Journal of Libyan Academy Bani Walid 2025
مجلة الأكاديمية الليبية بني وليد
e-ISSN: 3104-3860
Volume 1, Issue 4, 2025, Pages: 268-278
Website: https://journals.labjournal.ly/index.php/Jlabw/index

Cybercrimes And Combating Mechanisms In International Law

Hana Almabrouk Khalifa Altayari *
Assistant Professor, Department of International Law, Faculty of Law, Surman, University of Sabratha, Libya.
Email: hanaaltayari2022@gmail.com

الجرائم الإلكترونية وآليات مكافحتها في القانون الدولي

هناء المبروك خليفة الطياري*
أستاذ مساعد بقسم القانون الدولي -كلية القانون صرمان -جامعة صبراتة – ليبيا.

Received: 28-08-2025	**Accepted:** 15-10-2025	**Published:** 06-11-2025

Abstract
The digital revolution, which has touched all areas of life, has led to the emergence of a new type of crime known as cybercrime, which has posed numerous challenges in the modern era. Therefore, this study aims to define cybercrime by explaining its definition, characteristics, and classifications. It also aims to identify mechanisms for combating these crimes, such as international agreements, some of the efforts of international organizations, and cooperation between countries to combat this crime. It also addresses the challenges it faces, such as legal challenges, the most important of which are: conflicting national laws and protecting national sovereignty, and technical challenges, including the development of technological means and the use of encryption and hidden systems. This study highlights the main problem of this research: to what extent are international efforts sufficient and effective in combating cybercrime? This study adopts a descriptive approach to clarify the concept of cybercrime and define its characteristics and classifications. It also uses an analytical approach to analyze the legal texts contained in international agreements, and a critical approach to evaluate the effectiveness of international legal mechanisms to combat cybercrime**.**

Keywords: Cybercrime – Combating mechanisms – International agreements – International efforts – International organizations.

الملخص
إن الثورة المعلوماتية التي لامست جميع مجالات الحياة أدت إلى ظهور نوع جديد من الجرائم عرفت باسم الجرائم الإلكترونية التي أصبح لها العديد من التحديات في العصر الحديث، لذلك تهدف هذه الدراسة لتحديد مفهوم الجرائم الإلكترونية وذلك من خلال بيان تعريفها وخصائصها وتصنيفاتها، ومعرفة آليات مكافحة هذه الجرائم كالاتفاقيات الدولية وبعض جهود المنظمات الدولية والتعاون بين الدول لمكافحة هذه الجريمة والتحديات التي تواجهها كالتحديات القانونية ومن أهمها: تعارض القوانين الوطنية وحماية السيادة الوطنية، والتحديات التقنية والتي من بينها تطور الوسائل التكنولوجية واستخدام التشفير والأنظمة

المخفية، ومن خلال ذلك تظهر لنا الإشكالية الرئيسية لهذا البحث والمتمثلة في إلى إي مدى تعتبر الجهود الدولية كافية وفعالة في مكافحة الجرائم الإلكترونية؟ وتعتمد هذه الدراسة على المنهج الوصفي لبيان مفهوم الجرائم الإلكترونية وتحديد خصائصها وتصنيفاتها، والمنهج التحليلي لتحليل النصوص القانونية الواردة في الاتفاقيات الدولية، والمنهج النقدي لتقييم مدى فاعلية الآليات القانونية الدولية لمكافحة الجرائم الإلكترونية.

الكلمات المفتاحية : الجرائم الإلكترونية – آليات المكافحة – الاتفاقيات الدولية – الجهود الدولية – المنظمات الدولية.

المقدمة

تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وفي ظل الثورة الرقمية المتسارعة، أصبحت الجريمة الإلكترونية واحدة من أخطر التحديات التي تواجه النظام القانوني الدولي المعاصر، فقد تجاوزت هذه الجرائم النطاق المحلي لتأخذ طابعاً عابراً للحدود، وهذه الجرائم لم تعد تقتصر على أعمال الاختراق أو القرصنة التقليدية، بل باتت تشمل أنظمة معقدة ومتطورة، مثل الهجمات على البنى التحتية الحيوية، والابتزاز الرقمي، والاحتيال المالي، والتجسس الإلكتروني، بل وحتى التأثير على السياسات العامة للدول.

وقد برزت محاولات دولية متعددة لمواجهة هذا النوع من الجرائم، تمثلت في إبرام اتفاقيات ومعاهدات إقليمية ودولية، مثل اتفاقية بودابست اعام 2001، إلى جانب تأسيس آليات للتعاون بين الدول عبر منظمات دولية متخصصة، كالإنتربول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة. إلا أن هذه الجهود لا تزال تواجه تحديات فعلية، وهذا ما يفرض ضرورة تكاثف الجهود الدولية لمكافحتها.

أهمية البحث:

تبرز أهمية البحث من الناحية العلمية بالمساهمة في إثراء المعرفة القانونية الدولية، وفهم أعمق لهذه الظاهرة، وإبراز مواطن الضعف والنقص في الاتفاقيات الدولية القائمة في ظل غياب اتفاقية دولية موحدة تجرم جميع الجرائم الإلكترونية. أما من الناحية العملية فتبرز أهمية البحث في عرض حلول عملية لمكافحة هذه الجرائم، ودعم صناع القرار وحماية الحقوق والحريات، ورفع الوعي القانوني والتقني، وتشجيع التعاون القانوني.

أهداف البحث:

1- بيان مفهوم الجرائم الإلكترونية، وعرض خصائصها.
2- تحديد طرق مكافحة الجرائم الإلكترونية.
3- بيان التحديات التي تواجه مكافحة الجرائم الإلكترونية.

منهج البحث:

تعتمد هذه الدراسة على المنهج الوصفي وذلك في وصف الجرائم الإلكترونية وتصنيفاتها، والمنهج التحليلي لتحليل النصوص القانونية للاتفاقيات الدولية ذات الصلة بموضوع البحث، وكذلك المنهج النقدي في تقييم مدى فاعلية الآليات القانونية الدولية لمكافحة الجرائم الإلكترونية.

نطاق البحث: يقتصر نطاق دراسي في هذا البحث على دراسة مفهوم الجرائم الإلكترونية، والأليات الدولية لمكافحة هذه الجرائم، وما تواجهه من تحديات.

إشكالية البحث:

تتمثل الإشكالية الرئيسية للبحث في مدى فاعلية التشريعات الدولية في مكافحة الجرائم الإلكترونية والحد من انتشارها؟
وللإحاطة بكل جوانب الموضوع أدرجنا التساؤلات الفرعية التالية

1- ما هو مفهوم الجرائم الإلكترونية وماهي خصائصها وأنواعها؟
2- ماهي آليات مكافحة الجرائم الإلكترونية؟
3- ماهي التحديات التي تواجه مكافحة الجرائم الإلكترونية؟

خطة البحث:

تم تقسيم البحث إلى مطلبين: تناولت في (المطلب الأول) مفهوم الجرائم الإلكترونية، خصصت الفرع الأول لبيان تعريف الجرائم الإلكترونية وبيان خصائصها، وفي الفرع الثاني تناولت تصنيفات الجرائم الإلكترونية، وتطرقت في (المطلب الثاني) لبيان مكافحة الجرائم الإلكترونية في القانون الدولي والتحديات ذات الصلة، تناولت الجهود الدولية لمكافحة الجرائم الإلكترونية في الفرع الأول، بينما أفردت الفرع الثاني لبيان التحديات التي تواجه مكافحة الجرائم الإلكترونية.

المطلب الأول -مفهوم الجرائم الإلكترونية

إن مفهوم الجرائم الإلكترونية ظهر نظراً للتطورات التكنولوجية التي شهدها العالم، وأصبحت الأجهزة الإلكترونية جزءاً مهماً في الحياة اليومية للإنسان (لطفي، 2019، صفحة ص 156)، لذلك سنتناول في هذا المطلب مفهوم الجرائم الإلكترونية، وذلك من خلال التطرق إلى بيان تعريف الجرائم الإلكترونية والتعرف على خصائصها في الفرع الأول، ومن تم نخصص الفرع الثاني لبيان تصنيفات الجرائم الإلكترونية، وذلك على النحو التالي:

الفرع الأول – تعريف الجرائم الإلكترونية وبيان خصائصها:

أولاً-تعريف الجرائم الإلكترونية:

لم يتوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وبالتالي تعددت التعريفات التي قدمها الفقه والقضاء للجريمة الإلكترونية ويرجع السبب في ذلك إلى اختلاف الزاوية المنظور من خلالها إلى تلك الجرائم، فهناك جانب من الفقه يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبيها أو استنادا لمعايير أخرى حسب القائلين بها (حجازي د.، 2019، صفحة 12)، فعرفها البعض بالاعتماد على الوسيلة المستخدمة في ارتكابها بأنها: (الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام حاسب) (حجازي ع.، 2006، صفحة 24)، وبعبارة أخرى (تلك الجرائم التي يكون دور الحاسب الآلي فيها إيجابياً أكثر منه سلبياً)، ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها:(الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً)، أما منظمة التعاون الاقتصادي والتنمية (OECD) فقد عرفتها بأنها (كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية) (عفيفي، 2003، صفحة 3)، وتعرف الجريمة الإلكترونية أيضا بأنها (نمط من أنماط الجرائم المدونة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات)، كما تم تعريف الجريمة الإلكترونية بالاعتماد على معيار شخصي يستوجب أن يكون فاعل هذه الجرائم ملماً بتقنية المعلومات، واستخدام الحاسوب لإمكانية اعتبارها من الجرائم الإلكترونية ، وتم تعريف الجرائم الإلكترونية وفقاً لهذا المعيار بأنها(أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب)، كما تم تعريفها أيضاً بأنها(أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسه لمرتكبه والتحقيق فيه وملاحقته قضائياً).وتم تعريف الجرائم الإلكترونية كذلك بالاستناد لمعايير أخرى حيث تمت الإشارة إلى تعريفات متعددة منها. من أمثلتها تلك التي عرفتها بأنها:(الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح)، كما عرفت بأنها: (فعل إجرامي، أيا كانت صلته بتقنية المعلومات، فيه يتكبد المجني عليه نتيجة له خسارة ويحقق الفاعل ربحاً عمدياً) (الشواء، 1993، صفحة 516).

كما هناك تعريفات تعتمد على معيار محل الجريمة ووسيلة ارتكابها "الكمبيوتر"، وتعرف الجريمة الإلكترونية وفق هذا المعيار بأنها:(أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب)، وكما تم تعريفها بأنها:(الجريمة التي يستخدم فيها الحاسوب كوسيلة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها) (محمد، 2018، صفحة 437).

وتعرف الجرائم الإلكترونية باختصار على أنها (الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال) (محمد و الجليدي، 2024، صفحة 4).

ثانياً -خصائص الجرائم الإلكترونية: -

للجرائم الإلكترونية خصائص تجعل من الصعب الانتباه إليها، مما يجعل محاربتها صعبة ومعقدة للغاية، وأهم هذه الخصائص هي كما يلي:

1- صعوبة اكتشاف الجريمة الإلكترونية وإثباتها:

يعود هذا لقدرة الجاني على التخفي وإخفاء أداة الجريمة وآثارها، فالكشف عن الجريمة الإلكترونية تحتاج لوقت طويل للكشف عنها أو تكتشف بمحض الصدفة ويعود هذا لقدرة الجاني على تدمير الأدلة بسهولة وبوقت قصير جدا قد لا يتجاوز الدقيقة الواحدة (بورشاق ز.، 2022، صفحة 244) ،ومن الأمثلة على ذلك قيام الجاني بإرسال فيروسات إلى جهاز المجني عليه أو سرقة بياناته والتجسس عليه دون علمه (القهيوي، 2023، صفحة 15).

2-الجريمة الإلكترونية عابرة للحدود:

مثل هذه الجرائم لها أبعاد دولية، تتخطى آثارها ونتائجها أكثر من دولة، فتؤدي إلى حدوث أضرار مادية ومعنوية تمس مصالح أساسية للدول، والنظام العام فيها، سواء على الصعيد الأمني أو الاقتصادي أو الاجتماعي، لذلك اتفق أغلب الفقهاء والمشرعين على أن الجرائم الإلكترونية تعد من جرائم أمن الدولة (الجمل، 2022، صفحة 14).

3-وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات:

من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعلومات الخاصة للكمبيوتر في أي مرحلة من مراحل تشغيل المعالجة الآلية للبيانات، سواء في مرحلة إدخال البيانات، أو عند مرحلة المعالجة، أو أثناء مرحلة إخراج

المعلومات، وتعد هذه الخاصية شرط أساسي لابد من توافره حتى يمكننا البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، وبتخلفه تنتفي الجريمة الإلكترونية (الشكري، 2008، صفحة 115).

4- الجريمة الإلكترونية جريمة مستحدثة:

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، فلا غرابة أن تعد الجرائم الإلكترونية سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكانياته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها (العجمي، 2014، صفحة 25).

5- جرائم هادئة:

"إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر (محمد د.، 2018، صفحة 442) ،وقد يقوم الجاني بجريمته بشكل غير ملحوظ لتمتعه بالقدرات الفنية التي تمكنه من ارتكاب جريمته بدقة، بحيث لا يستطيع المجني عليه ملاحظة ذلك (بلواح، 2020، صفحة 42).

6- الجريمة الإلكترونية جريمة مغرية للمجرمين:

نظراً للصفات التي تتمتع بها مثل هذه الجريمة، والصعوبات التي تثور عند محاولة اكتشافها أو ملاحقتها، فإن ذلك يشكل إغراء كبير للمجرمين وخصوصاً أنه يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم، ونتيجة لكل ما سبق تعد مثل هذه الجرائم جريمة تستهوي الكثيرين لسهولتها، وكثرة مكاسبها (العجمي، 2014، صفحة 22).

7-الجرائم **الإلكترونية يتميز فيها المجرم بكونه مجرم عائدا إلى الإجرام:** أي بمعنى أن المجرم يعود كثيرا إلى ارتكاب جرائم أخرى في مجال الحاسب الآلي، انطلاقاً من الرغبة في سد الثغرات أو التوصل إلى أهداف أو سرقة الأموال أو الابتزاز، إضافة إلى سبب عدم كشفهم وسهولة ارتكاب الجريمة وإخفاء الأدلة (الكريم، 2023، صفحة 97).

الفرع الثاني – تصنيفات الجرائم الإلكترونية: -

هناك إجماع بين فقهاء القانون والمختصين على أن الجرائم الإلكترونية ليست محصورة في فئة أو نوع واحد، وأن هناك اختلاف في التصنيفات التي وضعت لها (بنوسي، 2024، صفحة 125)، وعليه تصنف الجرائم الإلكترونية إلى نوعين من هذه الجرائم. الأول هو جريمة المعلومات على شبكة الإنترنت هذا عندما يستهدف مرتكبو الجرائم الإلكترونية الانترنت. أما بالنسبة للجريمة الثانية غير المعلوماتية في الانترنت، أي عندما يكون الانترنت وسيلة لارتكاب جرائم إلكترونية.

أولاً-الإجرام المعلوماتي على الإنترنت: -

1-القرصنة: يقصد بها قرصنة أجهزة الحاسب بالقنابل البريدية والفيروسات المدمرة بغرض اتلاف البيانات والمعلومات لغرض التخريب، وهذا يشكل خطورة أمنية كبرى عندما يتم اقتحام خوادم البنوك والمؤسسات الحكومية السيادية لتخريب ما بها من بيانات ومعلومات أو سرقتها (زعتر، 2023، صفحة 72).

2-نشر الفيروس: تتحقق هذه الجريمة بقيام الجاني بإدخال أو تبديل أو محو بيانات في النظام المعلوماتي بطريقة غير مشروعة لتحقيق أغراض قانونية، وكذلك إتلاف وإفساد برامج ومكونات النظام المعلوماتي بواسطة إدخال فيروسات تتسبب في إحداث شلل تام أو جزئي لمكونات النظام (بشينة، 2024، صفحة 505).

3-القنابل الإلكترونية: أو ما يعرف باسم الشفرات، وهي جزء خبيث من التعليمات البرمجية يتم إدخاله قصداً في البرنامج لتنفيذ مهمة ضارة عند تفعيلها بواسطة حدث معين، فهو ليس فيروساً رغم أنه عادة ما يتصرف بطريقة مماثلة حيث يتم إدخاله خلسة في البرنامج فيظل في وضع السكون حتى تستوفي الشروط المحددة.

4-اقتحام الويب: وذلك بهدف محاولة التحكم بموقع الويب بطريقة احتيالية، حتى يتحكم بتغيير محتوى الموقع الأصلي أو حذف بيانات من عليه، فقد تم الإبلاغ عن حالات طلب فيها المهاجم فدية، وحتى نشر مواد فاحشة على الموقع.

5- المطاردة السيبرانية: تستخدم كأداة من قبل الدول لمحاربة خصومها، كما أن هذه الهجمات باتت هدفاً للتنظيمات التي تسعى من خلالها إلى تحقيق مكاسب مالية، وقد يتم استخدام هذه الهجمات أيضاً لغرض الانتقام من بعض أنظمة الحكم نتيجة مواقفهم السياسية، الآمر الذي دفع العديد من دول العالم إلى وضع استراتيجيات متكاملة لمواجهتها، ورفع ميزانيتها المتعلقة بالأمن السيبراني، ومن أهم الهجمات التي تعرضت لها الدول على سبيل المثال الهجمات السيبرانية الروسية ضد منشآت الطاقة الأوكرانية من عام 2015 إلى عام 2022 (الباسوسي، 2023، صفحة 150).

6-سرقة الهوية: تحدث سرقة الهوية عندما يسرق شخص ما هويتك ويتظاهر بأنه انت للوصول إلى الموارد المالية للضحية: مثل بطاقات الائتمان والحسابات المصرفية والمزايا الأخرى باسمك (الصغير، 2013، صفحة 45).

7-التلاعب بالبيانات: هو تغيير غير مصرح به للبيانات قبل أو أثناء الدخول إلى نظام الحاسوب ثم تغييرها مرة أخرى بعد انتهاء المعالجة، أي أنه يتم تغيير المعلومات الاصلية التي سيتم إدخالها، إما عن طريق شخص يكتب البيانات أو فيروس

مبرمج لتغيير البيانات، أو مبرمج قاعدة البيانات أو التطبيق أو أي شخص آخر يشارك في عملية الإنشاء والتسجيل أو ترميز البيانات أو فحصها أو تحويلها أو نقلها (غانم، 2023، صفحة 27).

ثانياً-الإجرام غير المعلوماتي في شبكة الإنترنت: -

1-الابتزاز: ونقصد بهذا استخدام الانترنت لمضايقة أو تهديد شخص ما بصفة مستمرة، كما يتضمن تعقب هذا الشخص في الحياة الواقعية والظهور في منزل هذا الشخص وعمله مهددين أملاكه بل وعائلته، أي يمكننا القول إنها عملية تهديد إلكترونية وفعلية للضحية، وقد لا يكون التهديد في البداية عبر الانترنت اتصالا فعليا، إلا أنه يمكن أن يتطور وقد يؤدي لاستخدام العنف، ولهذا السبب فهي جريمة خطيرة (لخضر، 2023، صفحة 512).

2-تجارة الجنس والدعارة: والتي تتم على مواقع إلكترونية مخصصة، هدفها تجاري يستغل فيه بعض الفئات كالأطفال والنساء لغايات جدب عملاء إلكترونيين والترويج للمثلية من خلال إعلانات إشهارية غير أخلاقية والتي تدر عليهم مبالغ طائلة، وهذه الممارسات قد تكون سبباً لجرائم إلكترونية ذات طبيعة جنسية عبر الفضاء الإلكتروني، وهذا كله يؤدي لترويجها كسلعة استهلاكية خاصة بدول العالم الإسلامي (غانم، 2023، صفحة 25).

3-التجسس الإلكتروني على الحكومات: غير خاف أن التطور في المجال الإلكتروني المعلوماتي سهل من مهمة التجسس، فالمجرم الإلكتروني سواء كان شخص واحد أو تنظيم يمكنه التجسس سواء على الأشخاص أو المنظمات وحتى الدول أو أجهزتها، ويأخذ التجسس عدة صور، فقد يكون تجسس اقتصادي أو عسكري أو سياسي (محمد د.، 2018، صفحة 449).

4-السب والقذف والتشهير: تعد من الجرائم الإلكترونية واسعة الانتشار عبر الشبكات، حيث تستخدم أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته، وقد يكون عبر خطوط الاتصال أو عبر البريد الإلكتروني أو عبر صفحات الويب، أو عبر غرف المحادثة أو الدردشة (الكعبي، 2009، صفحة 114).

5-الاعتداء على الحياة الشخصية للأفراد: ويقصد بها كأن يقوم الفاعل بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكنه يطلع الغير عليها دون إذنه، ومن صور التعدي على حرمة الحياة الخاصة تسجيل المحادثات الشخصية، أو مراقبتها بأي وسيلة، والتصنت على المكالمات بطرق غير مشروعة (حسين، 2011، صفحة 7).

6-السرقة والنصب والاحتيال: يعد هذا النوع من الجرائم واسع الانتشار عبر الانترنت، وذلك بسبب عدم وضوح المصدر بالنسبة لمستخدمي هذه الشبكة، فضلاً على عدم توفر سبل الحماية اللازمة للحد من تلك الجرائم، ولعل أشهر صورها النصب ببطاقات الائتمان والذي يكون إما من حاملها الشرعي أو من الغير، وإن من بين الوسائل المعتمدة في تلك الجرائم عبر الانترنت هي وسيلة البريد الإلكتروني (الملط، 2006، صفحة 203).

7-الاعتداء على الملكية الفكرية: قد صنفها مكتب الأمم المتحدة للمخدرات والجريمة من خلال استبيان تم عرضه على الدول ومنظمات القطاع الخاص والمنظمات الحكومية الدولية إلى ثلاث فئات:

أ-الأفعال الماسة بسرية المعلومات وحماية بيانات الحاسب، كالدخول غير المشروع لجهاز الحاسب واختراق الخصوصية.

ب- الأعمال ذات الصلة بأجهزة الحاسب الشخصية التي تسبب الضرر.

ج- الأفعال ذات الصلة بمحتويات الحاسب كإنتاج وحيازة الصور الإباحية (زعتر، 2023، صفحة 72).

المطلب الثاني: مكافحة الجرائم الإلكترونية في القانون الدولي والتحديات ذات الصلة: -

تتضمن مكافحة الجرائم الإلكترونية تكاثف الجهود الدولية كإبرام الاتفاقيات الدولية والتعاون بين الدول لتبادل المعلومات والخبرات، وتطوير أساليب موحدة، ووضع الأطر القانونية المناهضة لها، وهو ما سنتطرق إليه في الفرعيين التاليين، وذلك كما يلي:

الفرع الأول: آليات مكافحة الجرائم الإلكترونية: سنتطرق في هذ الفرع إلى بيان آليات مكافحة الجرائم الإلكترونية والتي من بينها الاتفاقيات الدولية ذات الصلة، والمنظمات الدولية، والتعاون الدولي لمكافحة الجرائم الإلكترونية وذلك على النحو التالي:

أولاً-الاتفاقيات الدولية

1- اتفاقية بودابست 2001 بشأن الجريمة السيبرانية: دخلت هذه الاتفاقية حيز التنفيذ سنة 2004، وتسمى بالاتفاقية الأوروبية لجرائم الانترنت، وتتكون من 44 مادة موزعة على عدد من الأبواب، (شوقي، 2019، صفحة 46)، وتعد هذه الاتفاقية أول اتفاقية دولية شاملة بشأن التصدي للأفعال الإجرامية، التي تتم ضد أو بواسطة الحاسبات الآلية وشبكات الاتصالات المعقودة في مدينة بودابست بالمجر في 11/23/ 2001 من قبل (26) دولة من الاتحاد الأوروبي، إضافة إلى كندا واليابان وجنوب افريقيا والولايات المتحدة الأمريكية، حيث ركزت الاتفاقية على ثلاثة محاور أساسية هي (شحادة، 2006، صفحة 20):

أ-تنسيق التشريعات الوطنية.

ب-وضع أساليب تسهل اجراء التحقيقات والملاحقة الجزائية عبر شبكات الأنظمة الإلكترونية.
ج- وضع نظام تعاون دولي سريع وفعال (صالح و حسين، 2022، صفحة 15).
وفي عام 2003 تم وضع بروتوكول إضافي بهدف التأكيد على مضمون اتفاقية بودابست، وفي عام 2022 تم وضع البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية (فيالة، 2024، صفحة 843).
2- اتفاقية أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي 2014: تعتبر اتفاقية ذات طابع إقليمي تضم دول الاتحاد الافريقي، لغرض تدارك انتشار الجرائم الإلكترونية التي تشكل تهديداً حقيقياً لأمن الاتحاد، وتهدف إلى تحديد الأهداف والتوجهات الرئيسية لمجتمع المعلومات في افريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيا المعلومات والاتصال للدول الأعضاء والمجموعة الاقتصادية الدولية وكفالة الأمن المعلوماتي والإطار القانوني الضروري لظهور اقتصاد المعرفة في أفريقيا، وتهدف أيضا إلى تحديث القوانين الجنائية في قمع الجريمة الإلكترونية من خلال وضع سياسات لاعتماد جرائم جديدة خاصة بتكنولوجيا المعلومات والاتصالات ومواءمة نظام العقوبات الموجود فعلياً في الدول الأعضاء مع المناخ التكنولوجي الحديث، وقد حددت الاتفاقية الجرائم الخاصة بتقنية المعلومات في :
أ-الهجمات على أنظمة الكمبيوتر.
ب- الخروقات على البيانات المحوسبة.
ج-الجرائم ذات صلة بالمحتوى.
د- الجرائم المتعلقة بإجراءات تأمين الرسائل الإلكترونية (الشارفي، 2024، صفحة 121).
3- اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية: اعتمدت الجمعية العامة للأمم المتحدة اتفاقية جديدة ملزمة قانوناً تهدف إلى منع ومكافحة الجريمة السيبرانية، لتتوج بذلك عملية تفاوض استمرت خمس سنوات، حيث اكتملت صياغة مسودتها النهائية في 9 أغسطس 2024، وسيتم فتح الاتفاقية للتوقيع في حفل رسمي تستضيفه فيتنام في عام 2025، وستدخل الاتفاقية حيز التنفيذ بعد 90 يوماً من تصديق الدول الأربعين عليها، وتهدف هذه الاتفاقية إلى زيادة فعالية جهود منع ومكافحة الجرائم السيبرانية، بما في ذلك من خلال تعزيز التعاون الدولي وتوفير الدعم الفني وبناء القدرات، خاصة إلى الدول النامية (المتحدة، 2024).

ثانياً-المنظمات الدولية ذات الصلة

1-منظمة **الإنتربول:** أنشأت المنظمة الدولية للشرطة الجنائية (الإنتربول) خلال عام 2004م، وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات لمواجهة هذا النوع من الجرائم، وذلك من خلال (هروال، 2007، صفحة 153) :
أ- إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار(24) ساعة 7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف .
ب-استخدام وسائل حديثة في تلك المكافحة، كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج Excalibur للتحليل والمقارنة الأتوماتيكية لتلك الصور.
ت- تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها (نمر و بوكرشيدة، 2021-2020، صفحة 29).
وتعد شرطة الانتربول منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود الوطنية للدول، بما فيها الجرائم المعلوماتية، وذلك ما أكدته نتائج الدورة رقم (77) للجمعية العامة لمنظمة الانتربول، حيث دعا الأمين العام للإنتربول السيد "بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صوره بما فيه الإرهاب المعلوماتي، وقد نجحت المنظمة الدولية للشرطة الجنائية الإنتربول خلال الأعوام الأخيرة في جعل اسمها من أكثر الأسماء التي يخشاها المجرمون (المصري، 2011، صفحة 100).
2- **منظمة اليوروبول:** أنشأ جهاز اليوروبول في عام 1995 واعتمد في عام 1999م، كوكالة تابعة للاتحاد الأوروبي كأهم آلية في مكافحة الجريمة الإلكترونية، ومن نشاطات جهاز اليوروبول في مجال مكافحة الجريمة الإلكترونية أعلنت اليوروبول نتيجة لاتفاق مشترك في ديسمبر 2020 (عرفة و حوري، 2025)، عن إطلاق "منصة فك تشفير مبتكرة" ضمن اختصاصها والتي ستديرها مركز الجرائم الإلكترونية الأوروبي EC3 وتطويرها بالتعاون الوثيق مع مركز البحوث المشتركة للاتحاد الأوروبي، ويستخدم اليوروبول بالفعل أساليب تحليل البيانات المتقدمة لمكافحة جرائم الانترنت بفعالية تشمل هذه الأساليب مجموعة من التقنيات المتقدمة بما في ذلك :رصد البيانات الرقمية، وتقنيات الذكاء الاصطناعي، ودعم التحقيقات وتحديد الضحايا والمشتبه بهم، ومن الآليات الدولية لليوروبول في الحد من الجرائم الإلكترونية تبادل المعلومات بين الدول، وتنسيق التدابير الإدارية وغير الإدارية، وتسهيل تسليم المجرمين عبر الحدود (عرفة و حوري، 2025).

ثالثاً-التعاون الدولي لمكافحة الجريمة الإلكترونية:

يعتبر التعاون الدولي من أهم أساليب مكافحة الجرائم الإلكترونية وملاحقة مرتكبيها، فبغير ذلك التعاون الدولي سيرتفع معدل ارتكاب تلك الجرائم، وذلك لعدم وجود اتفاقيات وآليات موحدة للقبض على مرتكبيها وكيفية التعامل معهم، مما يؤدي إلى إفلاتهم من العقاب، ويقتضي التعاون الدولي التخفيف من تلك الفوارق بين القوانين العقابية الوطنية، لأن التنافر بين هذه الأنظمة يجعل المجرمين يبحثون عن الأنظمة القانونية التي تعاقبهم أو التي ترأف بحالهم (أنور، 2010، صفحة 545)، ولتكريس هذا التعاون لابد من التركيز على الانضمام للمعاهدات الدولية في مجال مكافحة الجرائم المعلوماتية، وتوحيد القوانين بين الدول المختلفة والمتعلقة بمكافحة الجرائم المعلوماتية (الزبدي، 2033، صفحة 128). ومن صور التعاون الدولي ما يلي:

1- التحقيق: يعرف التحقيق بأنه: "عمل قانوني يقوم به المختصون في ضبط الجرائم المعلوماتية من فاعل ودليل إلكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذا النوع من الجرائم لإقامة العدل" (موسى، 2009، صفحة 166)، وهناك مجموعة من الإجراءات التي يجب الالتزام بها عند القيام بالتحقيق الابتدائي في الجرائم الإلكترونية ومن بين هذه الإجراءات (السوفي، 2017، صفحة 14)مثلاً: معاينة مسرح الجريمة ، وذلك لضمان آلية منظمة للتحقيق في مسرح الجريمة، وتوثيق حالة مسرح الجريمة، وتوثيق الجهاز المستخدم في الجريمة والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة، وتوثيق أجهزة التخزين مثل الأقراص المضغوطة الموجودة في مسرح الجريمة ، وتصوير مسرح الجريمة، وحفظ الأدلة والمواد الرقمية، وحفظ الوثائق المطبوعة، وحفظ الأجهزة، إجراء استرجاع للوثائق العالقة والملغاة أو التي تم حذفها، ونقل الأدلة التي يتم ضبطها (الباقي، 2018، صفحة 286).

2- التسليم: ويكون ذلك في حالة إذا ما امتنعت الدولة عن اتخاذ الإجراءات الجزائية المطلوبة، بحق المتهم الموجود في إقليمها، حيث يقع عليها واجب تسليمه إلى الدولة المعنية بالجريمة المرتكبة، لتقوم بمحاكمته وفقاً لقوانينها، ونظراً لأهمية الجهود الدولية في مكافحة الجرائم الإلكترونية، فقد أصدرت منظمة الأمم المتحدة قرارها رقم (63/55) في 4- 12- 2000 اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات للأغراض الإجرامية دعت فيها إلى (تعزيز التعاون بين الدول في مكافحة إساءة استعمال السلطة لأغراض إجرامية) (صالح و حسين، 2022، صفحة 14)، كما عقدت العديد من المؤتمرات لمواجهة جرائم الحاسب الآلي، منها مؤتمر جرائم الحاسب الآلي الدولية الذي عقد في الفترة من 29- 2000/5/31م، بمدينة أوسلو النرويجية، شاركت فيه العديد من الدول والهيئات والمنظمات الدولية، وتم التطرق فيه إلى أنواع جرائم الحاسب الآلي والتحديات الفنية والقانونية والتشغيلية التي تعيق مواجهة هذه الجرائم (عبابنة، 2005، صفحة 180).

3-المساعدة القانونية المتبادلة: يتعين على مقدمي الخدمات الالتزام بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من قانون 04/09 تحت تصرف السلطات المختصة، كما يتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق (شوقي، 2019، صفحة 71).

الفرع الثاني: التحديات الدولية التي تواجه مكافحة الجرائم الإلكترونية:

على الرغم من الجهود الدولية المبذولة في مكافحة الجرائم الإلكترونية، إلا أن ثمة تحديات ومعوقات تقف دون تحقيق هذه الجهود، وهو ما سنتناوله في هذا الفرع على النحو التالي

أولاً-التحديات القانونية

تتعدد التحديات القانونية التي تحول دون تحقيق التعاون الدولي ومن أهم هذه التحديات: القصور التشريعي للدول لاختلاف نظمها القانونية، وتحديات تتعلق بتنازع الاختصاص القضائي فيما بين الدول، وأخرى تختص بتسليم المجرمين والإنابة القضائية.

1- **القصور التشريعي للدول لاختلاف نظمها القانونية**: يعني عدم وجود نظام قانوني لدى الدول خاص بمكافحة الجرائم الإلكترونية، فما يكون مباحا في أحد الأنظمة قد يكون مجرما في نظام آخر، ويرجع ذلك لعدة أسباب منها:

أ- اختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع إلى أخر وبالتالي اختلاف السياسة التشريعية من مجتمع إلى أخر (عبدالهادي، 2020، صفحة 50).

ب- طرق التحري والتحقيق والمحاكمة التي تكون فعالة في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كالمراقبة الإلكترونية، وطرق جمع الاستدلالات بالتجسس المأذون به من قبل السلطات المختصة قد يكون أمرًا متاحًا وقانونيًا في دولة ما في حين يعتبر من قبيل التعدي على الحقوق والحريات العامة وبالتالي غير مشروع في دولة أخرى، ونجد أن الكثير من الوثائق الدولية تشجع الدول الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة وهذا من شأنه التخفيف من حدة الاختلاف الكبير بين النظم القانونية الإجرائية، ويساهم في الدفع نحو التعاون الدولي بشكل فعال (بشينة، 2024، صفحة 512).

2- **تنازع الاختصاص القضائي فيما بين الدول:** تثير الجرائم المعلوماتية العديد من المشكلات نظراً لطبيعتها الخاصة المعقدة والسرعة التي يتم فيها ارتكابها، وقدرة الجناة على الهرب والتخفي، بالإضافة إلى أنها عابرة للحدود والقارات، فقد يتم ارتكاب هذه الجرائم داخل نطاق إقليمي لدولة وتحقيق آثارها خارج هذا النطاق، مما يؤدي إلى تعقيدات كبيرة في تحديد الاختصاص القانوني والقضائي لهذه الجرائم (مخيمر، 2023، صفحة 506)،كما لا يمكن لدولة ما أصدرت الحكم بالإدانة على أحد مرتكبي هذه الجرائم أن تلزم الدولة التي يتواجد بها المجرم على تطبيق العقوبة عليه وذلك احتراما لسيادة تلك الدولة، وتطبيقاً لمبدأ إقليمية النص الجزائي الذي ينص على أن قواعد القانون الجنائي لا تطبق إلا في حدود الإقليم الخاضع لسيادة الدولة، وكما أن الدول تختلف عن بعضها البعض في موضوع الجرائم الإلكترونية من حيث اعتبار الفعل المرتكب عبر شبكة الانترنت والحواسيب جريمة أم لا، ويرجع سبب ذلك إلى القيم القانونية والسياسية والأخلاقية والثقافية لكل دولة (القهيوي، 2023، صفحة 75)، إذا تثير مسألة الاختصاص في الجرائم الإلكترونية على المستوى الدولي مشكلة تتعلق باختلاف التشريعات والنظم القانونية من دولة لأخرى، والتي قد ينجم عنها تنازع في الاختصاص بين الدول والتي تتميز بكونها عابرة للحدود (نمر و بوكرشيدة، 2020-2021، صفحة 46).

3- تحديات تتعلق بتسليم المجرمين والإنابة القضائية:

وهي تلك التحديات المتعلقة بفكرة السيادة حيث أنه من المعروف أن كل دولة تقوم بحل نزاعاتها داخليا لاعتبارها ترتبط بفكرة السيادة، وبالتالي فان الزج بفكرة السيادة قد يعوق التعاون القضائي بين الدول المختلفة في مكافحة الجرائم العامة وإشكالية البطء في الإجراءات الأصل بالنسبة لطلبات الإنابة القضائية الدولية أن تسلم بالطرق الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي قد يتعارض مع طبيعة أعمال الانترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على التعاون الدولي في مكافحة هذه الجرائم، أما فيما يتعلق بإشكالية تسليم المجرمين فهي ترجع لمبدأ ازدواجية التجريم كشرط أساسي لتسليم المجرمين أيضا ما يعرف بالتزاحم في طلبات التسليم أي أن عدة دول تطلب نفس الشخص كونه ارتكب نفس الجريمة في عدة دول أو العديد من الجرائم الإلكترونية في دول مختلفة، ولا يشترط في تزاحم الطلبات أن تتعاصر في وصولها إلى الدولة المطلوب إليها، طالما أن الشخص المطلوب مازال متواجد على إقليمها ولم يتم تسليمه إلى أي من الدول التي تطالب بالتسليم (عبدالهادي، 2020، صفحة 51).

ثانياً-التحديات التقنية

لقد أفرزت التكنولوجيات الجديدة للمعلومات عدة تحديات تتسم بالخطورة، ومن أهم هذه التحديات: تطور الوسائل التكنولوجية، وانتشار الاتصالات المشفرة، ونقص الكوادر المتخصصة.

1- تطور الوسائل التكنولوجية: يشكل التطور المستمر في التكنولوجيا تحدياً كبيراً لجهود مكافحة الجرائم الإلكترونية مع كل ابتكار جديد تظهر ثغرات يمكن استغلالها من قبل المجرمين (الله، 2024)، ويعد التقدم التكنولوجي السريع والمستمر تحدياً رئيسياً، فمع كل تقدم جديد في التكنولوجيا تظهر أساليب جديدة لارتكاب الجرائم الإلكترونية، ويزداد تعقيد الجرائم الإلكترونية مع تطور التقنيات (التحديات القانونية في مكافحة الجريمة الإلكترونية، 2025)، مما يتطلب خبرات تقنية متقدمة للكشف عنها والتحقيق فيها، ويصعب على التشريعات مواكبة هذا التطور السريع مما يترك ثغرات قانونية يمكن للجناة استغلالها. (العتيبي، بلا تاريخ).

2- انتشار الاتصالات المشفرة: يشير انتشار الاتصالات المشفرة إلى الاستخدام المتزايد للتشفير من قبل الافراد والمؤسسات لحماية سرية اتصالاتهم، ويتضمن التشفير ترميز رسالة أو بيانات بطريقة لا يمكن فك تشفيرها إلا من قبل شخص لديه المفتاح اللازم، وبينما يعد التشفير أداة مفيدة لحماية المعلومات الحساسة، يمكن للمجرمين استخدامه أيضًا للتواصل دون خوف من المراقبة، ومن أكبر التحديات التي يواجهها المحققون في مواجهة انتشار الاتصالات المشفرة صعوبة تتبع أنشطة الأفراد وجمع الأدلة ضدهم، فعندما تكون الاتصالات مشفرة يصبح من الأصعب بكثير على المحققين اعتراضها ومراقبتها، مما قد يصعب جمع الأدلة وبناء قضية ضد المشتبه بهم، وكما يثير مخاوف أوسع نطاقًا بشأن الخصوصية والأمن وبينما يمكن للتشفير أن يساعد في حماية المعلومات الحساسة، ويمكن للأفراد والمؤسسات استخدامه أيضًا لتجنب التدقيق والتهرب من إنفاذ القانون، ويبرز هذا ضرورة بدل جهود مستمرة لمواكبة أحداث الاتجاهات والتقنيات من أجل مكافحة هذه الجرائم بفعالية (باتيل، 2023).

3-نقص الكوادر المتخصصة: هناك طلب متزايد على الكوادر المتخصصة في مجال الأمن السيبراني ولكن العرض لايزال محدود، مما يتطلب ذلك تدريب الكوادر على أحدث التقنيات والأساليب المستخدمة في الجرائم الإلكترونية وهو ما يحتاج إلى استثمارات كبيرة (العتيبي، بلا تاريخ).

الخاتمة

في نهاية البحث توصلنا إلى مجموعة من النتائج والتوصيات كالآتي:

أولاً-النتائج:

1- تمثل الجرائم الإلكترونية وما يعتريها من تحديات خطرا يهدد الاستقرار الدولي لكونها عابرة للحدود، ليس من السهل اثباتها، ويرتكبها أشخاص على درجة عالية من الذكاء والاحتراف، لذلك أهتم المجتمع الدولي بمكافحتها.
2- الجرائم الإلكترونية جرائم متطورة فمن الصعب حصر أنواعها، أو التنبؤ بأساليب وطرق ارتكابها.
3- لا تستطيع أي دولة لوحدها مكافحة الجرائم الإلكترونية، لذلك لابد من الدخول في اتفاقيات دولية خاصة بمكافحة الجرائم الإلكترونية، والتي تعتبر من أهم وسائل مكافحة هذه الجريمة والتصدي لها على الصعيد الدولي.
4- يعد اختلاف الأنظمة القانونية للدول إشكالية كبيرة تعترض سبيل التعاون الدولي بين تلك الدول في مجال مكافحة الجرائم الإلكترونية، لما يترتب على ذلك الاختلاف من مشكلات تطبيق القانون، وما يثيره هذا الاختلاف من مشكلات في الواقع العملي، يجعل التعاون الدولي أمراً صعباً.
5- بالرغم من أهمية الدور الذي يؤديه التعاون الدولي في مكافحة الجرائم الإلكترونية، إلا أنه تعترضه عدة تحديات دولية، لعل من أهمها القصور التشريعي للدول، تنوع واختلاف النظم القانونية الإجرائية، تنازع الاختصاص القضائي الدولي، والتحديات الخاصة بتسليم المجرمين.

ثانياً-التوصيات:

1-تعزيز التعاون التقني والقانوني بين الدول في مجال مكافحة الجريمة الإلكترونية من خلال تقديم كل الوثائق ذات الصلة أو نسخ منها، وتبادل البيانات وتحديد أماكن الأشخاص، وإجراء عمليات البحث والتفتيش.
2-ضرورة الانضمام للاتفاقيات الدولية المعنية بمكافحة الجرائم الإلكترونية، لزيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مكافحة هذه الجريمة.
2- نوصي بإنشاء محكمة دولية خاصة بمعاقبة مرتكبي الجرائم الإلكترونية.

المراجع

أ. نبيلة هبة هروال .(2007). *الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة*. الإسكندرية: دار الفكر الجامعي.

أحمد الباسوسي .(2023). *الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة: حالات مختارة*. مجلة كلية الاقتصاد والعلوم السياسية، الجامعة المصرية الروسية، المجلد 24.(4)

أحمد خليفة الملط .(2006). *الجرائم المعلوماتية* (المجلد 2). القاهرة: دار الفكر الجامعي.

أحمد صباح عبد الكريم. (مارس، 2023). *الجرائم الناشئة عن التطور التكنولوجي وأثرها في السياسة الجنائية*. أطروحة دكتوراه، كلية القانون، جامعة كربلاء.

الأمم المتحدة. (24 ديسمبر، 2024). *الجمعية العامة للأمم المتحدة تعتمد اتفاقية تاريخية لمكافحة الجريمة السيبرانية*. تم الاسترداد من https://libya.un.org

الطيب بلواح .(2020). *الجريمة في القضاء الإلكتروني* (المجلد 1). عمان: دار وائل للنشر والتوزيع.

التحديات القانونية في مكافحة الجريمة الإلكترونية. (17 يونيو، 2025) *قانون تك*. تم الاسترداد من https://www.9an0n4dz.com

حرز الله محمد لخضر .(2023). *جرائم الإنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية*. مجلة المفكر، المجلد 18(1)، بسكرة، الجزائر.

حشيفة عبد الهادي .(2020). *التعاون الدولي في مجال مكافحة الجرائم الإلكترونية*. رسالة ماجستير، جامعة زيان عاشور، كلية الحقوق والعلوم السياسية، الجلفة.

د. أنوار امحمد محمد، و د. عبير عبد الله الجليدي. (يونيو، 2024). *الجرائم الإلكترونية والاعتداء على حقوق الملكية الفكرية في ظل البيئة الرقمية في بعض من دول العالم والوطن العربي*. مجلة غريان، العدد 29.

د. حازم حسن الجمل .(2022). *الحماية الجنائية للأمن الإلكتروني*. القاهرة: دار الفكر والقانون.

د. خالد حسن أحمد لطفي .(2019). *بيانات ومعلومات الكمبيوتر*. الإسكندرية: دار الفكر الجامعي.

د. رحموني محمد .(2018). *خصائص الجريمة الإلكترونية ومجالات استخدامها*. مجلة الحقيقة، العدد 41.

د. رضا محمد عبد العزيز مخيمر. (أبريل، 2023). *مدى تأثير التكنولوجيا على السياسة الجنائية في ضوء قانون تقنية المعلومات: دراسة تحليلية مقارنة*. جامعة الأزهر، الإصدار 38.(2)

د. سامي الشواء .(1993). *الغش المعلوماتي كظاهرة إجرامية مستحدثة*. المؤتمر السادس للجمعية المصرية للقانون الجنائي (ص. 516). القاهرة.

د. عبد الفتاح بيومي حجازي .(2019). *الدليل الجنائي والتزوير في جرائم الكمبيوتر*. الإسكندرية: دار الفكر الجامعي.

د. عبد الفتاح بيومي حجازي .(2006) .*مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي* .الإسكندرية: دار الفكر الجامعي.
د. علوي علي أحمد الشارفي .(2024) .*الوجيز في جرائم تقنية المعلومات* (المجلد 1). برلين: المركز الديمقراطي العربي للدراسات السياسية والاستراتيجية.
د. عيش تمام شوقي .(2019) .*الجريمة المعلوماتية: دراسة تأصيلية مقارنة* (المجلد 1). بسكرة: مطبعة الرمال، الوادي.
د. فريحة حسين .(2011) .*الجرائم الإلكترونية والإنترنت* .مجلة المعلوماتية، العدد 36. تم الاسترداد من https://search.mandumah.com
د. محمد محمود فيالة. (يوليو، 2024) .*القانون الدولي والتحديات المعاصرة: الجريمة السيبرانية نموذجاً* .مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد 1.
د. محمد مهدي صالح، و جمال علي حسين. (تشرين الأول، 2022) .*الجريمة الإلكترونية وسبل مواجهتها على المستويين الوطني والدولي* .مجلس النواب، دائرة البحوث والدراسات النيابية، قسم القانونية.
د. هدية أحمد محمد زعتر. (يونيو، 2023) .*الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها* .مجلة البحوث القانونية والاقتصادية.
زغودة بورشاق .(2022) .*أسباب الجريمة الإلكترونية من منظور سوسيو-أنثروبولوجي* .المؤتمر العلمي الدولي الافتراضي، جامعة المدية، برلين، ألمانيا.
زينات طلعت شحادة .(2006) .*الأعمال الإجرامية التي تستهدف الأنظمة المعلوماتية* .بيروت: دار صادر.
سعد فهد سعد المطيري. (بلا تاريخ) .*مفهوم الجرائم الإلكترونية وسماتها* .المجلة القانونية للدراسات والبحوث القانونية.
سليمان أبو نمر، و يوسف بوكرشيدة .(2020–2021) .*مكافحة الجريمة المعلوماتية في إطار القانون الدولي* .جامعة محمد خضير بسكرة، كلية الحقوق والعلوم السياسية.
شيريشجودا باتيل. (10 يناير، 2023) .*التحديات التحقيقية في جرائم الإنترنت في العصر الجديد* .تم الاسترداد من https://www.linkedin.com
عادل يوسف عبد النبي الشكري .(2008) .*الجريمة المعلوماتية وأزمة الشرعية الجزائرية* .مجلة الكوفة، العدد 7، مركز دراسات الكوفة، العراق.
عبد الله دغش العجمي .(2014) .*المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة* .رسالة ماجستير، جامعة الشرق الأوسط.
عفيفي كامل عفيفي .(2003) .*جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون* .بيروت: منشورات الحلبي الحقوقية.
عمر محمود محمد القهيوي .(2023) .*إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية* .رسالة ماجستير، جامعة الشرق الأوسط.
فاتن علي بشينة. (يونيو، 2024) .*الجرائم المعلوماتية وسبل مكافحتها على الصعيد الدولي* .مجلة الأصالة، المجلد 2.(9)
م.م سكينة طالب خير الله. (19 ديسمبر، 2024) .*الجرائم الإلكترونية وتحديات الأمن السيبراني في القرن الواحد والعشرين* . جامعة المستقبل. تم الاسترداد من https://uomus.edu.iq
محمد العتيبي. (بلا تاريخ) .*مكافحة الجرائم الإلكترونية: الحلول، القوانين، وطرق الحماية* .مكتب المحامي محمد العتيبي. تم الاسترداد من https://mohammedalotaibi.sa
محمد الكعبي .(2009) .*الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت* .القاهرة: دار النهضة العربية.
محمد بنوسي .(2024) .*تصنيف الجرائم الإلكترونية وفقاً لطبيعة الحق المعتدى عليه: دراسة مقارنة بين التشريع الفلسطيني والإماراتي* .مجلة جامعة العين للأعمال والقانون.
محمد جواد محمد غانم .(2023) .*إجراءات التحقيق الابتدائي في الجريمة الإلكترونية: دراسة مقارنة* .رسالة ماجستير، الجامعة العربية الأمريكية، كلية الدراسات العليا.
محمد فتحي أنور .(2010) .*تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف: دراسة مقارنة* . أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس.
محمد نذير بن عرفة، و يوسف حوري .(2025) .*اليوروبول كآلية لمكافحة الجريمة الإلكترونية* .مجلة الدراسات القانونية والسياسية، المجلد 11.(1)
محمود أحمد عبابنة .(2005) .*جرائم الحاسوب وأبعادها الدولية* .عمان: دار الثقافة للنشر والتوزيع.
مصطفى عبد الباقي .(2018) .*التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة* .جامعة بيروت، دراسات علوم الشريعة والقانون، المجلد 45.(4)
مصطفى محمد موسى .(2009) .*التحقيق الجنائي في الجرائم الإلكترونية* (المجلد 1). القاهرة: مطابع الشرطة.

نور الهدى السوفي .(2017) *التحقيق في الجريمة المعلوماتية*. رسالة ماجستير، جامعة قاصدي مرباح، ورقلة، الجزائر.
وليد الزبدي .(2033) *القرصنة على الإنترنت والحاسوب: التشريعات القانونية* (المجلد 1). عمان: دار أوسامة.
يوسف الصغير .(2013) *الجريمة المرتكبة عبر الإنترنت*. رسالة ماجستير، جامعة مولود معمري، تيزي وزو، الجزائر.
يوسف المصري .(2011) *الجرائم المعلوماتية والرقمية للحاسوب والإنترنت* (المجلد 1). عمان: دار العدالة.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.