



أنواع الجرائم الإلكترونية وتحديات مكافحتها

Types of air forces and the challenges of combating them

الباحث/ حمد محمد الدوسري

aldosarihm@gmail.com, QATAR، (قطر)، كلية القانون جامعة لوسيل،

تاريخ القبول: 2025/05/14

تاريخ الاستلام: 2025/05/02

ملخص:

في ظل التطور التكنولوجي المتسارع، برزت الجرائم الإلكترونية كأحد التحديات البارزة التي تواجه الأفراد والدول على حد سواء، لما تنطوي عليه من تهديدات تمس الأمن المعلوماتي والاقتصادي والاجتماعي. حيث يتناول البحث الإطار المفاهيمي للجرائم الإلكترونية، وخصائصها التي تميزها عن الجرائم التقليدية، ومن ثم ينتقل إلى تصنيف هذه الجرائم وفقاً لطبيعتها، مع بيان الدوافع المتعددة التي تقف خلف ارتكابها، سواء كانت اقتصادية أو نفسية أو اجتماعية.

كما يعالج البحث المعوقات التي تعترض سبل مكافحتها، سواء كانت قانونية أو تقنية أو مؤسسية، مستعرضاً الأسس التي يجب أن تُبنى عليها جهود المواجهة. ويُختتم البحث باستعراض الأساس القانوني لمكافحة هذا النوع من الجرائم، مسلطاً الضوء على الجهود الوطنية المبذولة، بالإضافة إلى التعاون الدولي الذي يُعد ركيزة أساسية في التصدي لجرائم عابرة للحدود بطبيعتها.

الكلمات المفتاحية: الجرائم الإلكترونية، الأمن المعلوماتي، الجرائم غير التقليدية، الدوافع الإجرامية، التحديات القانونية، المكافحة التقنية، الأسس القانونية، الجهود الوطنية، التعاون الدولي، الجرائم العابرة للحدود.

Abstract:

In light of rapid technological development, cybercrime has emerged as one of the most prominent challenges facing individuals and states alike, due to the threats it poses to information security, economic security, and social security. This study examines the conceptual framework of cybercrime and its characteristics, which distinguish it from traditional crimes. It then classifies these crimes according to their nature, highlighting the various motives behind their commission, whether economic, psychological, or social.

The study also addresses the obstacles to combating cybercrime, whether legal, technical, or institutional, and outlines the foundations upon which efforts must be built. The study concludes by reviewing the legal basis for combating this type of crime, highlighting national efforts and international cooperation, which is a fundamental pillar in combating transnational crimes.

Keywords: Cybercrime, Information Security, Non-Traditional Crimes, Criminal Motives, Legal Challenges, Technical Combat, Legal Foundations, National Efforts, International Cooperation, Transnational Crimes.

* المؤلف المرسل

مقدمة:

مع التوسع الهائل في استخدام التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في مختلف مجالات الحياة، ظهرت أنواع جديدة من الجرائم تختلف عن الجرائم التقليدية، ويُطلق عليها الجرائم الإلكترونية أو الرقمية، حيث تعتمد هذه الجرائم على اختراق أنظمة الحماية الإلكترونية، والتلاعب بالبيانات أو تدميرها، بهدف الحصول على معلومات سرية قد تُستخدم لتحقيق أهداف مالية أو معنوية، ويُطلق على مرتكبي هذه الأفعال لقب القراصنة الإلكترونيين.

وثُعد الجرائم الإلكترونية من أكثر الجرائم انتشارًا في السنوات الأخيرة، حيث أصبحت تحتل المرتبة الثانية من حيث عدد الجرائم التي يتم الإبلاغ عنها على مستوى العالم، وتشكل هذه الجرائم خطرًا حقيقيًا على الشركات والمؤسسات، لما تسببه من خسائر مالية جسيمة، ويُعتبر التصدي لها أمرًا ضروريًا من خلال إصدار تشريعات صارمة، وتشمل خطورتها أنها لا تنقيد بالحدود الجغرافية، فقد يُنفذ الهجوم الإلكتروني من دولة بعيدة عن الدولة المتضررة، كما أن أساليب ارتكاب هذه الجرائم تتطور بشكل مستمر، مما يزيد من صعوبة مكافحتها.

أمام هذا التهديد المتنامي أصبح من الضروري أن تتخذ الحكومات إجراءات فاعلة لمواجهة، وفي هذا الصدد لم تكن دولة قطر بمعزل عن هذه التحديات، فحرصت على تطوير قوانينها للتعامل مع الجرائم الإلكترونية، واستند المشرع القطري في ذلك إلى تجارب دولية مقارنة، فعمل على وضع أدوات تشريعية وتقنية تساعد في الحد من هذا النوع من الجرائم، وضمان حماية أمن المعلومات والبيانات الوطنية.

وثُعد مكافحة الجرائم الرقمية من القضايا البارزة في مختلف التشريعات على المستويات العربية والإقليمية والدولية، بما في ذلك القانون القطري، فقد أولى المشرع القطري اهتمامًا خاصًا لمواجهة هذه الظاهرة الحديثة، من خلال تفعيل منظومة الأمن الرقمي، وضمان حماية التعاملات الإلكترونية من محاولات الاختراق والاعتداء، ويعكس هذا الاهتمام حجم التحديات التي فرضتها هذه الجرائم في العصر الرقمي، مما جعل التصدي لها ضرورة قانونية وتقنية في آن واحد.⁽¹⁾

إشكالية الدراسة: مع التوسع المستمر في استخدام التكنولوجيا في الحياة اليومية، لقد أصبحت البيئة الرقمية مهيأة لظهور أنماط جديدة من الجرائم، من خلال تتبع الجهود المبذولة في ميدان الأمن الإلكتروني، حيثُ تبين أن هناك سباقاً عالمياً في تطوير تقنيات الحماية، ومع ذلك فإن كل تقنية جديدة تُقابل بتقنيات اختراق أكثر تطوراً، مما جعل خبراء الأمن الرقمي يتفقون على أن تحقيق أمن سيبراني كامل بنسبة تصل إلى معدل الصفرية في الاختراق، أمر غير ممكن، ولكن الهدف الواقعي هو تقليل حجم الاختراقات وتخفيف آثارها، على مستوى العالم العربي، حيثُ يظهر أن هناك ضعفاً في التفاعل مع هذه الظاهرة، ومن هنا تبرز الإشكالية في محاولة الإجابة عن السؤال التالي: ما هو المفهوم القانوني للجريمة الرقمية وما أبرز خصائصها؟ وما هو الموقف الذي تبناه المشرع القطري لمواجهتها؟

أهمية الدراسة: تظهر أهمية البحث من جانبين رئيسيين، الأول هو الأهمية العلمية، حيث يُعتبر موضوع الجرائم الرقمية من المواضيع الحديثة نسبياً، والتي تمتد آثارها إلى كل مجالات الحياة، وقد أصبحت هذه الجرائم تنتشر بسرعة وتشكل خطراً متزايداً، كما تسعى الدراسة إلى تحليل المخاطر والتحديات المرتبطة بها، أما الجانب الثاني فهو الأهمية التطبيقية، حيث يمكن أن تسهم نتائج هذه الدراسة في دعم الجهات الأمنية والمهتمين بمجال الأمن السيبراني، من خلال توضيح الجوانب الأساسية التي يجب مراعاتها عند التعامل مع هذا النوع من الجرائم، وتقديم رؤى عملية تساعد في تطوير أساليب الوقاية والمكافحة.

أهداف الدراسة: تهدف هذه الدراسة إلى تحقيق مجموعة من الغايات المهمة منها:

- التعريف بالجرائم الإلكترونية وخصائصها.
- بيان الدوافع التي تقف خلف ارتكاب هذا النوع من الجرائم. بالإضافة إلى تصنيف أنواعها المختلفة.
- كما تهدف إلى مناقشة أبرز المشكلات التي تطرحها هذه الجرائم.
- استعراض الوسائل التي يعتمد عليها القانون القطري في مواجهتها والحد من آثارها السلبية.

منهجية البحث

استخدم الباحث المنهج التأصيلي التحليلي لدراسة الجريمة الإلكترونية، ومدى مؤاتمة السياسات التشريعية الوطنية والدولية، مستعرضاً آليات مكافحتها.

خطة البحث

- المبحث الأول: ماهية الجرائم الإلكترونية.

-المطلب الأول: تعريف الجرائم الإلكترونية.

-المطلب الثاني: خصائص الجرائم الإلكترونية.

● المبحث الثاني: أنواع الجرائم الإلكترونية ودوافع ارتكابها.

-المطلب الأول: أنواع الجرائم الإلكترونية.

-المطلب الثاني: دوافع ارتكابها.

● المبحث الثالث: معوقات وتحديات مكافحة الجرائم الإلكترونية.

-المطلب الأول: أسس مكافحة الجرائم الإلكترونية.

-المطلب الثاني: تحديات مكافحة الجرائم الإلكترونية.

● المبحث الرابع: الأساس القانوني لمكافحة الجرائم الإلكترونية.

-المطلب الأول: الجهود الوطنية لمكافحة الجرائم الإلكترونية.

-المطلب الثاني: الجهود الدولية لمكافحة الجرائم الإلكترونية.

المبحث الأول

ماهية الجرائم الإلكترونية

يُقصد بذلك أنها أي نشاط إجرامي يتم من خلال الأجهزة الذكية أو عبر الشبكات أو الأنظمة المعلوماتية، سواء كان استخدام هذه الوسائل كأداة أو كمسرح للجريمة أو حتى كهدف لها، وتواجه التشريعات المحلية والدولية تحديًا كبيرًا في التعامل مع هذا النوع من الجرائم، نظرًا لاختلاف طبيعة الفضاء الرقمي عن باقي المجالات التقليدية كاليابسة أو البحر أو الجو أو حتى الفضاء الخارجي، فالبيئة الإلكترونية لا تخضع للمفاهيم القانونية الكلاسيكية، مما يجعل من الصعب في بعض الأحيان إيجاد توصيف قانوني دقيق وموحد للجرائم الرقمية.

حيث تُعد الجريمة الرقمية من الأنواع المستحدثة في عالم الجرائم، ومن جانب التنفيذ فإن مرتكبوها يمتلكون مهارات تقنية عالية ومعرفة متقدمة بالتعامل مع الأنظمة المعلوماتية، ورغم شيوعها وانتشارها الكبير، إلا أن تعريفها ما يزال محل اختلاف بين الاجتهادات الفقهية والقضائية، وسوف نتولى تعريف الجريمة الإلكترونية بالمطلب الأول وخصائصها بالمطلب الثاني.⁽²⁾

المطلب الأول: تعريف الجرائم الإلكترونية

تُعرف الجريمة الإلكترونية بأنها كل فعل أو امتناع عن فعل يصدر عن نية إجرامية، ويؤدي إلى الإضرار بمصلحة قانونية محمية، باستخدام الوسائل التقنية الحديثة، كما تُعرف أيضًا بأنها الاعتداء غير المشروع على أنظمة وبرامج الحاسوب، أو الشبكات الإلكترونية، أو البيانات الرقمية، سواء تم ذلك عن طريق التعديل أو الاختراق أو النسخ أو الاستخدام دون إذن، ويختلف تعريف هذه الجريمة بحسب السياق القانوني والغرض من استخدام المصطلح، ففي بعض الحالات تقتصر الجريمة الإلكترونية على الأفعال التي تخل بسرية المعلومات وسلامة النظم الحاسوبية، بينما في سياقات أخرى تشمل الجرائم التي تُرتكب باستخدام الحاسوب لتحقيق أرباح شخصية أو إيذاء الغير، كسرقة الهوية أو نشر المحتوى الضار.

ولهذا فإن الجريمة الرقمية مصطلح واسع يصعب حصره في تعريف قانوني موحد، ما يسبب تحديًا في توجيه الاتهام وتحديد الاختصاص، ومن الضروري عند محاولة ضبط مفهوم الجريمة الإلكترونية أن يُؤخذ بعين الاعتبار دور الأدلة الرقمية، والتي قد تظهر في أي نوع من أنواع الجرائم سواء كانت رقمية أو تقليدية، ولهذا يفضل بعض المختصين التركيز على طبيعة الأدلة الإلكترونية بدلاً من محاولة وضع تعريف شامل وواسع للجريمة الرقمية، كما تُفهم الجريمة الرقمية بأنها انتهاك يستهدف الفضاء السيبراني وأمنه، ويُقصد بالأمن السيبراني الإجراءات المتبعة لحماية مصالح الدولة والمجتمع داخل البيئة الإلكترونية، ويتضح من ذلك أن الجريمة الإلكترونية تشمل كل فعل غير قانوني يتم باستخدام الأجهزة الحاسوبية ويستهدف البيانات والمعلومات والأنظمة الرقمية.⁽³⁾

حيث يُستخدم مصطلح الجريمة الرقمية أو الإلكترونية للدلالة على الأفعال غير المشروعة التي ترتكب من خلال أو عبر شبكة الإنترنت، والتي تستهدف بشكل مباشر سلامة وأمن المعلومات، أو أمن الدولة، أو الأفراد أو الأموال، إذ يمكن تعريف هذه الجريمة بأنها كل فعل يتم تنفيذه بواسطة تقنيات المعلومات الحديثة، مثل الحواسيب والهواتف الذكية وشبكات الاتصال، وتُعد من الجرائم الخطيرة التي لا تقتصر آثارها على المجال الإلكتروني فحسب، بل تمتد لتؤثر على الجوانب الاقتصادية والاجتماعية والأمنية للدول والمجتمعات، وتتضمن الجرائم الرقمية مجموعة واسعة من الانتهاكات، مثل جرائم النصب والاحتيال المالي، وعمليات البيع والشراء الوهمية التي تتم عبر مواقع إلكترونية غير موثوقة، إضافة إلى اختراق أجهزة الحاسوب وسرقة البيانات والمعلومات الحساسة، ومن بين أبرز هذه المعلومات تلك التي تتعلق بالحسابات البنكية أو البيانات الشخصية للمستخدمين.

كما تشمل أيضاً عمليات الدخول غير المصرح به إلى الأنظمة الإلكترونية وتحميل البرمجيات الخبيثة والتجسس على الأفراد، ولا تقتصر هذه الجرائم على الجانب المالي، بل تمتد لتشمل الجوانب الأخلاقية والاجتماعية، مثل نشر المحتوى الإباحي خاصة المتعلق بالأطفال، أو التحريض على الكراهية والعنف، أو التشجيع على الانتحار، أو الإساءة إلى الحياة الشخصية للآخرين، كما تدخل تحت هذا النوع من الجرائم، تلك الأفعال التي تستهدف المؤسسات الأمنية والسيادية بهدف الإضرار بالدولة، مما يزيد من خطورتها ويجعل مواجهتها أمراً بالغ الأهمية.

ويختلف تعريف الجريمة الإلكترونية من جهة إلى أخرى بحسب زاوية النظر إليها، فهناك من يعتمد المقاربة الجنائية التي تركز على أن هذه الجرائم ما هي إلا تطور لبعض الجرائم التقليدية، لكنها أصبحت أكثر خطورة وانتشاراً بسبب دعم التكنولوجيا الحديثة لها، وهناك من يفضل المقاربة القانونية، والتي تنظر إلى هذه الجرائم على أنها نوعان: النوع الأول هو الجرائم التي تستهدف البنية التقنية نفسها، مثل اختراق الشبكات وتعطيل الأنظمة، والنوع الثاني هو الجرائم التي تُرتكب باستخدام التقنية كوسيلة، مثل الاحتيال الإلكتروني أو الابتزاز أو القرصنة(4).

المطلب الثاني: خصائص الجرائم الإلكترونية

تتصف الجرائم الرقمية بعدة خصائص تجعلها مختلفة تماماً عن الجرائم التقليدية، ومن أبرز هذه الخصائص أنها جرائم عابرة للحدود، أي أنها لا تلتزم بقيود الجغرافيا أو السيادة الوطنية، فمرتكب الجريمة قد يكون في دولة، بينما الضحية في دولة أخرى، وقد يحدث الضرر في مكان ثالث مختلف تماماً، ويرجع ذلك إلى طبيعة شبكة الإنترنت التي تربط بين ملايين الأجهزة في مختلف أنحاء العالم، وهذا ما يصعب من عملية التحقيق والملاحقة القانونية، ويجعل التعاون الدولي ضرورة حتمية في هذا المجال، ومن الخصائص المهمة أيضاً، أن هذه الجرائم تُعد مغرية بالنسبة للجاني، إذ يمكنه تنفيذها دون الحاجة إلى التواجد الفعلي في مسرح الجريمة، فيكفي أن يمتلك جهاز حاسوب واتصال بالإنترنت ليقوم بالفعل الإجرامي من على بُعد.

كما أن صعوبة تتبع آثار الجريمة الرقمية وعدم ظهور الأدلة الملموسة بالشكل المعتاد يجعل من الصعب اكتشاف الفاعل أو تحديد هويته، مما يمنحه نوعاً من الأمان المزيّف ويشجعه على تكرار الجريمة، فإن الجرائم الرقمية تُعرف بسهولة وسرعة تنفيذها، حيث يمكن ارتكابها في لحظات بسيطة بمجرد الضغط على زر، دون الحاجة إلى تخطيط طويل أو مجهود جسدي كبير، وهي بذلك تختلف عن الجرائم التقليدية التي قد تتطلب وقتاً للإعداد والتجهيز، كما أن هذه الجرائم قد تُنفذ بطرق خفية يصعب اكتشافها في الوقت المناسب، ولهذا يصفها البعض بأنها "جرائم الياقات البيضاء"، لأنها غالباً ما تُرتكب من قبل أفراد ذوي مهارات تقنية عالية، وتستهدف المصالح الكبرى بحدوء ودقة (5).

وتتميز الجريمة الرقمية أو السيبرانية بعدة خصائص تجعل منها ظاهرة فريدة في عالم الجريمة، وتفرض على الجهات القانونية والأمنية تحديات جديدة وغير تقليدية في طرق الكشف عنها والتعامل معها، ومن أهم هذه الخصائص:

أولاً: صعوبة الإثبات: فالجاني غالباً ما يستخدم أدوات تقنية متقدمة جداً، ويستغل سرعته في تنفيذ الجريمة في غضون ثوانٍ معدودة، كما أن تلك الجرائم قد تُرتكب باستخدام برامج خبيثة أو تقنيات تشفير عالية تجعل من الصعب تتبع أثرها، والأسوأ من ذلك هو سهولة محو الأدلة الرقمية أو التلاعب بها، إذ يمكن للجاني أن يحذف الملفات أو يغيّر محتواها أو يخفي مصدرها ببضع نقرات، مما يجعل مهمة المحققين معقدة، كما أن العديد من الأنظمة القضائية في بعض الدول لا تزال تتحفظ على قبول الأدلة الرقمية، بحجة أنها أدلة غير مادية، تتكون من بيانات وحقول مغناطيسية لا يمكن إدراكها بالحواس الطبيعية للإنسان، وهو ما يُضعف موقف الضحية ويعقد مسار العدالة.

ثانياً: امتناع الضحية عن الإبلاغ: حيث أظهرت الدراسات والتقارير أن نسبة كبيرة من ضحايا الجرائم الإلكترونية لا يقومون بالتبليغ عنها، إما لأنهم لا يكتشفون تعرضهم للجريمة أصلاً، وإما لأنهم يخشون من التشهير أو المساس بسمعتهم، خصوصاً إذا كانت الجريمة تتعلق بمعلومات حساسة أو مؤسسة مالية أو تجارية كبرى، وفي أحيان كثيرة تُكتشف الجريمة بالمصادفة وبعد مرور وقت طويل على حدوثها، ما يؤدي إلى صعوبة استرجاع البيانات أو محاسبة الجاني.

ثالثاً: طبيعة الجريمة الناعمة والمتخفية: فهذه الجرائم تُوصف بأنها ناعمة لأنها لا تلاحظ بسهولة، وغالباً ما تقع أثناء تواجد الضحية على الشبكة دون أن يشعر بحدوثها، حيث يتمتع المجرم الإلكتروني بمهارات تقنية متقدمة تمكنه من سرقة الأموال أو إرسال الفيروسات أو التجسس على الضحية دون أن يترك وراءه أثراً واضحاً، كما أن الهجوم الإلكتروني قد يكون على شكل برمجية مخفية داخل ملف عادي، أو عبر رابط مموه، ما يجعل الضحية عرضة للاختراق دون وعي أو انتباه.

رابعاً: الجرائم الرقمية تُرتكب عن بُعد: وهذه خاصية جوهرية تميز هذا النوع من الجرائم، فالجرم قد يكون في دولة تختلف تماماً عن الدولة التي يتواجد فيها الضحية، وهذا ما يعقد عملية ملاحقته قانوناً، حيث تتطلب هذه الحالة إجراءات قانونية ودبلوماسية

معقدة لتسليمه ومحاكمته، كما قد تصطدم بإشكالات تتعلق بتحديد الاختصاص القضائي بين الدول، فكل دولة لها نظامها القضائي وتشريعاتها الخاصة، وهو ما يستدعي التنسيق من خلال الاتفاقيات الدولية والمعاهدات الأمنية، لحسم النزاعات المتعلقة بالقانون الواجب التطبيق، أو الدولة المختصة بالمحاكمة، وكل ذلك يعرقل سير العدالة ويمنح الجاني فرصة أكبر للإفلات من العقاب. (6)

المبحث الثاني

أنواع الجرائم الإلكترونية ودوافع ارتكابها

تعتبر الجرائم الإلكترونية من الجرائم المتجددة التي تتطور باستمرار مع تطور التكنولوجيا، حيث يبتكر المجرمون طرقاً وأساليب جديدة للقيام بجرائمهم الإلكترونية، حيث تتنوع الجرائم السيبرانية بشكل كبير، مما يجعل من الصعب تحديد جميع أنواعها بدقة، ولكن يمكن تصنيفها في مجموعة من الأنواع الرئيسية التي تمثل تهديداً كبيراً للأفراد والشركات على حد سواء، وسوف نتولى أنواع الجرائم الإلكترونية بالمطلب الأول ودوافع ارتكابها بالمطلب الثاني.

المطلب الأول: أنواع الجرائم الإلكترونية

من أبرز أنواع الجرائم السيبرانية هي القرصنة الإلكترونية، حيث يقوم الجاني باختراق أنظمة الكمبيوتر الخاصة بالضحية بهدف الوصول إلى البيانات المخزنة داخل الأجهزة أو حتى التلاعب بها، ويتضمن هذا النوع من الجرائم سرقة البيانات الحساسة مثل كلمات المرور أو المستندات المالية، وقد يسبب هذا النوع من الهجمات أضراراً ضخمة للشركات، سواء من ناحية فقدان البيانات أو تعطيل الأنظمة التقنية، غالباً ما يكون الهدف من هذه القرصنة هو الاستفادة المالية أو تدمير السمعة أو الأمن المؤسسي. (7)

أما نشر الفيروسات فيعد من أكثر الأنشطة الضارة انتشاراً في العالم الرقمي، الفيروسات هي برامج خبيثة تُستخدم لاستهداف الأجهزة والأنظمة بهدف تدمير أو تعطيل البيانات والبرامج المخزنة فيها، في كثير من الأحيان، يقوم المهاجمون بنشر الفيروسات لتوسيع دائرة الأضرار الاقتصادية، حيث تؤدي هذه الفيروسات إلى خسائر اقتصادية تقدر بمليارات الدولارات سنوياً على مستوى العالم، وتمثل الفيروسات تهديداً بالغ الخطورة على الأنظمة الأمنية، إذ تؤدي إلى إهدار الموارد وزيادة تكاليف الصيانة وإصلاح الأجهزة، بالإضافة إلى التسبب في تدهور أداء الأنظمة التشغيلية.

ويوجد هناك الإرهاب الإلكتروني، الذي أصبح يشكل تهديداً حقيقياً في العديد من الدول حول العالم، ويتمثل في استخدام الهجمات السيبرانية كأداة لتخويف الناس وزعزعة استقرار الدول، من خلال استهداف الشبكات الحساسة مثل الشبكات الحكومية أو العسكرية، إذ يسعى الإرهابيون إلى نشر الفوضى وإحداث اضطرابات كبرى في النظم الأمنية للدول، ليتضمن هذا النوع من الهجمات استخدام الفيروسات أو البرمجيات الخبيثة لتعطيل الخدمات الأساسية مثل الخدمات المالية أو خدمات الصحة، وقد يتم ذلك عبر شبكة الإنترنت، مما يجعل من الصعب تحديد مكان الهجوم أو الجاني. (8)

جرائم المحتوى إذ تعد من الأنواع المنتشرة في العالم الرقمي، حيث يُستخدم الإنترنت كأداة للتنمر على الأفراد أو المؤسسات، هذا النوع من الجرائم يتضمن تهديدات أو مضايقات مستمرة عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي، ويشمل أيضًا نشر معلومات خاطئة أو تشويه السمعة، قد تتضمن هذه الجرائم أيضًا سرقة الهوية الرقمية أو انتحال شخصية الأفراد على الإنترنت، مما يؤدي إلى أضرار نفسية واجتماعية للمستهدفين.

أما الاحتيال الإلكتروني فيمثل نوعًا آخر من الجرائم السيبرانية التي تشهد تزايدًا كبيرًا في عصرنا الراهن، إذ يعتمد هذا النوع من الجرائم على خداع الأفراد أو الشركات للحصول على معلومات حساسة مثل أرقام بطاقات الائتمان أو تفاصيل الحسابات البنكية، عادةً ما يتم هذا الاحتيال عبر رسائل البريد الإلكتروني أو مواقع الإنترنت المزيفة التي تشبه المواقع الرسمية للبنوك أو الشركات الكبرى، الهدف هو الحصول على معلومات شخصية ومالية بهدف استخدامها في عمليات مالية غير قانونية.⁹

المطلب الثاني: دوافع ارتكابها

تعد الجريمة الرقمية ظاهرة معقدة تتنوع أسبابها ودوافعها باختلاف أهداف مرتكبيها، كما تتعدد أشكالها بتعدد الوسائل التقنية المتاحة ويتطور أساليب الهجوم السيبراني، بحسب البيئة النفسية والاجتماعية والثقافية والتقنية التي يعيش فيها مرتكب الجريمة، ومن أبرز هذه الدوافع:

أولاً: الدوافع المالية أو الاقتصادية: حيث يسعى العديد من مرتكبي الجرائم الرقمية إلى تحقيق مكاسب مادية سريعة وغير مشروعة من خلال استغلال الثغرات الأمنية في المواقع الإلكترونية، خاصة في ظل تزايد معدلات البطالة وانعدام الاستقرار المعيشي في بعض المجتمعات، مما يدفع البعض نحو سرقة البيانات البنكية، أو اختراق الحسابات الإلكترونية، أو استهداف المواقع التجارية بهدف الابتزاز أو البيع غير المشروع، كما أن بعضهم يتجه إلى انتهاك حقوق الملكية الفكرية من خلال نسخ وبيع البرمجيات بطريقة غير قانونية، وهو ما يشكل خطرًا كبيرًا على الشركات المنتجة والمستهلكين على حد سواء.

ثانيًا: الدوافع الشخصية أو النفسية: وهي دوافع قد تكون بدافع الفضول أو الرغبة في التعلم والتجربة، حيث يقوم بعض الأفراد باختراق الأنظمة فقط لإثبات قدرتهم على تجاوز الحماية الأمنية، وقد تتحول هذه المحاولات إلى أعمال إجرامية متعمدة، خصوصًا إذا صاحبها إضرار بالبيانات أو استغلال للمعلومات، كما أن بعض الجرائم تُرتكب بدافع الانتقام من جهة عمل أو مؤسسة أو حتى أفراد، ما يجعلها أكثر خطورة وتهديدًا، وفي بعض الحالات تكون بدافع الملل أو التسلية فقط، دون وعي بعواقب تلك الأفعال، وهو ما يُعرف في الأوساط التقنية باسم "الاختراق العشوائي".¹⁰

ثالثًا: الدوافع السياسية أو الأيديولوجية: حيث يستخدم بعض المجرمين الفضاء الإلكتروني كمنصة للتعبير عن مواقفهم السياسية أو تنفيذ أجنداث أيديولوجية معينة، ويُعد هذا النوع من الجرائم من أخطر الأنواع، خاصة حينما يتعلق بالإرهاب الإلكتروني،

والذي انتشر بشكل خاص في منطقة الشرق الأوسط، حيث يستخدم الإرهابيون الشبكات الرقمية لأغراض مثل نشر الدعاية، أو جمع التبرعات، أو التحريض على العنف، أو تنفيذ عمليات الحرب النفسية، كما تُستهدف المواقع الحكومية أو المؤسسات الأمنية كجزء من هذه الهجمات.

رابعاً: الدوافع الذهنية أو التحدي التقني: ويُقصد بها أن بعض الجناة يُقدمون على ارتكاب الجريمة بدافع استعراض قدراتهم العقلية والتقنية، إذ يرون في النظام المعلوماتي المعقد تحدياً يحفزهم على اختراقه والتغلب عليه، فيسعون لكسر الحواجز الأمنية بهدف إثبات الذات أو التفوق على الأنظمة، وهو ما يُلاحظ بوضوح عند فئة "الهاكرز الأخلاقيين" الذين يتحول بعضهم إلى مرتكبي جرائم عند تجاوزهم حدود المسموح قانوناً (11)

المبحث الثالث

معوقات وتحديات مكافحة الجرائم الإلكترونية

لا يوجد هناك ما يمنع من التصدي للجريمة السبرانية، ولكن يوجد هناك بعض المعوقات والتحديات التي تواجه سلطات انفاذ القانون، في التطبيقات العملية على أرض الواقع، إذ يصبح لكل فعل إجرامي ردة فعل من الجانب القانوني والقضائي، وسوف نتولى أسس مكافحة الجرائم الإلكترونية بالمطلب الأول وتحديات مكافحتها بالمطلب الثاني .

المطلب الأول: أسس مكافحة الجرائم الإلكترونية

مع تطور الجريمة الإلكترونية وتزايد تهديداتها، أصبحت من أخطر القضايا التي تواجه السلطات الأمنية، مما يضع تحديات جديدة تتطلب حلولاً مبتكرة وفعالة. ومن أجل التصدي لهذه الجرائم، يجب العمل على تفعيل مجموعة من الأسس التي تساعد على تعزيز الجهود المبذولة لمكافحتها. ومن بين هذه الأسس، المراجعة الدورية للنظم القانونية الحالية للتأكد من قدرتها على التعامل مع الجرائم الإلكترونية، وإذا لزم الأمر، يجب تعديل هذه القوانين لتتماشى مع تطورات هذا النوع من الجرائم، مما يساهم في تحسين فعالية التحقيقات،

ومن الضروري تخصيص دراسات متواصلة لإيجاد حلول عملية تهدف إلى الحفاظ على الأمان الإلكتروني وعلى مستوى الأفراد والمؤسسات، من الحلول المهمة في هذا السياق هو وضع سياسات فعالة لنقل البيانات والمعلومات عبر الحدود الدولية بطريقة تضمن أمانها، مما يساعد في تعزيز التعاون بين الدول لمكافحة الجرائم الإلكترونية عبر الإنترنت، كما يجب الاستفادة من خبرات المؤسسات المتخصصة في تكنولوجيا المعلومات لضمان أن جميع الأدوات والأنظمة المتطورة التي يتم تطويرها تكون قادرة على التصدي للتهديدات الإلكترونية بفعالية.

كما لا بد من توعية جميع الأطراف المعنية، سواء من الأفراد أو المؤسسات، حول أهمية التصدي للجرائم الإلكترونية وتفعيل إجراءات وقائية على مستوى أوسع، وهذا يتطلب تقديم برامج تدريبية متخصصة تضمن للأفراد في المجال الأمني اكتساب المهارات الضرورية للتعامل مع الجرائم الإلكترونية بكفاءة.

كما ينبغي تعزيز الإجراءات المتعلقة بالتحقيقات الفنية في مسرح الجريمة، وضمان وجود أنظمة متطورة للتعامل مع الأدلة الرقمية بطريقة منظمة وآمنة، ومن الأمور الأساسية أيضاً توفير الأدوات التكنولوجية الحديثة التي تتيح للأجهزة الأمنية مواجهة التحديات المتزايدة في مجال الأدلة الإلكترونية، حيث يجب أن تتوفر برامج وأجهزة تحليلية متطورة للتعامل مع الأدلة التي يتم جمعها

بشكل سريع وفعال، ولضمان التنسيق بين مختلف الأجهزة الأمنية والمؤسسات المعنية، من المهم وجود مختبرات متخصصة للتحليل الرقمي ضمن الهيكل التنظيمي للأجهزة الأمنية، ما يساعد في تنظيم العمل بشكل منهجي واحترافي. (12)

المطلب الثاني: تحديات مكافحة الجرائم الإلكترونية

مكافحة الجرائم السيبرانية تعتبر من أكثر القضايا الشائكة في عصرنا الراهن، نظراً للخصائص الفريدة التي تتمتع بها وتجعل من الصعب مواجهتها وحلها، حيث تواجه الجهات الأمنية العديد من المعوقات والتحديات التي تعقد تعجل ملاحقة المجرمين وتقديمهم للعدالة أمراً في غاية الصعوبة.

ومن أبرز هذه التحديات هي: ضعف البنية التحتية التقنية والقانونية في بعض البلدان، حيث تفتقر بعض الدول إلى النظم القانونية المتطورة التي تتيح لها التعامل مع الجرائم الإلكترونية بشكل فعال، مما يزيد من صعوبة التحقيقات وفعالية الإجراءات المتخذة ضد الجناة، كما تعد صعوبة تحديد وقوع الجريمة واحدة من أكبر التحديات التي تواجه الخبراء في مجال جمع الاستدلالات، فبينما يتم ارتكاب الجرائم السيبرانية عادة في بيئة غير مرئية، إذ يصعب تحديد توقيت وقوع الهجوم أو طريقة تنفيذه، وهذا يعني أن التحقيقات قد تستغرق وقتاً طويلاً للوصول إلى نتائج ملموسة، نظراً لأن الأدلة قد تكون مشوشة أو غير موجودة، مما يجعل من الصعب تعقبهم أو تقديمهم للمحاكمة (13).

ويمثل التعاون الدولي عائقاً كبيراً في مكافحة الجرائم السيبرانية، على الرغم من وجود بعض الاتفاقيات الدولية التي تدعو إلى التعاون بين الدول في مجال مكافحة الجرائم السيبرانية، إلا أن هناك تحديات قانونية وثقافية تمنع التطبيق الفعلي لهذه الاتفاقيات، فبعض الدول لا تتفق على كيفية تعريف الجريمة السيبرانية أو كيف يجب أن تتم معالجة الأدلة الرقمية، مما يخلق صعوبة في التعاون بين الدول في تقديم المجرمين للعدالة، كما تُعد عدم وجود نموذج قانوني موحد للجرائم الإنترنت في معظم الدول من التحديات الكبرى، في حين أن بعض الدول قد تكون قد وضعت قوانين لمكافحة الجريمة السيبرانية، إلا أن هذه القوانين قد تختلف بشكل كبير من دولة إلى أخرى، مما يعرقل العمل المشترك بين الدول في مجال مكافحة الجرائم السيبرانية. (14)

حيث تواجه الجهات الأمنية العديد من التحديات في مكافحة الجرائم السيبرانية على المستوى الدولي، ومن أبرز هذه التحديات عدم وجود نموذج موحد للسلوك الإجرامي، حيث لم تتفق الأنظمة القانونية في دول العالم على تعريف موحد للجريمة السيبرانية أو ما يُعتبر إساءة لاستخدام النظم المعلوماتية، كما أن الاختلافات في العادات والتقاليد بين الدول تجعل بعض الأنشطة تعتبر جريمة في دولة ما بينما لا تُعتبر كذلك في دولة أخرى، وهذا الاختلاف يعقد عملية تحديد الأنشطة الإجرامية وتطبيق القوانين بشكل عالمي، مما يتطلب تحديث التشريعات المحلية لتواكب التطورات في الجرائم السيبرانية وتعريفاتها، أما اختلاف الإجراءات القانونية في مكافحة الجريمة السيبرانية بين الدول فيعقد من التحديات الكبرى، فبعض الطرق المستخدمة

للتحقيق والمحاكمة قد تكون فعالة في دولة ما لكنها قد لا تُناسب الأنظمة القانونية في دولة أخرى، وقد تكون بعض التقنيات غير مسموح بها في بعض الدول، مما يؤدي إلى تباين في فاعلية الإجراءات على مستوى العالم.

ومن أبرز التحديات **مشكلة الاختصاص القضائي** في الجرائم السيبرانية، حيث يمكن أن تتم الجريمة في دولة معينة من قبل شخص أجنبي، وهنا تكون القضية خاضعة للاختصاص القضائي للدولة التي وقع فيها الجرم، طبقاً للمبدأ الإقليمي، أو قد تتمثل التحديات في الجرائم التي تهدد أمن دول أخرى من خلال أنظمة تقع في دولة معينة، وفي هذه الحالة، قد يتم رفع القضية أمام الدولة التي تعرض أمنها للتهديد، لحل هذه المشكلة إذ يجب أن يتم عقد اتفاقيات دولية تتيح توحيد قواعد الاختصاص القضائي وضمان تسهيل الإجراءات في جميع الدول (15).

كما أن هناك صعوبات تتعلق **بالتدريب**، حيث يعتقد بعض القيادات الإدارية في بعض الدول أن التدريب في مجال الجرائم السيبرانية قد يكون له تأثير سلبي على سير العمل، مما يعيق تطور المهارات اللازمة لمكافحة الجرائم الإلكترونية، كما أن **الفوارق الفردية بين الأشخاص** تؤثر في مدى قدرة الأفراد على اكتساب المهارات المطلوبة، فقد يكون هناك أفراد ليس لديهم اهتمام كبير بالمجال في حين أن هناك آخرين يتمتعون بكفاءة عالية، كما أن بعض المدربين لا يرون الدورات التدريبية كمرحلة مهمة لتطوير العمل، مما يؤثر سلباً على العملية التعليمية بشكل عام.

وأحد التحديات الأخرى التي تواجه مكافحة الجرائم السيبرانية هي **الصعوبات المرتبطة بالمساعدة القضائية الدولية**، حيث تتطلب طلبات الإنابة القضائية بين الدول عادةً أن يتم تسليمها عبر الطرق الدبلوماسية، مما يجعل الإجراءات بطيئة ومعقدة، وهو ما يتعارض مع سرعة الإنترنت وجرائمه، لتحقيق سرعة وفاعلية في تقديم المساعدة القضائية يجب أن يتم اعتماد طرق أسرع وأكثر فعالية لتسليم الطلبات القضائية، مثل تحديد سلطة مركزية يمكن من خلالها تبسيط وتسريع إجراءات التعاون الدولي في مكافحة الجرائم السيبرانية (16).

المبحث الرابع

الأساس القانوني لمكافحة الجرائم الإلكترونية

تعتبر الجريمة السيبرانية واحدة من أبرز التهديدات التي تواجه الأفراد والدول على حد سواء، إذ تؤثر بشكل كبير على حياة المواطنين الشخصية وأمن الدول وسيادتها، ويعود ذلك إلى التطور التكنولوجي السريع والمتواصل، الذي غير بشكل جذري كافة جوانب الحياة اليومية، وأدى إلى ظهور العديد من التحديات التي تتعلق بحماية الخصوصية وأمن المعلومات، حيث أصبحت هذه الجريمة تمس جميع القطاعات، من الأفراد إلى الشركات والدول. ولقد أصبح من الضروري اتخاذ تدابير قانونية صارمة لمواجهة هذا النوع من الجرائم، ومع تزايد أساليب الجريمة السيبرانية وانتشارها السريع، وسوف نتولى الجهود الوطنية لمكافحة الجرائم الإلكترونية بالمطلب الأول والجهود الدولية بالمطلب الثاني.

المطلب الأول: الجهود الوطنية لمكافحة الجرائم الإلكترونية

لقد سن المشرع القطري مجموعة من القوانين التي تهدف إلى مكافحة الجرائم الإلكترونية في إطار سعي الدولة لحماية الأمن السيبراني، بداية من قانون العقوبات القطري، إلى قانون مكافحة الجرائم الإلكترونية رقم 14 لعام 2014 ليحدد الأطر القانونية ويحرم الأفعال المرتبطة بالجريمة السيبرانية، فقد عرف بالمادة الأولى من القانون، تقنية المعلومات والشبكة المعلوماتية والبرامج المعلوماتية والبيانات الإلكترونية والأفعال الأخرى الذي تنطوي على أفعال إجرامية، وفي المادة الثانية حدد الدخول غير المصرح به إلى المواقع الإلكترونية أو النظم المعلوماتية وأعتبرها جريمة على شقين جنحة وجناية، حيث خصص المشرع هذه المادة لحماية المواقع الإلكترونية التابعة للأجهزة الحكومية والمجالس الوطنية، وكذلك الهيئات والشركات التابعة للدولة، كما تم إضافة حماية للنظم المعلوماتية التي تتعامل مع البيانات الحساسة، وقد نص بالمادة 16 على عدم استبعاد أي دليل ناتج عن هذه الجرائم تم الحصول عليها بمعرفة الجهات المختصة (17).

ويأتي ذلك الحد من المخاطر التي قد تنجم عن التهديدات الإلكترونية، وقد جاءت هذه التشريعات في ظل تزايد الجرائم المرتكبة باستخدام تقنيات المعلومات الحديثة، مثل الإنترنت ووسائل الاتصال الإلكترونية، ما جعل من الضروري تحديث القوانين الوطنية لمواكبة هذا التطور السريع. فقد أدى انتشار الجرائم السيبرانية إلى تهديد استقرار وأمن الدولة، وهو ما دفع المشرع القطري إلى تضمين مفاهيم جديدة في التشريعات القانونية لتعريف هذا النوع من الجرائم ووضع إجراءات قانونية مناسبة لمكافحتها، كما فرضت الحاجة إلى توعية المجتمع حول أهمية الحفاظ على الأمان السيبراني وتطوير الوعي الرقمي لتجنب الوقوع في فخ هذه الجرائم، وفي ظل هذه التحديات كان من الضروري على المشرع القطري الاستمرار في تحديث القوانين وتحديد نطاق الجريمة السيبرانية بشكل واضح، وذلك لتواكب المستجدات التكنولوجية التي تطرأ على المستوى المحلي والدولي، هذا ما يفرضه الواقع

التمثل في التحولات المستمرة في مجال تكنولوجيا المعلومات، بما يتطلب تحديث مستمر للإجراءات التشريعية والرقابية لمواكبة هذه التغيرات ولتوفير حماية فعالة للمواطنين والمؤسسات من المخاطر الإلكترونية(18).

أولاً : اللجنة الوطنية لأمن المعلومات: تأسست اللجنة الوطنية لأمن المعلومات بموجب القرار الأميري رقم 19 لسنة 2016، الذي أقر إنشاء هذه اللجنة برئاسة رئيس مجلس الوزراء ووزير المواصلات والاتصالات، مع تعيين نائب للرئيس، بالإضافة إلى تضمين عضوية ممثلين عن مجموعة من الجهات الحكومية الهامة مثل وزارة الداخلية، وزارة الدفاع، وزارة الخارجية، وزارة التجارة والصناعة، وزارة المالية، وزارة المواصلات والاتصالات، وزارة العدل، النيابة العامة، مصرف قطر المركزي، وجهاز أمن الدولة. تهدف هذه اللجنة إلى تعزيز أمن المعلومات في الدولة وحمايته من أي تهديدات أو اختراقات قد تحدث في الفضاء الإلكتروني(19).

وقد نص القرار الأميري في المادة رقم 3 على منح اللجنة صلاحيات واسعة لتحقيق أهدافها المتعلقة بأمن المعلومات في قطر، حيث يمكن للجنة اتخاذ كافة الإجراءات اللازمة لضمان حماية المعلومات الوطنية من أي تهديدات إلكترونية. من بين أبرز المهام التي كُلفت بها اللجنة: إنشاء قنوات اتصال فعالة مع الجهات الدولية المتخصصة في مجال أمن المعلومات، فضلاً عن التعاون مع المؤسسات الدولية ذات الصلة بهذا القطاع، وذلك من أجل متابعة المستجدات والتطورات المتعلقة بالأمن السيبراني على الصعيدين الإقليمي والدولي، كما أن اللجنة مسؤولة عن وضع الأطر القانونية والعملية التي تنظم التعاون مع الدول الأخرى لمكافحة الجرائم السيبرانية وتعزيز الحماية الوطنية للمعلومات، وذلك في إطار تشريعي يضمن تقديم استجابة فعالة في حال حدوث أي انتهاك أو تهديد للأمن السيبراني القطري، مما يعكس التزام الدولة بالتحرك السريع والمتكامل لمكافحة الجرائم الإلكترونية على المستوى المحلي والدولي.(20)

ثانياً : الوكالة الوطنية للأمن السيبراني: تم تأسيس الوكالة الوطنية للأمن السيبراني بموجب القرار الأميري رقم 1 لسنة 2021، بهدف تعزيز حماية الأمن السيبراني في الدولة والحفاظ على المصالح الحيوية الخاصة بالدولة من أي تهديدات قد تنشأ في الفضاء السيبراني. تم منح الوكالة صلاحيات واسعة تشمل وضع السياسات والاستراتيجيات الخاصة بالأمن السيبراني، بالإضافة إلى العمل على تحديث هذه السياسات بشكل مستمر لمواكبة التطورات السريعة في هذا المجال الحيوي.

تهدف الوكالة إلى ضمان توفير بيئة آمنة على الإنترنت من خلال التحكم في المخاطر السيبرانية وتعزيز الوعي العام حول كيفية حماية البيانات والمعلومات الشخصية على الإنترنت، ومن بين المهام الأساسية الموكلة للوكالة، إعداد الاستراتيجية الوطنية للأمن السيبراني التي تشمل جميع جوانب الحماية الإلكترونية التي تحتاجها الدولة في مواجهة التهديدات الحديثة والمتطورة، والعمل على تحديث السياسات المتعلقة بالأمن السيبراني بما يتناسب مع التحديات التي قد تطرأ، مثل الهجمات الإلكترونية التي

تستهدف المؤسسات الحكومية والخاصة على حد سواء. كما تتضمن مسؤوليات الوكالة وضع أطر فعالة لإدارة المخاطر السيبرانية التي قد تؤثر على الأمن الوطني، سواء كان ذلك من خلال تحسين تقنيات الحماية أو تعزيز قدرات الردع والتفاعل السريع في حالات الطوارئ(21).

وعلى الرغم من أن الوكالة لم تذكر بشكل واضح في نص القرار آلية محددة للتعاون الدولي لمكافحة الجرائم السيبرانية، إلا أن المادة الأولى من القرار تشير إلى ضرورة التعاون مع الجهات الدولية والمحلية المعنية بالأمن السيبراني، وذلك من خلال توقيع مذكرات تفاهم واتفاقيات دولية مع الدول والمنظمات المتخصصة، من خلال هذا التعاون، يمكن للوكالة تبادل المعلومات الأمنية المتعلقة بالتهديدات السيبرانية، مما يساهم في تعزيز قدرة الدولة على الاستجابة بسرعة وفعالية للتحديات الإلكترونية على المستوى الدولي.

كما تقوم الوكالة بتقديم تقارير دورية عن الوضع الأمني السيبراني، سواء على الصعيد المحلي أو الإقليمي أو الدولي، مما يساهم في تعزيز الشفافية والرقابة المستمرة في مجال الأمن السيبراني، كما تعمل الوكالة على رفع مستوى الوعي الوطني فيما يتعلق بالأمن السيبراني من خلال برامج تدريبية وندوات توعوية تستهدف مختلف فئات المجتمع، بهدف تعزيز الثقافة الرقمية وضمان استعداد الجميع لمواجهة أي تهديدات إلكترونية قد تواجههم، من خلال هذه المبادرات، تسعى الدولة إلى ضمان تكامل الجهود على كافة الأصعدة لحماية المواطنين والمؤسسات من الجرائم السيبرانية التي قد تؤثر على استقرار الدولة وأمنها.(22)

المطلب الثاني: الجهود الدولية لمكافحة الجرائم الإلكترونية

في إطار التعاون الدولي لمكافحة الجريمة السيبرانية، ظهرت العديد من المنظمات والهيئات والمجالس الدولية التي تلعب دوراً رئيسياً في تطوير الاتفاقيات التي تهدف إلى تعزيز التعاون بين الدول في مواجهة هذه الظاهرة المتزايدة، مع تزايد الخسائر الناجمة عن الجرائم السيبرانية، وخاصة مع توسع نطاق هذه الجرائم لتتجاوز الحدود الوطنية، حيث أصبحت الحاجة إلى التعاون الدولي أكثر إلحاحاً، ونظراً لكون الجريمة السيبرانية من الجرائم التي لا تعترف بالحدود الجغرافية أو الحواجز الثقافية، فقد أصبحت تشكل تهديداً حقيقياً يتجاوز قدرات الدول على مواجهته منفردة، فهي تنتقل عبر الشبكات والأنظمة بسهولة، ويمكن أن يكون مرتكبها في دولة والضحية في دولة أخرى، مما يفرض على المجتمع الدولي، وخاصة الدول ضمن الأقاليم الجغرافية المتقاربة، أن تتعاون بشكل مشترك لمكافحة هذا النوع من الجرائم ووضع أطر قانونية إقليمية تساعد على تبادل المعلومات والخبرات، وتعزيز الأمن السيبراني(23).

وقد برزت اتفاقية بودابست كأول اتفاقية دولية لمكافحة الجرائم المعلوماتية، وقد تم اعتمادها من قبل المجلس الأوروبي في 23 نوفمبر 2001 بمدينة بودابست عاصمة المجر، وبدأ العمل بها في الأول من يوليو عام 2004، وقد صُممت الاتفاقية لتكون

إطارًا مرجعيًا عالميًا، حيث تضمنت أربعة فصول رئيسية تناولت الأهداف العامة، والمبادئ التشريعية، والإجراءات الجنائية، وأطر التعاون الدولي، وقد دعت الاتفاقية الدول إلى تجريم عدد من الأفعال مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، واعتراض البيانات، والتدخل في النظام أو البيانات، بالإضافة إلى الجرائم المتعلقة بالمحتوى مثل نشر المواد الإباحية التي تستغل الأطفال، وكذلك الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية.

كما جاء على مستوى القارة الأفريقية اتفاق مهم هو اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي، والتي اعتمدت في 27 يونيو 2014 في مدينة مالابو عاصمة غينيا الاستوائية، خلال الدورة الثالثة والعشرين لمؤتمر الاتحاد، وقد تضمنت الاتفاقية 38 مادة، وهدفت إلى وضع إطار قانوني مشترك لحماية المعطيات الشخصية، وتعزيز التعاون بين الدول الأعضاء في مواجهة الجرائم السيبرانية، من خلال توفير قواعد تنظم تجريم الأفعال الإلكترونية، وتحقيق التوازن بين احترام الحقوق الفردية وضمان الأمن السيبراني(24).

وعلى المستوى العربي أقر مجلس وزراء الداخلية العرب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 21 ديسمبر 2010، وتم توقيعها في مقر الأمانة العامة لجامعة الدول العربية في القاهرة، وقد تضمنت الاتفاقية 43 مادة موزعة على أبواب مختلفة تناولت المبادئ العامة، والأفعال المجرّمة، والإجراءات القانونية، والتعاون القضائي، وتسليم المجرمين، وقد جاءت هذه الاتفاقية استجابةً للتحديات التي تفرضها الجرائم الإلكترونية على الأمن القومي العربي، وسعيًا لتوحيد الجهود العربية في التصدي لهذه الظاهرة العابرة للحدود،

وكل هذه الجهود تؤكد أن التعاون الإقليمي أصبح ضرورة ملحة لمواجهة تصاعد الجريمة السيبرانية، سواء من خلال وضع اتفاقيات موحدة، أو من خلال تبادل الخبرات والتجارب وتطوير القدرات الوطنية في مجال الأمن السيبراني، وفي الاتفاقية تم التأكيد في القسم الأول على ضرورة تعزيز التعاون، وتوطيد العلاقات بين الدول العربية لمكافحة جرائم تقنية المعلومات، وذلك من أجل درء أخطر هذه الجرائم والحفاظ على أمن الدول وسلامة مجتمعاتها ومصالحها الحيوية.

وقد تضمن الاتفاق تفاصيل حول تعزيز الجهود المشتركة بين الدول العربية لتطبيق تشريعات صارمة تساهم في حماية النظم المعلوماتية، كما جاء في الفصل الثاني تفصيل دقيق للأفعال التي تُعتبر جرائم، وفي الفصل الثالث تناول نطاق تطبيق الأحكام الإجرائية بشكل موسع، بينما خصص الفصل الرابع لإطار التعاون القضائي والقانوني بين الدول، وفي الفصل الخامس تم ذكر الأحكام الختامية، ومع أن الاتفاقية أكدت احترام سيادة الدول الأعضاء وخاصة فيما يتعلق بالولاية القضائية وغيرها من وظائف السيادة.

إلا أنها تفرض على كل دولة من الدول الأعضاء تعديل تشريعاتها الداخلية لتجريم الدخول غير المشروع إلى نظم تقنية المعلومات، واعتراض البيانات أو إعادة استخدامها بطرق غير قانونية، والاحتتيال باستخدام تلك الوسائل، والاعتداء على الحياة الخاصة، إضافة إلى تجريم الجرائم المتعلقة بالمواد الإباحية والإرهاب واستخدام أدوات الدفع الإلكترونية بطرق غير مشروعة، وقد تضمنت المادة الحادية والعشرون من الاتفاقية إلزام الدول الأطراف بتشديد العقوبات المفروضة على الجرائم التقليدية في حال ارتكابها عبر استخدام تقنيات المعلومات، كما أقر المشرع القطري آليات متعددة في تشريعاته لمكافحة الجرائم السيبرانية، حيث قام بتطبيق عقوبات صارمة على مرتكبي هذه الجرائم، إلا أن تلك العقوبات تبقى غير كافية لتعكس خطورة الجرائم السيبرانية وتطورها السريع(25).

كما دعت الأمم المتحدة إلى وضع قواعد قانونية دقيقة وواضحة تتعلق بالأدلة الإلكترونية، وذلك بهدف تسهيل جمعها وتوثيقها وقبولها في المحاكم، وقد شددت على أهمية تطوير آليات مناسبة لمصادرة أو استرداد الأموال والعوائد التي يتم الحصول عليها من خلال الجرائم السيبرانية، بالإضافة إلى تدريب القضاة والمدعين العامين ومسؤولي إنفاذ القانون بشكل متخصص على كيفية التعامل مع الجرائم الإلكترونية، وخاصة تلك المرتبطة بالاحتتيال والقرصنة وسرقة المعلومات.

ومن بين التوصيات أيضاً كان هناك تركيز كبير على ضرورة وضع سياسات واضحة تحمي ضحايا جرائم الحاسوب، وتقديم الدعم القانوني والنفسي لهم، مع اعتماد قواعد أخلاقية لاستخدام الحواسيب والبرمجيات، وتشجيع المستخدمين على الالتزام بها من أجل تقليل المخاطر والحد من الانتهاكات الإلكترونية، وقد جاءت هذه التوصيات نتيجة تزايد حجم الخسائر التي تسببها الجرائم السيبرانية على المستوى العالمي، بالإضافة إلى تعقيدها وسرعة انتشارها، مما يتطلب من المجتمع الدولي تنسيق الجهود والعمل المشترك لاحتواء آثارها والحد من انتشارها(26).

الخلاصة :

في ختام هذا البحث، نصل إلى حقيقة واضحة وهي أن الجريمة السيبرانية أصبحت من أخطر التهديدات التي تواجه المجتمعات الحديثة، فهي لا تعرف حدودًا جغرافية، وتمتاز بسرعة انتشارها وتطور أساليبها، كما أنها تستهدف الأفراد والمؤسسات على حد سواء، مما يجعل التعامل معها أمرًا معقدًا يتطلب تعاونًا دوليًا وتحديثًا مستمرًا للتشريعات،

وقد أظهر البحث أن مواجهة هذا النوع من الجرائم لا يقتصر على سن القوانين فحسب، بل يجب أن يشمل أيضًا إعداد كوادر بشرية مؤهلة، وتوفير الأدوات التكنولوجية الحديثة، وتعزيز الوعي الأمني لدى أفراد المجتمع، كما أن الاستثمار في الأمن السيبراني، والتعاون مع الدول المتقدمة في هذا المجال، يمثل خطوة أساسية نحو حماية الأمن القومي، ومن المهم كذلك أن يتم التركيز على نشر ثقافة الاستخدام الآمن للتكنولوجيا، خاصة بين فئة الشباب والأطفال، لأنهم الأكثر عرضة لهذه التهديدات، وبذلك يمكننا القول أن التصدي للجريمة السيبرانية هو مسؤولية جماعية تتطلب تكامل الجهود من جميع الأطراف لحماية الفضاء الرقمي وضمان أمن المجتمعات واستقرارها.

النتائج: من خلال الدراسة نستنتج:

- أن الجريمة السيبرانية تُعرف على أنها فعل عمدي أو امتناع ينشأ نتيجة الاستخدام غير المشروع لتقنيات المعلومات، سواء عبر الهواتف الذكية أو الحواسيب، بهدف الاعتداء على الأموال المادية أو المعنوية أو على الخصوصية الفردية.
- تشمل الجرائم السيبرانية جميع الأنشطة التي تستهدف البيانات الرقمية والمعلوماتية، حيث تتعرض تلك البيانات للسرقة أو التخريب أو الاختراق، وتستهدف كذلك الأنظمة الإلكترونية والإنترنت بشكل عام.
- تُعد الجرائم الإلكترونية من أخطر أنواع الجرائم الحديثة، إذ تنشأ عن الاستخدام غير المشروع للتقنيات الرقمية والمعلوماتية، وتتم غالبًا من خلال أجهزة الحاسوب أو الهواتف الذكية وبوسائل يصعب تتبعها أو التنبؤ بها.
- لا تعترف الجرائم الإلكترونية بالحدود الجغرافية أو الثقافية، ما يجعل مكافحتها أكثر تعقيدًا، وتزداد خطورتها عندما تستهدف خصوصية الأفراد أو تمسّ مصالح الدول ومؤسساتها الرسمية.
- تمثل الجريمة السيبرانية تحديًا قانونيًا كبيرًا، للدول التي لم تواكب تشريعاتها التقدم التكنولوجي المتسارع، حيث يجد المشرع نفسه في سباق دائم مع تطور أساليب الجرائم المعلوماتية، ويواجه صعوبة في إدراج جميع أشكال هذه الجرائم ضمن القوانين الجنائية التقليدية، نظرًا لتعدد أنواعها وابتكار طرق تنفيذها بشكل مستمر.
- تُشكّل الهجمات السيبرانية تهديدًا مباشرًا للأمن الوطني، حيث يمكن أن تستهدف شخصيات عامة أو مؤسسات حكومية، -

قد تؤدي إلى اختراقات خطيرة تسفر عن تهديد الأمن الداخلي وزعزعة الاستقرار، مما يجعل من الضروري تعزيز القدرات الوطنية في مواجهة هذا النوع من الجرائم.

الاقتراحات:

- اتخاذ إجراءات فعالة لتعزيز قدرات أجهزة العدالة الجنائية في مجال التحقيقات الرقمية، وذلك من خلال تزويدها بالتقنيات والأدوات الحديثة، وتدريب أفرادها على المهارات اللازمة لاكتشاف وتتبع الجرائم السيبرانية، مع الاستفادة من تقنيات مثل البيانات الضخمة، والذكاء الاصطناعي، والحوسبة عالية الأداء في تطوير السياسات الأمنية.
- التأكيد على إجراء مراجعة دورية وشاملة للتشريعات الوطنية المرتبطة بالأمن السيبراني، للتأكد من فعاليتها ومواكبتها للتطورات التقنية، مع إدخال التعديلات اللازمة لتغطية الثغرات القانونية.
- نشر ثقافة الوعي الرقمي بين أفراد المجتمع، مع التركيز على فئة الشباب والأطفال، وتوعيتهم بالمخاطر المحتملة المرتبطة بالاستخدام غير الآمن للإنترنت، والتأكيد على أهمية حماية البيانات الشخصية وعدم الانخداع بالمواقع المشبوهة.

قائمة المراجع:

- 1- أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، مجلد 13، العدد 44، 31 يناير/كانون الثاني 2020.
- 2- طاهر محمود أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية القاهرة، 2019.
- 3- ماينو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 4، العدد 1، 2022/7.
- 4- قطاف سليمان، بوقرين عبدالحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 5، العدد 2، 2022/6.
- 5- راشد حمدان، المتطلبات الحديثة لمكافحة الجريمة السيبرانية في المملكة العربية السعودية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، مجلد 2، العدد 76، يناير/2022.
- 6- رانا مصباح عبدالمحسن، آليات مكافحة الجرائم السيبرانية في السعودية دراسة تحليلية، المجلة القانونية، المجلد 15، العدد 5، فبراير/2023.
- 7- د.لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، دفا تر السياسة والقانون، المجلد 2، العدد 2، يونيو/2009.
- 8- د.طلال أبو عفيفة، أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، دار الجندي للنشر والتوزيع، 2013.

- 9- رعد الراوي، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون المعلوم القانونية والسياسية، مجلد 10، العدد 39، ديسمبر/2021.
- 10- سيدي محمد الأمين، الجريمة السيبرانية وتكاملية النص الوطني الإقليمي والدولي، جامعة الحسن الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، مختبر البحث قانون الأعمال، المجلد 47، 2019.
- 11- محمد قاسم، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية، المجلد 30، العدد 61، ديسمبر/2014.
- 12- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (2000).
- 13- اتفاقية بودابست لمكافحة الجرائم المعلوماتية (2001).
- 14- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010).
- 15- الاتفاقية الإفريقية للأمن السيبراني وحماية البيانات الشخصية (2014).
- 16- القانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية في قطر.
- 17- قرار أميري رقم (19) لسنة 2016 بإنشاء اللجنة الوطنية لأمن المعلومات.
- 18- قرار أميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني.

الهوامش:

- 1 أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، مجلد 13، العدد 44، 31 يناير/كانون الثاني 2020، ص 68.
- 2 أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق ص 69.
- 3 طاهر محمود أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية القاهرة، 2019، ص 41.
- 4 مابنو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 4، العدد 1، 2022/7، ص 27.
- 5 مابنو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مرجع سابق ص 31.
- 6 أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق ص 89.
- 7 قطاف سليمان، بوقرين عبدالحليم، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 5، العدد 2، 2022/6، ص 104.
- 8 طاهر محمود أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، مرجع سابق، ص 35.
- 9 طاهر محمود أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، مرجع سابق، ص 43.
- 10 أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق ص 39.
- 11 طاهر محمود أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، مرجع سابق، ص 32.

- 12 راشد حمدان، المتطلبات الحديثة لمكافحة الجريمة السيبرانية في المملكة العربية السعودية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، مجلد 2، العدد 76، يناير/2022، ص 48.
- 13 رانا مصباح عبدالمحسن، اليات مكافحة الجرات السيبرانية في السعودية دراسة تحليلية، المجلة القانونية، المجلد 15، العدد 5، فبراير/2023، ص 118.
- 14 رانا مصباح عبدالمحسن، اليات مكافحة الجرات السيبرانية في السعودية دراسة تحليلية، مرجع سابق، ص 119.
- 15 د.لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، دفا تر السياسة والقانون، المجلد 2، العدد 2، يونيو/2009، ص 148.
- 16 رانا مصباح عبدالمحسن، اليات مكافحة الجرات السيبرانية في السعودية دراسة تحليلية، مرجع سابق، ص 121.
- 17 راشد حمدان، المتطلبات الحديثة لمكافحة الجريمة السيبرانية في المملكة العربية السعودية، مرجع سابق، ص 47.
- 18 د.طلال أبوعفيفة، أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، دار الجندي للنشر والتوزيع، 2013، ص 18.
- 19 القرار الأميري رقم 19 لسنة 2016، بإنشاء اللجنة الوطنية لأمن المعلومات.
- 20 أحمد عبيس نعمة، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق ص 79.
- 21 رعد الراوي، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون المعلوم القانونية والسياسية، مجلد 10، العدد 39، ديسمبر/2021، ص 6.
- 22 سيدي محمد الأمين، الجريمة السيبرانية وتكاملية النص الوطني الإقليمي والدولي، جامعة الحسن الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، مختبر البحث قانون الأعمال، المجلد 47، 2019، ص 33.
- 23 رعد الراوي، القصور التشريعي في مواجهة الهجمات السيبرانية، مرجع سابق، ص 208.
- 24 محمد قاسم، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية، المجلد 30، العدد 61، ديسمبر/2014، ص 31.
- 25 د.طلال أبوعفيفة، أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، ص 21.
- 26 سيدي محمد الأمين، الجريمة السيبرانية وتكاملية النص الوطني الإقليمي والدولي، مرجع سابق، ص 56.