

الجرائم السيبرانية وآليات مكافحتها في التشريع الليبي

عبد الرحمن مفتاح الباشا

باحث قانوني

Abdoellbasha1@gmail.com*

Cybercrimes and mechanisms for combating them in Libyan legislation

Abdalrahman Muftah Albasha

Legal Researcher

المخلص

تتناول هذه الدراسة موضوع الجريمة السيبرانية في إطارها القانوني المعاصر، باعتبارها من الجرائم المستحدثة التي أفرزتها الثورة الرقمية، والتي أضحت تمثل تحدياً جوهرياً أمام الأنظمة القانونية التقليدية، وتهدف الدراسة إلى تأصيل المفهوم القانوني للجريمة السيبرانية وبيان خصائصها، حيث يتضح أنها تقوم على استخدام الوسائل التقنية، وتتسم بالسرعة والدقة، فضلاً عن طبيعتها العابرة للحدود وصعوبة اكتشافها وتعقب مرتكبيها، الأمر الذي يفرض ضرورة تطوير آليات قانونية وإجرائية متخصصة لمواجهتها. كما تعالج الدراسة الإطار التشريعي الدولي لمكافحة الجريمة السيبرانية، من خلال إبراز أهمية الاتفاقيات الدولية، وفي مقدمتها اتفاقية بودابست، في توحيد المفاهيم القانونية وتعزيز التعاون القضائي بين الدول، خاصة في مجالات تبادل الأدلة الرقمية وتتبع الجناة، وعلى الصعيد الوطني، تستعرض الدراسة جهود المشرع الليبي، لاسيما من خلال إصدار قانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، الذي أسهم في وضع إطار قانوني لتجريم الأفعال المرتبطة بالأنظمة المعلوماتية وحماية البيانات. ويخلص البحث إلى أن التشريع الليبي قد وضع أساساً قانونياً مهماً لمواجهة الجريمة السيبرانية، مدعوماً بإنشاء أطر مؤسسية متخصصة، غير أن فعاليته لا تزال تواجه عدة تحديات، من أبرزها قصور التنظيم الإجرائي للأدلة الرقمية، والحاجة إلى رفع الكفاءة التقنية للجهات المختصة، فضلاً عن محدودية التعاون الدولي، وعليه توصي الدراسة بضرورة تطوير التشريعات الوطنية، وتعزيز البنية المؤسسية والتقنية، وتفعيل آليات التعاون الدولي، بما يضمن تحقيق حماية فعالة للفضاء الرقمي، مع الحفاظ على التوازن بين متطلبات الأمن وصون الحقوق والحريات الأساسية.

الكلمات الدالة: الأدلة الرقمية، الاحتيال الإلكتروني، الجريمة السيبرانية، الخصوصية الرقمية، الأمن السيبراني.

Abstract

This study examines cybercrime within its contemporary legal framework, as one of the emerging forms of crime resulting from the digital revolution, which has become a fundamental

challenge to traditional legal systems. The study aims to establish the legal concept of cybercrime and identify its main characteristics. It is evident that cybercrime relies on technological means and is characterized by speed and precision, in addition to its transnational nature and the difficulty of detecting and tracing its perpetrators. This necessitates the development of specialized legal and procedural mechanisms to effectively address it.

The study also addresses the international legislative framework for combating cybercrime by highlighting the importance of international conventions, foremost among them the Budapest Convention, in unifying legal concepts and enhancing judicial cooperation among states, particularly in the areas of digital evidence exchange and offender tracking. At the national level, the study reviews the efforts of the Libyan legislator, especially through the enactment of Law No. (5) of 2022 on combating cybercrime, which has contributed to establishing a legal framework for criminalizing acts related to information systems and data protection.

The study concludes that Libyan legislation has laid an important legal foundation for addressing cybercrime, supported by the establishment of specialized institutional frameworks. However, its effectiveness still faces several challenges, most notably the inadequacy of procedural regulations concerning digital evidence, the need to enhance the technical capacity of competent authorities, and the limited scope of international cooperation. Accordingly, the study recommends the development of national legislation, strengthening institutional and technical infrastructures, and activating international cooperation mechanisms to ensure effective protection of cyberspace, while maintaining a balance between security requirements and the protection of fundamental rights and freedoms.

Keywords: Digital Evidence, Electronic Fraud, Cybercrime, Digital Privacy, Cybersecurity

المقدمة

تعد الجريمة السيبرانية من أبرز الظواهر الإجرامية الحديثة التي أثارت اهتمام الباحثين على حد سواء، نظرًا لتأثيرها الكبير على الأفراد والمؤسسات والدول، فقد أصبح الفضاء السيبراني، نتيجة للتطور التكنولوجي الهائل في مجال الاتصالات وتقنيات المعلومات، أداة أساسية للتواصل وتبادل المعرفة والمعلومات، ولكنه في الوقت ذاته أصبح مرتفعًا خصبًا لارتكاب الجرائم الرقمية التي تنسم بالتعقيد والتطور المستمر، وبات من الواضح أن الاعتماد المتزايد على الحواسيب والشبكات المعلوماتية في العمليات الاقتصادية والإدارية والاجتماعية خلق بيئة جديدة للتهديدات، تتطلب من الدول وضع أطر قانونية وإجرائية متطورة لمواجهةها والحد من آثارها السلبية.

وتكتسب الجريمة السيبرانية أهميتها الخاصة من كونها عابرة للحدود الوطنية، حيث يمكن ارتكابها في دولة واحدة، فيما تتأثر دول أخرى بنتائجها، ومن أبرز أشكال هذه الجرائم: الاختراق غير المشروع للأنظمة، التجسس الإلكتروني، الاحتيال المالي الرقمي، الابتزاز الإلكتروني، ونشر المحتوى الضار أو المسيء عبر الشبكات، إلى جانب التعدي على الملكية الفكرية وانتهاك حقوق الأفراد والمؤسسات، كما تنسم هذه الجرائم بخصائص تجعل مكافحتها أكثر صعوبة مقارنة بالجرائم التقليدية، منها الاعتماد على المهارات التقنية، السرعة، القدرة على التمويه، وانخفاض معدلات التبليغ عن الوقائع، مما يستلزم تطوير التشريعات، وتعزيز التعاون بين الجهات الوطنية والدولية، وتفعيل دور المؤسسات المتخصصة.

وعلى المستوى الدولي، سعى المجتمع الدولي إلى وضع أطر قانونية لمكافحة الجريمة السيبرانية، أبرزها اتفاقية بودابست لعام 2001، التي وفرت أول معايير قانونية إجرائية للتعامل مع الجرائم الإلكترونية، واتفاقية المجلس الأوروبي للجرائم السيبرانية، التي عززت التعاون القضائي الدولي في هذا المجال، أما على المستوى الوطني برزت جهود الدولة عبر إصدار قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، وإنشاء الهيئة الوطنية لأمن وسلامة المعلومات بموجب قرار مجلس الوزراء رقم 28 لسنة 2013، بما يعكس إدراك المشرع لأهمية حماية الفضاء الرقمي ووضع آليات فعالة لرصد الجرائم الإلكترونية والتحقيق فيها.

أهمية البحث:

تتبع أهمية هذه الدراسة من كونها تساهم في إثراء المكتبة القانونية الليبية من خلال تناول موضوع مستحدث في مجال القانون الجنائي يتمثل في الجرائم السيبرانية، وهو موضوع ما زال في طور البحث والتطوير على الصعيد الأكاديمي ويكتسي أهمية خاصة لما يطرحه من إشكاليات قانونية وتقنية متشابكة، كما أن الدراسة تبرز خصوصية التنظيم التشريعي الليبي لهذه الجرائم ومدى اتساقه مع المبادئ والمعايير الدولية، وهو ما يمنحها قيمة نظرية بارزة.

حدود البحث

يقتصر هذه البحث على تناول الجرائم السيبرانية في التشريع الليبي، من خلال تحليل النصوص القانونية ذات الصلة، وبالأخص قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية وما ارتبط به من نصوص في قانون العقوبات، كما تنحصر الحدود الموضوعية للبحث في استعراض الإطار المفاهيمي للجرائم السيبرانية، والإطار التشريعي المنظم لها في ليبيا، ثم بيان آليات مكافحة القانونية والمؤسسية والتقنية، مع الإشارة إلى أبرز التحديات التي تعترض فعالية المواجهة. أما من حيث الحدود الزمانية، فإن الدراسة تتناول الفترة الممتدة من صدور القانون رقم (5) لسنة 2022م وحتى الوقت الراهن، نظراً لكون هذه المرحلة قد شهدت تحولاً مهماً في بنية المجتمع الليبي الرقمية وتنامياً ملحوظاً لصور الجريمة الإلكترونية، وفيما يتعلق بالحدود المكانية، فإن نطاق البحث ينحصر في الدولة الليبية، مع الاستعانة أحياناً بالمقارنات الدولية كلما دعت الضرورة إلى ذلك، بهدف الاستفادة من التجارب الرائدة في هذا المجال.

أهداف البحث

- 1- بيان الإطار المفاهيمي للجرائم السيبرانية وتوضيح خصائصها وسماتها المميزة.
- 2- تحليل الإطار التشريعي الليبي المتعلق بالجرائم السيبرانية، مع التركيز على قانون الجرائم الإلكترونية رقم (5) لسنة 2022م.
- 3- دراسة آليات مكافحة القانونية والمؤسسية والتقنية في ليبيا.
- 4- إبراز أوجه القصور في التشريع الوطني مقارنة بالتطورات العالمية.
- 5- اقتراح جملة من الحلول التشريعية والعملية لتعزيز فعالية مكافحة الجرائم السيبرانية في ليبيا.

إشكالية البحث

تنبثق إشكالية هذا البحث في التساؤل الرئيسي الآتي: إلى أي مدى استطاع التشريع الليبي مواكبة ظاهرة الجرائم السيبرانية، وما مدى فعاليته في مكافحتها في ضوء التحديات التقنية والمؤسسية الراهنة؟ ويتفرع عن هذا السؤال الرئيسي عدد من التساؤلات الفرعية، من أبرزها:

- 1- ما المقصود بالجرائم السيبرانية وما أبرز صورها؟

2- كيف نظم المشرع الليبي هذه الجرائم من خلال قانون مكافحة الجرائم الالكترونية والتشريعات ذات الصلة؟

3- ما هي آليات المواجهة القانونية والمؤسسية الوطنية لمكافحة الجرائم السيبرانية؟

منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي لدراسة النصوص والواقع العملي، بالإضافة إلى المنهج المقارن لمقارنة التشريع الليبي بالتجارب الدولية الناجحة.

خطة البحث

المبحث الأول: الإطار العام للجريمة السيبرانية

المبحث الثاني: الإطار القانوني لمكافحة الجريمة السيبرانية على المستوى الدولي والوطني

المبحث الأول: الإطار العام للجريمة السيبرانية

يعد موضوع الجريمة السيبرانية من أبرز القضايا المعاصرة التي فرضت نفسها على الساحة العلمية والعملية، إذ يكتسب أهميته المتزايدة من الطابع الدولي لشبكة الإنترنت، تلك الشبكة التي أصبحت بمثابة سلاح ذي حدين؛ فهي من جهة وسيلة فاعلة للتواصل والتقارب وتبادل المعلومات والمنافع بين البشر، ومن جهة أخرى قد تتحول إلى أداة لارتكاب شتى صور الجرائم والتعدي على حقوق الغير، ومن ثم برزت الحاجة الملحة إلى مواجهة هذا الجانب المظلم للفضاء السيبراني والحد من مخاطرة. وفي هذا السياق تجدر الإشارة إلى أن الكونغرس الأمريكي أصدر سنة 1984 قانوناً خاصاً بمكافحة الجرائم المرتبطة بالمعالجة الحاسوبية والدخول غير المشروع إلى أنظمة الحواسيب، متضمناً بياناً واضحاً للأنشطة المحظورة في هذا المجال، وقد شكل ذلك خطوة رائدة في إدراك خطورة هذه الجرائم ووضع أسس لمواجهتها تشريعياً (العسقلاني، 2023م، صفحة 80). وتكمن خطورة الموضوع في ارتباطه المباشر بالمعلومة وأمنها، بوصفها الركيزة الأساسية للحياة المعاصرة وموضع اهتمام الأفراد والدول والمنظمات، وتتجلى صور الجريمة السيبرانية في الاختراق والحذف والتعديل والحجب والتعطيل، وهي جرائم اتسع نطاقها بفعل الخصائص التقنية للفضاء السيبراني، مما صعب ملاحقتها قانونياً، ومن ثم يقتضي الأمر تكثيف التعاون الدولي وتفعيل الآليات الوطنية للحد منها، وعليه فقد تم تقسيم هذا المبحث على النحو الآتي:

المطلب الأول: مفهوم الجريمة السيبرانية وخصائصها.

تقتضي دراسة الجريمة السيبرانية الوقوف أولاً على مفهومها القانوني والخصائص المميزة لها، باعتبارها الإطار النظري لفهم طبيعتها، ومن ثم يمكن هذا التحديد من التمييز بينها وبين غيرها من الجرائم التقليدية.

الفرع الأول: مفهوم الجريمة السيبرانية

يستعمل مصطلح الجريمة السيبرانية في الفقه الحديث للدلالة على الجرائم المرتبطة بتقنيات المعلومات والاتصالات، وقد نشأ هذا المصطلح وتطور باعتباره انعكاساً لظاهرة الإجراء المستحدث المرتبط باستخدام شبكة الإنترنت، ويشمل نطاقه كل فعل إيجابي أو امتناع عمدي يتم من خلال الاستغلال غير المشروع لتكنولوجيا المعلومات، سواء كان الاعتداء منصباً على

الممتلكات المادية أو المعنوية أو على حرمة الحياة الخاصة للأفراد، وهناك من يطلق عليها أيضاً بتسمية مصطلح الجريمة الإلكترونية (قادري، 2023م، صفحة 324).

ويرجع أصل صياغة هذا المصطلح لأول مرة إلى ويليام جيبسون سنة 1982، غير أن التطور التشريعي والفقهى لاحقاً وسع من مفهومه، بحيث تجاوز مدلول "جرائم الحاسوب" بمعناه الضيق ليغدو مفهوماً أشمل يضم كافة الأفعال التي تستهدف البيانات أو الأنظمة المعلوماتية أو ترتكب بواسطتها، ومن هنا برزت محاولات فقهية وأكاديمية لتعريف الجريمة السيبرانية بوصفها جملة من الأفعال غير المشروعة التي تنصب على البيانات أو البرمجيات أو الموارد المعلوماتية، سواء بالاختراق أو التلاعب أو الاستغلال أو التعطيل (بوقريط، 2025م، صفحة 205).

وقد عرفها البعض أيضاً على أنها "سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم الرقمي على فوائد مادية ومعنوية، وغالباً ترتكب هذه الجرائم عبر القرصنة أو الاختراق للأنظمة المعلوماتية" (العيش، 2022م، صفحة 194).

كما عرفها آخرون بأنها "السلوك غير المشروع المنافي للأخلاق أو غير المسموح به المرتبطة بالشبكات المعلوماتية فهي تعد من الجرائم العصر الرقمي التي تطل بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية" (الصحفي، 2020م، صفحة 8).

وبالتالي فإن الجريمة السيبرانية تعد فعلاً مجرمًا، يتميز عن غيره من صور الإجرام التقليدي بارتباطه الوثيق بالثورة التقنية، وبما ينطوي عليه من خطورة خاصة تتمثل في السرعة، والدقة، وعبور الحدود، فضلاً عن صعوبة تعقب مرتكبيها، مما يستدعي بذل جهود تشريعية وقضائية متكاملة لمواجهتها.

ويعرف المشرع الليبي الجريمة السيبرانية (الإلكترونية) في إطار القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية بأنها: "كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات، بالمخالفة لأحكام هذا القانون" (المادة 1 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ويرى الباحث أن تعريف المشرع الليبي للجريمة السيبرانية في القانون رقم (5) لسنة 2022 يشمل جوهر الفعل الإجرامي المرتبط بتقنيات المعلومات الحديثة، حيث يحدد نطاق الجريمة بالوسيلة المستخدمة (الحاسب الآلي أو شبكة المعلومات الدولية أو غيرها من تقنيات المعلومات)، مما يبين مدى اهتمام المشرع بضبط الجرائم الرقمية.

الفرع الثاني: خصائص الجريمة السيبرانية

أدت الطفرة التكنولوجية في مجال الاتصالات والمعلومات إلى إحداث نقلة نوعية في حياة الإنسان، وفوقت له أدوات عصرية للتواصل وتبادل المعرفة، غير أنها في المقابل أسفرت عن بروز أنماط إجرامية مستحدثة لم يعرفها القانون التقليدي، إذ لم يكن المشرع يتصور وقوعها في السابق. فقد ظهرت جرائم جديدة تمس سرية البيانات والمعلومات، إلى جانب تطور خطير للجرائم التقليدية التي باتت تمارس بوسائل تقنية أكثر تطوراً، ومن هنا برزت الجريمة السيبرانية كظاهرة إجرامية متفردة بخصائصها، تميزها عن غيرها من الجرائم التقليدية، وذلك على النحو التالي: —

أ. خطورة الجريمة السيبرانية فهي تعد من أخطر الجرائم المعاصرة، لما لها من تأثير مباشر على حياة الأفراد والمؤسسات، وقد تتسبب في خسائر اقتصادية كبيرة للدول، كما أنها تتميز بأنها لا تتطلب قوة جسدية، بل تعتمد على المهارة التقنية والذكاء (ثنيان، 2012م، صفحة 22).

ب. الاعتماد على الوسائل التقنية في تنفيذ الجريمة فهي تتم باستخدام الحاسب الآلي كأداة لارتكاب الجريمة، وتستخدم شبكة الانترنت كوسيلة لذلك (هروال، 2014م، صفحة 37).

ت. انخفاض معدلات التبليغ عن الجرائم حيث لا يتم التبليغ عن الجرائم السيبرانية، خاصة تلك التي تمس المؤسسات والشركات التجارية، ويرجع ذلك إلى خشية الضحايا من الإضرار بسمعتهم أو اهتزاز ثقة العملاء، الأمر الذي يعقد مهمة السلطات القضائية في رصد الجرائم وتوثيقها.

ث. صعوبة مكافحة الجريمة فهي تعد جريمة مخفية بحيث لا يستطيع الشخص أو الشركة اكتشافها إلا بعد حصولها في بعض الأحيان؛ وذلك لأنها جريمة صامتة تحدث عن بعد (قاسم، 2024م، صفحة 100).

ج. جريمة عابرة للحدود حيث تمتاز الجرائم السيبرانية بكونها عابرة للحدود الوطنية، إذ يمكن ارتكابها في دولة واحدة بينما تتأثر دول أخرى بالنتائج (العجمي، 2014م، صفحة 20)، وهذا الأمر يفرض على التشريعات الوطنية تنسيق جهودها مع القانون الدولي والاتفاقيات الإقليمية لضمان فعالية مكافحة هذه الجرائم، ويبرز دور التعاون بين الأجهزة القضائية والأمنية عبر الحدود.

ح. الحاجة للخبرة التقنية العالية يتطلب ارتكاب الجرائم السيبرانية مستوى عالٍ من المعرفة التقنية والخبرة في مجال الحاسب الآلي، الأمر الذي يضعها ضمن فئة الجرائم المتخصصة (المهدي، 2021م، صفحة 114).

ومن خلال ما سبق، يؤكد الباحث أن خصائص الجريمة السيبرانية تجعلها تحدياً قانونياً وأمنياً معقداً، يستدعي تطوير آليات تشريعية وتقنية متقدمة، وتفعيل التعاون الدولي لضمان فعالية مكافحتها.

المطلب الثاني: تصنيفات الجريمة السيبرانية

لا تعد الجريمة السيبرانية نوعاً واحداً، بل تختلف بحسب الأساس والمعيار الذي يعتمد عليه الفقهاء في تقسيمها، فمنهم من يميز بين الجرائم التي ترتكب على نظم الحاسوب وتلك التي ترتكب بواسطته، ومنهم من يصنفها وفق الأسلوب المتبع في ارتكاب الجريمة، أو حسب الدافع والغاية من ارتكابها، كما يعتمد آخرون على تعدد محل الاعتداء أو تعدد الحقوق المعتدى عليها (حملوى، 2025م، صفحة 37)، ومن هذا المنطلق، يمكن تقسيم جرائم الحاسوب إلى فئتين أساسيتين: الجرائم الواقعة على الأموال، والجرائم الواقعة على الحياة الخاصة.

الفرع الأول: الجرائم الواقعة على الأموال

تستهدف هذه الفئة الممتلكات المالية للأفراد أو المؤسسات، وتعد من أكثر أشكال الجريمة السيبرانية انتشاراً، نظراً لاعتماد المجتمع الحديث على التكنولوجيا في المعاملات المالية والإدارية، وتعد تهديداً مباشراً للاقتصاد الوطني والدولي، وتستدعي تطوير آليات قانونية متقدمة لمكافحتها.

وتشمل الجرائم الواقعة على الأموال كل الأفعال التي تنطوي على الاعتداء على الممتلكات الرقمية أو المالية باستخدام الحاسوب أو شبكة الإنترنت، ومن أبرز أمثلتها:

أ. الاحتيال الإلكتروني: ويشمل التحايل على الأفراد أو المؤسسات للحصول على أموال بطرق غير مشروعة، مثل الرسائل المزيفة أو المواقع الوهمية.

ب. السرقة الإلكترونية: سرقة الأموال مباشرة من الحسابات البنكية أو بطاقات الدفع الإلكترونية.

ت. التزوير الرقمي: تعديل البيانات المالية أو المستندات الإلكترونية لتحقيق مكاسب غير قانونية.

ث. الاختراق المالي: الدخول غير المشروع إلى أنظمة المؤسسات المالية بهدف الاستيلاء على الأموال أو المعلومات الحساسة المتعلقة بها (بيظام، 2023م، صفحة 111).

ويرى الباحث أن الجرائم السيبرانية على الأموال تشكل تحديًا كبيرًا للقوانين الوطنية والدولية، إذ تتطلب أساليب رقابية وتقنية متقدمة للتصدي لها وحماية الاقتصاد الرقمي.

الفرع الثاني: الجرائم الواقعة على الحياة الخاصة

تركز هذه الفئة على حقوق الأفراد الشخصية، إذ تهدف إلى حماية الحياة الشخصية والمعلوماتية من الاعتداء أو الاستغلال غير القانوني، وتعتبر هذه الجرائم ذات خطورة كبيرة على سمعة الأفراد والمؤسسات، وقد تؤدي إلى أضرار معنوية ومادية جسيمة، تشمل الجرائم الواقعة على الحياة الخاصة كل الأعمال التي تنطوي على انتهاك الخصوصية أو التعدي على الحقوق الشخصية باستخدام التكنولوجيا، ومن أبرز الأمثلة:

أ. التجسس الإلكتروني: جمع معلومات شخصية أو مؤسسية دون إذن، مثل التنصت على المراسلات أو مراقبة الأجهزة عن بعد.

ب. الابتزاز الإلكتروني: استغلال المعلومات أو الصور الخاصة لتهديد الضحايا للحصول على مكاسب غير مشروعة.

ت. التشهير الإلكتروني والسب والقذف: نشر معلومات مضللة أو مسيئة عبر الإنترنت بهدف الإضرار بسمعة الأفراد أو المؤسسات.

ث. اختراق الخصوصية: التسلل إلى الحسابات الشخصية أو الأجهزة الإلكترونية دون إذن، بما في ذلك البريد الإلكتروني ووسائل التواصل الاجتماعي (يعقوب، 2014م، صفحة 223).

ويخلص الباحث إلى أن الجرائم السيبرانية ضد الحياة الخاصة تتطلب تشريعات صارمة وتوعية مجتمعية لحماية حقوق الأفراد وحفظ الخصوصية الرقمية.

المبحث الثاني: الإطار القانوني لمكافحة الجريمة السيبرانية على المستوى الدولي والوطني

تعد الجريمة السيبرانية من أبرز التحديات القانونية والأمنية في العصر الرقمي، لما لها من آثار تتجاوز الحدود الوطنية وتؤثر على الأفراد والمؤسسات والدول على حد سواء، ومن هذا المنطلق، أصبح من الضروري وضع آليات قانونية فعالة لمكافحتها، سواء على المستوى الدولي من خلال الاتفاقيات والمعاهدات التي تنظم التعاون بين الدول وتبادل المعلومات، أو على المستوى الوطني عبر تشريعات متخصصة تحدد الجرائم الإلكترونية وعقوباتها، وتضع أطراً لإجراءات التحقيق والملاحقة القضائية، بهدف الحد من الأضرار المادية والمعنوية الناجمة عن هذه الجرائم، وضمان حماية الأنظمة المعلوماتية، والحفاظ على الأمن السيبراني في مختلف المجالات الاقتصادية والاجتماعية والسياسية.

وفي ضوء ما سبق، سيتم تناول الموضوع وفق التقسيم المعتمد بين الآليات القانونية الدولية والآليات القانونية الوطنية لمكافحة الجريمة السيبرانية.

المطلب الأول: الآليات القانونية الدولية لمكافحة الجريمة السيبرانية.

تصنف الجريمة السيبرانية ضمن الجرائم العابرة للحدود، إذ يمتد تأثيرها إلى عدة دول، ويصعب أحياناً تتبع الأدلة أو الحفاظ عليها، مما يجعل القوانين الوطنية وحدها غير كافية لمواجهتها بفعالية، لذلك أصبح من الضروري وجود إطار دولي متكامل يسعى لوضع التدابير والإجراءات اللازمة للحد من انتشار هذه الجرائم ومعاقبة مرتكبيها (السلمي، بدون معلومات سنة النشر، صفحة 588)، وفي سياق تحليل الآليات القانونية لمكافحة الجرائم السيبرانية على المستوى الدولي، سنتناول الجهود الدولية المبذولة للحد من هذا النوع من الجرائم، مع التركيز على التدابير الحديثة المعتمدة لاحتوائها ضمن الاتفاقيات الدولية، ويتضمن هذا التحليل دراسة عدد من الاتفاقيات البارزة، مثل اتفاقية مجلس أوروبا – بودابست لعام 2001 واتفاقية مجلس أوروبا لعام 2004، مع إلقاء الضوء على التطورات والتحديات التي تناولتها هذه الاتفاقيات لتعزيز الأطر القانونية والإجرائية في مكافحة الجرائم السيبرانية.

الفرع الأول: اتفاقية مجلس أوروبا – بودابست لسنة 2001

أُبرمت اتفاقية مجلس أوروبا بودابست في 23 نوفمبر 2001، وأطلقت عليها اسم اتفاقية الجريمة عبر العالم السيبراني (الإنترنت)، بهدف توفير إطار قانوني يساعد الدول في مواجهة الجريمة السيبرانية، وقد وقعت عليها 43 دولة أوروبية عضواً في المجلس الأوروبي، وتعتبر هذه الاتفاقية خطوة رئيسية في مكافحة الجرائم السيبرانية، إذ تؤكد في مادتها الثالثة على أن النشاط التقني يعد جزءاً لا يتجزأ من النشاط المادي، ويفهم استخدام التقنية على أنه استخدام الحواسيب وتكنولوجيا الاتصالات بكافة أشكالها (الربيعي، الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة)، 2024م، صفحة 83).

وتركز الاتفاقية على وضع قواعد لمكافحة الجرائم السيبرانية من الناحية الموضوعية والإجرائية، مع الاعتراف بأن مواجهة هذه الجرائم تتطلب تعاوناً دولياً فعالاً، وقد نصت الاتفاقية على مجموعة من المبادئ الإجرائية العامة، أهمها:

- أ. تنسيق تطبيق القانون الجنائي الوطني مع مكافحة الجرائم السيبرانية، وتأمين سلطات التحقيق والملاحقة.
- ب. إنشاء نظام فعال للتعاون الدولي يشمل التحقيقات الجنائية وتوثيق الأدلة الإلكترونية.
- ت. إلزام الدول الموقعة باستخدام الأدلة الرقمية والإلكترونية أمام القضاء، مع التركيز على جرائم الحواسيب.
- ث. ضمان تنفيذ الصلاحيات والإجراءات ضمن النظام القضائي لكل دولة.

كما تضمنت الاتفاقية إجراءات جنائية جديدة، من أبرزها:

- أ. الحفظ السريع للمعطيات المخزنة: لضمان الاحتفاظ بالأدلة قبل تلفها أو فقدانها نتيجة تغير البيانات.
- ب. تجميع معلومات المشتركين: لتحديد هوية الجاني عبر معلومات الاستخدام وفترة الاشتراك.
- ت. التفتيش المعلوماتي: إجراء التفتيش على البيانات الإلكترونية بموجب إذن رسمي وشروط محددة.
- ث. الدخول على المعطيات المعلوماتية: تمكين السلطات من الوصول إلى المعلومات المخزنة وجمع الأدلة في الوقت الفعلي.

- ج. إجراء التنصت: اعتراض المراسلات بعد موافقة قضائية للتحقق من وقوع الجريمة السيبرانية.
- ح. التعاون الدولي: تبادل المعلومات والأدلة بسرعة، وتأمين البيانات المستخدمة كأدلة.
- خ. الالتزام والتنفيذ: إصدار تشريعات وطنية لتحديد المسؤوليات الجنائية ومواجهة التحديات الدولية (الربيعي، الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة)، 2024م، صفحة 84).

كما ناقشت الاتفاقية مسائل مهمة تتعلق بمقدمي الخدمات الرقمية، مثل مدى إلزامهم بالاحتفاظ ببيانات المرور لفترة محددة، وتطوير المصطلحات القانونية المستخدمة في مكافحة الجرائم السيبرانية، سواء بالاعتماد على المفاهيم التقليدية (التفتيش والضبط) أو استخدام مصطلحات جديدة تتماشى مع التكنولوجيا الحديثة.

الفرع الثاني: اتفاقية المجلس الأوروبي للجرائم السيبرانية

تعد اتفاقية مجلس أوروبا لعام 2004 واحدة من أبرز الاتفاقيات الدولية المخصصة لمكافحة الجريمة السيبرانية، صدرت هذه الاتفاقية عن المجلس الأوروبي ووقعتها 32 دولة، ودخلت حيز التنفيذ في يوليو 2004، وتركز الاتفاقية على تحديد الجرائم التي تمس النظم المعلوماتية، مع إبراز الأساليب الإجرائية المعتمدة للتحقيق فيها، وتشمل الجرائم التي تناولتها الاتفاقية:

أ- الجرائم المرتبطة بالنظام المعلوماتي: مثل الهجمات على سرية وتكامل وتوافر البيانات أو نظم الحاسوب، بما في ذلك التدخل والاختراق.

ب- الجرائم المتعلقة بالمحتوى: مثل الإنتاج أو النشر غير المشروع للمواد الإباحية للأطفال عبر النظم المعلوماتية.

ت- الجرائم المتعلقة بحقوق الملكية الفكرية: وتشمل استغلال أو انتهاك الحقوق الرقمية بطرق غير مشروعة.

وفيما يخص الإجراءات الإجرائية، نصت الاتفاقية على مجموعة من التدابير لتعزيز فعالية التحقيق:

أ- إجراء التفتيش والضبط على أنظمة الحاسوب، مع التركيز على تحليل البيانات بشكل ملموس وسريع.

ب- الحفظ السريع للبيانات المخزنة: لضمان الحفاظ على الأدلة قبل تلفها، خصوصاً في الجرائم المرتكبة على شبكة الإنترنت.

ت- إصدار نسخة من البيانات: يسمح للسلطات بالوصول إلى معلومات المشتركين عبر مزودي خدمات الإنترنت، بما يساهم في تحديد هوية الجناة.

ث- اعتراض بيانات المحتوى: تمكين السلطات من اعتراض الرسائل والمعلومات المنقولة عبر وسائل الاتصال، مع الأخذ في الاعتبار المعايير الدولية لتعزيز فعالية هذه الإجراءات (الربيعي، الجريمة السيبرانية وآليات مكافحتها) (دراسة مقارنة)، 2024م، صفحة 84).

كما لعبت الاتفاقية دوراً مهماً في تعزيز التعاون القضائي الدولي، من خلال إنشاء وحدة Eurojust التي تهدف إلى تنسيق جهود الدول الأعضاء في الاتحاد الأوروبي لمكافحة الجرائم السيبرانية، بما في ذلك أمر القبض الأوروبي الذي يتيح تسليم المجرمين بسرعة بين الدول الأعضاء.

المطلب الثاني: التدابير التشريعية والمؤسسية الوطنية لمكافحة الجريمة السيبرانية

في ظل التحول الرقمي السريع واعتماد المجتمعات على التقنيات الحديثة في مختلف مجالات الحياة، برزت الجريمة السيبرانية كأحد أبرز التحديات التي تهدد الأمن القومي والاقتصاد الوطني، وتمس الحقوق الفردية والمؤسسية على حد سواء، فهذه الجرائم التي تتسم بالتطور التكنولوجي المستمر والطابع العابر للحدود، لم يعد بالإمكان مكافحتها عبر أدوات القانون التقليدي وحدها، مما استدعى وضع تشريعات متخصصة تتعامل مع خصوصية الفضاء الرقمي وطبيعة الجريمة الإلكترونية.

وفي هذا السياق، اتجه المشرع الليبي إلى إصدار قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، الذي يمثل إطاراً قانونياً متكاملاً، يجمع بين التجريم الرادع والإجراءات الوقائية والتقنيات الحديثة لحماية المعلومات والأنظمة الرقمية، ومن هنا تبرز أهمية دراسة التدابير التشريعية والمؤسسية الوطنية، باعتبارها الركيزة الأساسية التي تمكن الدولة من مواجهة الجرائم

السيبرانية بفعالية، وضمان حماية المجتمع والاقتصاد الوطني من المخاطر التي قد تنجم عن إساءة استخدام التكنولوجيا، وفيما يلي سنتناول التدابير التشريعية والمؤسسية الوطنية لمكافحة الجريمة السيبرانية، مستعرضين الأطر القانونية والإجراءات المؤسسية التي اعتمدها المشرع الليبي لضمان حماية الفضاء الرقمي وتعزيز الأمن السيبراني.

الفرع الأول: التدابير التشريعية الوطنية لمكافحة الجرائم السيبرانية

مع التطور السريع في مجال التكنولوجيا والاتصالات، باتت الجريمة السيبرانية تهدد الأمن المعلوماتي، والاقتصاد الوطني، وحقوق الأفراد، مما استدعى تدخل الدولة لإصدار تشريعات متخصصة لمكافحتها، وفي هذا السياق يمثل قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية خطوة تشريعية وطنية مهمة تهدف إلى حماية الفضاء الرقمي وضمان الأمن السيبراني في ليبيا.

ومن أبرز أهداف القانون حماية المعاملات الإلكترونية، وضمان العدالة والأمن المعلوماتي، والحفاظ على النظام العام والآداب العامة، ودعم الاقتصاد الوطني، وتعزيز الثقة العامة في صحة وسلامة المعاملات الإلكترونية، ويطبق القانون على الجرائم المرتكبة داخل ليبيا أو خارجها إذا امتدت نتائجها إلى الأراضي الليبية، وهو ما يعكس إدراك المشرع للطبيعة العابرة للحدود للجرائم السيبرانية، وقد تضمن القانون إجراءات وتدابير واضحة لتجريم مختلف الأفعال، منها:

أ- الدخول غير المشروع إلى أنظمة المعلومات (الاختراق)، مع تحديد عقوبات متدرجة حسب خطورة الفعل وأثره على النظام المعلوماتي (ينظر المادة 11-12 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ب- الاعتراض أو التعرض للبيانات وحيازة برامج فك الترميز، بما يضمن عدم استغلال الوسائل التقنية للإضرار بالآخرين (ينظر المادة 13-14 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ت- التعدي على الأنظمة المعلوماتية لتحقيق منفعة مادية أو استخدام المخرجات غير المشروعة، وهو ما يعكس اهتمام القانون بحماية الاقتصاد الوطني والمصالح الفردية والمؤسسية (ينظر المادة 15-16 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ث- الترويج للمواد الإباحية، التحريض على الدعارة، ومضايقة الغير، بما يعكس حرص القانون على حماية القيم الاجتماعية والأخلاقية للمجتمع (ينظر المواد 19-22 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ج- حماية حقوق المؤلف والأعمال الرقمية، والتصدي لتقليد البطاقات المصرفية الإلكترونية أو استعمالها بشكل غير مشروع، مما يضمن حفظ الملكية الفكرية والأمن المالي (ينظر المواد 24-26-28 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ح- التصنت غير المشروع والمخاطر على الأمن الوطني، بالإضافة إلى إجراءات المصادرة وإبعاد الأجنبي لضمان فعالية العقوبات. (ينظر المواد 47-50-51 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية)

ومن خلال ما سبق يمكن القول إن المشرع الليبي قد تبني مجموعة من التدابير الوقائية والإجرائية المتكاملة، استهدفت التصدي للجرائم السيبرانية على نحو يوازن بين مقتضيات الأمن وحماية الحقوق والحريات، فقد أدرك خطورة هذه الجرائم وما تطرحه من تهديدات مباشرة لأمن الدولة وسيادتها، فضلاً عن أثارها السلبية على الحقوق الأساسية للأفراد ومصالح المؤسسات، وهو ما جعله يسن القانون رقم (5) لسنة 2022 كإطار قانوني متكامل يهدف إلى تحقيق الحماية والردع والوقاية في آن واحد.

ومن جانبه، عزز المشرع الوسائل الوقائية من خلال إجازة المراقبة الإلكترونية المشروطة برقابة قضائية صارمة، وإلزام مزودي خدمات الاتصالات والإنترنت بحفظ البيانات والتعاون مع السلطات المختصة، مع فرض واجب إزالة أو حجب المحتوى غير المشروع، وهو ما يعكس إرادة واضحة في تضيق فرص استغلال الفضاء الرقمي في أنشطة غير قانونية، ومن جانب آخر، أرسى القانون تدابير إجرائية متقدمة، مثل التفتيش والحجز الإلكتروني، وتوسيع الاختصاص القضائي ليشمل الجرائم ذات الطابع العابر للحدود، إضافة إلى تكريس التعاون القضائي الدولي باعتباره شرطاً لا غنى عنه لمكافحة هذا النوع من الإجرام المستحدث.

ويلاحظ الباحث أن القانون لم يقتصر على تجريم الأفعال فقط، بل أقر أيضاً دوراً فعالاً للهيئة الوطنية لأمن وسلامة المعلومات، والتي تمنحها صلاحيات مراقبة ما ينشر عبر وسائل التقنية الحديثة وحجب المحتوى غير القانوني، مع مراعاة الضوابط القضائية لحماية الحقوق الفردية، بما يعكس توازناً بين الأمن السيبراني وحقوق المواطنين.

كما يلاحظ الباحث أن التشريع الليبي، رغم تقدمه في حماية الحقوق الفردية من خلال إشراف القضاء على عمليات المراقبة، يحتاج إلى تطوير متكامل للأدوات القانونية والتقنية، بما يحقق توازناً فعالاً بين مكافحة الجرائم الإلكترونية وحماية الخصوصية، ويضمن سلامة الأدلة الرقمية من التلاعب أو الضياع.

وفي هذا الإطار، يقترح الباحث الاستفادة من النماذج المقارنة الأوروبية، التي وضعت آليات دقيقة لجمع الأدلة الرقمية، وضوابط واضحة للاستعانة بالخبراء الفنيين، وإجراءات محددة للتفتيش الرقمي، وذلك لتطوير التشريع الليبي بما يتواءم مع التطورات التقنية السريعة في البيئة الإلكترونية، ويضمن فعالية القضاء في مواجهة الجريمة السيبرانية.

الفرع الثاني: التدابير المؤسسية الوطنية لمكافحة الجرائم السيبرانية

إلى جانب التدابير التشريعية التي أقرها المشرع الليبي بموجب القانون رقم (5) لسنة 2022 المتعلق بمكافحة الجرائم السيبرانية، لم يتوقف الإطار القانوني عند سن النصوص القانونية أو وضع الإجراءات الوقائية وحسب، بل تم تدعيمه بآلية مؤسسية متخصصة تمثلت في إنشاء الهيئة الوطنية لأمن وسلامة المعلومات بموجب قرار مجلس الوزراء رقم (28) لسنة 2013، لتكون الجهة المركزية المعنية برسم السياسات الوطنية في مجال الأمن السيبراني، ومتابعة التهديدات الرقمية، وتنسيق الجهود الوطنية والدولية لمواجهة المخاطر المستحدثة في هذا المجال، حيث نصت المادة الأولى على أن للهيئة الشخصية الاعتبارية والذمة المالية المستقلة، وتتبع وزارة الاتصالات والمعلوماتية، ويكون مقرها الرئيسي في طرابلس مع إمكانية إنشاء فروع في مختلف المدن والمناطق.

وتهدف الهيئة إلى وضع السياسات والمعايير الاستراتيجية اللازمة لتأمين البيانات الرقمية، وإدارة الشبكات الوطنية، وتوفير خدمات التشفير والمصادقة الإلكترونية، بالإضافة إلى وضع آليات الاستجابة الفورية للحوادث المعلوماتية، وتعزيز حوكمة الإنترنت على المستويين المحلي والدولي، كما تختص الهيئة بإعداد الدراسات والتحليل والخطط ورفع كفاءة الأمن المعلوماتي، إلى جانب تقييم الشبكات والأنظمة، وإجراء اختبارات الاختراق للكشف عن نقاط الضعف ومعالجتها، والتواصل مع المنظمات الإقليمية والدولية لتطوير الخبرات واستراتيجيات العمل (ينظر المادة 3-4 من قرار رقم 28 لسنة 2013 م بإنشاء الهيئة الوطنية لأمن وسلامة المعلومات).

والى جانب الإطار المؤسسي، أنشأت وزارة العدل إدارة خاصة لأبحاث الجرائم الإلكترونية تابعة لمركز الخبرة القضائية والبحوث عام 2016 (ينظر المادة 1 من قرار وزير العدل رقم 26 لسنة 2016م بشأن إنشاء إدارة مكافحة أبحاث الجريمة

الإلكترونية بمركز الخبرة القضائية والبحوث)، وذلك بعد تصاعد وقائع الابتزاز الإلكتروني وغيرها من الجرائم المرتبطة بالفضاء الرقمي، وقد وسع المشرع الليبي نطاق مأموري الضبط القضائي بموجب قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ليشمل الموظفين الذين يصدر في حقهم قرار من رئيس مجلس الوزراء بناء على اقتراح الهيئة الوطنية لأمن وسلامة المعلومات، مما يتيح لهم القيام بمهام ضبط الجرائم الإلكترونية وجمع الأدلة الرقمية (ينظر المادة 52 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية).

ومما لا شك فيه أن الجمع بين الإطار المؤسساتي المتمثل في الهيئة الوطنية لأمن وسلامة المعلومات وإدارة أبحاث الجرائم الإلكترونية، والتدابير التشريعية المنظمة لمأموري الضبط القضائي ومراقبة المعلومات الرقمية، يشكل حجر الزاوية في جهود ليبيا لمواجهة الجريمة السيبرانية، ومع ذلك تبقى الحاجة ماسة لتطوير آليات تفصيلية للتفتيش الإلكتروني، وضمان سلامة الأدلة الرقمية، واستحداث تنظيم قانوني للاستعانة بالخبراء الفنيين، بما يضمن تحقيق العدالة الجنائية وحماية الحقوق الفردية في ظل التحديات التقنية المتسارعة.

وعلى الرغم من التدابير التشريعية والمؤسساتية التي اعتمدها المشرع الليبي لمكافحة الجرائم السيبرانية، تظل هناك تحديات جوهرية تعيق فعالية المكافحة، فهذه الجرائم الرقمية تتم في بيئة غير مرئية، حيث يمكن للجاني التلاعب بالبيانات أو محوها خلال ثوانٍ، ما يجعل ضبطها مرهوناً بخبرة فنية متخصصة، ومن أبرز الصعوبات إثبات الجريمة بسبب انعدام الدليل المادي، سهولة تدمير الأدلة، وتعقيد الوصول إليها نتيجة التشفير وطبيعة الجريمة عن بعد.

الخاتمة

لقد أظهرت الدراسة أن الجريمة السيبرانية تمثل أحد أبرز التحديات القانونية والأمنية المعاصرة، حيث تمتاز بخصائص تجعلها فريدة ومعقدة مقارنة بالجرائم التقليدية، فهي تعتمد على التكنولوجيا الحديثة، تتسم بالسرعة والدقة، عابرة للحدود الوطنية، وتتطلب مستوى عالٍ من الخبرة التقنية، ومن خلال تحليل الإطار القانوني الدولي والوطني، يمكن القول إن الجريمة السيبرانية لم تعد مجرد تهديد محدود للأفراد، بل أصبحت تمس الأمن القومي والاقتصاد الوطني والحقوق الفردية والمؤسساتية، مما يستدعي وضع استراتيجيات شاملة لمكافحتها.

وأظهرت الدراسة أن الاتفاقيات الدولية، مثل اتفاقية بودابست لعام 2001 واتفاقية المجلس الأوروبي للجريمة السيبرانية، وضعت أسساً قوية لمكافحة الجرائم السيبرانية على المستوى الدولي، من خلال تحديد أنواع الجرائم والإجراءات الإجرائية اللازمة للتحقيق، بالإضافة إلى تعزيز التعاون القضائي بين الدول، هذه الاتفاقيات تؤكد أن الجريمة السيبرانية تتطلب نهجاً عالمياً منسقاً، نظراً لطبيعتها العابرة للحدود وصعوبة جمع الأدلة الرقمية وملاحقة مرتكبيها.

وعلى الصعيد الوطني، أظهرت الدراسة أن ليبيا قامت بخطوات مهمة عبر إصدار قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، وإنشاء الهيئة الوطنية لأمن وسلامة المعلومات بموجب القرار رقم 28 لسنة 2013، بالإضافة إلى إنشاء إدارة أبحاث الجرائم الإلكترونية، وتتمثل أهمية هذه المؤسسات في وضع السياسات والمعايير الاستراتيجية لحماية البيانات الرقمية، وإدارة الشبكات الوطنية، وإجراء اختبارات الاختراق للكشف عن نقاط الضعف، وكذلك مراقبة الرسائل والمكالمات تحت إشراف قضائي لحماية الحقوق الفردية.

أولاً: النتائج

- 1- يتضح من الدراسة أن الجريمة السيبرانية لم تعد تقتصر على اختراق الحواسيب أو سرقة البيانات، بل تشمل مجموعة واسعة من الأفعال غير المشروعة، منها الاحتيال المالي الإلكتروني، الابتزاز الرقمي، التجسس على الخصوصيات، التزوير الرقمي، ونشر المحتوى الضار على الشبكات، ويعد تعريف المشرع الليبي للجريمة السيبرانية شاملاً لهذه الأفعال، مع التركيز على الوسيلة التقنية المستخدمة.
- 2- تتميز الجريمة السيبرانية بعدة خصائص تجعل مكافحتها صعبة، منها الخطورة المباشرة على الأفراد والمؤسسات، والاعتماد الكامل على الوسائل التقنية الحديثة، صعوبة الاكتشاف والتبليغ، الطابع العابر للحدود.
- 3- رغم التقدم التشريعي في ليبيا، هناك ثغرات واضحة في الإطار القانوني، مثل عدم تفصيل إجراءات التفتيش الإلكتروني، وضوابط جمع الأدلة الرقمية، ونقص المعايير للاعتماد على الخبراء الفنيين، وهو ما قد يحد من فعالية التحقيق والملاحقة القضائية.
- 4- أن تأسس الهيئة الوطنية لأمن وسلامة المعلومات وإدارة أبحاث الجرائم الإلكترونية يعكس وعي الدولة بضرورة وجود هيكل مؤسسي قوي قادر على التعامل مع الجرائم الإلكترونية، إلا أن نجاح هذه المؤسسات يعتمد على تطوير قدراتها التقنية وتنظيم أعمالها بشكل مستمر لمواكبة التطورات الرقمية.
- 5- التوازن بين مكافحة الجريمة وحماية الخصوصية، يظهر التشريع الليبي إدراكه لأهمية حماية حقوق الأفراد، حيث خضع المراقبة الرقمية والإجراءات الخاصة للتفتيش القضائي، وهو ما يمثل محاولة لتحقيق التوازن بين الأمن الرقمي والحقوق الفردية، رغم الحاجة لمزيد من التفصيل لضمان حماية فعالة للحقوق الرقمية.

ثانياً: التوصيات

- 1- تطوير الإطار التشريعي الوطني من خلال صياغة نصوص قانونية تفصيلية لإجراءات التفتيش الرقمي وحفظ الأدلة الرقمية، بما يضمن موثوقيتها وقابليتها للاستخدام في التحقيقات القضائية.
- 2- وضع معايير دقيقة للاستعانة بالخبراء الفنيين أثناء التحقيقات لضمان سلامة ودقة الأدلة.
- 3- تعزيز التعاون الدولي من خلال الانضمام إلى الاتفاقيات الدولية والإقليمية لمكافحة الجرائم الإلكترونية وتفعيل أدوات التعاون القضائي، بما في ذلك تبادل الأدلة، ومتابعة مرتكبي الجرائم العابرة للحدود، تبادل الخبرات والتدريب المشترك مع الدول التي تتمتع بتجربة ناجحة في مكافحة الجرائم الإلكترونية.
- 4- رفع مستوى التوعية وبناء القدرات من خلال إعداد برامج تدريبية متقدمة للعاملين في مجال الأمن السيبراني، تشمل مهارات التحليل الرقمي واستجابة الحوادث، وتعزيز الثقافة الرقمية بين أفراد المجتمع، من خلال حملات توعية تهدف لتقليل مخاطر الجريمة السيبرانية، خصوصاً في المؤسسات التجارية والتعليمية.
- 5- تطوير البنية المؤسسية الوطنية من خلال دعم الهيئة الوطنية لأمن وسلامة المعلومات وتمكينها من إنشاء مكاتب ومختبرات تقنية متقدمة في مختلف المناطق، لضمان سرعة الاستجابة للحوادث المعلوماتية.

الهوامش

1. آسيا السبتي، عمر بوقريط. (2025م). الجرائم مفهومها وآليات مكافحتها. مجلة الحقوق والعلوم الانسانية، صفحة 205.
2. المادة 1 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.

3. أيمن العسقلاني. (2023م). الجرائم المعلوماتية كأحد عوائق الاتصال المؤسسي بدول مجلس التعاون الخليجي. المجلة الدولية للاعلام والاتصال، صفحة 80.
4. ثنينان آل ثنيان. (2012م). إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية. رسالة ماجستير، جامعة نايف للعلوم الأمنية، صفحة 22.
5. حسام بن ميسية، عبد المولى حملاوى. (2025م). آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري. رسالة ماجستير، معهد الحقوق، المركز الجامعي عبد الحفيظ بو الصوف ميله، صفحة 17.
6. حمزه السلمي. (بدون معلومات سنة النشر). الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي. مجلة الجامعة العراقية، صفحة 588.
7. رضا المهدي. (2021م). الجرائم السيبرانية وآليات مكافحتها في لتشريع الجزائري. مجلة إيليزا للبحوث والدراسات، صفحة 114.
8. روان الصحفي. (2020م). الجرائم السيبرانية. المجلة الالكترونية الشاملة متعددة التخصصات، صفحة ص8.
9. سميرة بيطام. (2023م). تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية. مجلة كلية القانون والعلوم السياسية، صفحة 111.
10. عبد الحليم يعقوب. (2014م). الإعلام الجديد والجريمة الإلكترونية. الدار العالمية للنشر، صفحة 223.
11. عبد الله العجمي. (2014م). المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة. رسالة ماجستير، جامعة الشرق الأوسط، صفحة 20.
12. علي قويدري، أمال العيش. (2022م). الجريمة السيبرانية مفهومها وسبل الوقاية منها. مجلة نوميرس الاقتصادية، صفحة ص194.
13. مراد قاسم. (2024م). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية دراسة مقارنة. المجلة العصرية للدراسات القانونية، صفحة 100.
14. نبيلة هروال. (2014م). جرائم الانترنت دراسة مقارنة. إطروحة دكتوراه كلية الحقوق والعلوم السياسية، جامعة جامعة أبي بكر بلقايد – تلمسان، صفحة 37.
15. نور الهدى قادري. (2023م). الجريمة السيبرانية وآليات مكافحتها – مواجهة تحديات الأمن السيبراني. المجلة الجزائرية للحقوق والعلوم السياسية، صفحة 324.
16. نورهان الربيعي. (2024م). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). مجلة الفارابي للعلوم الإنسانية، صفحة 83.
17. نورهان الربيعي. (2024م). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). مجلة الفارابي للعلوم الإنسانية، صفحة 84.
18. نورهان الربيعي. (2024م). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). مجلة الفارابي للعلوم الإنسانية، صفحة 84.
19. ينظر المادة 1 من قرار وزير العدل رقم 26 لسنة 2016م بشأن انشاء إدارة مكافحة ابحاث الجريمة الالكترونية بمركز الخبرة القضائية والبحوث.

20. ينظر المادة 11-12 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
21. ينظر المادة 13-14 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
22. ينظر المادة 15-16 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
23. ينظر المادة 3-4 من قرار رقم 28 لسنة 2013 م بإنشاء الهيئة الوطنية لأمن وسلامة المعلومات.
24. ينظر المادة 52 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
25. ينظر المواد 19-22 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
26. ينظر المواد 24-26-28 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.
27. ينظر المواد 47-50-51 من قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية.