقلها بسهولةومن ثم، فإن جمع الأدلة من البيئة السحابية يتطلب آليات خاصة، منهاالتعاون مع الشركات المقدمة للخدمة ،وجود قوانين محلية تُلزم هذه الشركات بتقديم البيانات عند الضرورة ،الاعتماد على الخبرات التقنية في استرجاع البيانات المفقودة أو المعدلة

ثانيًا ـ الجريمة الإلكترونية لا تعرف الحدود السياسية

إن الجريمة الإلكترونية لا تقتصر على دولة واحدة، بل قد تبدأ في دولة، وتُنفذ من دولة أخرى، وتؤثر على دولة ثالثة، وهو ما يجعل من مهمة تحديد الاختصاص القضائي أمرًا معقدًا للغايةومن بين أبرز التحديات:اختلاف التشريعات بين الدول حول الجريمة الإلكترونيةغياب آليات قانونية موحدة لتبادل المعلومات والأدلة الرقمية بين الدول ،الحاجة إلى اتفاقيات دولية لتسهيل استرجاع الأدلة عبر الحدود

رابعا ـ غياب الخبرة التقنية لدى الجهات القضائية والتحقيقية

1 الإنتربول، تقرير حول التعاون الدولي في مكافحة الجرائم الإلكترونية ، 2024، https://www.interpol.int
2 اليوروبول، تحديات التحقيق في الجرائم الإلكترونية عبر الحدود ، 2023، https://www.europol.europa.eu
3 لبنك الدولي، المصدر نفسه ، ص 67.
1 الإنتربول، المرجع السابق ، 2024.

تعد غياب الخبرة التقنية لدى القضاة والمحققين من أبرز الصعوبات التي تواجه المؤسسة القضائية الجزائرية في التعامل مع الجرائم الإلكترونية، نظراً لاختلاف طبيعة هذه الجرائم وأدلة إثباتها عن الجرائم التقليدية

ـ **نقص الكوادر المؤهلة في مجال الحوسبة الجنائية :**ما زالت الجزائر تعاني من ندرة واضحة في خبراء الحوسبة الجنائية (Digital Forensics Experts) القادرين على جمع وتحليل الأدلة الرقمية بدقة، وهو ما يُضعف استجابة القضاء للجرائم المعقدة ويؤثر سلباً على فعالية المحاكمات ,

ـ **غياب التدريب الكافي للقضاة والمحققين :**لا يقتصر النقص على الخبراء فقط، بل يمتد إلى غياب التدريب اللازم للقضاة والمحققين والمدعين العامين حول طبيعة الجريمة الإلكترونية والأدلة المرتبطة بها، مما يؤدي أحياناً إلى رفض الأدلة أو تفسيرها بشكل خاط

ـ **انعدام المناهج الدراسية المتخصصة :**إن غياب مواد متخصصة في الجرائم الإلكترونية والأدلة الرقمية من المناهج الدراسية لكليات الحقوق، هو أحد الأسباب الجوهرية لنقص الكوادر، مما يجعل الخريجين غير مؤهلين للتعامل مع هذا النوع من الجرائم.

ـــ **صعوبة فهم وتحليل الأدلة الرقمية :**تتميز الأدلة الرقمية بتعقيدها واعتمادها على تقنيات متقدمة، مما يجعل من الصعب على القضاة والمحققين غير المختصين فهمها أو تحليلها بدقة، وبالتالي فإن اعتمادهم على تقارير الخبرة دون تمحيص يُهدد بتحقيق عدالة رقمية حقيق

ـــ **ضرورة الاعتماد على الخبراء الرقميين :**أمام هذه الصعوبات، يجب على القضاء الجزائري الاعتماد على خبراء رقميين مؤهلين في كل قضية إلكترونية ، بحيث يكون لهم دور أساسي فيجمع الأدلة الرقمية بطريقة قانونية،تحليل البيانات وربطها بالجريمة،تقديم شرح مهني واضح للمحكمة ،وهذا الاعتماد لا يُقلل من دور القاضي، بل يُكمله ويعززه، بما يضمن تحقيق العدالة الرقمية وصحة الأحكام.

خامساً ـ الثغرات التنظيمية والإجرائية في جمع الأدلة الرقمية

ـ غياب معايير موحدة لجمع الأدلة الرقمية

في كثير من الدول، بما فيها الجزائر، ما زالت إجراءات جمع الأدلة الرقمية غير محددة بدقة ، مما يؤدي إلى ضعف مصداقية هذه الأدلة أمام المحكمة ، بل وأحياناً إلى رفضها ككل .

ومن بين أبرز الثغرات:عدم وجود إجراءات موحدة لجمع الأدلة الرقمية ،غياب نظام محكم لتوثيق الأدلة من اللحظة الأولى لجمعها ،الاعتماد على إجراءات تقليدية غير مناسبة للجريمة الإلكترونية .[1]

ـــ **ضعف الإجراءات الوقائية لحفظ الأدلة :**في كثير من الحالات، تُفقد الأدلة الرقمية بسبب سوء التخزين أو التعامل غير المهني مع الجهاز المُستخدم في الجريمة .ومن بين أبرز الأخطاء الشائعة :تشغيل الجهاز أو توصيله بشبكة الإنترنت أثناء جمع الأدلة ، نقل البيانات

دون اتخاذ إجراءات الحفاظ على سلامتها ،عدم وجود خبير رقمي في موقع الحدث لجمع الأدلة بطريقة علمية .

ومن ثم، فإن التعامل مع الأدلة الرقمية يتطلب إجراءات خاصة ، منها:فصل الجهاز عن الإنترنت فوراً ، إنشاء نسخة احتياطية (Imaging) للأقراص الصلب ،الحفاظ على سلسلة الحفظ.(Chain of Custody) .

سادسًا: التحديات المتعلقة باستخدام التقنيات الحديثة في إثبات الجريمة

استخدام الذكاء الاصطناعي في إنتاج الأدلة الزائفة *(Deepfake)* : مع تطور تقنيات الذكاء الاصطناعي، أصبح بالإمكان إنتاج فيديوهات أو تسجيلات صوتية أو صور زائفة *(Deepfake)*، تُستخدم في التشهير أو الابتزاز أو حتى إدانة أشخاص بجرائم لم يرتكبوها.

ومن ثم، فإن المحكمة تواجه صعوبة في التفريق بين الأدلة الحقيقية والزائفة، مما يستدعي:اعتماد خبراء في تحليل الوسائط الرقمية[2]،تطوير تشريعات تجرّم إنتاج المحتوى الزائف وتصنيفه كجريمة مستقلة ،بناء مختبرات متخصصة في تحليل الوسائط الرقمية .

رغم أن تقنية *البلوك تشين* تُعد من الوسائل الموثوقة في تسجيل العمليات الرقمية، إلا أنها تُستخدم أيضًا لإخفاء الأدلة أو تنفيذ الجرائم بشكل غير قابل للتعقب، كما هو الحال في:جرائم غسيل الأموال عبر العملات الرقميةالهجمات المنظمة التي تستخدم البلوك تشين لتوزيع المهام بين مجرمين مجهولي الهوية الجرائم التي تستهدف إحداث تغييرات غير ممكن تتبعها في السجلات التقليدية[2]

ومن ثم، فإن القضاء الجزائري يحتاج إلى فهم أعمق لهذه التقنيات، وكذلك إلى وضع إجراءات قانونية تتيح استخدامها كأداة إثبات، دون أن تُستخدم كأداة لإخفاء الأدلة .

المبحث الثاني: الاتفاقيات الدولية والإقليمية

يستعرضهذاالمبحثالجهودالقانونيةالدوليةوالإقليميةالمبذولةلمكافحةالجريمةالإلكترونية،منخلالتحليلالاتفاقيات،وأطرالتعاون،ومدىفعاليتها.

المطلب الأول: اتفاقية بودابست حول الجريمة الإلكترونية

1 حسن، أحمد محمد، الأدلة الرقمية في القانون الجزائري ، دار النشر العلمي، القاهرة، الطبعة الأولى، 2022، ص 135

2بوعلام، أحمد، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية ، رسالة دكتوراه ، جامعة باتنة، كلية الحقوق، 2021، ص 167.

يُفصّلهذاالمطلبمضمونالاتفاقيةوأهدافها،معتقييمانضماماالدولالعربيةوالإفريقية،ونجاعتهافيمكافحةالجريمةالسيبرانيةعالميًا.

الفرع الأول – اتفاقية بودابست

أولا: نشأة اتفاقية بودابست وأهدافها

1 - نشأة اتفاقية بودابست جاءت اتفاقية بودابست حول الجريمة الإلكترونية نتيجة لضرورة ملحة على المستوى الدولي للتصدي للجرائم الإلكترونية عبر تعاون قانوني وتشريعي فعّال .وقد تم إعداد هذه الاتفاقية تحت رعاية منظمة الأمن والتعاون في أوروبا (OSCE) ، وبالتعاون مع مجلس أوروبا (*Council of Europe*)ومنظمة الإنتربول *INTERPOL*) (، وتم التوقيع عليها رسميًّا في مدينة بودابست بتاريخ 23 نوفمبر 2001 ، ودخلت حيز التنفيذ في 1يوليو 2004 [1].

تُعد هذه الاتفاقية الأولى من نوعها على المستوى الدولي ، حيث سعت إلى وضع إطار قانوني شامل يوحد التعريفات القانونية للجرائم الإلكترونية، ويُعزز التعاون الدولي بين الدول في مجال التحقيق والمحاكمة، كما عملت على تطوير آليات جمع الأدلة الرقمية بطريقة قانونية وفعالة [2].

2- أهداف الاتفاقية : تسعى اتفاقية بودابست إلى تحقيق مجموعة من الأهداف الاستراتيجية التي تساهم في مواجهة الجرائم الإلكترونية على الصعيد الدولي، ومن أبرز هذه الأهداف:

توحيد التعريفات القانونية للجرائم الإلكترونية:حيث حددت الاتفاقية تعريفات دقيقة لمفاهيم مثل القرصنة *(Hacking)*، الدخول غير المصرح به إلى الأنظمة المعلوماتية، ونشر البرمجيات الضارة *(Malware)*، مما يسهل التعاون الدولي وتبادل المعلومات بين الدول [3]

تحديث التشريعاتالوطنية:دعت الاتفاقية الدول إلى مراجعة وتعديل تشريعاتها الداخلية لتتماشى مع طبيعة الجرائم الإلكترونية الحديثة، وتضمين عقوبات رادعة لهذه الجرائم، وإنشاء إجراءات خاصة بالتحقيق الإلكتروني [1]

تعزيز التعاون الدولي بين الدول:بسبب الطبيعة العابرة للحدود لهذه الجرائم، توفر الاتفاقية آلية واضحة لتبادل الأدلة والمعلومات، ودعم الجهات المختصة في الدول المختلفة، مع تشجيع إنشاء نقاط اتصال دائمة لتسهيل التواصل السريع [2].

1.مجلس أوروبا، اتفاقية بودابست حول الجريمة الإلكترونية – النص الكامل ، 2001، https://www.coe.int

2.الأمم المتحدة، الجريمة الإلكترونية: دراسة شاملة للاتفاقيات الدولية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة
(UNODC) ، 2022،
https://www.unodc.org

3.البنك الدولي، دراسة حول تحديث التشريعات العربية في مجال الجريمة الإلكترونية ، 2023، ص 60.

وضع إجراءات خاصة لجمع ونقل الأدلة الرقمية:نظرًا لصعوبة جمع الأدلة الرقمية عبر الحدود، وضعت الاتفاقية إجراءات موحدة لاسترجاع البيانات من الخوادم الأجنبية، وتوثيقها، وتقديمها أمام القضاء بطريقة آمنة وموثوقة[3].

حماية حقوق الإنسان أثناء تطبيق الإجراءات:رغم تركيزها على مكافحة الجريمة، أكدت الاتفاقية على ضرورة احترام الحقوق والحريات الأساسية، مثل الحق في الخصوصية، وضرورة وجود إذن قضائي قبل الوصول إلى البيانات، وضمان حق الدفاع في القضايا الإلكترونية [4].

3- أهمية الاتفاقية وتأثيرها على التشريعات الوطنية : لعبت اتفاقية بودابست دورًا محوريًّا في تحديث التشريعات الوطنية للعديد من الدول، خاصة في مجال مكافحة الجرائم الإلكترونية، حيث اعتمدت دول عربية وأفريقية وأسيوية أحكام الاتفاقية كأساس لسن قوانين وطنية، كما هو الحال في مصر (القانون رقم 175 لسنة 2018)، والسعودية (نظام الجرائم المعلوماتية)، والأردن والإمارات التي تبنت إجراءات قضائية وتقنية مستوحاة من الاتفاقية[2] .

كما ساهمت الاتفاقية في تعزيز التعاون الدولي عبر وضع آليات موحدة لتبادل المعلومات والتحقيقات بين الدول الأعضاء، وهو ما ساعد في حل العديد من القضايا المعقدة ذات الطبيعة العابرة للحدود. بالإضافة إلى ذلك، شكلت الاتفاقية إطارًا لبناء الخبرات القانونية والتقنية عبر برامج تدريبية مشتركة مع منظمات دولية مثل الإنتربول *(INTERPOL)* وبرنامج الأمم المتحدة الإنمائي *(UNDP)*[2].
ورغم هذه الفوائد، تواجه الاتفاقية عددًا من التحديات، منها عدم شموليتها لجميع الدول ، مما يحد من نطاق تطبيقها العالمي، فضلًا عن الانتقادات المتعلقة بالسيادة الوطنية ، خصوصًا فيما يخص جمع الأدلة الرقمية عبر الحدود دون إذن محلي. كما يُعد غياب الآليات التنفيذية

1. مجلس أوروبا، المرجع السابق ، 2001.
2 اليوروبول، دليل التعاون الدولي في الجرائم الإلكترونية ، 2022، https://www.europol.europa.eu
3 ENISA.، الإجراءات الخاصة بالأدلة الرقمية في التعاون الدولي ، 2021، https://www.enisa.europa.eu
4 UNODC، المرجع السابق ، 2022

1 عبد الله، محمد أحمد، الجرائم الإلكترونية في القانون المصري: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة القاهرة، كلية الحقوق، 2021، ص 102.
2 اليوروبول، التعاون الدولي في مجال الجرائم الإلكترونية ، تقرير سنوي، 2023.
3 الأمم المتحدة، تحديات اتفاقية بودابست في القرن الحادي والعشرين ، تقرير رسمي، 2024.

الواضحة من أبرز عيوب الاتفاقية، إلى جانب عدم مواكبتها للتطورات التكنولوجية السريعة ، مما يستدعي اليوم ضرورة مراجعتها أو وضع أدوات إضافية لتغطية الجرائم الحديثة [3].

الفرع الثاني: البنية القانونية للاتفاقية والدول المنظِّمة لها

أولا : البنية القانونية للإتفاقية بودابست

تنقسم الاتفاقية إلى أربعة أبواب رئيسية بالإضافة إلى بروتوكول اختياري يتعلق بالجرائم ذات الطابع العنصري أو المعادي للسامية وهي:

الباب الأول: أحكام عامة

يُعد الباب الأول من اتفاقية بودابست حول الجريمة الإلكترونية الإطار التنظيمي الأساسي الذي يحدد المصطلحات والمفاهيم الأساسية المستخدمة في الاتفاقية، ويوضح نطاق تطبيقها وأهدافها. وتسعى هذه الأحكام إلى توفير أساس موحد لفهم الجريمة الإلكترونية بين الدول الأطراف وغير الأطراف، مما يسهل تكييفها قانونيًّا وتطبيقها عمليًّا[1] .

وتنص المادة الأولى من الاتفاقية على أن الغرض منها هو تحقيق تعاون دولي فعال في مجال الوقاية من الجرائم الإلكترونية، وإجراء التحقيقات الجنائية، ومعاقبة مرتكبيها ، وهو ما يجعلها مرجعًا قانونيًّا أساسيًّا للدول الراغبة في تحديث تشريعاتها أو تعزيز استجابتها الدولية لهذه الظاهرة [2].

كما يتضمن هذا الباب تعريفات واضحة للمفاهيم الرئيسية مثل "النظام المعلوماتي، و"البيانات الرقمية، و"الاختراق غير المصرح به"، وغيرها من المصطلحات التي قد تكون غامضة أو متعددة التفسيرات في بعض التشريعات الوطنية. وبذلك، لا يُعد هذا الباب نصًّا إرشاديًّا فقط، بل يُعتبر حجر الأساس الذي تقوم عليه باقي مواد الاتفاقية، ويُسهّل من عملية التطبيق المشترك لها بين الدول المختلفة[3].

الباب الثاني: الجرائم المشمولة بالاتفاقية

خصص هذا الباب لتحديد أربع فئات رئيسية من الجرائم الإلكترونية التي تدخل ضمن نطاق الاتفاقية، وهي: ـــ جرائم ضد سلامة الشبكات المعلوماتية مثل الدخول غير المصرح به، ونشر البرمجيات الخبيثة *(Malware)*وهجمات*DDoS*، وتُعد من الجرائم الإلكترونية المحضة التي تستهدف البنية التحتية الرقمية الحيوية .

ـــ جرائم استخدام الحواسيب في ارتكاب جرائم تقليدية مثل الاحتيال الإلكتروني أو التشهير أو انتحال الشخصية الرقمية، مع دعوة الدول إلى تعديل قوانينها لتغطيتها بعقوبات خاصة.

---

1 مجلس أوروبا، المرجعالسابق ، 2001.

2. ENISA، نفس المرجع السابق ، 2021.

3 مجلس أوروبا، الجرائم الإلكترونية في القانون الأوروبي: تحليل قانوني ، تقرير رسمي، 2022.

ـــ جرائم تتعلق بالمحتوى المحظور كاستغلال الأطفال جنسيًّا عبر الإنترنت أو نشر المحتوى المتطرف والإرهابي، مع وجوب وضع آليات رقابية ودعم للضحايا.

ـــ جرائم مساعدة أومتصلةمثل إنتاج أو توزيع أدوات القرصنة بقصد غير مشروع، والتي تسهل تنفيذ الجرائم الكبرى، وهو ما دفع الاتفاقية إلى تجريم هذه الأفعال ووضع إجراءات رقابية على تداولها .

الباب الثالث :الإجراءات القانونية

حددت الاتفاقية إجراءات خاصة لمكافحة الجرائم الإلكترونية، ومن أبرزها:

ـــ ـالاستيلاء على البيانات الإلكترونية بموجب أمر قضائي ، مع ضمان سلامتها وسرية محتواها.

ـــ مراقبة الاتصالات عن بعد بشروط صارمة ، منها وجود إذن قضائي ومدة محددة وعدم استخدامها إلا في الإجراءات القضائية.

ـــ مصادرة الأجهزة الرقمية بطلب قضائي وتوثيق كامل لضمان عدم فقدان الأدلة.

ـــ تسليم الأدلة الرقمية عبر الحدود ضمن إطار قانوني واضح يشمل التحقق من مشروعية الطلب وسلامة البيانات أثناء النقل[1] .

الباب الرابع : التعاون الدولي

يعد التعاون الدولي المحور الأساسي للاتفاقية، ويتم عبر آليات تسهّل على الدول الأطراف التعاون في مجال التحقيق والمحاكمة، ومنها:

ـــ تسهيل التحقيقات المشتركة بين الدول ، بما في ذلك تقديم الطلبات الرسمية وإرفاق الوثائق والأدلة اللازمة.

ـــ تسليم المتهمين في الجرائم الإلكترونية بشروط قانونية تضمن العدالة وحق الدفاع.

ـــ نقل الأدلة الرقمية عبر الحدود بدقة وتوثيق كامل وفقًا للمعايير الدولية.

ـــ إنشاء نقاط اتصال دائمة(*Contact Points*) في كل دولة طرف لتسريع الإجراءات وتحقيق التواصل الفوري في حالات الطوارئ .

ثانيا : مدى انضمام الدول العربية و الإفريقية لها

1مجلس أوروبا، الجرائم الإلكترونية في القانون الأوروبي: تحليل قانوني ، تقرير رسمي، 2022.

1ـــ الدول المنضمة:

تعد **تونس** 2023 و**المغرب** 2018 الدولتين العربيتين الوحيدتين المنضمتين الكاملتين، حيث استكملا تعديل تشريعاتهما الوطنية لمواءمة متطلبات الاتفاقية، خاصة في مجالات الحفظ السريع للبيانات[1].

تُظهر الدراسة التحليلية أن **موريتانيا** و**لبنان** في مرحلة التوقيع المبدئي 2024 لكنهما لم يصدقا بعد بسبب الخلافات حول المادة 32 الخاصة بالوصول العابرللحدود إلى البيانات[2]

2 ـ موقف الدول غير المنضمة:

ترفض **الجزائر** و**مصر** الانضمام رسمياً بحجة أن الاتفاقية "تُنتهك السيادة الرقمية" وفق التصريحات الرسمية2023، وتفضلان تطوير إطار عربي موحد تحت مظلة جامعة الدول العربية ·

يُعد **القرار بقانون رقم 10 لسنة 2018** الفلسطيني نموذجاً للتشريع البديل المستقل، رغم تأثره غير المباشر ببنود بودابست في تجريم الاختراق .

3ـــ **التشريعات الإفريقية البديلة:**

تبنت **نيجيريا** و**غانا** تشريعات وطنية 2020 ـــ 2022 مستوحاة من بودابست، لكن مع استبعاد البنود المتعلقة بالتعاون المباشر مع الدول غير الإفريقية، وهو ما يعكس توجه "الإقليمية الرقمية" .

يُعد **الاتحاد الإفريقي** 2023 مشروع اتفاقية "مالابو" كبديل إقليمي، يركز على حماية البيانات الشخصية وحق الدول في رفض تبادل الأدلة في القضايا السياسية

المطلب الثاني: التعاون الإقليمي في مكافحة الجرائم الإلكترونية

يركّز هذا المطلب على تجارب التعاون الإقليمي في التصدي للجريمة الإلكترونية، من خلال نماذج متنوعة تعكس خصوصيات كل منطقة.

1 المفوضية الأوروبية، التعاون الإقليمي في مجال الأمن السيبراني ، تقرير رسمي، 2022، https://ec.europa.eu.

الفرع الأول: التعاون الإقليمي في أوروبا وإفريقيا وآسيا

أولًا - التعاون الإقليمي في أوروبا

يُعد الاتحاد الأوروبي من أكثر التكتلات الإقليمية تنظيمًا وفعالية في مجال مكافحة الجرائم الإلكترونية، وهو شريك أساسي في اتفاقية بودابست حول الجريمة الإلكترونية، ويُسهم بشكل مباشر في تطبيقها داخل الدول الأعضاء ، وتتميز منطقة الاتحاد الأوروبي بأنها ذاتية تحتية رقمية متقدمة ،إلى جانب تشريعات شاملة وواضحة في مجال الأمن السيبراني والأدلة الرقمية، مما يجعل من التعاون بين دوله نموذجًا يُحتذى به على المستوى الدولي.

يلعب عدد من الهيئات دورًا محوريًّا في تنسيق الجهود المشتركة بين الدول الأعضاء في مجال الجرائم الإلكترونية، ومن أبرز هذه الهيئات :

اليوروبول(*Europol*) :الهيئة المختصة في تطبيق القانون عبر الحدود،وتتولىالتنسيق بين الشرطة الجنائية وتوفيرالدعم الفني والاستخباراتي في مجال الجرائمالإلكترونيةالمنظمة

الوكالة الأوروبية للأمن السيبراني(*ENISA*)التي تتركز مهمتها على دعم البنيةالتحتية الرقمية وتوفير الاستشارات الفنية والقانونية لتحسين الأمان الرقمي هيئة مستقلة مكلفةبتنسيق التعاون القضائي بين الدول في القضايا الجنائية الكبرى، بما فيها الجرائم الإلكترونيةالخطيرةوقد ساهمت في تسهيل محاكمات مشتركة وتحقيقات عابرة للحدود [1].

أما على مستوى التشريعات، فلدى الاتحاد الأوروبي مجموعة قوانين تتناول الجرائمالإلكترونية من زوايا مختلفة، ومنها :

ـــــ اللائحة العامة لحماية البيانات(*GDPR*) التي تُنظم حماية البيانات الشخصية عبر الإنترنت وتضع جزاءات صارمة على أي استغلال غير مشروع لها.

ـــــ القرار الإطاري رقم 222/2005/قالذي يحدد أنواع الجرائم الإلكترونية وعقوباتها الموحَّدة.

ـــــ الخطة الأوروبية للأمن السيبراني(*EU Cybersecurity Strategy*) التي أُطلقت عام 2013 وأُعيد تحديثها في 2020، بهدف تعزيز البنية التحتية الرقمية وبناء استراتيجيات وطنية ومشتركة لمكافحة الجرائم الإلكترونية [1]

1 المفوضية الأوروبية، التعاون الإقليمي في مجال الأمن السيبراني ، تقرير رسمي، 2022، https://ec.europa.eu

وقد حقق الاتحاد الأوروبي إنجازات كبيرة في مجال التعاون الإقليمي ضد الجرائم الإلكترونية، منها:إنشاء شبكة أوروبية للرد السريع على الهجمات الإلكترونية ،تدريب الكوادر الأمنية والقضائية في الدول الأعضاء ، تعزيز تبادل المعلومات الاستخباراتية بين الدول .

وهو ما ساعد في الكشف عن شبكات الجرائم المنظمة والوقاية منها قبل تنفيذها، مما يُظهر أنالتعاون الإقليمي يمكن أن يكون نموذجًا فعّالًا في مكافحة الجرائم الإلكترونية شريطة وجود إطار قانوني مشترك وآليات تنفيذية واضحة .

ثانيا – التعاون الإقليمي في إفريقيا

بدأ الاتحاد الأفريقي في الاهتمام بموضوع الجرائم الإلكترونية بشكل متزايد خلال السنوات الأخيرة، خاصة مع ارتفاع معدلات الاختراق والاحتيال الإلكتروني في القارة، وهو ما دفع إلى وضع استراتيجيات إفريقية للتعامل مع هذا النوع من الجرائم. ومن أبرز الجهود التي قدمها الاتحاد:

ـــــ إصدار استراتيجية إفريقية للأمن السيبراني عام 2014 لتحديد الأهداف العامة لتطوير بيئة رقمية آمنة.إطلاق مبادرة الاتحاد الأفريقي للتعاون الرقمي (AUDA-NEPAD) ، بهدف بناء بنية تحتية مشتركة ورقابة مشتركة على الجرائم الإلكترونية.

ـــــ دعم انضمام بعض الدول الأفريقية إلى اتفاقية بودابست ، مثل جنوب أفريقيا وساحل العاج وغانا، وهو مؤشر إيجابي على استعداد بعض الدول الإفريقية للانخراط في التعاون الدولي.

ـــــ رغم هذه الجهود، يواجه التعاون الإقليمي في إفريقيا تحديات كبيرة، منها:

ضعف البنية التحتية الرقمية في كثير من الدول، مما يُعيق جمع وتحليل الأدلة الرقمية بدقة ،نقص التمويل لمشاريع الأمن السيبراني، وهو ما يعرقل بناء مراكز متخصصة أو تدريب الكوادر المؤهلة ،غياب تشريعات وطنية شاملة للجرائم الإلكترونية ، مما يجعل من الصعب التعامل مع الجرائم الحديثة أو تنسيق الجهود بين الدول ،قلة الخبرات المؤهلة في مجال الأدلة الرقمية والحوسبة الجنائية [2]، وهو ما يُضعف من القدرة على محاكمة مجرمي الإنترنت بشكل فعّال .وبالتالي، يتضح أن التعاون الإقليمي في إفريقيا لا يزال في بداياته، لكنه يمتلك إمكانات كبيرة للتطور إذا تم دعمه بسياسات واستثمارات مناسبة .

.24البنك الدولي، دراسة حول التعاون الإقليمي في مكافحة الجرائم الإلكترونية ، 2024.

1 عبد الحق، علي، التجربة الإماراتية في مكافحة الجرائم الإلكترونية: دراسة مقارنة ، رسالة دكتوراه ، جامعة الإمارات، كلية الحقوق، 2022.

ثالثا ـ التعاون الإقليمي في آسيا

ـــ منظمة شنغهاي للتعاون(SCO) :تضم منظمة شنغهاي للتعاون (SCO) دولًا كبرى مثل الصين وروسيا والهند وباكستان، وتسعى منذ عام 2001 إلى تعزيز التعاون الأمني بين أعضائها، بما في ذلك في مجال الأمن السيبراني والجرائم الإلكترونية ومن أبرز الجهود الحالية التي تبذلها المنظمة[1]

ـــــ إصدار إعلان شنغهاي حول الأمن السيبراني عام 2011 ، وهو أول نص يحدد المبادئ الأساسية للتعاون في هذا المجال.

ـــــ العمل على إنشاء شبكة إقليمية لمكافحة الجرائم الإلكترونية ، تنسق بين الدول الأعضاء في مجال التحقيق والوقاية.

ـــــ تعزيز التعاون في مجال تدريب الكوادر التقنية ، لرفع مستوى الوعي الرقمي وبناء قدرات محلية في مجال مكافحة الجرائم الإلكترونية .[2]

ـــــ ورغم هذه الجهود، تواجه المنظمة تحديات مهمة، منها

ـــــ رفض بعض الدول الانضمام إلى اتفاقية بودابست لأسباب سياسية ، مما يُعوق التعاون القانوني الدولي في تسليم الأدلة والمتهمين.

ـــــ اختلاف التشريعات الوطنية بين الدول الأعضاء ، وهو ما يُعقّد من تطبيق معايير موحدة.

ـــــ غياب آليات تنفيذية واضحة للمبادرات المشتركة ، مما يجعل من الصعب ترجمة هذه المبادرات إلى إجراءات عملية فعالة.

ـــ رابطة دول جنوب شرق آسيا(ASEAN) :تضم رابطة دول جنوب شرق آسيا (ASEAN) 10دول، وقد بدأت في اتخاذ خطوات جادة لتعزيز التعاون في مجال الجرائم الإلكترونية، خاصة مع تصاعد تأثير هذه الجرائم على الاقتصاد الرقمي والمجتمعات المحلية. ومن أبرز الجهود التي قدمتها الرابطة:

ـــــ إنشاء شبكة التعاون السيبراني الإقليمي (ASEAN-CERT) ، التي تنسق بين الدول الأعضاء في مجال التحقيق والوقاية من الجرائم الإلكترونية[2].

ـــــ عقد ورش عمل مشتركة حول الأمن السيبراني ، لرفع مستوى الوعي وتدريب الكوادر في مجال الوقاية والتحقيق.

---

1 منظمة شنغهاي للتعاون ((SCO، إعلان شنغهاي حول الأمن السيبراني ، 2011، https://eng.sectsco.org

2 منظمة شنغهاي للتعاون ((SCO، تقرير حول التعاون في مجال الأمن السيبراني بين الدول الأعضاء ، 2023.

1 ASEAN، خطة التعاون الإقليمي في مجال الأمن السيبراني ، 2022، https://asean.org

ـــ دعم بعض الدول مثل سنغافورة وماليزيا وإندونيسيا في تطوير تشريعات وطنية شاملة ، وهو ما يُعد خطوة أولى نحو بناء بيئة قانونية وتقنية متكاملة في مجال الجرائم الإلكترونية

وقد حقق التعاون الإقليمي في آسيا نتائج ملموسة، منها:
ـــ تعزيز التعاون بين الدول الأعضاء في مجال تبادل المعلومات الاستخباراتية الرقمية ، مما ساعد في الكشف عن شبكات إجرامية عابرة للحدود.

ـــ تدريب الكوادر في مجال الأدلة الرقمية ، وهو أمر ضروري لبناء نظام قضائي قادر على التعامل مع طبيعة الجرائم الإلكتروني.

ـــ تطوير خطوط ساخنة للإبلاغ عن الجرائم الإلكترونية ، وهو ما يسهل الوصول إلى الضحايا وتسجيل القضايا في وقت مبكر[2] .

الفرع الثاني: التعاون الإقليمي العربي والخليجي

أولاً: التعاون الإقليمي في العالم العربي (جامعة الدول العربية)

رغم ارتفاع معدلات الجرائم الإلكترونية في عدد من الدول العربية، إلا أن التعاون العربي في هذا المجال ما يزال محدوداً مقارنة بالتكتلات الإقليمية الأخرى، وذلك بسبب غياب إطار قانوني عربي موحد للجرائم الإلكترونية وعدم توفر آليات تنفيذية واضحةومع ذلك، هناك مبادرات تُظهر رغبة في تعزيز هذا التعاون، مثل إعلان القاهرة للتعاون في مجال الأمن السيبراني لعام 2017 ، وهو أول نص عربي رسمي يركز على التحديات المشتركة في مجال الجرائم الإلكترونيةومن بين الجهود الأخرى:
ـــ انضمام دول مثل مصر والمغرب وتونس إلى اتفاقية بودابست ، وهو مؤشر إيجابي على استعداد هذه الدول للتعاون الدولي في مجال تبادل الأدلة الرقمية.

ـــ مبادرات الاتحاد البريدي العربي والاتحاد العربي للاتصالات لدعم البنية التحتية الرقمية وتعزيز التعاون الرقمي بين الدول العربية.

إلا أن التعاون العربي يواجه تحديات كبيرة، منها:
ـــ غياب إطار قانوني موحد يؤدي إلى اختلاف التكيفات القانونية وتعدد المصطلحات.

ـــ ضعف البنية التحتية الرقمية في بعض الدول، مما يُعيق جمع وتحليل الأدلة الرقمية.

ـــ نقص الكوادر المؤهلة في مجال الأمن السيبراني والأدلة الرقمية.

2البنك الدولي، دراسة حول التعاون الإقليمي في مكافحة الجرائم الإلكترونية ، 2024.

ـــــ غياب آليات التنفيذ والتنسيق بين الجهات الوطنية ، مما يحد من فعالية المبادرات والقرارات.

وبالتالي، فإن العالم العربي بحاجة إلى بناء آليات تعاون إقليمي أكثر تنظيماً وفعالية ، بهدف توفير بيئة آمنة لمكافحة الجرائم الإلكترونية وحماية البيانات والمستخدمين العرب.

ثانياً: التعاون الخليجي (مجلس التعاون الخليجي)

يعد مجلس التعاون الخليجي من أكثر التجمعات العربية تنظيماً وفعالية في مجال التعاون الرقمي والأمن السيبراني. وقد تميزت دول الخليج بمجموعة من المبادرات، منها:

إنشاء مركز الخليج للأمن السيبراني عام 2016 كمؤسسة إقليمية تُعنى بتطوير استراتيجيات موحدة لمواجهة الجرائم الإلكترونية

ـــــ توقيع مذكرة تفاهم للتعاون في مجال الجرائم الإلكترونية بين دول المجلس، تنظم تبادل المعلومات والأدلة الرقمية بين الدول الأعضاء[1].

ـــــ عقد مؤتمرات دورية لتدريب الكوادر الأمنية والقضائية ، وهي خطوة استراتيجية نحو بناء قدرات بشرية مؤهلة[2]

كما حقق مجلس التعاون الخليجي إنجازات مهمة، منها:

ـــــ تبادل المعلومات الاستخباراتية بين الدول الأعضاء ، مما ساعد في الكشف عن هجمات سيبرانية قبل تنفيذها.

ـــــ تعزيز التعاون في مجال جمع الأدلة الرقمية عبر تحديد إجراءات مشتركة لحفظ وتحليل الأدلة.

ـــــ وضع استراتيجيات وطنية للأمن السيبراني في جميع الدول الأعضاء، وهو مؤشر على الوعي المتزايد بخطورة الجرائم الإلكترونية.

الفرع الثالث: التحديات المشتركة في التعاون الإقليمي

تشترك مختلف التكتلات الإقليمية في مواجهة مجموعة من التحديات التي تعرقل فعالية التعاون في مجال الجرائم الإلكترونية، ومن أبرزها:

ـــــ غياب التشريعات الموحَّدة:فالنقص في النصوص القانونية الموحَّدة يجعل من الصعب توحيد التعريفات والعقوبات، ويُعقّد التعاون القضائي والشرطي بين الدول .

1الأمم المتحدة، تحديات اتفاقية بودابست في القرن الحادي والعشرين ، تقرير رسمي، 2024.

2 عبد الله، محمد أحمد، الجرائم الإلكترونية في القانون المصري: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة القاهرة، كلية الحقوق، 2021.

ـــــ نقص الكوادر المؤهلة:حيث يعاني العديد من التكتلات، خصوصاً في الدول النامية، من نقص كبير في الخبرات المؤهلة في مجال الأمن السيبراني والأدلة الرقمية .

ـــــ الاختلاف في الأولويات السياسية:إذ تولي بعض الدول أولوية أكبر للقضايا الاقتصادية أو العسكرية، وتُهمِل الاستثمار في الأمن الرقمي، مما يؤدي إلى عدم توازن في التعاون الإقليمي

ـــــ الخلافات السياسية بين الدول:وفي بعض المناطق، مثل الشرق الأوسط وجنوب آسيا، تُعيق الخلافات السياسية والعسكرية بين الدول تحقيق تعاون إقليمي فعّال في مجال الجرائم الإلكترونية .

المطلب الثالث: التعاون الدولي في مكافحة الجرائم في مكافحة الجرائم الإلكترونية

يقيّم هذا المطلب نجاحات التعاون الدولي من جهة، والعقبات السياسية والتقنية التي تعيقه من جهة أخرى، مع اقتراح سبل لتعزيزه مستقبلًا.

الفرع الأول : الإنجازات التعاون الدولي و التحديات التي تواجهه

أولا – الإنجازات الرئيسية للتعاون الدولي في مجال الجرائم الالكتروني

انشاء إطار قانوني دولي موحد :ساهمت اتفاقية بودابست حول الجريمة الإلكترونية التي أصدرها مجلس أوروبا عام 2001 في وضع أول إطار قانوني دولي شامل لتحديد الجرائم الإلكترونية وعقوباتها، ووضع إجراءات خاصة لجمع الأدلة الرقمية ونقلها عبر الحدود[1]
وقد تم اعتماد هذه الاتفاقية كمرجع أساسي من قبل العديد من الدول غير الأعضاء أيضًا، مما يدل على توسيع نطاق تأثيرها القانوني خارج نطاقها الجغرافي الأصلي.

2 تعزيز التعاون القضائي والشرطي: سمحت الاتفاقية وعدد من المبادرات الدولية بتعزيز التعاون بين الشرطة الجنائية والنيابات والمحاكم في مختلف الدول ، من خلال توفير آليات رسمية لتسليم المتهمين، وتبادل المعلومات الاستخباراتية، وتنظيم تحقيقات مشتركةمثال:
ـــ يوروبول (Europol) في أوروبا.

ـــ إنتربول (INTERPOL) على المستوى العالمي.

1مجلس أوروبا، اتفاقية بودابست حول الجريمة الإلكترونية – النص الكامل ، 2001، https://www.coe.int
2الأمم المتحدة، الجريمة الإلكترونية: دراسة شاملة للاتفاقيات الدولية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) 2022 https://www.unodc.org

ـــــ المركز الإقليمي العربي للأمن السيبراني الذي أُنشئ تحت رعاية جامعة الدول العربية

3 تطوير آليات جمع وتبادل الأدلة الرقمية :تم إنشاء معايير دولية لجمع وحفظ ونقل الأدلة الرقمية ، بما يضمن سلامتها وموثوقيتها عند استخدامها أمام المحاكم، مما ساهم في زيادة مصداقية الأدلة الرقمية في القضايا الإلكترونية [1].

4 بناء الخبرات والكوادر المؤهلة :من خلال برامج تدريبية ومشاريع تعاونية، تم تدريب الآلاف من القضاة، والمحامين[2]، وضباط الشرطة، وخبراء الأمن السيبراني في مختلف أنحاء العالم، مما ساعد في تقليل الفجوة بين النصوص القانونية والتطبيق العملي [2].

5 مكافحة الجرائم الإلكترونية ذات الطابع العالمي: ساهم التعاون الدولي في تحقيق نتائج ملموسة في مجال مكافحة الجرائم الإلكترونية المنظمة ، مثل:

ـــــ التجارة بالبشر عبر الإنترنت .

ـــــ الابتزاز الإلكتروني عبر الحدود .

ـــــ القرصنة المالية الكبرى التي تستهدف البنوك والمؤسسات العالمية .

ثانيا ـ التحديات التي تواجه التعاون الدولي

1 **عدم انضمام جميع الدول إلى الاتفاقيات الدولية** : رغم نجاح اتفاقية بودابست في جذب عدد كبير من الدول، إلا أن هناك دولًا كبرى لم تنضم إليها لأسباب سياسية أو قانونية، مثل روسيا والصين والهند وإيران ، مما يجعل من الصعب تطبيق آليات التعاون بشكل كامل .

2 غياب التشريعات الوطنية الموائمة :في كثير من الدول، لا تزال التشريعات الوطنية غير متوافقة تمامًا مع المعايير الدولية ، مما يؤدي إلى صعوبة تنفيذ طلبات التعاون الدولي أو تسليم المتهمين[3].

3 الخلافات السياسية بين الدول: بعض الدول ترفض التعاون مع دول أخرى بسبب الخلافات السياسية أو العسكرية ، حتى في مجال الجرائم الإلكترونية، وهو ما يُعيق التحقيقات المشتركة ويُضعِف من فعالية التعاون الدول [1].

---

[2] عبد الله، محمد أحمد، الجرائم الإلكترونية في القانون المصري: دراسة قانونية تحليلية ، رسالة دكتوراه ، جامعة القاهرة، كلية الحقوق، 2021.

2منظمة شنغهاي للتعاون ((SCO، تقرير حول التعاون في مجال الأمن السيبراني بين الدول الأعضاء ، 2023.

ENISA3، الإجراءات الخاصة بالأدلة الرقمية في التعاون الدولي ، 2021، https://www.enisa.europa.eu

4 الاختلاف في مفاهيم الخصوصية والأمن : تختلف الدول في فهمها لحدود الخصوصية والأمن الوطني ، مما يؤدي إلى صراعات في تطبيق بعض مواد الاتفاقية ، خاصة فيما يتعلق بجمع الأدلة الرقمية عبر الحدود دون إذن محلي

5 التطور السريع للتكنولوجيا مقابل بطء التشريعات :بينما تتطور التقنيات المستخدمة في ارتكاب الجرائم الإلكترونية بسرعة كبيرة، فإن التشريعات الدولية والوطنية غالبًا ما تكون متأخرة ، مما يترك ثغرات قانونية يستغلها مجرمو الإنترنت.

6 نقص التمويل والبنية التحتية في الدول النامية : في العديد من الدول النامية، لا توجد البنية التحتية الرقمية المناسبة ولا التمويل الكافي لدعم التعاون الدولي في مجال الجرائم الإلكترونية، وهو ما يُضعف من قدرتها على المشاركة الفاعلة في هذه الجهود .[2]

الفرع الثاني: مدى فعالية التعاون الدولي

أظهرت مؤشرات عديدة فعالية التعاون الدولي في مكافحة الجرائم الإلكترونية، منها زيادة عدد القضايا التي تم حلها عبر هذا التعاون بنسبة تجاوزت 60% خلال العقد الماضيوانخفاض معدلات الجرائم الإلكترونية الخطيرة في المناطق المنظمة مثل أوروبا والخليج العربي وجنوب شرق آسيا بالإضافة إلى ارتفاع مستوى الوعي العام والسياسي حول أهمية مكافحة هذه الجرائم، مما دفع العديد من الحكومات إلى زيادة الاستثمار في الأمن السيبراني وسن تشريعات أكثر صرامة.

ومن الناحية التشريعية، ساهم التعاون الدولي في توحيد المفاهيم والتعاريف القانونية للجريمة الإلكترونية ، وهو ما ساعد العديد من الدول على تحديث تشريعاتها الوطنية لتتماشى مع المعايير الدولية، كما هو واضح في اعتماد عدد من الدول العربية والأفريقية على اتفاقية بودابست كمصدر إلهام لتشريعات محلية، ومع ذلك، يواجه هذا التعاون تحديات تتمثل في غياب آليات تنفيذية واضحة ، وعدم توافق بعض التشريعات الوطنية مع المعايير الدولية ، مما يُعيق تسليم الأدلة أو المتهمين بين الدول .

الفرع الثالث: مقترحات لتحسين فعالية التعاون الدولي

1ـــ دعوة الدول غير المنضمة إلى الانضمام إلى اتفاقية بودابست

رغم فعاليتها، لم تنضم دول كبرى مثل الصين والهند وباكستان إلى الاتفاقية. ولذلك يُقترح: دعوة هذه الدول للانضمام.1

1عبد الحق، علي، التجربة الإماراتية في مكافحة الجرائم الإلكترونية: دراسة مقارنة ، رسالة دكتوراه ، جامعة الإمارات، كلية الحقوق، 2022.

2 المركز العربي للأمن السيبراني، تقرير حول تحديات البنية التحتية الرقمية في الدول العربية ، 2023.

تقديم حوافز قانونية وتقنية لتسهيل الانضمام، ويجب أن تأتي هذه الدعوات من هيئات دولية ذات وزن مثل الإنتربول أو الاتحاد الدولي للاتصالات(ITU) .

2 ـــ تحديث الاتفاقية لتواكب التطورات التكنولوجية : مع ظهور جرائم جديدة مثل تلك المرتبطة بالذكاء الاصطناعي والعملات المشفرة والمحتوى الرقمي المزيف(Deepfake) ، يُقترح:

ـــ توسيع نطاق الاتفاقية لتغطي هذه الجرائم.

ـــ إدخال آليات تنفيذية واضحة لجمع الأدلة الرقمية ونقلها بين الدول، ويجب أن يتم هذا التحديث بشكل دوري

3ـــ **تعزيز التعاون الإقليمي الموازي للتعاون الدولي :**يلعب التعاون الإقليمي دوراً مهماً في تسريع الإجراءات وتجنب الصعوبات اللغوية والتشريعية، ويُقترح:

دعم التكتلات الإقليمية لبناء آليات تعاون محلية، إنشاء مراكز إقليمية للأمن السيبراني تقوم بالتحقيق المشترك وتحليل الأدلة وتدريب الكوادر .

4ـــ بناء كوادر مؤهلة في مجال الأدلة الرقمية

5ـــ تعزيز ثقافة الأمان الرقمي على المستوى الدولي :واجهة الجريمة الإلكترونية بشكل شامل، يُقترح:

ـــ إطلاق حملات توعية رقمية عالمية تستهدف مختلف الفئات العمرية.

ـــ توفير موارد تعليمية مجانية حول كيفية حماية البيانات والتعرف على أساليب الاحتيال.

ـــ إدراج موضوعات الأمن السيبراني في المناهج الدراسية، ودعم الجامعات لإنشاء مراكز بحثية متخصصة.

ـــ تشجيع الشراكات بين القطاع الحكومي والخاص لتطوير البرامج التدريبية التطبيقية .

يهدف الفصل الثاني من هذه الدراسة إلى استعراض الإطار القانوني والتنظيمي للجريمة الإلكترونية ، من خلال تحليل النصوص التشريعية الوطنية، ودور القضاء في مكافحتها، والتحديات القانونية في إثبات الجريمة، بالإضافة إلى دراسة آليات التعاون الدولي والإقليمي في هذا المجال .

.1 الأمم المتحدة، تحديات اتفاقية بودابست في القرن الحادي والعشرين ، تقرير رسمي، 2024.

وقد توصلت الدراسة إلى مجموعة من الاستنتاجات المهمة على النحو التالي:

أولًا: تعددت التشريعات الوطنية لمكافحة الجرائم الإلكترونية في عدد من الدول العربية والغربية ، مثل قوانين السعودية، والإمارات، ومصر، والأردن، والدول الأوروبية، وقد حاولت هذه التشريعات مواكبة طبيعة الجرائم الحديثة، من حيث تعريفها، ومعاقبتها، وتحديد الإجراءات الخاصة لإثباتها. ومع ذلك، لا تزال هناك ثغرات تشريعية واضحة ، خاصة فيما يتعلق بمواكبة التطور التكنولوجي السريع، وغياب الشمولية في بعض التعريفات، وضعف آليات تنفيذ الأحكام المتعلقة بالجرائم العابر للحدود.

ثانيًا: يُعدّ القضاء عنصرًا محوريًّا في مكافحة الجرائم الإلكترونية ، إلا أنه يواجه صعوبات كبيرة، منها:

ـــــ نقص الخبرات المؤهلة في مجال الأدلة الرقمية.

ـــــ غياب المعايير الموحَّدة لقبول الأدلة الإلكترونية أمام المحاكم.

ـــــ التحديات المرتبطة باختصاص القضاء في الجرائم عبر الحدود .

ـــــ التأخير في إصدار الأحكام بسبب تعقيدات الإجراءات واعتمادها على خبرات نادرة.

ثالثًا: تُعدّ الأدلة الرقمية أحد أهم المصادر لإثبات الجريمة الإلكترونية ، ولكن طبيعتها غير الملموسة، وسهولة تعديلها أو حذفها، وغياب البنية التحتية المناسبة لحفظها، يجعل من جمعها وتقديمها أمام القضاء تحديًا كبيرًا يتطلب حلولًا تشريعية وتقنية متداخلة[1].

رابعًا: لعبت اتفاقية بودابست دورًا محوريًّا في توحيد الجهود الدولية لمكافحة الجرائم الإلكترونية ، وهي تُعدّ أول إطار قانوني دولي شامل ينظم هذا المجال. ومع ذلك، فإن عدم انضمام بعض الدول الكبرى إليها لأسباب سياسية أو قانونية، وغياب الآليات التنفيذية الواضحة، يُضعف من فعاليتها الكاملة.

خامسًا: حقق التعاون الإقليمي نتائج إيجابية في بعض المناطق مثل الاتحاد الأوروبي ومجلس التعاون الخليجي ، بينما ما زال محدودًا في مناطق أخرى مثل العالم العربي وإفريقيا، بسبب ضعف البنية التحتية، وقلة الكوادر، وعدم وجود إطار قانوني إقليمي موحد.

سادسًا: أظهرت الدراسة أن التعاون الدولي فعّال في بعض الحالات، خاصة في مجال تبادل المعلومات والاستخبارات الرقمية ، لكنه ما زال يواجه تحديات كبيرة، تتضمن الخلافات السياسية بين الدول، واختلاف التشريعات الوطنية، وغياب آلية تنفيذية مركزية.وباختصار، أكد الفصل الثاني على ضرورة تحديث التشريعات الوطنية لتتماشى مع المعايير الدولية ،

1مجلس أوروبا ، اتفاقية بودابست حول الجريمة الإلكترونية ـــ تحديات المقترحة ، 2024

وتعزيز بناء الكوادر المؤهلة، وتطوير آليات جمع الأدلة الرقمية، وتوسيع نطاق التعاون الدولي والإقليمي لمواجهة هذه الجرائم التي لا تعترف بالحدود.

الخاتمة

في ختام دراستي الموسومة بـ " الإطار القانوني للجريمة الإلكترونية في التشريع الوطني والدولي " أن هذه الدراسة جاءت انطلاقًا من حاجة ملحة إلى فهم شامل ومتخصص للجريمة الإلكترونية باعتبارها واحدة من أخطر الظواهر الجنائية في العصر الرقمي، حيث تُعد الجريمة الإلكترونية تحديًا قانونيًا وأمنيًا معقدًا يتطلب استجابة متعددة الأبعاد. وقد ركزت على تساؤل بحثي محوري هو: كيف يمكن فهم الجريمة الإلكترونية في ضوء تطوراتها المعاصرة، وما مدى كفاءة الأطر القانونية الوطنية والدولية في مواجهتها؟ للإجابة عن هذا السؤال، اعتمد الباحث المنهج والمنهج التحليلي سعى من خلاله إلى تقديم إطار مفاهيمي

دقيق للجريمة الإلكترونية، واستعراض أنواعها وآثارها السلبية، كما تم تحليل النصوص القانونية الجزائرية الخاصة بالجرائم الإلكترونية، وتقييم التجارب التشريعية في عدد من الدول العربية والغربية، بالإضافة إلى دراسة آليات التعاون الدولي والإقليمي في مجال مكافحتها، مع التركيز على اتفاقية بودابست كمرجع في هذا المجال.

وبذلك تكون الدراسة قد ساهمت في سد جزء من الفجوة المعرفية في مجال الجرائم الإلكترونية من منظور قانوني محض، وهو ما لا يزال نادرًا في الأدبيات العربية، خاصة من حيث ربط الجانب النظري بالتطبيقات القضائية والتشريعية الواقعية، مما يجعل منها مرجعاً علمياً مهماً لتطوير المنظومة القانونية الجزائرية في هذا المجال

أهم النتائج المتوصل إليها

أظهرت الدراسة أن هناك تطورًا تشريعيًّا ملحوظًا في عدد من الدول العربية والغربية ، مع وجود قوانين محدَّثة تتناول الجرائم الإلكترونية بشكل شامل ،ومع ذلك لا تزال هناك ثغرات قانونية واضحة تتعلق بعدم مواكبة بعض التشريعات للتطورات التكنولوجية الحديثة، وغياب الشمولية في التعريفات، وضعف آليات إثبات الجريمة.

أظهرت الدراسة أن القضاء يلعب دورًا محوريًّا في مكافحة الجريمة الإلكترونية، لكنه يواجه صعوبات كبيرة، خاصة فيما يتعلق بتفسير النصوص القانونية أمام واقع غير ملموس، وجمع الأدلة الرقمية، وتحديد الاختصاص القضائي في الجرائم العابر للحدود .

يعد قانون 09-04 خطوة متقدمة في محاربة الجريمة الإلكترونية ،إلا أنه لا يغطي بشكل كافي جميع الجوانب المتعلقة بالجريمة الإلكترونية .

إفتقار القانون الجزائري رقم 12 المؤرخ في فبراير 2012 لتعريف موحد للجريمة الإلكترونية

نقص الخبرات البشرية المؤهلة في مجال الأدلة الرقمية يُعتبر أحد أكبر المعوقات أمام تحقيق العدالة الجزائرية .

ضعف البنية التحتية الرقمية للمحاكم الجزائية الجزائرية في مواجهة الجرائم الإلكترونية .

إن اتفاقية بودابست تُعدّ المرجع الأساسي في مجال التعاون الدولي حول الجرائم الإلكترونية ،ومع ذلك فإن عدم انضمام بعض الدول الكبرى مثل روسيا والصين ، ووجود خلافات سياسية بين الدول، تُضعف من فعالية هذا التعاون

لقد أظهرت بعض التكتلات على المستوى الإقليمي مثل مجلس التعاون الخليجي والاتحاد الأوروبي نجاحات ملحوظة، بينما ما زال التعاون العربي والإفريقي محدودًا.

الإقتراحـــــات

بناءً على النتائج التي تم التوصل إليها، يقدم الباحث مجموعة من الإقتراحات التي تهدف إلى تعزيز مكافحة الجريمة الإلكترونية على المستويات المختلفة:

.1على المستوى الوطني

- تحديث التشريعات الوطنية لتكون أكثر شمولية ومواءمة مع المعايير الدولية.
- إنشاء محاكم ونيابات متخصصة في الجرائم الإلكترونية.
- توفير برامج تدريبية للقضاة والمحامين والخبراء في مجال الأدلة الرقمية.
- تعزيز البنية التحتية الرقمية ودعم الجهات الحكومية المسؤولة عن الأمن السيبراني.

.2على المستوى الإقليمي

- تعزيز التعاون بين الدول العربية والإسلامية في مجال الجرائم الإلكترونية.
- إنشاء مركز عربي للأمن السيبراني مشابه لمركز الخليج.
- تبني إطار قانوني إقليمي موحد لمكافحة الجرائم الإلكترونية.

.3على المستوى الدولي

- تشجيع الدول التي لم تنضم إلى اتفاقية بودابست على الانضمام إليها.
- تعديل الاتفاقية لمواكبة التطورات التكنولوجية الجديدة.
- تعزيز آليات التنفيذ والتنسيق بين الدول الأعضاء.

.4على المستوى التعليمي والثقافي

- إدراج مواد دراسية حول الأمن السيبراني في المناهج التعليمية.
- إطلاق حملات توعية مجتمعية حول مخاطر الجرائم الإلكترونية وكيفية الوقاية منها.

بهذا نكون قد أنهينا هذه الدراسة التي تناولت الجريمة الإلكترونية من منظور قانوني متكامل ، وشملت التعريف بها، وتحليل أنواعها وآثارها، واستعراض الإطار القانوني الوطني، ودراسة دور القضاء، وتقييم التعاون الدولي والإقليمي .

وقد أظهرت الدراسة أن الجريمة الإلكترونية ليست مجرّد قضية قانونية، بل هي ظاهرة معقدة تتطلب تكاملاً بين القانون، والتكنولوجيا، والتعليم، والأمن، والتعاون الدولي .كما أظهرت أن هناك تقدمًا ملموسًا في مجال التشريعات والتعاون الدولي ، إلا أن التحديات ما زالت كبيرة ، وتحتاج إلى جهود متواصلة من الدول والمجتمع الدولي .

وفي الأخير، فإن هذه الدراسة تُعدّ مدخلًا علميًّا مهمًّا في دراسة الجريمة الإلكترونية من منظور قانوني، وتساهم في وضع رؤية شاملة وقابلة للتطبيق في مكافحة هذه الظاهرة الخطيرة.

قائمة المصادر و المراجع

مراجع باللغة العربية

أولاً: الكتــب

1. محمد بن مكرم بن منظور الأنصاري ، لسان العرب ،دار صادر، بيروت، لبنان، الطبعة الثالثة 2003
2. أحمد، حسن محمد، *الأدلة الرقمية في القانون الجزائري*، دار النشر العلمي، القاهرة، الطبعة الأولى، 2022 .
3. فهد لن مسعود العتيبي، *الجريمة المعلوماتية في التشريع السعودي (دراسة تطبيقية)* ، نادي الرياض الأدبي، الطبعة 1، 2018
4. أبو إسحاق ابراهيم بن علي الشيرازي، *المهذب في الفقه الشافعي*، دار الكتب العلمية، بيروت مجلد 22003 .
5. السليمان، عبد الرحمن، *الجرائم الإلكترونية بين الواقع والقانون*، دار النهضة العربية، القاهرة، 2015 .
6. عاشور، *الجرائم المعلوماتية في التشريع المقارن*، دار النهضة العربية، 2020 .
7. عطية، محمود حسن، *الأمن السيبراني وحماية المعلومات في العصر الرقمي*، دار النشر للجامعات، الإسكندرية، 2019،
8. عطية، محمود حسن، *الأمن السيبراني في الدول العربية: تحديات وحلول*، دار النشر العلمي، بيروت، الطبعة الثانية 2023
9. عوض، كريم، *الجرائم الإلكترونية وتحديات الأمن السيبراني*، المركز القومي للبحوث الاجتماعية والجنائية ، القاهرة 2018.
10. عبد الوهاب، عبد اللهأحمد، *الجريمة الإلكترونية بين التشريع والتطبيق*، دار الجامعة الجديدة، الإسكندرية،مصر ، 2019.

ثانيًا: الأطروحات والمذكرات

1. أبو السعود، أحمد محمد، *جرائم الاحتيال الإلكتروني: دراسات قانونية تحليلية*، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، 2020.
2. أحمد، سمير عبد الرحمن، *جرائم الإنترنت: دراسة قانونية شاملة*، رسالة دكتوراه ، جامعة الزقازيق، كلية الحقوق، 2021.
3. بلعيد، عبد الرحمان، *الجريمة الإلكترونية في التشريع الجزائري*، رسالة دكتوراه ، جامعة الجزائر 2، كلية الحقوق، 2021.
4. بوعلام، أحمد، *الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية*، رسالة دكتوراه ، جامعة باتنة، كلية الحقوق،2021
5. بن عمر، يوسف، *جرائم الإنترنت: دراسة قانونية تحليلية*، رسالة دكتوراه ، جامعة البليدة، كلية الحقوق، 2020 .
6. عبد الحق، علي، *التجربة الإماراتية في مكافحة الجرائم الإلكترونية: دراسة مقارنة*، رسالة دكتوراه ، جامعة الإمارات، كلية الحقوق، 2022.
7. عبد الهادي، محمد أحمد، *جرائم الإنترنت: دراسة قانونية تحليلية*، رسالة دكتوراه ، جامعة عين شمس، كلية الحقوق، 2021
8. عبد الله، نادية محمد، *الجرائم الإلكترونية وآثارها النفسية والاجتماعية*، رسالة ماجستير ، جامعة دمشق، كلية الحقوق، 2020 المرزوقي، عبد الرحمن علي، *جرائم الإنترنت: دراسة مقارنة في القانون الجنائي*، رسالة ماجستير ، جامعة الإمارات العربية المتحدة، 2021.
9. زبيري، محمد، *دراسة قانونية للجريمة الإلكترونية في الجزائر*، رسالة ماجستير غير ، جامعة قسنطينة، كلية الحقوق، 2020
10. صالح، عمر عبد الكريم، *جرائم التجارة الإلكترونية: دراسة قانونية واقتصادية*، رسالة دكتوراه ، جامعة دمشق، كلية الحقوق، 2020 .

ثالثًا: الملتقيات والمجلات

1. بوعزيز، *ثقافة الإبلاغ عن الجرائم الإلكترونية*، مجلة العلوم الجنائية، العدد 7، 2023.
2. قرار المحكمة العيا الجزائرية رقم 1548، مجلة القضاء، العدد 4، 2001 .

المراجع

3علي عبد العزيز، *المسؤولية الجنائية في الجرائم الإلكترونية*، مجلة الحقوق، جامعة الكويت، العدد 45 .

رابعًا: التقارير والوثائق الرسمية

1. الإنتربول، *تقرير حول التعاون الدولي في مكافحة الجرائم الإلكترونية*، 2024.
2. الأمم المتحدة(UNODC) ، *الجريمة الإلكترونية: دراسة شاملة للاتفاقيات الدولية*، 2022.
3. البنك الدولي، *دراسة حول تحديث التشريعات العربية في مجال الجريمة الإلكترونية*، 2023 .
4. التقرير السنوي للبنك المركزي الجزائري، 2023 .
5. المركز الوطني للأمن المعلوماتي(CNSI) ، *تقرير حول التحديات المؤسسية في مكافحة الجريمة الإلكترونية*، 2025 .
6. تقرير المعهد الوطني لأدلة الجنائية الجزائرية، يناير .
7. وزارة العدل الجزائرية، *الجريدة الرسمية للجمهورية الجزائرية*، عدد 12، 2023

خامسا: الجرائد والدوريات:

الجريدة الرسمية الجزائرية، العدد 12، قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 غشت 2009 .
الجريدة الرسمية الجزائرية، العدد 15، قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 غشت 2009.
الجريدة الرسمية الجزائرية، العدد 32، قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 غشت 2009.
الجريدة الرسمية الجزائرية، العدد 44، قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 غشت 2009.
المجلة الجزائية التونسية، الفصل 226 مكرر.
مجلة القضاء والقانون (الجزائر)، العدد 4 لسنة 2021 .

مراجع أجنبية

Parker, D. (2020). Cybercrime and International Law:Jurisdictional Challenges and EnforcementMechanisms. African Journal of BiomedicalResearch, 7(2), pp. 45–67.

UNODC (United Nations Office on Drugs and Crime). (2023). Global Cybercrime Legislation: Trends and Gaps. Vienna: UNODC Publications, pp. 112–130.

فهرس المحتويات

العنوان	الصفحة
مقدمة	1
الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية	8
المبحث الأول:مفهوم الجريمة الإلكترونية وخصائصها	10
المطلب الأول: مفهوم الجريمة الإلكترونية	10
الفرع الأول : التعريف اللغوي للجريمة الإلكترونية	10
الفرع الثاني : التعريف الإصطلاحي للجريمة الإلكترونية	11
الفرع الثالث :نعريف الجريمة الإلكترونية في التشريع الجزائري	12
المطلب الثاني: الخصائص المميزة للجريمة الإلكترونية	13
الفرع الأول : جريمة غير مادية عابرة للحدود	13
الفرع الثاني : صعبة الإثبات والتتبع	18
الفرع الثالث : التطور التكنولوجي السريع	19
المطلب الثالث: الفرق بين الجريمة الإلكترونية والجريمالتقليدية	19
الفرع الأول : من حيث الوسائل المستخدمة	20
الفرع الثاني : من حيث البئة الرقمية	20
الفرع الثالث : من حيث الآثار المترتبة	21
المبحثالثاني:أنواعالجريمة الإلكترونية وآثارها على الفردوالمجتمع	23
المطلب الأول: أنواع الجريمة الإلكترونية	22
الفرع الأول : جريمة القرصنة والتجسس (الهكر)	23
الفرع الثاني : جريمة الإحتيال المالي	27
الفرع الثالث : جريمة الإعتداء على الخصوصية و الإبتزاز	29
المطلب الثاني: آثار الجريمة الإلكترونية على الفرد والمجتمع	31
الفرع الأول : آثار الجريمة الإلكترونية على الفرد	32
الفرع الثاني :آثار الجريمة الإلكترونية على المجتمع	34
الفصل الثاني :لإطار القانوني و التنظيمي للجريمة الإلكترونية	**39**
المبحث الأول: التنظيم القانوني الوطني للجريمة الإلكترونية	**41**
المطلب الأول: النصوص القانونية المعتمدة في التشريع الجزائري لمكافحة الجريمة الإلكترونية	41
الفرع الأول :قوانين مكافحة الجرائم الإلكترونية	41
الفرع الثاني :تحليل وتقويم النصوص القانونية	48
الفرع الثالث :المقترحات لإصلاح الإطار القانوني الجزائي	51
المطلب الثاني: دور القضاء في التصدي للجرائم الإلكترونية	53
الفرع الأول :تحليل الأحكام القضائية الجزائرية في مجال الجرائم الإلكترونية	53
الفرع الثاني :اجراءات القضاء الجزائري وتحدياته	54

الفرع الثالث : التوصيات لتطوير دور القضاء الجزائري في مجال الجرائم الإلكترونية	57
المطلب الثالث: الصعوبات القانونية في اثبات الجريمة الإلكترونية	61
الفرع الأول : طبيعة الأدلة الرقمية وصعوبتها	62
الفرع الثاني :التحديات المتعلقة بالبيانات المشفرة و التخزين السحابي	63
الفرع الثالث :الصعوبات المتعلقة بالتخزين السحابي والحدود الرقمية	63
المبحث الثاني:الإتفاقيات الدولية و الإقليمية	68
المطلب الأول: اتفاقيت بودابست	69
الفرع الأول :البنية القانونية لإتفاقية بودابست	71
المطلب الثاني : التعاون الإقليمي في مكافحة الجريمة الإلكترونية	76
الفرع الأول :التعاون الإقليمي في أوروبا إفريقيا وآسيا	76
الفرع الثاني :التعاون الإقليمي العربي الخليجي	80
الفرع الثالث :التحديات المشتركة في التعاون الدولي	82
الخاتمة	92
قائمة المصادر المراجع	98

ملخص الدراسة

تتناول هذه الدراسة ظاهرة الجريمة الإلكترونية تحليلاً قانونياً شاملاً، عبر تحديد مفهومها وتصنيف أنماطها، ورصد آثارها على الفرد والمجتمع. كما تقوّم الأطر التشريعية في دول عربية وغربية، مع تقييم فاعلية القضاء الجزائري في مواجهتها، ودراسة آليات التعاون الدولي - لا سيما اتفاقية بودابست. وتسعى للإجابة عن إشكالية كفاءة التشريعات الوطنية والدولية في الحد من هذه الجرائم. اعتمدت المنهج الوصفي والتحليلي، فجمعت البيانات الوصفية وحللت النصوص القانونية، لتخلص إلى ثلاث نتائج جوهرية: تميز الجريمة الإلكترونية عن التقليدية في الطبيعة والأدوات، تفاوت التطور التشريعي بين الدول، وأهمية التعاون الدولي رغم المعوقات السياسية والقانونية.

الكلمات المفتاحية:
الجريمة الإلكترونية - القانون الجنائي - التعاون الدولي - اتفاقية بودابست - الأدلة الرقمية.

Abstract

This study provides a comprehensive legal analysis of cybercrime, defining its conceptual framework, classifying its typologies, and examining its societal impacts. It evaluates legislative frameworks in select Arab and Western nations, assesses the efficacy of the Algerian judiciary in countering these crimes, and explores international cooperation mechanisms - particularly the Budapest Convention. The research addresses the core question of national and international legal instruments' effectiveness in combating cybercrime. Employing a descriptive and analytical methodology, it synthesizes empirical data and scrutinizes legal texts, concluding with three key findings: cybercrime's fundamental distinction from traditional crime in nature and tools, uneven legislative progress globally, and the critical role of international cooperation despite persistent political and legal challenges.

Keywords:
Cybercrime - Criminal Law - International Cooperation - Budapest Convention - Digital Evidence.