الجرائم السيبرانية في القانون الجنائي

الباحث/ يزيد صالح المحيميد

باحث لدرجة الماجستير بجامعة ميداوشن

الايميل: **almohimeedyazeed@gmail.com**

(ISSN: 2537- 0758)

الجرائم السيبرانية في القانون الجنائي

الباحث/ يزيد صالح المحيميد

الملخص:

تُعد الجرائم السيبرانية من أخطر التحديات التي تواجه المجتمعات الحديثة في ظل التطورات المتسارعة في تكنولوجيا المعلومات والاتصالات، حيث أدى الانتشار الواسع لاستخدام الإنترنت إلى بروز أنماط إجرامية جديدة تستهدف الأفراد والمؤسسات والدول عبر الفضاء الرقمي. وقد أصبحت هذه الجرائم ذات طابع معقد ومتجدد، يصعب اكتشافها وتتبع مرتكبيها نظرًا لطبيعتها العابرة للحدود واعتمادها على تقنيات متقدمة مثل التشفير وإخفاء الهوية. وتتمثل أهمية الدراسة التي نحن بصددها في تناول ظاهرة الجرائم السيبرانية من منظور قانوني جنائي شامل، من خلال تحليل مفاهيمها وأنواعها وأطرها القانونية، إلى جانب استعراض التحديات الإجرائية والتقنية التي تعوق مكافحتها، واقتراح حلول فعالة لتطوير منظومة العدالة الجنائية لمواجهة هذه الظاهرة الآخذة في التوسع. وتبرز مشكلة الدراسة في عدم كفاية النصوص القانونية التقليدية في معالجة الأفعال الجرمية الرقمية، وما يرتبط بها من صعوبات في جمع الأدلة الرقمية وحفظها وإثباتها قانونيًا، فضلًا عن غياب التنسيق الدولي الكافي في مواجهة هذه الجرائم العابرة للحدود؛ ما يسمح بوجود ثغرات تشريعية وقضائية تستغلها الجماعات الإجرامية الإلكترونية. وقد طرحت الدراسة مجموعة من الأسئلة الجوهرية، منها مدى فاعلية القوانين الجنائية القائمة في التصدي لهذه الجرائم، والتحديات المتعلقة بإثبات الجريمة الرقمية، وآليات التعاون الدولي لمواجهتها. كما سعت الدراسة إلى تحقيق أهداف متعددة تمثلت في تحليل الإطار المفاهيمي والقانوني للجرائم السيبرانية، واستشراف التحديات المستقبلية، وتقديم توصيات لتحديث التشريعات، وتطوير القدرات التقنية والبشرية. وقد خلصت إلى أن مكافحة الجرائم السيبرانية تتطلب استراتيجية متكاملة تتضمن تحديث التشريعات باستمرار، وتبني تقنيات متطورة في التحقيق الرقمي، وبناء شراكات دولية فعالة لتبادل المعلومات والتعاون القضائي، مع تأكيد أهمية رفع الوعي المجتمعي وتعزيز ثقافة الأمن السيبراني لدى الأفراد والمؤسسات. ومن خلال ذلك، تسعى الدراسة إلى إرساء دعائم منظومة قانونية أكثر فاعلية واستجابة للتطورات التقنية، تضمن التوازن بين حماية المجتمع من التهديدات الرقمية، وبين صون الحقوق والحريات الأساسية للأفراد في البيئة الافتراضية.

الكلمات المفتاحية: الجرائم السيبرانية، القانون الجنائي، الأدلة الرقمية، التشريعات الإلكترونية، الأمن السيبراني، التعاون الدولي.

Abstract:

Cybercrime is one of the most serious challenges facing modern societies, given the rapid developments in information and communications technology. The widespread use of the internet has led to the emergence of new criminal patterns targeting individuals, institutions, and countries across the digital space. These crimes have become complex and evolving, making them difficult to detect and track down due to their cross-border nature and their reliance on advanced technologies such as encryption and anonymity. The importance of this study lies in its approach to the phenomenon of cybercrime from a comprehensive criminal legal perspective, by analyzing its concepts, types, and legal frameworks. It also reviews the procedural and technical challenges that hinder its combat, proposing effective solutions to develop the criminal justice system to confront this expanding phenomenon. The problem of this study lies in the inadequacy of traditional legal texts in addressing digital criminal acts, the associated difficulties in collecting, preserving, and legally proving digital evidence, and the lack of adequate international coordination to combat these cross-border crimes, which allows for legislative and judicial loopholes exploited by cybercriminal groups. The study raised a set of fundamental questions، including the effectiveness of existing criminal laws in addressing these crimes، the challenges related to proving digital crimes, and the mechanisms of international cooperation to address them. The study also sought to achieve multiple objectives, including analyzing the conceptual and legal framework of cybercrimes, anticipating future challenges, and providing recommendations for updating legislation and developing technical and human capabilities. It concluded that combating cybercrimes requires an integrated strategy that includes continuously updating legislation, adopting advanced digital investigation technologies, and building effective international partnerships for information exchange and judicial cooperation. It also emphasized the importance of raising community awareness and promoting a culture of cybersecurity among individuals and institutions. Through this, the study seeks to establish the foundations of a legal system that is more effective and responsive to technological developments، ensuring a balance between protecting society from digital threats and safeguarding the fundamental rights and freedoms of individuals in the virtual environment.

Keywords: cybercrime, criminal law, digital evidence, electronic legislation, cybersecurity, international cooperation.

(ISSN: 2537- 0758)

المقدمة

شهد العالم في العقود الأخيرة تطورًا تكنولوجيًا هائلًا أدى إلى تحول جذري في أنماط الحياة والتفاعلات الاجتماعية والاقتصادية. ومع انتشار استخدام الإنترنت وتقنيات المعلومات والاتصالات في مختلف المجالات، ظهرت أنماط جديدة من الجرائم تستغل هذه التقنيات وتتخذ من الفضاء السيبراني مسرحًا لها، وهو ما يعرف بالجرائم السيبرانية أو الجرائم الإلكترونية[١].

تمثل الجرائم السيبرانية تحديًا كبيرًا للأنظمة القانونية التقليدية، نظرًا لطبيعتها المتجاوزة للحدود الجغرافية وسرعة تطورها وصعوبة اكتشافها وإثباتها. فهي جرائم تتسم بالتعقيد والتطور المستمر، وتستهدف الأفراد والمؤسسات والدول على حد سواء؛ ما يجعل مكافحتها تحديًا يتطلب تضافر الجهود على المستويين الوطني والدولي[٢].

تعرّف الجرائم السيبرانية بأنها "الأفعال غير المشروعة التي ترتكب بواسطة الحاسب الآلي أو شبكات الاتصال أو تكون موجهة ضدهما، وتشكل انتهاكًا للحقوق والمصالح المحمية قانونًا". وتشمل هذه الجرائم مجموعة واسعة من الأفعال غير المشروعة، مثل الاختراق، والتجسس الإلكتروني، والاحتيال الإلكتروني، وسرقة الهوية، وجرائم الابتزاز الإلكتروني، وجرائم الإرهاب السيبراني، وغيرها.

ولقد أدت الزيادة المطردة في حجم هذه الجرائم وتأثيرها الكبير على الأمن القومي والاقتصادي للدول إلى ضرورة تطوير منظومة قانونية متكاملة لمكافحتها على المستويين الوطني والدولي. فقد سعت العديد من الدول إلى تحديث تشريعاتها الجنائية لتشمل تجريم الأفعال المرتكبة في الفضاء السيبراني، كما تم إبرام العديد من الاتفاقيات الدولية والإقليمية لمكافحة هذه الظاهرة الإجرامية العابرة للحدود.

إن التطور المستمر في وسائل تكنولوجيا المعلومات والاتصالات قد فرض تحديات جديدة على المشرع الجنائي، تتمثل في ضرورة تكييف النصوص القانونية التقليدية لتشمل الأفعال المستحدثة في البيئة الرقمية، أو استحداث نصوص جديدة تتناسب مع

---

[١] نعمة، أحمد عبيس، وكلنتر، زهراء عماد محمد. (٢٠٢٠). تكييف الهجمات السيبرانية في ضوء القانون الدولى. مجلة الكوفة للعلوم القانونية والسياسية، مج١٣، ع٤٤، ٤٩– ٧٤.

[٢] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩– ١٥٢.

طبيعة هذه الجرائم. كما فرض هذا التطور تحديات إجرائية تتعلق بإثبات هذه الجرائم وجمع الأدلة الرقمية وتقديمها أمام المحاكم[٣].

وتزداد خطورة الجرائم السيبرانية مع تزايد اعتماد المجتمعات على تكنولوجيا المعلومات في كافة أنشطتها الحيوية، وتحول العديد من الخدمات الأساسية إلى الفضاء الرقمي؛ ما يجعل هذه المجتمعات أكثر عرضة للهجمات السيبرانية التي يمكن أن تستهدف البنية التحتية الحيوية والمنشآت الحساسة؛ ما يؤثر بشكل مباشر في الأمن القومي للدول.

يهدف هذا البحث إلى دراسة الجرائم السيبرانية في إطار القانون الجنائي، من خلال تحليل مفهومها وأنواعها وخصائصها، والإطار القانوني لمكافحتها، والتحديات التي تواجه تطبيق القانون في هذا المجال، وآليات المكافحة الفعالة، والتحديات المستقبلية في هذا الإطار.

في ضوء ما سبق عرضه في المقدمة، يمكن القول بأن تطور الجريمة السيبرانية لم يأتِ بمعزل عن التحولات الاقتصادية والاجتماعية الكبرى التي فرضتها الثورة الصناعية الرابعة، حيث وفّرت البيئة الرقمية الجديدة فرصًا هائلة للمجرمين لتنفيذ أفعالهم دون التقيد بقيود الزمان والمكان. وقد أصبحت الجرائم السيبرانية أكثر احترافية في عصر الثورة الصناعية الرابعة، مع تزايد الاعتماد على الذكاء الاصطناعي والحوسبة السحابية؛ الأمر الذي أوجد فجوات قانونية جديدة تستدعي تحليلًا دقيقًا لطبيعة التحديات القانونية والأمنية المتولدة عن هذا الواقع الرقمي المتغير باستمرار. ويؤكد الملا أن القانون الجنائي في صيغته التقليدية لم يعد قادرًا بمفرده على احتواء هذه الظاهرة؛ ما يستلزم إعادة هيكلة المفاهيم والمناهج القانونية بما يتناسب مع الطبيعة الافتراضية للجريمة[٤].

ومن الزاوية التشريعية، يمثل غياب التجانس القانوني بين الدول عقبة أساسية في جهود المكافحة، حيث تختلف التعريفات القانونية للجريمة السيبرانية والعقوبات المترتبة

---

[٣] د. مصطفى البنداري أبو سعده، المنهجية القانونية بين القواعد النظرية والمهارات التطبيقية، دار النهضة العربية بالقاهرة، الطبعة الأولى، ٢٠٢٢– ٢٠٢٣

[٤] معاذ سليمان راشد محمد الملا الملا. (٢٠٢٤). الجرائم السيبرانية في عصر الثورة الصناعية الرابعة: الواقع والمأمول "دراسة وصفية تحليلية استشرافية في حقل القانون الجنائي". مجلة الدراسات الفقهية والقانونية، ١٩(ملحق خاص يوليو)، ٢٨–٢٨.

(ISSN: 2537- 0758)

عليها بين دولة وأخرى، وهو ما أشار إليه بونيف وعبد القادر[٥] في دراستهما عن موقف القانون الجزائري من الاتفاق الجنائي في الجرائم السيبرانية. فقد أبرز الباحثان أن غياب النصوص الصريحة التي تعالج مسألة "الاتفاق الجنائي الإلكتروني" يُعدّ من أهم الثغرات التي تستغلها التنظيمات الإجرامية السيبرانية، وأن التشريعات الوطنية، برغم بعض التعديلات، لا تزال عاجزة عن مواكبة السرعة التي تتغير بها أساليب ارتكاب الجرائم الرقمية؛ وهذا يسلط الضوء على الحاجة الملحّة لتوحيد المفاهيم القانونية إقليميًّا ودوليًّا، ووضع أطر تعاون قانوني أكثر فاعلية في هذا المجال.

أما من منظور علم الجريمة، فإن فهم دوافع المجرمين السيبرانيين لا يمكن أن يقتصر على الأبعاد التقنية أو القانونية، بل يجب توسيع التحليل ليشمل النماذج السوسيولوجية والنفسية التي تفسر سلوكهم. وفي هذا السياق، تُبرز دراسة سليمان، ومروة[٦] في تناول أهمية "نظرية الأنشطة الروتينية" بوصفها أداة تحليلية لفهم الجرائم السيبرانية، حيث توضح النظرية أن وقوع الجريمة يتطلب تقاطع ثلاثة عناصر: وجود هدف مناسب، وغياب الحماية الكافية، ووجود مجرم ذي دافعية. وفي البيئة الرقمية، غالبًا ما تكون هذه الشروط متوافرة؛ فالمجرم لا يحتاج إلى وجوده الفعلي في المكان، والحماية التقنية قد تكون ضعيفة أو قابلة للاختراق بسهولة، والهدف متاح في كل لحظة. وهذا التحليل يعكس الحاجة إلى اعتماد مقاربات وقائية متقدمة، لا تقتصر فقط على العقاب، بل تشمل الوقاية والتوعية ومراقبة الأنشطة الرقمية المشبوهة.

كما أن تحليل الإطار القانوني الوطني يشير إلى جهود بعض الدول، ومنها الجزائر، في تضمين الجرائم السيبرانية ضمن التشريعات الجنائية، لكن هذه الجهود لا تزال محدودة من حيث الشمول والتحديث. وقد أوضحت دراسة بوسام وبوناب[٧] أن القانون الجزائري قد أدرج بعض صور الجرائم السيبرانية في تعديلاته الأخيرة، غير أن التحديات التطبيقية لا تزال قائمة، مثل: صعوبة إثبات الجريمة الرقمية، ونقص الكفاءات

---

[٥] بونيف، & عبد القادر. (٢٠٢٥). موقف القانون الجزائري من الاتفاق الجنائي في الجرائم السيبرانية. مجلة البحوث القانونية والاقتصادية، ٨(١)، ٨٥٩-٨٧٤.

[٦] سليمان، & مروة. (٢٠٢٢). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوكية، ٦(٦)، ١١٤-١٣٠.

[٧] بوسام وصال، & بوناب آية. (٢٠٢٥). الجريمة السيبرانية في القانون الجنائي الجزائري (مكتبة كلية الحقوق والعلوم السياسية جامعة محمد البشير الابراهيمي برج بوعريريج).

المتخصصة في التحقيق الرقمي، وضعف البنية التحتية التقنية للأجهزة الأمنية والقضائية، كما تؤكد الدراسة أن القوانين القائمة لا تغطي جميع الأفعال الإجرامية الجديدة؛ مثل: الجرائم المرتبطة بالذكاء الاصطناعي أو العملات المشفرة؛ ما يعكس اتساع الفجوة بين الممارسة الإجرامية والتأطير القانوني.

انطلاقًا من هذه الإشكالات، تزداد الحاجة إلى إعادة النظر في مناهج التشريع والتقاضي لمواكبة تعقيدات البيئة الرقمية، من خلال تطوير منظومة قانونية مرنة وقابلة للتحديث الدوري، وتكثيف التعاون الدولي في مجال تبادل المعلومات والخبرات، إضافة إلى الاستثمار في تدريب وتأهيل الكوادر المتخصصة في التحقيقات السيبرانية؛ فالمعركة ضد الجريمة السيبرانية لا تُكسب فقط عبر النصوص القانونية، وإنما من خلال تكامل التشريع مع التقنية والعلم الاجتماعي، بما يضمن فعالية المكافحة ويحمي المجتمعات من التهديدات الرقمية المتزايدة.

ومن المتوقع أن يسهم هذا البحث في تعزيز فهم ظاهرة الجرائم السيبرانية وآليات مكافحتها، وتقديم مقترحات لتطوير المنظومة القانونية الخاصة بمكافحة هذه الجرائم، بما يتناسب مع طبيعتها المتغيرة والمتطورة باستمرار.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في تزايد معدلات الجرائم السيبرانية عالميًا وتنوع أشكالها وأساليب ارتكابها؛ ما يشكل تحديًا كبيرًا أمام المنظومة القانونية الجنائية التقليدية التي تعتمد على أسس قديمة لا تتماشى مع التعقيدات الرقمية الحديثة؛ ففي ظل الانتشار الواسع لتكنولوجيا المعلومات والاتصالات، أصبحت الجرائم السيبرانية أكثر تعقيدًا وتشعبًا؛ إذ يمكن أن تقف وراءها جهات متعددة، سواء كانت أفرادًا أم جماعات منظمة؛ ما يزيد من صعوبة تتبع الجناة وتحديد المسؤوليات، كما أن الطبيعة الرقمية لهذه الجرائم تجعل من عملية جمع الأدلة وحفظها وإثباتها أمام المحاكم عملية معقدة تتطلب تقنيات وأساليب متطورة لم يكن التقليدي منها نصيبها؛ ما يثير تساؤلات حول كفاية القوانين الجنائية الحالية في التعامل مع هذه الظاهرة المتجددة.

وتتعاظم الإشكالية مع التحديات المتعلقة بتطبيق القانون الجنائي على الجرائم السيبرانية، خاصةً في ظل اختلاف التشريعات الوطنية وتباين مستويات التطور التكنولوجي بين الدول؛ ما قد يؤدي إلى وجود ملاذات آمنة للمجرمين، كما أن مسألة الدليل الرقمي تُشكل تحديًا كبيرًا؛ حيث إن طبيعته المتغيرة وسهولة التلاعب به تُصعّب عملية إثبات الجرائم الرقمية وجمعها بشكل مقبول قانونيًا، وتسعى الدراسة إلى تقديم رؤية

(ISSN: 2537- 0758)

متكاملة تُوازن بين ضرورة تطوير قوانين فعالة لمكافحة الجرائم السيبرانية وحماية الحقوق والحريات الأساسية للأفراد، مع استعراض آليات التعاون الدولي الفعالة لمواجهة الجرائم العابرة للحدود.

أسئلة الدراسة:

١. ما مدى كفاية القوانين الجنائية التقليدية في مواجهة الجرائم السيبرانية المستحدثة؟
٢. ما التحديات التي تواجه تطبيق القانون الجنائي على الجرائم السيبرانية؟
٣. كيف يمكن التغلب على الصعوبات المتعلقة بإثبات الجرائم السيبرانية وجمع الأدلة الرقمية؟
٤. ما آليات التعاون الدولي الفعالة في مجال مكافحة الجرائم السيبرانية العابرة للحدود؟
٥. ما سبل تطوير المنظومة القانونية لمواكبة التطور المستمر في أساليب ارتكاب الجرائم السيبرانية؟

أهمية الدراسة:

تكتسب هذه الدراسة أهمية كبيرة في ظل التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصالات وتزايد معدلات الجرائم السيبرانية وتأثيرها في مختلف جوانب الحياة. **وتتمثل أهمية الدراسة في:**

الأهمية النظرية:

١. **تقديم إطار مفاهيمي متكامل:** تسهم الدراسة في تقديم إطار مفاهيمي متكامل للجرائم السيبرانية، يشمل تعريفها وخصائصها وأركانها وأنواعها؛ ما يعزز الفهم النظري لهذه الظاهرة.
٢. **تحليل الإطار القانوني:** تحلل الدراسة الإطار القانوني للجرائم السيبرانية على المستويين الوطني والدولي، وتقيم مدى كفايته في مواجهة هذه الجرائم.
٣. **دراسة التحديات الإجرائية:** تتناول الدراسة التحديات الإجرائية المتعلقة بإثبات الجرائم السيبرانية وجمع الأدلة الرقمية؛ ما يسهم في تطوير الأطر النظرية في هذا المجال.
٤. **تحليل آليات المكافحة:** تحلل الدراسة آليات مكافحة الجرائم السيبرانية، سواء على المستوى الوقائي أم العلاجي؛ ما يثري المكتبة القانونية في هذا المجال.

الأهمية التطبيقية:

١. **تطوير المنظومة القانونية:** تسهم الدراسة في تقديم مقترحات لتطوير المنظومة القانونية لمكافحة الجرائم السيبرانية، بما يتناسب مع طبيعتها المتغيرة.

٢. **تعزيز التعاون الدولي:** تسهم الدراسة في تقديم رؤية متكاملة لتعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية؛ ما يسهم في تطوير آليات التعاون العملية.
٣. **تحسين إجراءات التحقيق:** تقدم الدراسة مقترحات لتحسين إجراءات التحقيق في الجرائم السيبرانية وتطوير آليات جمع الأدلة الرقمية وحفظها وتقديمها أمام المحاكم.
٤. **تعزيز الوعي المجتمعي:** تسهم الدراسة في تعزيز الوعي المجتمعي بمخاطر الجرائم السيبرانية وسبل الوقاية منها؛ ما يعزز الأمن السيبراني للمجتمع.
٥. **دعم صانعي القرار:** توفر الدراسة معلومات وتحليلات تساعد صانعي القرار في وضع السياسات والاستراتيجيات الوطنية لمكافحة الجرائم السيبرانية.
٦. **مساعدة الأجهزة الأمنية:** تقدم الدراسة معلومات وأدوات تساعد الأجهزة الأمنية والقضائية في تطوير قدراتها في مجال مكافحة الجرائم السيبرانية.

في ضوء ما سبق، تكتسب هذه الدراسة أهمية خاصة في ظل التحديات المتزايدة التي تفرضها الجرائم السيبرانية على الأمن القومي والاقتصادي للدول، والحاجة الملحة إلى تطوير منظومة قانونية فعالة لمواجهة هذه التحديات.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق الأهداف التالية:

١. تحديد مفهوم الجرائم السيبرانية وخصائصها وأركانها وأنواعها من خلال تحليل التعريفات المختلفة في القوانين الوطنية والاتفاقيات الدولية.
٢. تحليل الإطار القانوني للجرائم السيبرانية عبر دراسة التشريعات الوطنية والاتفاقيات الدولية والإقليمية وتقييم مدى كفايتها وفعاليتها في مواجهة هذه الجرائم.
٣. دراسة التحديات الإجرائية في مكافحة الجرائم السيبرانية من خلال تحليل الصعوبات المتعلقة بإثبات الجرائم الرقمية وجمع الأدلة وحفظها وتقديمها أمام المحاكم.
٤. تحليل آليات مكافحة الجرائم السيبرانية عبر استعراض التدابير الوقائية والأمنية المتبعة وآليات التعاون الدولي ودور الأجهزة الأمنية المتخصصة.
٥. استشراف التحديات المستقبلية في مجال مكافحة الجرائم السيبرانية من خلال تحليل التطورات التقنية والقانونية وتأثيرها في المنظومة القانونية.
٦. تقديم مقترحات لتطوير المنظومة القانونية لمكافحة الجرائم السيبرانية وتعزيز الوعي المجتمعي بمخاطر الجرائم وسبل الوقاية منها.

(ISSN: 2537- 0758)

الدراسات السابقة:

١. **دراسة (نعمة، ٢٠٢٠)[٨] بعنوان: (تكييف الهجمات السيبرانية في ضوء القانون الدولى).** إن التطور الإلكتروني الهائل الذي نعيشه اليوم أدى إلى نشوء تحديات جديدة في المجتمع الدولي ومن هذه التحديات (الهجمات السيبرانية) التي تتميز بسهولة تنفيذها. فأصبح بإمكان الدول تأثير بعضها في بعض عن طريق الهجوم على البنية التحتية الأساسية بكبسة زر واحدة وبرغم ذلك إحداث آثار مدمرة؛ سواء في الحجم الدمار البشري أم المادي. إن المعالم الدقيقة للهجمات السيبرانية لا زالت غير محددة؛ لذلك خصصنا هذه الدراسة للبحث في مفهوم الهجمات السيبرانية والموائمة بينها وبين قواعد القانون الدولي المكتوبة منها والعرفية.

٢. **دراسة (مشوش، ٢٠١٩)[٩] بعنوان: (الجهود الدولية لمكافحة الإجرام السيبراني).** إن التعاون الدولي في مجال مكافحة الجريمة السيبرانية يأخذ مظهرين، الأول يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي، أما المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الإجرام السيبراني فهو التعاون الفني؛ إذ لا يقتصر هذا التعاون الدولي على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول.

International Cooperation In Combating Cybercrime Has Two Aspects. The First Concerns The Need To Cooperate In Law Enforcement To Prosecute, And Punish Criminals After Committing The Crime, Which Cross Jurisdictions With Different Legal Systems, Namely, Judicial Cooperation.. The Second Aspect Of International Cooperation In Combating Cybercrime Is Technical Cooperation. International Cooperation Is Not Limited To Mutual Judicial Assistance, But Also Involves Technical Assistance And The Exchange Of Experience Between States.

---

[٨] نعمة، أحمد عبيس، وكلنتر، زهراء عماد محمد. (٢٠٢٠). تكييف الهجمات السيبرانية في ضوء القانون الدولى. مجلة الكوفة للعلوم القانونية والسياسية، مج١٣، ع٤٤، ٤٩– ٧٤.

[٩] مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣– ٧٢٦.

٣. **دراسة (مصطفى، ٢٠٢٢)[١٠] بعنوان: (الحرب السيبرانية الصينية الأمريكية).** شهد الفضاء السيبراني صراعات وحروب إلكترونية، بين الدول حتى الفواعل غير الدولية سعيًا من كل طرف للسيطرة على مصادر المعلومة، وفرض نفسها قوة سيبرانية؛ لأن من يتحكم في هذا الفضاء الجيوبوليتيكي الافتراضي يتحكم في المجالات الأخرى فالتطور التكنولوجي الهائل الذي شهده العالم أدى إلى ظهور تحول رقمي جديد؛ فأصبح العالم يتحدث عن الاقتصاد الرقمي والمدن الذكية والدبلوماسية الرقمية ودول رقمية، هذا التفاعل الجديد أدى إلى ظهور الصين والولايات المتحدة الأمريكية قوتين سيبرانيتين، في هذا الفضاء سعت كل واحدة إلى تطوير استراتيجيات وبرامج جوسسة حتى تجنيد قراصنة الإنترنت من أجل السيطرة على بيانات الطرف الأخر، هذا الوضع المتأزم أدى بالقوتين إلى ضرورة التفكير في حوكمة الفضاء السيبراني، من خلال منظمات دولية على غرار الأمم المتحدة من أجل تقنينه وتجريم الهجومات الإلكترونية التي تؤدي إلى تدمير اقتصاديات الدول والشركات وتشويه سمعة شخصيات عالمية عبر تقنيات التزييف العميق والبرامج الضارة وإرسال فيروسات فتاكة على غرار دوس وحصان تراودة وغيرها.

٤. **دراسة (بوطلاعة، ٢٠٢٢)[١١] بعنوان: (صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة).** برز الفضاء السيبراني عنصرًا مؤثرًا في النظام الدولي يكشف عن أنماط جديدة من المخاطر والتهديدات السيبرانية التي زاد من حدتها توظيفه لأغراض عسكرية حتى أضحى مهددًا رئيسًا للأمن والسلم الدوليين في ظل تراجع دور منظومة الأمن الجماعي وانتهاج الدول لسياسات عسكرية أحادية الجانب خارج إطار الأمم المتحدة.

Cyberspace has emerged as an influential element in the international system, revealing new patterns of cyber risks and threats that have been exacerbated by its use for military purposes

---

[١٠] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

[١١] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة. مجلة العلوم القانونية والاجتماعية، مج٧، ع٤، ٨١٠- ٨٢٧.

(ISSN: 2537- 0758)

until it has become a major threat to international peace and security in light of the decline in the role of the collective security system and the adoption of unilateral military policies by states outside the framework of the United Nations. This article aims to highlight the most important of those risks and threats and their ability to affect international peace and security and to propose a model framework to enhance the security of this space.

٥. **دراسة (بوطلاعة، ٢٠٢٢)[١٢] بعنوان: (الهجمات السيبرانية علي البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام).** تشكل الهجمات السيبرانية تهديدًا حقيقيًّا للبنية التحتية الحرجة للدول وأمنها القومي، في ظل رقمنة القطاعات الحيوية بعد ما عاشه العالم خلال أزمة كورونا، وانتشار المدن الذكية، ما سوف ينجر عنه المزيد من المخاطر المحتملة على كل واجهة متصلة بالإنترنت. في هذا السياق نبحث في هذه الدراسة الحماية القانونية لهذه البنية التحتية الحرجة من الهجمات السيبرانية في ظل القانون الدولي غير السيبراني وتقييم مدى شمولية قواعده ومبادئه في ظل غياب قانون دولي سيبراني متخصص ودقيق.

٦. **دراسة (حيمد، ٢٠١٩)[١٣] بعنوان: (رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة).** هدفت الدراسة إلى وضع رؤية استراتيجية لمكافحة الجرائم السيبرانية، حيث تم تطبيقها على أعضاء هيئة التدريس بأكاديمية الشرطة اليمنية وقطاع التأهيل والتدريب بالوزارة، عددهم ١٢١ مفردة، وتم استخدام المنهج الوصفي التحليل، والاستبانة أداة دراسة، ومن نتائج الدراسة أن واقع التطرف والإرهاب السيبراني: استغلال شبكة الإنترنت للتحريض على العنف والتطرف، أوجدت العولمة الرقمية فرصة للتشبيك بين الجماعات المتطرفة، بروز أدوات وأنماط حديثة لتجنيد المتطرفين عبر الإنترنت. وأن دور مكافحة الجرائم السيبرانية في تعزيز الأمن الإنساني: تنمية الوعي الاجتماعي بمخاطر ارتكاب الجرائم السيبرانية، والإسهام في تحقيق أهداف الأمن الإنساني بأبعاده المختلفة، والعمل على تحقيق الوقاية المبكرة

---

[١٢] بوطلاعة، وداد، و بوكورو، منال. (٢٠٢٢). صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة. مجلة العلوم القانونية والاجتماعية، مج٧، ع٤، ٨١٠- ٨٢٧.

[١٣] حيمد، محمد مسعد، و مصفى، مصطفى جاد الحق. (٢٠١٩). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. المجلة العربية الدولية للمعلوماتية، مج٧، ع١٢، ٨٣- ١٠٠.

من الجرائم السيبرانية، ورفع نسبة الكفاءة الوطنية والوسائل الأمنية المستخدمة لحماية البنية التحتية الوطنية، وتعزيز الحماية الشخصية على مستوى الفرد. وتوفير الحماية للبنية التحتية الوطنية. وأن معوقات مكافحة الجرائم السيبرانية: قلة الخبرة وضعف التأهيل والتدريب لدى عناصر مكافحة الجرائم السيبرانية، وجود قصور تشريعي كبير في تجريم وردع ارتكاب الجرائم السيبرانية، سهولة الوصول للضحايا عن طريق شبكة الإنترنت. تدني نسبة الإبلاغ عن الجرائم السيبرانية لتجنب الإساءة للسمعة أو زعزعة ثقة العملاء. ومن أهم التوصيات: سرعة إعداد مشروع قانون يسمى (قانون الأمن السيبراني) يعزز مكافحة الجرائم السيبرانية، وحماية المجتمع اليمني سيبرانيًّا، إنشاء هيئة وطنية متخصصة للأمن السيبراني، لحماية الفضاء السيبراني اليمني، إنشاء نيابة متخصصة للتحقيق، ومواجهة وضبط كافة أنواع الجرائم السيبرانية، إنشاء وحدة أمنية نوعية بوزارة الداخلية متخصصة بمكافحة الجرائم السيبرانية، مهامها (مرفقة بالتفصيل بالرؤية الاستراتيجية)، ضرورة توعية المجتمع اليمني– أفرادا ومؤسسات– بطرق الحماية من الجرائم السيبرانية.

٧. **دراسة (ابن داود، ٢٠٢٠)[١٤] بعنوان: (الجرائم السيبرانية: دراسة تأصيلية مقارنة)**. يعنى هذا البحث ببيان الجرائم السيبرانية، وتأصيلها الفقهي، ومقارنتها بالنظام السعودي. بيّن الباحث في هذا البحث: أهمية الموضوع، وأسباب اختياره، وأهدافه، والدراسات السابقة، ومنهج البحث وتقاسيمه، وحقيقة الجرائم السيبرانية، وأركانها، وصورها، وخصائصها، وأنواعها، وأسبابها، وحكم الجرائم السيبرانية على وجه الابتداء والرد، وأثر ارتكاب الجرائم السيبرانية، والاختصاص القضائي في الجرائم السيبرانية، وجهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية، ثم ختمه الباحث بالنتائج، والتوصيات، وفهرس المصادر.

This paper investigates cybersecurity crimes, their jurisprudential roots, and compare them with the Saudi jurisprudential law. The researcher explained the importance of the topic, its goals, the previous literature, the methodology of the research; and investigated cybersecurity crimes, their pillars, forms, types, characteristics, and the jurisprudential verdicts on

[١٤] ابن داود، عبد العزيز بن فهد بن محمد. (٢٠٢٠). الجرائم السيبرانية: دراسة تأصيلية مقارنة. مجلة الاجتهاد للدراسات القانونية والاقتصادية، مج٩، ع٣، ١٤٤– ١٦٦.

(ISSN: 2537- 0758)

cybersecurity crimes, and their impact legally and jurisprudentially, and demonstrated the Saudi Arabia anti-cybersecurity crime efforts. The researcher completed his paper with findings and recommendations; and the list of references.

٨. **دراسة (حسنين، ٢٠١٩)[١٥] بعنوان: (دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي: دراسة مقارنة)**. ترجع أهمية الدراسة محل البحث لأهمية دور الشرطة في مجال مكافحة جرائم المعلوماتية لما فرضته المتغيرات على الساحة الدولية ومنها ما تفرضه التحديات التي تواجه مرحلة النمو الاقتصادي الرقمي التي تمر بها البلاد، التي تستلزم وجود مناخ اقتصادي مستقر يعتمد على المنافسة الشريفة وتكافؤ الفرص، فضلًا عن تطور أنماط الجريمة بمختلف أشكالها باستخدام الحاسب الآلي؛ سواء التي تنال من الأشخاص أم الأموال أم المصلحة العامة. لقد هدفت الدراسة محل البحث إلى: النهوض بدور الشرطة في مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي أسوة بالتجارب في الدول المتقدمة، من خلال دراسة تحليلية مقارنة. وانطلاقًا من أهمية موضوع الدراسة محل البحث، ونظرًا لما عرضه الباحث سابقًا، ولضرورة تقتضيها البحوث العلمية فقد رأينا أن نقدم لموضوع دراستنا في أربعة مباحث، يتناول دور الشرطة الوقائي في مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي في مبحث أول، ثم يتناول دور الشرطة في ملاحقة وتعقب مرتكبي الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي في مبحث ثانٍ، ثم يتناول دور جهاز الشرطة الدولية (الإنتربول) بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي في مبحث ثالث، ثم يتناول مقترحات تطوير الدور الأمني لجهاز الشرطة بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي في مبحث رابع. وفي نهاية المطاف انتهي الباحث إلى مجموعة من النتائج مقدمًا عدة توصيات بشأن النهوض بدور الشرطة في مكافحة الجرائم السيبرانية المستحدثة؛ ومن ثم تحقيق الأمن المعلوماتي وما ينعكس أثره في العلوم الإنسانية ومن ثم إثراؤها.

---

[١٥] حسنين، سعد عاطف عبد المطلب. (٢٠١٩). دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي: دراسة مقارنة. مجلة بحوث كلية الآداب، ج١١٨، ٤٨١-٥٨٧.

٩. **دراسة (الحجار، ٢٠٢١)[١٦] بعنوان: (الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل).** لقد أسهم رقي المجتمعات وتقدمها في شتى المجالات إلى ظهور نمط جديد من الجريمة ارتبط بالتطور التقني والمعلوماتي المعقد والسريع، الذي أطلق عليه عدة مسميات مثل: الجريمة السيبرانية، أو الجريمة المعلوماتية، أو الجريمة الإلكترونية، ونظرا لأن إثبات الجريمة يتطلب دليلًا جنائيًا يبني عليه القاضي حكمه، فقد ظهر ما يسمى بالأدلة الرقمية، ولعل هذه الدراسة تحقق أهدافها من خلال بيان ماهية هذا النوع من الجرائم، وبيان ماهية الأدلة التي تثبتها، ومحاولة إبراز حضور هذه الأدلة أو غيابها في مواد القوانين والتشريعات المحلية والعالمية، أظهرت نتائج الدراسة وجود ثغرات وفراغ تشريعي يعتري الدليل الرقمي، ووجود نقص وضعف في التعامل مع الواقع التقني الذي فرض نفسه في كافة مناحي الحياة، بما فيها الحياة القانونية والقضائية، بالإضافة إلى عدم وجود اتفاق على تعريف المصطلحات المتعلقة بهذا النوع من الجرائم، وقد أوصت الدراسة بعدد من التوصيات كان أهمها ضرورة العمل على نشر التوعية الإلكترونية بين العاملين في السلك القانوني، وتدريب الكوادر الفنية على تقنيات البحث الجنائي الرقمي، بالإضافة إلى تعزيز عمل القضاء في إصدار أحكام وقوانين وتشريعات تستند إلى الدليل الجنائي الرقمي.

١٠. **دراسة (الطريف، ٢٠٢٠)[١٧] بعنوان: (اتجاهات الشباب السعودي نحو الجرائم السيبرانية وخطورتها: دراسة ميدانية).** إن الوعي بالجرائم السيبرانية بين الشباب السعودي أمر مهم، خاصة أن استخدام الإنترنت أصبح نمط حياة اليوم؛ ومن ثم يجب أن يكون الوعي بالجريمة السيبرانية جزءًا من ضرورة حياة المجتمعات المعاصرة؛ ومن هنا حاولت الدراسة فهم مدى إدراك الشباب السعودي واتجاهاتهم نحو خطورة الجرائم السيبرانية، والتفاعلات عبر الفضاء السيبراني، واعتمدت الدراسة في تحليلاتها على عينة غير احتمالية بلغ حجمها (٣٠٠) مفردة، تم جمعها من الشباب الجامعي في الفئة العمرية ١٨-٢٤ سنة، التي تدرس الآن في المرحلة

---

[١٦] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩- ١٥٢.

[١٧] الطريف، عبد الرحمن بن سالم بن فهاد. (٢٠٢٠). اتجاهات الشباب السعودي نحو الجرائم السيبرانية وخطورتها: دراسة ميدانية. مجلة بحوث كلية الآداب، ع١٢٣، ج٣، ١٨٣٣- ١٨٨٣.

(ISSN: 2537- 0758)

الجامعية، من الذكور بجامعة شقراء. وخلصت الدراسة إلى أن من أخطار الجرائم السيبرانية من وجهة نظر عينة الدراسة تشويه السمعة والإضرار بها، وتعرض أفراد المجتمع إلى الابتزاز، التي جاءت في المرتبة الأولى بنسبة ٩٦% ومتوسط حسابي ١.٩٢، وهو ما يعكس حجم الخطر الذي يحيط بأفراد المجتمع نتيجة انتشار الجرائم السيبرانية وتزايد معدلاتها، كما أوضحت نتائج الدراسة أن الوسائل الأكثر تأثيرًا في نشر الجريمة السيبرانية من وجهة نظر عينة الدراسة كان الاستخدام المستمر لمواقع التواصل الاجتماعي بنسبة ٩٩.٥% ومتوسط حسابي بلغ ١.٩٧، وأن الشباب هم الفئة الأولى المستهدفة من الجرائم السيبرانية بنسبة ١٠٠% ومتوسط حسابي بلغ ٢.٠.

١١. **دراسة (بهلول، ٢٠٢١)[١٨] بعنوان: (الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها)**. تعتبر الجرائم السيبرانية من أخطر الجرائم التي يشهدها العالم اليوم، التي تشكل الوجه السلبي لانتشار استعمال تكنولوجيات الإعلام والاتصال والانتقال من العالم التقليدي إلى العالم الرقمي الذي يقوم على اقحام التكنولوجيا في جميع مجالات الحياة، ومع الانتشار الهائل لهذه الجرائم فقد أصبحت تشكل تهديدًا ليس فقط للأفراد، بل للدول ومؤسساتها، وما زاد من خطورتها أنها أصبحت موجهة بدرجة كبيرة إلى فئة الأطفال لما تشكله هذه الفئة من ضحية سهلة لارتكاب هذه الجرائم دون تعرض المجرم لخطر التفطن لجرمه أو حتى اكتشافه، الأمر الذي جعل العمل على حماية الأطفال من مخاطر الجرائم السيبرانية والوقاية منها يتزايد كل يوم ويفرض على الدول تسخير كافة الوسائل القانونية والمادية التي من شأنها المساهمة في الوقاية من مخاطر الجرائم السيبرانية الواقعة على الطفل بمختلف أشكالها ومكافحتها، بما يحول دون انتشارها وتطورها بصورة أكبر مما هي عليه اليوم.

١٢. **دراسة (مهدي، ٢٠٢١)[١٩] بعنوان: (الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري)**. شهد العالم في الألفية الأخيرة تحولات عميقة على كل

---

[١٨] بهلول، سمية. (٢٠٢١). الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. مجلة العلوم القانونية والاجتماعية، مج٦، ع٤، ٢٨٦– ٣٢٤.

[١٩] مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١– ١٢٥.

المستويات الاقتصادية والاجتماعية والثقافية خاصة التكنولوجية، حيث تحولت المجتمعات من مجتمعات استهلاكية إلى مجتمعات صناعية إلى مجتمعات إلكترونية سيبرانية بفضل ما قدمته التكنولوجية الحديثة من خدمات رقمية سريعة قليلة التكاليف بدقة متناهية وبمردودية أكبر، وعلى الرغم من إيجابيات هذه التقانة، فإنها بالمقابل شكلت هاجسًا لكل المجتمعات بسبب إفرازها لمجموعة من السلبيات أهمها ما يعرف بالجرائم السيبرانية. ونظرًا لخصوصية هذه الجرائم باعتبار أنها جرائم عابرة للجغرافيا ولا تميز بين مجتمعات وأخرى، فإن الجزائر تعتبر هي أيضًا من الدول التي عرفت في السنوات الأخيرة ارتفاع مؤشر هذه الجرائم بشكل ملموس، بحسب التقارير الأمنية والعلمية أيضًا، وهو ما جعل المشرع يفكر في سن مجموعة من التشريعات للتصدي لهذه الظاهرة السيبرانية.

In the last millennium، the world has Know a deep transformation in many fields such as the economic, social and cultural fields, especially the technological filed, where the society changed from consuming societies to industrial societies to electronic, cyber societies thanks to what modern technology has provided of quick digital services, with low cost, great accuracy and great return. Despite the positivity of this technology, it become an obsession to societies because of the negativity it has provided such as cybercrime.

١٣. **دراسة (عبدالحميد، ٢٠٢٢)[٢٠] بعنوان: (الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي:** دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة). سعت الورقة للتعرف على الجرائم السيبرانية في زمن كورونا وآثارها على الأمن القومي. وتطرقت إلى مفهوم الهجوم السيراني، مشيرة إلى تزايد تلك الجرائم مع ظهور جائحة كوفيد (١٩). وقد تناولت تحديد طبيعة كوفيد (١٩) تقييم أضراره الاقتصادية وتأثيره على الظاهرة الإجرامية. وأوضحت انحسار الجرائم التقليدية في زمن مرض فيروس كورونا. وعرضت وسائل ارتكاب الجرائم السيبرانية وتقييم مشهدها في زمن كورونا. واستعرضت تقرير جهاز الإنتربول الدولي

[٢٠] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها علي الأمن القومي الاقتصادي: دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠١، ١٨– ٢٥.

(ISSN: 2537- 0758)

(٢٠٢٠) الذي يؤكد تزايد الجرائم السيرانية في زمن كورونا. وتناولت مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتزايد الجرائم السيبرانية في زمن كوفيد (١٩). وأشارت إلى تزايد هجمات الإرهاب السيبراني على المؤسسات والمرافق الطبية في زمن كورونا. وتطرقت إلى الجرائم السيبرانية والأمن الاقتصادي القومي في زمن كورونا ومدى تطور نظرية الأمن القومي للدول، مشيرة إلى مفهوم الأمن القومي الاقتصادي، كما أوضحت آثار الجرائم السيرانية عليه. وتناولت تحليلًا اقتصاديًا للأمم المتحدة بشأن الوضع الاقتصادي العالمي وآفاقه (٢٠٢٢). واختتمت الورقة بالإشارة إلى تقرير البنك الدولي عن الآفاق الاقتصادية الإقليمية عام (٢٠٢٢).

١٤. **دراسة (عبدالحميد، ٢٠٢٢)[٢١] بعنوان: (الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي:** دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة**).** استعرض المقال الجرائم السيبرانية في زمن كورونا وآثارها على الأمن القومي الاقتصادي. ويعد هذا الجزء الحلقة الثانية من البحث وتناول فيها استراتيجية الباحث لمواجهة الجرائم السيبرانية في زمن كوفيد (١٩) واشتملت على الإشكاليات التي فرضتها الدراسة واستوجبت استراتيجية لحلها ومنها أن مرافق ومؤسسات البنى التحتية لمختلف دول العالم المتقدم تبين هشاشة النظام الاقتصادي، وطبيعة مرض فيروس كورونا، ومخاطر العملات الرقمية المشفرة وآثرها على الأمن القومي الاقتصادي، وتزايد ارتكاب الجرائم السيبرانية في زمن (كوفيد ١٩) وتطور وسائل ارتكابها، تحقيق الأمن السيبراني، وتزايد هجمات الإرهاب السيبراني على المؤسسات والمرافق الطبية في زمن كوفيد (١٩). وتطرق إلى أن بعض ركائز الاستراتيجية قد تتضمن تدابير أمنية للتعامل بها مع منظومة الأمن السيبراني ومنها تعزيز التعاون الدولي في مجال مكافحة مرض فيروس كورونا (كوفيد ١٩)، وضرورة إنشاء جهاز لمكافحة الأوبئة والأمراض يتبع منظمة الصحة العالمية ويكون له فروع في المكاتب الإقليمية للمنظمة في مناطق دول العالم، وسرعة إصدار العملات الرقمية للبنوك المركزية أحد بدائل العملات الرقمية المسفرة لتفادي مخاطرها، تعزيز تدابير الأمن السيبراني في مجال العمل عن بعد،

[٢١] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠٠، ٢٤- ٣٣.

الأمن المادي هو خط الدفاع الأول لتحقيق الأمن السيبراني. واختتم المقال بعرض النتائج؛ ومن أبرزها أن العملات الرقمية المشفرة القاسم المشترك في أخطر الجرائم السيبرانية التي تزايدت في زمن كوفيد (١٩)، وأن الأمن المادي هو خط الدفاع الأول لتحقيق الأمن السيبراني لمكافحة الجرائم السيبرانية، وعرض التوصيات الخاصة بتعزيز الأمن السيبراني ومنها ضرورة اتخاذ تدابير جديدة بشأن مراجعة دورية للأمن السيبراني.

١٥. **دراسة (معروف، ٢٠٢٢)[٢٢] بعنوان: (المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية)**. استهدفت الدراسة الكشف عن المشاكل والصعوبات التي تواجه الأجهزة المكلفة بالتحقيق القضائي في الجرائم التي ترتكب في الفضاء الإلكتروني؛ وذلك من خلال دراسة العراقيل التي تواجه المحققين أثناء إجراءات البحث والتحري؛ مثل: العراقيل المتعلقة بخصوصية الدليل الإلكتروني؛ لكونها من بين أكبر العوائق التي يسعى الخبراء من خلالها للوصول إلى الطرق التي تمكن من إثباتها، ويتطلب ذلك ضرورة الاستعانة بوسائل وتقنيات فنية وعلمية متطورة يجب أن تتبعها الأجهزة الأمنية والقضائية في أثناء سير عمليات التحري. إضافة إلى العراقيل المرتبطة بخصوصية التحقيق في الجرائم السيبرانية؛ فالإجراءات والأساليب التي تقوم بها الأجهزة المعنية بالتحقيق تعتبر من أعقد العمليات التي تواجه المحققين؛ مثل: قيام الجاني بتشفير وترميز الحاسب الآلي، وهذه من بين الصعوبات المتعلقة بالتفتيش، وصعوبة ضبط البيانات إذا كانت في شبكات معلوماتية لدولة أخرى، والعراقيل المتعلقة بإجراءات الإنابة القضائية أو تسليم المجرمين.

١٦. **دراسة (عبدالرازق، ٢٠٢٣)[٢٣] بعنوان: (آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية)**. تهدف الدراسة إلى التعرف على آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية، حيث تعد هذه الجرائم من الجرائم المستحدثة التي تمثل خطرًا وتهديدًا على أمن الفرد والمجتمع وعلى كافة

---

[٢٢] معروف، كريم. (٢٠٢٢). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج٤، ع٢، ١٥٨- ١٦٦.

[٢٣] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.

(ISSN: 2537- 0758)

الأجهزة الأمنية في الدولة. وقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت في العالم كله إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا؛ ما ترتب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، فظاهرة الجرائم السيبرانية تعتبر نتاجًا طبيعيًّا لثورة الاتصالات والتكنولوجيا التي أصبحت واسعة الانتشار، التي تحدث عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بهدف تدميرها أو الحصول على معلومات سرية؛ سواء عسكرية أم اقتصادية؛ لذلك سعت المملكة العربية السعودية لحماية مصالحها الوطنية من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني، حيث قامت بإنشاء الهيئة الوطنية للأمن السيبراني بالأمر الملكي رقم ٦٨٠١ بتاريخ ١٤٣٩/٢/١١هـ، لتكون هذه الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، ولحماية المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية والقطاعات الحكومية. واعتمدت الدراسة على المنهج الوصفي التحليلي، واشتملت الدراسة على ثلاثة مباحث بينت ماهية الجريمة السيبرانية، وبيان خصائصها، وصورها، وأركانها، والتعرف على دوافع وأساليب ارتكابها، والتعرف على جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية والتصدي لها. وقد توصلت الدراسة للعديد من توصيات التي ساهمت في الحد من الجرائم السيبرانية ومكافحتها.

١٧. **دراسة (أحمد، ٢٠٢٢)[٢٤] بعنوان: (مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية)**. هدفت هذه الدراسة إلى معرفة الجريمة السيبرانية التي أصبحت خطرًا على الفرد والمجتمع وعلى أمن الدولة؛ لأنها تتقدم بوتيرة سريعة باستخدام المجرمين أحدث التقنيات في تنفيذ هجماتهم السيبرانية. هناء جاءت فكرة هذا البحث ليلقي مزيدًا من الضوء على التطورات التكنولوجيا والجريمة السيبرانية لإلقاء الضوء على مشاكلها وتقييمها، وذلك لتعظيم الاستفادة من مميزاتها وتفادي مخاطرها وسبل التعاون الإقليمي والدولي لمكافحتها، حيث إنه من الصعوبة بمكان بل من المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي والقضاء عليها ومحاكمة مرتكبيها؛ ولهذا قدمت هذه الورقة نظرة حول الجريمة

[٢٤] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

السيبرانية في المبحث الأول، وتناول الاتفاقيات العربية والدولية في المبحث الثاني، ووضع النتائج والتوصيات في خاتمة البحث.

١٨. **دراسة (الفتلاوي، ٢٠٢٣)[٢٥] بعنوان: (الأدلة غير المباشرة ودورها في إثبات جرائم السيبرانية:** دراسة قانونية تحليلية في ضوء الاجتهاد القضائي للمحاكم الدولية**).** تعتمد العديد من القضايا على الأدلة غير المباشرة في الإثبات أمام المحاكم الدولية، لكن موضوع الأدلة غير المباشرة لم يأخذ مكانه من الدراسة والتحليل، فأغلب الدراسات القانونية قد تعرضت لهذا الموضوع في نطاق القانون الوطني، فقد ترتكب الجرائم في ظل غياب الأدلة المباشرة تثبت حقيقة الواقعة، وينطبق ذلك بشكل خاص على طبيعة المحاكمات الدولية؛ لذلك من الصعب إن لم يكن من المستحيل إثبات حقيقة الواقعة المزعومة بالاعتماد على الأدلة المباشرة فقط؛ لذا يبرز هنا دور الأدلة غير المباشرة وضرورتها. فضلًا عن أهميتها الخاصة في عملية إثبات الجرائم الدولية بشكل عام، والجريمة السيبرانية على وجه الخصوص، وتكمن هذه الأهمية في الدور الذي تضطلع به الأدلة غير المباشرة في إثبات هذه الجرائم– السيبرانية– أمام المحاكم الدولية.

- **تعقيب على الدراسات السابقة:**

تُظهر الدراسات السابقة تنوعًا واضحًا في زوايا تناول ظاهرة الجرائم السيبرانية، سواء من حيث البعد القانوني أم السياسي أم الأمني أم الإجرائي، وهو ما يعكس الطبيعة المركبة والمعقدة لهذه الجرائم في ظل التحول الرقمي العالمي المتسارع. وقد تميزت هذه الدراسات بتقديم رؤى متعددة، بعضها سعى إلى التأصيل النظري والفقهي للجريمة السيبرانية، وبعضها الآخر ركز على البُعد الميداني والتطبيقي في تحليل الإشكالات والتحديات الحالية والمستقبلية.

ابتداءً، تبيّن من خلال دراسة (نعمة، ٢٠٢٠) أن هناك إشكالًا حقيقيًا في مواءمة الهجمات السيبرانية مع القواعد التقليدية للقانون الدولي العام؛ إذ إن غموض المعايير المتعلقة بتكييف هذه الهجمات كـ "أعمال عدائية" يخلق فراغًا قانونيًا يحد من فعالية الرد القانوني الدولي. وتلاقي هذه الإشكالية صدى في دراسة (بوطلاعة، ٢٠٢٢) التي

[٢٥] الفتلاوي، أحمد عبيس نعمة، والخزعلي، بهاء عبد الحسين عبد علي. (٢٠٢٣). الأدلة غير المباشرة ودورها في إثبات جرائم السيبرانية: دراسة قانونية تحليلية في ضوء الاجتهاد القضائي للمحاكم الدولية. مجلة الكوفة للعلوم القانونية والسياسية، مج١٦، ع٥٦، ١١٨– ١٢٨.

(ISSN: 2537- 0758)

تناولت التأثير المتزايد للفضاء السيبراني على السلم والأمن الدوليين، معتبرةً أن السياسات الأحادية التي تنتهجها بعض الدول تُقوّض منظومة الأمن الجماعي، ما يستدعي ضرورة بناء نظام قانوني دولي موحّد للفضاء السيبراني.

من جهة أخرى، برز في دراسة (مشوش، ٢٠١٩) التركيز على التعاون الدولي، حيث تم تفصيل أبعاد التعاون القضائي والفني في مكافحة الجريمة السيبرانية. وعلى الرغم من أهمية هذا التناول، فإن الواقع العملي يكشف أن هذا التعاون لا يزال يواجه معوقات سياسية وتشريعية، وهو ما أكدته أيضًا دراسة (أحمد، ٢٠٢٢) من خلال تحليلها للاتفاقيات الإقليمية والدولية. وقد أوضح الباحثون محدودية هذه الاتفاقيات في ظل عدم التزام بعض الدول بتطبيق بنودها بفعالية، بالإضافة إلى ضعف آليات المتابعة.

أما الدراسات التي تناولت التحديات الإجرائية، مثل دراسة (الحجار، ٢٠٢١) ودراسة (معروف، ٢٠٢٢)، فقد سلّطت الضوء على الصعوبات التي تواجه المحقق الجنائي في التعامل مع الأدلة الرقمية، وغياب التفسير القضائي الموحد لها، فضلًا عن قلة الخبرة الفنية اللازمة لدى الكوادر الأمنية والقضائية؛ ومن هنا تبرز الحاجة إلى تعزيز البنية التحتية القانونية والتقنية، مع تطوير برامج تدريبية متخصصة في مجال التحقيقات الرقمية، وهو ما دعت إليه أيضًا دراسة (حيمد، ٢٠١٩) ضمن رؤيتها الاستراتيجية لمكافحة الجرائم السيبرانية في اليمن، التي شددت على ضرورة إنشاء هيئات أمنية وقضائية متخصصة.

كما تميزت بعض الدراسات بتناول بُعد معياري وتحليلي، مثل دراسة (ابن داود، ٢٠٢٠) التي قدّمت تأصيلًا فقهيًا وقانونيًا للجرائم السيبرانية وفق النظام السعودي، ما يُعزز البُعد المقارن في هذا المجال. ومع ذلك، فإن قلة الدراسات المقارنة بين النظم القانونية العربية المختلفة يُعدّ من أوجه القصور المعرفي التي تستوجب المعالجة المستقبلية.

وفي السياق ذاته، قدمت دراسات مثل (عبدالحميد، ٢٠٢٢) و(مهدي، ٢٠٢١) رؤى تحليلية هامة حول التحديات القانونية والاقتصادية المرتبطة بالجرائم السيبرانية، خاصة في ظل جائحة كوفيد-١٩، التي كشفت عن هشاشة بعض الأنظمة السيبرانية للدول، وهو ما دفع إلى التفكير في وضع استراتيجيات أكثر شمولًا، ترتكز على مفهوم الأمن السيبراني كأحد أركان الأمن القومي الاقتصادي.

من جانب آخر، فإن دراسة (الطريف، ٢٠٢٠) التي ركزت على وعي الشباب السعودي بخطورة الجرائم السيبرانية، تكشف عن أهمية البُعد الاجتماعي في مقاربة هذه الظاهرة، وتبرز ضرورة إدماج التوعية الرقمية في السياسات التعليمية والإعلامية الوطنية. هذا ما يتكامل مع دراسة (بهلول، ٢٠٢١) التي خصصت بحثها للوقاية من الجرائم السيبرانية ضد الأطفال، وأوضحت الثغرات في الحماية القانونية لهذه الفئة الضعيفة.

وأخيرًا، فإن دراسة (الفتلاوي، ٢٠٢٣) تناولت مسألة الأدلة غير المباشرة في إثبات الجرائم السيبرانية، مسلطةً الضوء على الصعوبات التي تواجه المحاكم الدولية في إصدار أحكام قائمة على هذا النوع من الأدلة، ما يدعو إلى مراجعة المعايير الإثباتية القضائية الدولية بما يتلاءم مع خصوصيات الجرائم الرقمية.

- **خلاصة التعقيب:**

تؤكد الدراسات السابقة على أن الجرائم السيبرانية تشكّل تحديًا مركبًا لا يمكن التعامل معه بمنهج أحادي البعد، بل يتطلب تنسيقًا بين التشريعات، والسياسات الأمنية، والتعاون الدولي، إضافة إلى الوعي المجتمعي والتقني. ومع ذلك، يلاحظ أن هناك فجوات في بعض الجوانب، منها قلة الدراسات الميدانية الحديثة، والقصور في تناول الأبعاد الاقتصادية والاجتماعية للجرائم السيبرانية في البيئات العربية تحديدًا؛ ومن ثم فإن هذا البحث يسعى إلى سد بعض هذه الفجوات من خلال معالجة الجريمة السيبرانية ضمن الإطار القانوني الجنائي الحديث، مع الأخذ في الاعتبار التحديات الإجرائية والتشريعية التي تفرضها البيئة الرقمية المتغيرة.

- **ما يميز دراستنا عن الدراسات السابقة**:

تتفق دراستنا مع الدراسات السابقة في تناول موضوع الجرائم السيبرانية، لكنها تتميز بالشمولية والتكامل في تناول الموضوع. فبينما ركزت الدراسات السابقة على جوانب محددة من الجرائم السيبرانية، مثل الإطار القانوني في دولة معينة، أو الأدلة الرقمية، أو الهجمات السيبرانية على البنية التحتية، أو آليات المكافحة في دولة محددة، أو الاتفاقيات الدولية، فإن دراستنا تقدم رؤية متكاملة للجرائم السيبرانية في إطار القانون الجنائي، تشمل جميع هذه الجوانب وغيرها.

كما تتميز دراستنا بتناول التحديات المستقبلية في مجال مكافحة الجرائم السيبرانية، واستشراف آفاق التطور في هذا المجال، وتقديم مقترحات لتعزيز المنظومة القانونية لمكافحة هذه الجرائم. بالإضافة إلى ذلك، تتميز دراستنا بالتركيز على التوازن بين فعالية

(ISSN: 2537- 0758)

مكافحة الجرائم السيبرانية وحماية الحقوق والحريات الأساسية للأفراد، في ظل التطورات التكنولوجية المتسارعة.

وأخيرًا تتميز دراستنا بتناول آليات التعاون الدولي في مكافحة الجرائم السيبرانية بشكل مفصل، وتحليل التحديات التي تواجه هذا التعاون، وتقديم مقترحات لتعزيزه.

المبحث الأول

مفهوم الجرائم السيبرانية وخصائصها وأنواعها

المطلب الأول

تعريف الجرائم السيبرانية وخصائصها وأركانها

الفرع الأول

تعريف الجرائم السيبرانية

شهد مفهوم الجريمة السيبرانية تطورًا كبيرًا مع تطور تكنولوجيا المعلومات والاتصالات، وقد تعددت التعريفات التي قدمها الفقهاء والتشريعات والمنظمات الدولية لهذا المفهوم. **ويمكن تصنيف هذه التعريفات إلى عدة اتجاهات:**

الاتجاه الضيق: يقصر مفهوم الجريمة السيبرانية على الأفعال غير المشروعة التي تستهدف نظم المعلومات والبيانات الإلكترونية ذاتها. ومن أنصار هذا الاتجاه الفقيه الأمريكي "باركر" الذي عرّف الجريمة السيبرانية بأنها "أي فعل غير مشروع يتطلب معرفة بتكنولوجيا الحاسب الآلي لارتكابه أو التحقيق فيه أو ملاحقته"[٢٦].

الاتجاه الواسع: يوسع مفهوم الجريمة السيبرانية ليشمل جميع الأفعال غير المشروعة التي ترتكب باستخدام الحاسب الآلي وشبكات الاتصال أو تكون موجهة ضدهما. ومن أنصار هذا الاتجاه الفقيه "هافنر" الذي عرّف الجريمة السيبرانية بأنها "أي جريمة يمكن ارتكابها عن طريق نظام حاسوبي أو شبكة حاسوبية، والجرائم التي تشمل حيازة معلومات غير قانونية ونشرها وعرضها عبر نظام حاسوبي أو شبكة حاسوبية"[٢٧].

---

[٢٦] Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج٩، ع١، ١٧٥٢– ١٧٦٥. مسترجع من http://search.mandumah.com/Record/1484671

[٢٧] مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١– ١٢٥.

تعريفات المنظمات الدولية:

١. **منظمة الأمم المتحدة:** عرّفت الجريمة السيبرانية في المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين (٢٠٠٠) بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو في نطاق نظام حاسوبي أو شبكة حاسوبية"[٢٨].

٢. **الاتحاد الدولي للاتصالات:** عرّفها بأنها "الأفعال التي ترتكب ضد أفراد أو جماعات بدافع إجرامي، وبنية إلحاق الضرر بسمعتهم أو التسبب بأذى جسدي أو نفسي لهم، أو خسائر مالية لهم، وذلك باستخدام شبكات الاتصال الحديثة مثل الإنترنت أو الهواتف المحمولة"[٢٩].

٣. **اتفاقية بودابست لمكافحة جرائم الإنترنت (٢٠٠١):** لم تقدم تعريفًا محددًا للجريمة السيبرانية، بل اكتفت بتحديد الأفعال التي تعتبر جرائم سيبرانية، مثل الاعتداء على سرية وسلامة وتوافر البيانات والأنظمة الحاسوبية، والاحتيال المرتبط بالحاسوب، والجرائم المتعلقة بالمحتوى[٣٠].

التعريفات التشريعية:

١. **التشريع المصري:** عرّف قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ الجريمة السيبرانية بأنها "أي جريمة ترتكب باستخدام وسيلة أو أكثر من وسائل تقنية المعلومات أو أنظمة معلوماتية أو شبكة معلوماتية".

٢. **التشريع السعودي:** عرّف نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ الجريمة السيبرانية بأنها "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[٣١].

---

[٢٨] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩- ١٥٢.

[٢٩] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.

[٣٠] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٣١] الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.

(ISSN: 2537- 0758)

٣. **التشريع الإماراتي:** عرّف المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الجريمة السيبرانية بأنها "الأفعال التي تشكل انتهاكًا للتشريعات النافذة، سواء بالدخول غير المشروع إلى الأنظمة المعلوماتية، أو إتلاف البيانات والمعلومات، أو تعطيل الشبكات"[٣٢].

من خلال استعراض التعريفات السابقة، يمكن تعريف الجريمة السيبرانية بأنها "كل فعل أو امتناع عن فعل يرتكب عمدًا وينشأ عنه الاعتداء على الأموال المادية أو المعنوية، ويتم تنفيذه باستخدام وسيلة إلكترونية، سواء كانت هذه الوسيلة الإلكترونية محلًّا للاعتداء أم أداة لتنفيذه، ويكون معاقبًا عليه قانونًا".

الفرع الثاني
خصائص الجرائم السيبرانية

تتميز الجرائم السيبرانية بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، وتجعل من مكافحتها تحديًا كبيرًا للأجهزة الأمنية والقضائية. **ومن أهم هذه الخصائص:**

- **الطبيعة العابرة للحدود:** تتجاوز الجرائم السيبرانية الحدود الجغرافية للدول، فيمكن أن يكون الجاني في دولة والضحية في دولة أخرى ووسيلة ارتكاب الجريمة في دولة ثالثة؛ ما يثير إشكاليات تتعلق بالاختصاص القضائي وتطبيق القانون[٣٣].
- **السرعة والخفاء:** يمكن ارتكاب الجرائم السيبرانية بسرعة كبيرة وبشكل خفي؛ ما يصعب اكتشافها في الوقت المناسب. كما يمكن للجاني إخفاء هويته باستخدام تقنيات مختلفة، مثل: تغيير عنوان IP، أو استخدام شبكات الهوية المجهولة[٣٤].
- **التقنية العالية:** تتطلب الجرائم السيبرانية مهارات تقنية عالية، سواء في ارتكابها أم في التحقيق فيها وكشفها؛ ما يتطلب توفير كوادر متخصصة في مجال الأمن السيبراني والتحقيق الرقمي[٣٥].

---

[٣٢] د. محمد عادل عسكر، د. أكمل يوسف السعيد، القواعد الأساسية لأصول البحث القانوني مطبعة جامعة المنصورة، بدون تاريخ

[٣٣] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢– ٣٥٥.

[٣٤] معروف، كريم. (٢٠٢٢). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج٤، ع٢، ١٥٨– ١٦٦.

- **الأثر الواسع:** يمكن أن تؤثر الجرائم السيبرانية على عدد كبير من الضحايا في وقت واحد، بل يمكن أن تستهدف بنية تحتية حيوية لدولة بأكملها؛ ما يزيد من خطورتها.[٣٦]
- **صعوبة الإثبات:** يصعب إثبات الجرائم السيبرانية نظرًا لطبيعة الأدلة الرقمية التي يمكن محوها أو تعديلها بسهولة، وصعوبة ربط الجاني بالجريمة إذا استخدم تقنيات لإخفاء هويته[٣٧].
- **التطور المستمر:** تتطور الجرائم السيبرانية باستمرار مع تطور التكنولوجيا؛ ما يتطلب تطويرًا مستمرًا للتشريعات وآليات المكافحة[٣٨].
- **الطبيعة الاقتصادية:** غالبًا ما تكون الدوافع وراء ارتكاب الجرائم السيبرانية اقتصادية، مثل الاحتيال الإلكتروني، وسرقة البيانات المالية، والابتزاز الإلكتروني؛ ما يؤدي إلى خسائر اقتصادية كبيرة[٣٩].
- **استغلال الثغرات الأمنية:** تعتمد الجرائم السيبرانية على استغلال الثغرات الأمنية في النظم المعلوماتية؛ ما يتطلب جهودًا مستمرة لتحديث هذه النظم وسد الثغرات[٤٠].
- **تعدد الجهات الفاعلة:** يمكن أن تقف وراء الجرائم السيبرانية جهات مختلفة، بدءًا من الأفراد، مرورًا بالمنظمات الإجرامية، وصولًا إلى الدول التي يمكن أن تستخدم الهجمات السيبرانية وسيلة للحرب الهجينة[٤١].

---

[٣٥] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩- ١٥٢.

[٣٦] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢- ٣٥٥.

[٣٧] معروف، كريم. (٢٠٢٢). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج٤، ع٢، ١٥٨- ١٦٦.

[٣٨] مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١- ١٢٥.

[٣٩] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠١، ١٨- ٢٥.

[٤٠] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.

(ISSN: 2537- 0758)

- **انخفاض التكلفة:** تتميز الجرائم السيبرانية بانخفاض تكلفة ارتكابها مقارنة بالجرائم التقليدية، فلا تتطلب سوى حاسب آلي متصل بالإنترنت ومهارات تقنية معينة[٤٢].

تمثل هذه الخصائص تحديات كبيرة للمنظومة القانونية التقليدية، وتتطلب تطوير تشريعات وآليات مكافحة خاصة تتناسب مع طبيعة هذه الجرائم المتغيرة والمتطورة.

الفرع الثالث

أركان الجرائم السيبرانية

تقوم الجرائم السيبرانية، شأنها شأن الجرائم التقليدية، على أركان أساسية يلزم توافرها لقيام المسؤولية الجنائية. وتتمثل هذه الأركان في الركن المادي والركن المعنوي والركن القانوني، بالإضافة إلى ركن خاص بالجرائم السيبرانية؛ وهو الركن المعلوماتي أو التقني.

أولًا: **الركن المادي**:

يتمثل الركن المادي في السلوك الإجرامي الذي يقوم به الجاني؛ سواء كان إيجابيًا (فعل) أم سلبيًا (امتناع عن فعل)، الذي يترتب عليه نتيجة إجرامية، مع وجود علاقة سببية بين السلوك والنتيجة[٤٣]. ويتخذ السلوك الإجرامي في الجرائم السيبرانية أشكالًا متعددة، مثل الدخول غير المشروع إلى النظم المعلوماتية، أو اعتراض البيانات، أو إتلاف البرامج والبيانات، أو النشر غير المشروع للمحتوى، أو الاحتيال الإلكتروني. ويتميز الركن المادي في الجرائم السيبرانية بأنه يتم في بيئة افتراضية؛ ما يجعل إثباته أكثر صعوبة، ويتطلب وسائل تقنية متطورة لجمع الأدلة الرقمية[٤٤].

ثانيا: **الركن المعنوي**:

يتمثل الركن المعنوي في الإرادة الآثمة التي تتجه إلى ارتكاب الجريمة؛ سواء في صورة القصد الجنائي (العمد) أم الخطأ غير العمدي. وتتنوع صور الركن المعنوي في الجرائم السيبرانية بين:

---

[٤١] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

[٤٢] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

[٤٣] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.

[٤٤] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩- ١٥٢.

١. **القصد الجنائي العام:** ويتمثل في علم الجاني بعناصر الجريمة وإرادته لتحقيق هذه العناصر، مثل علمه بأنه يدخل إلى نظام معلوماتي دون تصريح وإرادته لهذا الدخول.
٢. **القصد الجنائي الخاص:** ويتمثل في نية خاصة يتطلبها القانون لقيام الجريمة، مثل نية الاحتيال في جرائم الاحتيال الإلكتروني، أو نية الإضرار في جرائم إتلاف البيانات.
٣. **الخطأ غير العمدي:** وقد تقوم بعض الجرائم السيبرانية على أساس الخطأ غير العمدي، مثل التسبب في انتشار فيروس معلوماتي بسبب الإهمال في تأمين النظام المعلوماتي[٤٥].

ثالثاً: الركن القانوني:

يتمثل الركن القانوني في النص القانوني الذي يجرم الفعل ويحدد عقوبته، تطبيقًا لمبدأ "لا جريمة ولا عقوبة إلا بنص". ويواجه الركن القانوني في الجرائم السيبرانية تحديات تتعلق بمدى كفاية النصوص القانونية التقليدية في تجريم الأفعال المستحدثة في البيئة الرقمية؛ ما دفع العديد من الدول إلى إصدار تشريعات خاصة بالجرائم السيبرانية[٤٦].

رابعاً: الركن المعلوماتي (التقني):

يتمثل الركن المعلوماتي في استخدام تقنية المعلومات والاتصالات في ارتكاب الجريمة؛ سواء كانت هذه التقنية محلًّا للاعتداء أم وسيلة لارتكاب الجريمة. وهذا الركن هو ما يميز الجرائم السيبرانية عن الجرائم التقليدية[٤٧].

ويتطلب هذا الركن توافر عناصر معينة، مثل وجود نظام معلوماتي (حاسب آلي، هاتف ذكي، جهاز لوحي)، ووجود بيانات ومعلومات إلكترونية، ووجود شبكة معلوماتية (الإنترنت، الشبكات الداخلية)، واستخدام هذه العناصر في ارتكاب الجريمة[٤٨].

---

[٤٥] مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١– ١٢٥.

[٤٦] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢– ٣١.

[٤٧] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩– ١٣٩٨.

[٤٨] الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩– ١٥٢.

(ISSN: 2537- 0758)

تمثل هذه الأركان الأساس القانوني لتجريم الأفعال في الفضاء السيبراني، وتحتاج إلى فهم عميق من قبل الأجهزة الأمنية والقضائية للتعامل مع الجرائم السيبرانية وإثباتها ومحاكمة مرتكبيها.

المطلب الثاني
أنواع الجرائم السيبرانية وتصنيفاتها

تتنوع الجرائم السيبرانية وتتعدد أنواعها وتصنيفاتها؛ وذلك نظرًا لتطور التكنولوجيا وتعدد استخداماتها. **ويمكن تصنيف الجرائم السيبرانية وفقًا لعدة معايير:**

الفرع الأول
تصنيف الجرائم السيبرانية وفقاً لطبيعة الاعتداء

١. **الجرائم التي تستهدف سرية البيانات والمعلومات:**
   - جرائم الدخول غير المشروع إلى النظم المعلوماتية.
   - جرائم اعتراض البيانات والاتصالات.
   - جرائم التجسس الإلكتروني.
   - جرائم سرقة البيانات والمعلومات الشخصية.
٢. **الجرائم التي تستهدف سلامة البيانات والمعلومات:**
   - جرائم إتلاف البيانات والبرامج.
   - جرائم الفيروسات والبرمجيات الخبيثة.
   - جرائم تعديل البيانات والمعلومات.
   - جرائم حجب الوصول إلى المعلومات (هجمات حجب الخدمة)[٤٩].
٣. **الجرائم التي تستهدف أموال الأفراد والمؤسسات:**
   - جرائم الاحتيال الإلكتروني.
   - جرائم سرقة البطاقات الائتمانية والحسابات المصرفية.
   - جرائم غسل الأموال الإلكتروني.
   - جرائم القرصنة المالية[٥٠].

[٤٩] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢– ٣٥٥.

٤. **الجرائم التي تستهدف الأشخاص:**
   - جرائم الابتزاز الإلكتروني.
   - جرائم التشهير والتهديد والمضايقة عبر الإنترنت.
   - جرائم انتحال الشخصية.
   - جرائم الاستغلال الجنسي للأطفال عبر الإنترنت.
   - جرائم الإرهاب الإلكتروني[٥١].

٥. **الجرائم التي تستهدف المجتمع:**
   - جرائم نشر المحتوى غير المشروع (العنصرية، الكراهية، التطرف).
   - جرائم انتهاك حقوق الملكية الفكرية.
   - جرائم القمار غير المشروع عبر الإنترنت.
   - جرائم الترويج للمخدرات والسلع المحظورة.

الفرع الثاني: تصنيف الجرائم السيبرانية وفقًا لدور تكنولوجيا المعلومات في ارتكابها:

أدى الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات في الحياة اليومية إلى تحوّل هذه الوسائل إلى أدوات مركزية في الأنشطة الإجرامية المستحدثة؛ ما دفع الفقه القانوني إلى اعتماد تصنيفات جديدة للجرائم، تأخذ في الاعتبار العلاقة بين الجريمة والتكنولوجيا. ومن أبرز هذه التصنيفات ما يعتمد على دور تكنولوجيا المعلومات في العملية الإجرامية؛ **أي: ما إذا كانت التكنولوجيا هدفًا للجريمة أم مجرد أداة لتنفيذها. وينقسم هذا التصنيف إلى نوعين رئيسين:**

١. **الجرائم التي تكون فيها تكنولوجيا المعلومات محلًّا للاعتداء:** وهي الجرائم التي تستهدف النظم المعلوماتية والبيانات ذاتها، مثل جرائم الدخول غير المشروع إلى النظم المعلوماتية، وجرائم إتلاف البيانات والبرامج، وجرائم اعتراض البيانات[٥٢].

---

[٥٠] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠٠، ٢٤- ٣٣.

[٥١] بهلول، سمية. (٢٠٢١). الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. مجلة العلوم القانونية والاجتماعية، مج٦، ع٤، ٢٨٦- ٣٢٤.

[٥٢] معروف، كريم. (٢٠٢٢). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج٤، ع٢، ١٥٨- ١٦٦.

(ISSN: 2537- 0758)

- جرائم الدخول غير المشروع (Unauthorized Access): وهي من أكثر الجرائم شيوعًا، وتُرتكب عندما يقوم شخص باختراق نظام معلوماتي دون تصريح قانوني أو إذن سابق من الجهة المالكة له؛ سواء كان الغرض هو العبث بالمعلومات، أم التجسس، أم التلاعب في البيانات. ويعد هذا الفعل خرقًا لسرية البيانات وانتهاكًا للحق في الخصوصية المعلوماتية، ويجرمه العديد من التشريعات العربية والدولية مثل المادة ٣ من اتفاقية بودابست (٢٠٠١) الخاصة بالجريمة السيبرانية.
- جرائم إتلاف أو تعديل البيانات والبرامج (Data/Program Alteration or Destruction): يقوم المجرم في هذا النوع من الجرائم بحذف، أو تعديل، أو إتلاف البيانات الرقمية أو البرامج الإلكترونية؛ ما يسبب أضرارًا كبيرة للجهات المتضررة؛ سواء كانت مؤسسات حكومية أم خاصة. هذه الجريمة لا تقتصر على الفعل المتعمد، بل تشمل أيضًا تحميل الفيروسات أو البرمجيات الخبيثة مثل "حصان طروادة" أو "برامج الفدية" (Ransomware).
- جرائم اعتراض البيانات (Data Interception): تعني التنصت أو التجسس على البيانات أثناء انتقالها عبر شبكة معلوماتية. قد يستهدف الجاني هنا الاستحواذ على معلومات حساسة مثل كلمات المرور، أو الحسابات البنكية، أو المستندات الرسمية أثناء إرسالها من مرسل إلى مستقبل، ما يُشكل خرقًا واضحًا لسرية الاتصالات الرقمية.
- تُظهر هذه الجرائم خطورتها في أنها تقوّض البنية التحتية المعلوماتية وتستهدف المكونات التقنية الأساسية للفضاء السيبراني؛ ما يجعل من الضروري تطوير تشريعات جنائية متخصصة تُعنى بحماية النظم والبيانات من هذه التهديدات النوعية.

٢. **الجرائم التي تكون فيها تكنولوجيا المعلومات وسيلة لارتكاب الجريمة:** وهي الجرائم التي يتم فيها استخدام تكنولوجيا المعلومات وسيلة لارتكاب جرائم تقليدية، مثل جرائم الاحتيال الإلكتروني، وجرائم الابتزاز الإلكتروني، وجرائم نشر المحتوى غير المشروع[٥٣].

[٥٣] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩– ١٣٩٨.

في هذا النوع من الجرائم، لا تكون تكنولوجيا المعلومات هدفًا مباشرًا للجاني، بل تُستخدم أداة لتسهيل ارتكاب جرائم تقليدية أخذت بُعدًا جديدًا نتيجة توظيف الوسائل الرقمية. وتُعد هذه الجرائم الأكثر شيوعًا وانتشارًا في المجتمعات المعاصرة، **وتشمل:**

- **جرائم الاحتيال الإلكتروني (Cyber Fraud):** يُستخدم الإنترنت ووسائل الاتصال الحديثة وسائل لخداع الضحايا والاستيلاء على أموالهم بطرق احتيالية، مثل إنشاء مواقع وهمية، أو إرسال رسائل بريد إلكتروني احتيالية (Phishing) تهدف للحصول على معلومات بنكية أو مالية. هذه الجرائم تزداد انتشارًا مع اعتماد المؤسسات المالية على الخدمات المصرفية الإلكترونية.
- **جرائم الابتزاز الإلكتروني (Cyber Extortion):** تُرتكب عندما يهدد الجاني الضحية بنشر صور أو معلومات شخصية حساسة ما لم يتم دفع مبالغ مالية أو تنفيذ مطالب معينة. وقد تستخدم تطبيقات التراسل أو منصات التواصل الاجتماعي لنشر أو تهديد الضحايا؛ ما يخلق آثارًا نفسية واجتماعية بالغة الخطورة، خصوصًا لدى الفئات الضعيفة كالمراهقين والنساء.
- **جرائم نشر المحتوى غير المشروع:** وتشمل الترويج للمخدرات، أو الأسلحة، أو المواد الإباحية، أو خطاب الكراهية، من خلال منصات إلكترونية أو شبكات التواصل الاجتماعي، التي تسهّل الوصول إلى جمهور واسع بسرعة كبيرة. كما تدخل ضمن هذه الجرائم، الممارسات المتعلقة بالتجنيد الإلكتروني لمصلحة الجماعات الإرهابية، ما يجعل هذه الأفعال تمثل تهديدًا مباشرًا للأمن القومي والاجتماعي.

يمثل هذا النوع من الجرائم تحديًا بالغًا للسلطات القانونية، نظرًا لسهولة إخفاء الهوية الرقمية، وسرعة انتشار الجريمة عبر الحدود، ما يتطلب تعزيز التعاون الدولي، وتطوير أدوات رصد ومراقبة رقمية، وتعديل التشريعات لتشمل الأفعال التقليدية حين تُرتكب بوسائل إلكترونية.

الفرع الثالث

تصنيف الجرائم السيبرانية وفقًا للتصنيف الوارد في الاتفاقيات الدولية

تصنف اتفاقية بودابست لمكافحة جرائم الإنترنت (٢٠٠١) الجرائم السيبرانية إلى أربع فئات رئيسة:

١. **الجرائم ضد سرية وسلامة وتوافر البيانات والأنظمة الحاسوبية:**
   - الدخول غير المشروع إلى النظم المعلوماتية.

(ISSN: 2537- 0758)

- الاعتراض غير المشروع للبيانات.
- التدخل في البيانات (الإتلاف، المحو، التعديل).
- التدخل في النظم (تعطيل عمل النظام المعلوماتي).
- إساءة استخدام الأجهزة (إنتاج أو حيازة أدوات لارتكاب الجرائم السابقة)[٥٤].

٢. **الجرائم المرتبطة بالحاسوب:**
- التزوير المرتبط بالحاسوب.
- الاحتيال المرتبط بالحاسوب[٥٥].

٣. **الجرائم المتعلقة بالمحتوى:**
- الجرائم المتعلقة بالمواد الإباحية للأطفال.
- الجرائم المتعلقة بانتهاكات حقوق الملكية الفكرية[٥٦].

٤. **الجرائم المتعلقة بانتهاكات الخصوصية:**
- جمع البيانات الشخصية بطرق غير مشروعة.
- معالجة البيانات الشخصية بطرق غير مشروعة.
- تسريب البيانات الشخصية[٥٧].

الفرع الرابع
تصنيف الجرائم السيبرانية وفقاً للجهة المستهدفة

١. **الجرائم السيبرانية ضد الأفراد:** وهي الجرائم التي تستهدف الأفراد وتمس حقوقهم وحرياتهم وممتلكاتهم، مثل جرائم الابتزاز الإلكتروني، وجرائم سرقة الهوية، وجرائم الاحتيال الإلكتروني (بهلول، ٢٠٢١).

---

[٥٤] حمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٥٥] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٥٦] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٥٧] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

٢. **الجرائم السيبرانية ضد الشركات والمؤسسات:** وهي الجرائم التي تستهدف الشركات والمؤسسات وتمس أصولها ومعلوماتها وسمعتها، مثل جرائم التجسس الصناعي، وجرائم سرقة البيانات التجارية، وجرائم القرصنة المالية[٥٨].

٣. **الجرائم السيبرانية ضد الدول والمنظمات الدولية:** وهي الجرائم التي تستهدف الدول ومؤسساتها ومنظماتها الدولية، وتمس أمنها القومي ومصالحها الحيوية، مثل جرائم الإرهاب الإلكتروني، وجرائم الحرب السيبرانية، وجرائم التجسس الإلكتروني.

الفرع الخامس
تصنيف الجرائم السيبرانية وفقاً لدوافع ارتكابها

- **الجرائم السيبرانية ذات الدوافع المالية:** وهي الجرائم التي ترتكب بدافع الحصول على منافع مالية، مثل جرائم الاحتيال الإلكتروني، وجرائم سرقة البيانات المالية، وجرائم الابتزاز الإلكتروني[٥٩].
- **الجرائم السيبرانية ذات الدوافع السياسية:** وهي الجرائم التي ترتكب بدوافع سياسية، مثل جرائم الحرب السيبرانية، وجرائم التجسس الإلكتروني، وجرائم نشر الدعاية السياسية.
- **الجرائم السيبرانية ذات الدوافع الشخصية:** وهي الجرائم التي ترتكب بدوافع شخصية، مثل جرائم الانتقام، وجرائم التشهير، وجرائم المضايقة[٦٠].
- **الجرائم السيبرانية ذات الدوافع الأيديولوجية:** وهي الجرائم التي ترتكب بدوافع أيديولوجية، مثل جرائم الإرهاب الإلكتروني، وجرائم نشر الكراهية والتطرف[٦١].

---

[٥٨] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠٠، ٢٤- ٣٣.

[٥٩] عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠٠، ٢٤- ٣٣.

[٦٠] بهلول، سمية. (٢٠٢١). الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. مجلة العلوم القانونية والاجتماعية، مج٦، ع٤، ٢٨٦- ٣٢٤.

[٦١] حميد، محمد مسعد، ومصفى، مصطفى جاد الحق. (٢٠١٩). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. المجلة العربية الدولية للمعلوماتية، مج٧، ع١٢، ٨٣- ١٠٠.

(ISSN: 2537- 0758)

المبحث الثاني
الإطار القانوني للجرائم السيبرانية
المطلب الأول
التشريعات الوطنية لمكافحة الجرائم السيبرانية

أدركت العديد من الدول أهمية وضع تشريعات خاصة لمكافحة الجرائم السيبرانية، نظرًا لخصوصية هذه الجرائم وعدم كفاية القوانين التقليدية في التعامل معها. وقد اتخذت هذه التشريعات أشكالًا مختلفة، من تعديل القوانين القائمة إلى سن قوانين خاصة بالجرائم السيبرانية.

الفرع الأول
نماذج للتشريعات الوطنية في الدول العربية

١. **المملكة العربية السعودية:** أصدرت المملكة نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ، ثم تم تحديثه بالمرسوم الملكي رقم م/٧ بتاريخ ١٤٤٣/٣/٢٧هـ. ويتضمن النظام تجريم العديد من الأفعال، مثل الدخول غير المشروع إلى النظم المعلوماتية، والتنصت على البيانات، وإنتاج ونشر البرمجيات الخبيثة، والاحتيال الإلكتروني، والابتزاز الإلكتروني، ونشر المحتوى غير المشروع. كما تم إنشاء الهيئة الوطنية للأمن السيبراني بالأمر الملكي رقم ٦٨٠١ بتاريخ ١٤٣٩/٢/١١هـ، لتكون الجهة المختصة بالأمن السيبراني في المملكة[٦٢].

٢. **جمهورية مصر العربية:** أصدرت مصر قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، الذي يتضمن تجريم مجموعة واسعة من الأفعال، مثل الدخول غير المشروع إلى النظم المعلوماتية، والاعتداء على سلامة البيانات والنظم، والتزوير الإلكتروني، والاحتيال الإلكتروني، وانتهاك الخصوصية، ونشر المحتوى غير المشروع. كما تم إنشاء المجلس الأعلى للأمن السيبراني بقرار رئيس الجمهورية رقم ٤٠٥ لسنة ٢٠٢٠، ليكون الجهة المسؤولة عن وضع استراتيجية الأمن السيبراني في مصر[٦٣].

---

[٦٢] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩– ١٣٩٨.

[٦٣] مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣– ٧٢٦.

٣. **دولة الإمارات العربية المتحدة:** أصدرت الإمارات المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، الذي تم تعديله بالمرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١. ويتضمن القانون تجريم مجموعة واسعة من الأفعال، مثل الدخول غير المشروع إلى النظم المعلوماتية، والاعتداء على البيانات الشخصية، والاحتيال الإلكتروني، ونشر المحتوى غير المشروع. كما تم إنشاء الهيئة الوطنية للأمن السيبراني بمرسوم بقانون اتحادي رقم ٢ لسنة ٢٠١٩، لتكون الجهة المسؤولة عن الأمن السيبراني في الدولة[٦٤].

٤. **الجزائر:** أصدرت الجزائر القانون رقم ٠٩-٠٤ المؤرخ في ٥ أوت ٢٠٠٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويتضمن القانون تجريم مجموعة من الأفعال، مثل الدخول غير المشروع إلى النظم المعلوماتية، والمساس بسلامة البيانات، والاحتيال الإلكتروني. كما تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المرسوم الرئاسي رقم ١٥-٢٦١ المؤرخ في ٨ أكتوبر ٢٠١٥م.

الفرع الثاني
نماذج للتشريعات الوطنية في الدول الأجنبية:

١. **الولايات المتحدة الأمريكية:** تعتبر الولايات المتحدة من أوائل الدول التي أصدرت تشريعات لمكافحة الجرائم السيبرانية. ففي عام ١٩٨٦، تم إصدار قانون الاحتيال والإساءة في استخدام الحاسوب (Computer Fraud and Abuse Act)، الذي تم تعديله عدة مرات ليشمل تجريم مجموعة واسعة من الأفعال، مثل الدخول غير المشروع إلى النظم المعلوماتية، ونشر البرمجيات الخبيثة، والاحتيال الإلكتروني. كما تم إصدار العديد من القوانين الأخرى، مثل قانون حماية خصوصية الاتصالات الإلكترونية (Electronic Communications Privacy Act) عام ١٩٨٦، وقانون حماية الأطفال على الإنترنت[٦٥].

---

[٦٤] ابن داود، عبد العزيز بن فهد بن محمد. (٢٠٢٠). الجرائم السيبرانية: دراسة تأصيلية مقارنة. مجلة الاجتهاد للدراسات القانونية والاقتصادية، مج٩، ع٣، ١٤٤- ١٦٦.

[٦٥] Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج٩، ع١، ١٧٥٢- ١٧٦٥. مسترجع من http://search.mandumah.com/Record/1484671

(ISSN: 2537- 0758)

٢. **المملكـــة المتحـــدة:** أصـدرت المملكـة المتحـدة قـانون إسـاءة اسـتخدام الحاسـوب (Computer Misuse Act) عام ١٩٩٠، الذي تم تعديله عدة مرات، آخرها في عام ٢٠١٥. ويتضمن القانون تجريم الدخول غير المشروع إلى النظم المعلوماتية، وتعديل البيانـات بـدون تصـريح، ونشـر البرمجيـات الخبيثـة. كمـا تـم إصـدار قـانون الاقتصـاد الرقمـي (Digital Economy Act) عام ٢٠١٧، الذي يتضـمن أحكامًا تتعلق بحماية البيانات الشخصية وحقوق الملكية الفكرية على الإنترنت[٦٦].

٣. **ألمانيا:** قامت ألمانيا بتعديل قانون العقوبات في عام ١٩٨٦ لإدخال جرائم الحاسب الآلـي، مثل التجسس علـى البيانـات، والاحتيـال الإلكترونـي، وتغيير البيانـات. ثم تم إصـدار قـانون خـدمات الإعـلام والاتصـالات (Telemedia Act) عـام ٢٠٠٧، الذي يتضـمن أحكامًا تتعلق بحمايـة البيانـات الشخصـية والمسؤولية القانونيـة لمقدمي خدمات الإنترنت[٦٧].

٤. **فرنسا:** أصدرت فرنسا قانون جوتي (Godfrain Law) عام ١٩٨٨، الذي يجرم الـدخول غيـر المشـروع إلـى الـنظم المعلوماتيـة وتعـديل البيانـات بـدون تصـريح. وتـم دمج هذا القانون لاحقًا في قانون العقوبات الفرنسي. كما تم إصدار قانون الثقة في الاقتصـاد الرقمـي (Law for Trust in the Digital Economy) عام ٢٠٠٤، الذي يتضـمن أحكامًا تتعلق بالمسؤولية القانونيـة لمقدمي خـدمات الإنترنـت والتجـارة الإلكترونية[٦٨].

الفرع الثالث

تقييم التشريعات الوطنية لمكافحة الجرائم السيبرانية

أصبحت الجرائم السيبرانية من أكبر التحديات الأمنية والتشريعية التـي تواجهها الدول في العصر الرقمي، نظرًا لتعقيداتها التقنية وتجاوزها للحدود الجغرافية والسيادية التقليدية. وقد استجابت معظم الدول لهذه التهديدات عبر سنّ قوانين وتشريعات وطنية تهدف إلى

---

[٦٦] Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج٩، ع١، ١٧٥٢– ١٧٦٥. مسترجع من http://search.mandumah.com/Record/1484671

[٦٧] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢– ٣١.

[٦٨] مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣– ٧٢٦.

الوقاية من هذه الجرائم وملاحقة مرتكبيها ومعاقبتهم، ومع ذلك فإن هذه التشريعات لا تزال تواجه العديد من التحديات التي تؤثر على فاعليتها، ويمكن تحليلها على النحو التالي:

- **تباين التشريعات بين الدول**:

يمثل اختلاف القوانين الوطنية من دولة لأخرى أحد أبرز المعوقات أمام فعالية مكافحة الجرائم السيبرانية. ففي حين تضع بعض الدول تشريعات متقدمة وشاملة تغطي مختلف أنواع الجرائم الإلكترونية، فإن دولًا أخرى لا تزال تفتقر إلى إطار قانوني واضح في هذا المجال، أو تحتفظ بتشريعات تقليدية غير ملائمة للبيئة الرقمية.

هذا التباين يؤدي إلى ما يُعرف بـ "الملاذات القانونية (Legal Havens)"، حيث يمكن للمجرمين الإلكترونيين استغلال ضعف أو غياب التشريعات في بعض الدول لتنفيذ أو إخفاء أنشطتهم الإجرامية، مع تجنب الملاحقة القضائية. كما أن هذا التباين يُصعّب من التعاون القضائي الدولي؛ إذ يتطلب تسليم المجرمين أو تبادل الأدلة توافقًا قانونيًا بين الأطراف المعنية، وهو أمر غير مضمون في ظل هذا الاختلاف[٦٩].

- **صعوبة مواكبة التطور التكنولوجي**:

يتميز الفضاء السيبراني بالتطور المتسارع في أدوات الاتصال والتشفير والهجوم، وهو ما يُشكّل تحديًا حقيقيًا للمشرعين في معظم دول العالم. فغالبًا ما تستغرق عملية إصدار القوانين سنوات، في حين أن التقنيات الجديدة تظهر في غضون أسابيع أو أشهر؛ ما يجعل العديد من التشريعات عاجزة عن التعامل مع الأفعال الجديدة غير المنصوص عليها قانونًا.

على سبيل المثال، تطورت أساليب الجرائم السيبرانية من الاختراقات البسيطة إلى استخدام الذكاء الاصطناعي، والتزييف العميق (Deepfake)، والبرمجيات الخبيثة المعقدة. مثل هذه الأساليب تتطلب تجريمًا دقيقًا وواضحًا، وهو ما يصعب تحقيقه دون وجود أطر تشريعية مرنة قابلة للتحديث السريع، أو آليات قانونية تتبنى ما يُعرف بـ"التجريم التقديري" الذي يسمح للقاضي بتوسيع التفسير القانوني بما يواكب التطورات التقنية[٧٠].

---

[٦٩] مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣– ٧٢٦.

[٧٠] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢– ٣٥٥.

(ISSN: 2537- 0758)

- **التوازن بين الأمن والحرية**:

تشكل محاولة تحقيق التوازن بين حفظ الأمن السيبراني واحترام الحقوق والحريات الأساسية للأفراد، مثل حرية التعبير وحق الخصوصية، تحديًا قانونيًا وأخلاقيًا كبيرًا. فقد تؤدي بعض التشريعات إلى فرض رقابة صارمة على الإنترنت، أو إلى استخدام تقنيات مراقبة تمسّ بالحريات الشخصية؛ ما يثير مخاوف تتعلق بفرض الدولة لهيمنة رقمية تتعارض مع المبادئ الديمقراطية وحقوق الإنسان.

من الأمثلة على هذه الإشكالية، القوانين التي تسمح بمراقبة المراسلات الإلكترونية أو فرض قيود على منصات التواصل الاجتماعي، إذ قد تُستخدم تحت مسوغ مكافحة الجرائم الإلكترونية، لكنها قد تنزلق إلى التضييق على المعارضين أو النشطاء؛ ومن ثم فإن التحدي هنا يكمن في صياغة تشريعات تحقق الأمن دون الإضرار بالحريات، من خلال النص على ضوابط رقابية وقضائية واضحة لاستخدام تقنيات المراقبة والتحقيق[٧١].

- **قصور القدرات التقنية والمؤسسية**:

حتى في حال وجود تشريعات مناسبة، فإن فعاليتها تعتمد إلى حدّ كبير على قدرة المؤسسات الوطنية على تطبيقها. وفي هذا السياق، تواجه العديد من الدول، خاصة النامية منها، نقصًا في الكوادر البشرية المؤهلة تقنيًا، وغيابًا للبنية التحتية الإلكترونية اللازمة لتحليل الأدلة الرقمية، وتتبع المجرمين، وتأمين الشبكات الوطنية.

كما أن غياب وحدات متخصصة في الشرطة أو النيابة العامة للتعامل مع هذه القضايا يضعف من كفاءة إنفاذ القانون، بل يؤدي أحيانًا إلى تمييع التحقيقات، أو رفض القضايا لعدم كفاية الأدلة الفنية؛ ومن هنا تبرز أهمية الاستثمار في بناء القدرات الوطنية، **من خلال:**

- ✓ إنشاء مراكز وطنية متخصصة في الأمن السيبراني.
- ✓ تدريب القضاة والمحققين على فهم وتحليل الأدلة الرقمية.
- ✓ تطوير التعاون المؤسسي بين الجهات الأمنية والقضائية ومزودي خدمات الإنترنت[٧٢].

---

[٧١] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢– ٣١.

[٧٢] حيمد، محمد مسعد، ومصفى، مصطفى جاد الحق. (٢٠١٩). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. المجلة العربية الدولية للمعلوماتية، مج٧، ع١٢، ٨٣– ١٠٠.

- **الحاجة إلى تحديث مستمر واستجابة تشريعية ديناميكية**:

من أبرز سمات التشريعات الناجحة في هذا المجال أنها قابلة للتعديل والتحديث الدوري، بما يواكب التطورات الرقمية المتسارعة. وقد بادرت بعض الدول إلى وضع أطر تشريعية مرنة تتضمن آليات قانونية تتيح للهيئات المختصة إصدار لوائح تنفيذية أو قرارات تنظيمية بسرعة دون الحاجة إلى تعديل القوانين الأساسية باستمرار.

ويُعتبر تبني مبدأ التشريع الوقائي والاستباقي أحد الأساليب القانونية الفعالة، حيث يُسمح بتجريم الأفعال التي "قد تشكل خطرًا مستقبليًا"؛ ما يساعد على سد الثغرات قبل أن يستغلها المجرمون. كما أن التعاون مع القطاع الخاص وشركات التقنية يعد أمرًا أساسيًا في تحديث التشريعات بما يعكس الواقع الرقمي[٧٣].

المطلب الثاني

الاتفاقيات الدولية والإقليمية لمكافحة الجرائم السيبرانية

نظرًا للطبيعة العابرة للحدود للجرائم السيبرانية، كان من الضروري تطوير إطار قانوني دولي لمكافحة هذه الجرائم، من خلال إبرام اتفاقيات دولية وإقليمية تهدف إلى تنسيق الجهود وتوحيد التشريعات وتعزيز التعاون الدولي في هذا المجال[٧٤].

الفرع الأول

الاتفاقيات الدولية لمكافحة الجرائم السيبرانية

١. **اتفاقية بودابست لمكافحة جرائم الإنترنت (٢٠٠١):** تعتبر اتفاقية بودابست من أهم الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية. تم اعتمادها من قبل مجلس أوروبا في ٢٣ نوفمبر ٢٠٠١، ودخلت حيز التنفيذ في ١ يوليو ٢٠٠٤. **وتهدف الاتفاقية إلى:**
   - توحيد التشريعات الوطنية في مجال مكافحة الجرائم السيبرانية.
   - وضع أسس للتعاون الدولي في التحقيق والملاحقة القضائية.

---

[٧٣] عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩– ١٣٩٨.

[٧٤] الأسدي، عبد الرسول عبدالرضا، والكرعاوي، نصيف جاسم محمد. (٢٠٢١). دور تقنية التأمين لمواجهة المخاطر والأضرار في ظل انتشار جائحة كورونا. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج١٣، ع٤، ٨١٤– ٨٤٣.

(ISSN: 2537- 0758)

- تحديد الأفعال التي تعتبر جرائم سيبرانية، مثل الدخول غير المشروع إلى النظم المعلوماتية، والاعتراض غير المشروع للبيانات، والتزوير والاحتيال المرتبط بالحاسوب، والجرائم المتعلقة بالمواد الإباحية للأطفال.

وقد انضمت إلى الاتفاقية العديد من الدول الأوروبية وغير الأوروبية، مثل الولايات المتحدة الأمريكية وكندا واليابان وأستراليا(٧٥).

٢. **بروتوكول بودابست الإضافي بشأن تجريم الأعمال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب بواسطة أنظمة الحاسب الآلي (٢٠٠٣):** تم اعتماد هذا البروتوكول في ٢٨ يناير ٢٠٠٣، ودخل حيز التنفيذ في ١ مارس ٢٠٠٦. ويهدف إلى تجريم نشر المواد العنصرية والمعادية للأجانب عبر شبكات الإنترنت(٧٦).

٣. **قرارات الجمعية العامة للأمم المتحدة:** أصدرت الجمعية العامة للأمم المتحدة عدة قرارات تتعلق بمكافحة الجرائم السيبرانية، منها:

- القرار ٦٣/٥٥ بتاريخ ٤ ديسمبر ٢٠٠٠ بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات.
- القرار ١٢١/٥٦ بتاريخ ١٩ ديسمبر ٢٠٠١ بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات.
- القرار ٢٣٩/٥٧ بتاريخ ٢٠ ديسمبر ٢٠٠٢ بشأن إنشاء ثقافة عالمية للأمن السيبراني.
- القرار ١٩٩/٥٨ بتاريخ ٢٣ ديسمبر ٢٠٠٣ بشأن إنشاء ثقافة عالمية للأمن السيبراني وحماية البنى التحتية المعلوماتية الحيوية (مشوش، ٢٠١٩).

٤. **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (٢٠٠٠):** برغم أن هذه الاتفاقية لا تتعلق بشكل مباشر بالجرائم السيبرانية، فإنها توفر إطارًا قانونيًا للتعاون الدولي في مكافحة الجريمة المنظمة، بما في ذلك الجرائم السيبرانية التي ترتكبها مجموعات إجرامية منظمة(٧٧).

---

(٧٥) أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

(٧٦) أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

(٧٧) Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج٩، ع١، ١٧٥٢- ١٧٦٥. مسترجع من http://search.mandumah.com/Record/1484671

٥. **المؤتمر الدولي الثالث عشر لمنع الجريمة والعدالة الجنائية (٢٠١٥):** أكد المؤتمر أهمية تعزيز التعاون الدولي في مكافحة الجرائم السيبرانية، وتطوير قدرات الدول في هذا المجال، وتبادل المعلومات والخبرات[٧٨].

الفرع الثاني
الاتفاقيات الإقليمية لمكافحة الجرائم السيبرانية

١. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٠):** تم اعتماد هذه الاتفاقية من قبل مجلس وزراء الداخلية العرب في ٢١ ديسمبر ٢٠١٠، ودخلت حيز التنفيذ في ٧ أكتوبر ٢٠١٤. **وتهدف الاتفاقية إلى:**
   - تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم السيبرانية.
   - توحيد التشريعات الوطنية في هذا المجال.
   - تحديد الأفعال التي تعتبر جرائم سيبرانية، مثل الدخول غير المشروع إلى النظم المعلوماتية، والاعتداء على سلامة البيانات، والاحتيال الإلكتروني، والجرائم المتعلقة بالمحتوى[٧٩].
٢. **اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (٢٠١٤):** تم اعتماد هذه الاتفاقية في ٢٧ يونيو ٢٠١٤، **وتهدف إلى:**
   - إنشاء إطار قانوني للأمن السيبراني وحماية البيانات الشخصية في أفريقيا.
   - تنظيم المعاملات الإلكترونية.
   - تعزيز الثقة في البيئة الرقمية.
   - مكافحة الجرائم السيبرانية[٨٠].
٣. **اتفاقية منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات الدولي (٢٠٠٩):** تم توقيع هذه الاتفاقية في ١٦ يونيو ٢٠٠٩، **وتهدف إلى:**
   - تعزيز التعاون بين الدول الأعضاء في مجال أمن المعلومات.

---

[٧٨] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٧٩] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٨٠] الفتلاوي، أحمد عبيس نعمة، والخزعلي، بهاء عبد الحسين عبد علي. (٢٠٢٣). الأدلة غير المباشرة ودورها في إثبات جرائم السيبرانية: دراسة قانونية تحليلية في ضوء الاجتهاد القضائي للمحاكم الدولية. مجلة الكوفة للعلوم القانونية والسياسية، مج١٦، ع٥٦، ١١٨- ١٢٨.

(ISSN: 2537- 0758)

- مكافحة الإرهاب المعلوماتي والجريمة المعلوماتية.
- حماية البنية التحتية المعلوماتية الحيوية[٨١].

٤. **اتفاقية مجلس أوروبا بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (اتفاقية ١٠٨) (١٩٨١)** :تعتبر هذه الاتفاقية من أقدم الاتفاقيات الدولية في مجال حماية البيانات الشخصية. تم اعتمادها في ٢٨ يناير ١٩٨١، ودخلت حيز التنفيذ في ١ أكتوبر ١٩٨٥. وتهدف إلى حماية الأفراد من إساءة استخدام البيانات الشخصية المعالجة آليًا[٨٢].

٥. **توجيه الاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات (٢٠١٣):** تم اعتماد هذا التوجيه في ١٢ أغسطس ٢٠١٣، **ويهدف إلى:**

- تقريب تشريعات الدول الأعضاء في مجال مكافحة الهجمات ضد أنظمة المعلومات.
- تعزيز التعاون بين السلطات المختصة في الدول الأعضاء.
- تحديد العقوبات المناسبة للجرائم السيبرانية[٨٣].

الفرع الثالث

تقييم الاتفاقيات الدولية والإقليمية لمكافحة الجرائم السيبرانية

تُمثل الاتفاقيات الدولية والإقليمية أحد المرتكزات الأساسية في التصدي للجرائم السيبرانية، لا سيما أن هذه الجرائم بطبيعتها تتجاوز الحدود الوطنية؛ ما يستدعي تعاونًا دوليًا واسع النطاق. وقد أدركت الدول والمنظمات الدولية هذه الحاجة، فبادرت إلى إبرام عدد من الاتفاقيات، من أبرزها **اتفاقية بودابست لمكافحة الجرائم السيبرانية (٢٠٠١)**، التي تُعد أول معاهدة دولية ملزمة قانونيًا في هذا المجال، إضافة إلى جهود إقليمية كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٠)، والاتفاقية الإفريقية للأمن السيبراني. ومع ذلك، وبرغم القيمة القانونية والتنظيمية لهذه الاتفاقيات، فإنها لا تزال تواجه عددًا من التحديات التي تؤثر على فاعليتها وواقعيتها، وتُعرض على النحو التالي:

---

[٨١] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

[٨٢] شرف، ياسين. (٢٠٢٣). الحماية الجنائية للمرأة في الفضاء الرقمي وفق مستجدات القانون ١٠٣.١٣. مجلة قانونك، ع١٥، ٤٧٢- ٤٩٥.

[٨٣] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢- ٣٥٥.

١. عدم شمولية الانضمام:

تشكل محدودية عدد الدول المنضمة لبعض الاتفاقيات الدولية عقبة رئيسة أمام فاعلية هذه الاتفاقيات. على سبيل المثال، لم تُوقّع بعض القوى التكنولوجية الكبرى مثل روسيا والصين والهند على اتفاقية بودابست، برغم أنها من بين الدول الأكثر تأثرًا وفاعلية في الفضاء السيبراني. ويترتب على هذا الغياب تقليص نطاق التعاون الدولي في التحقيق والملاحقة القضائية، وخلق ثغرات قانونية يُمكن للمجرمين استغلالها للتنقل أو تنفيذ العمليات من دول غير ملتزمة بهذه الاتفاقيات.

إن هذه الفجوة تُضعف من قدرة الدول الملتزمة على استكمال عمليات الإنابة القضائية، أو طلب تسليم المتهمين؛ ما يعوق جهود التعاون عبر الحدود. لذا، فإن نجاح أي اتفاقية دولية يعتمد إلى حد كبير على الانضمام الواسع والتمثيل العادل للدول المؤثرة في البيئة السيبرانية[٨٤].

٢. تباين تنفيذ الاتفاقيات:

في حال الانضمام الرسمي إلى الاتفاقيات الدولية، فإن هناك تفاوتًا ملحوظًا بين الدول من حيث درجة الالتزام والتطبيق الفعلي لأحكام هذه الاتفاقيات. فبعض الدول تُدمج الاتفاقيات في قوانينها الوطنية وتُوفر الأطر المؤسسية اللازمة لتنفيذها، في حين تكتفي دول أخرى بالتوقيع أو المصادقة دون اتخاذ خطوات تشريعية وتنظيمية ملموسة.

ويعود هذا التباين إلى عدة عوامل، منها ضعف البنية التحتية القانونية، أو نقص الموارد البشرية والتقنية، أو عدم وجود إرادة سياسية قوية. كما أن بعض الاتفاقيات لا تفرض آليات رقابة أو مساءلة صارمة تضمن التزام الدول؛ ما يؤدي إلى تفاوت في مستوى الحماية القانونية لمكافحة الجرائم السيبرانية بين دولة وأخرى، ويُضعف من أثر الاتفاقيات بوصفها مظلة شاملة[٨٥].

٣. التحديات السياسية وتأثيرها على التعاون السيبراني:

تُعد الاعتبارات السياسية من أهم العقبات أمام التطبيق الفعال للاتفاقيات الدولية. ففي كثير من الحالات، تُستخدم الأدوات السيبرانية وسائل ضغط أو وسائل حرب غير معلنة بين الدول؛ ما يؤدي إلى تسييس الفضاء السيبراني؛ ومن ثم قد تُرفض طلبات

---

[٨٤] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.

[٨٥] مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣- ٧٢٦.

(ISSN: 2537- 0758)

التعاون القانوني أو تسليم المطلوبين تحت ذرائع تتعلق بالسيادة أو الخلافات السياسية، حتى إن كانت الاتفاقية تنص على مثل هذا التعاون.

على سبيل المثال، قد ترفض بعض الدول التعاون مع دول أخرى بحجة "الاعتبارات الأمنية" أو "عدم وجود ثقة متبادلة"، ما يؤدي إلى فشل الاتفاقيات في تحقيق هدفها الأساسي المتمثل في تسهيل التعاون الدولي القضائي والتقني لمكافحة الجريمة السيبرانية. كما أن بعض الدول الكبرى ترفض الخضوع للاتفاقيات متعددة الأطراف وتُفضل إبرام اتفاقيات ثنائية تحقق لها قدرًا أكبر من التحكم والسيطرة؛ ما يُضعف من فكرة العمل الدولي الجماعي[٨٦].

٤. عدم مواكبة التطور التكنولوجي:

إن أحد العيوب البنيوية في أغلب الاتفاقيات الدولية هو بطء إجراءات التعديل والتطوير مقارنة بسرعة التحول الرقمي والتقني. فالاتفاقيات تُعد نصوصًا جامدة نسبيًا، يصعب تعديلها بسرعة، وبالتالي قد تفشل في مواكبة ظهور أشكال جديدة من الجرائم السيبرانية مثل الجرائم المرتبطة بالذكاء الاصطناعي، والتزييف العميق (Deepfake)، والهجمات على البنى التحتية الحيوية عبر أنظمة إنترنت الأشياء (IoT).

وقد أظهرت جائحة كوفيد-١٩ مدى هشاشة الأطر الدولية في التعامل مع الأشكال المستجدة من التهديدات السيبرانية، حيث ارتفعت معدلات الهجمات بشكل لافت، دون أن يكون هناك نصوص اتفاقية صريحة أو آليات تنسيقية كافية للتعامل مع مثل هذه الطوارئ. وبالتالي، هناك حاجة ملحة لأن تعتمد الاتفاقيات على صياغة مرنة، تشمل مفاهيم موسعة، وتُتيح التعديل السريع، مع إنشاء آليات استباقية للرصد والإنذار المبكر بشأن التهديدات التقنية المتجددة[٨٧].

المبحث الثالث

التحديات وآفاق مكافحة الجرائم السيبرانية

تواجه الجرائم السيبرانية تحديات معقدة تتطلب استراتيجيات شاملة ومتكاملة تجمع بين الإجراءات الفنية والقانونية والتنظيمية، في ظل التحول الرقمي المتسارع. ويبرز هذا

---

[٨٦] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

[٨٧] بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢- ٣٥٥.

المبحث من خلال تحليل جوانب عدة تتعلق بخصوصية الدليل الرقمي، وإجراءات التحقيق والملاحقة، وآليات الوقاية والتعاون الدولي، إضافة إلى التحديات التقنية والقانونية وآفاق المستقبل في مكافحة الجرائم السيبرانية[٨٨].

أولًا: خصوصية الدليل الرقمي وإشكالياته:

يمثل الدليل الرقمي جوهر التحقيقات الجنائية في الجرائم السيبرانية؛ فهو كل معلومة إلكترونية مخزنة أو منقولة يمكن الاعتماد عليها لإثبات وقوع الجريمة ونسبتها إلى الجاني. وتختلف أشكال الدليل الرقمي بين البيانات المخزنة على وسائط مثل الأقراص الصلبة والهواتف الذكية، والبيانات المتدفقة عبر الشبكات مثل رسائل البريد الإلكتروني والمحادثات، إلى جانب البيانات الوصفية التي تشمل تفاصيل إنشاء الملفات وتعديلها.

يتسم هذا الدليل بخصائص فريدة مثل عدم ملموسيته وسهولة التلاعب به، وهو ما يشكل تحديًا كبيرًا في الحفاظ على سلامته ومصداقيته. وفي هذا السياق، **تظهر بعض الإشكاليات الأساسية:**

- استخدام تقنيات التشفير وإخفاء الهوية (مثل شبكات VPN وبرامج Tor) التي قد تعيق عملية تتبع الأدلة.
- خطر التدمير الذاتي للبيانات في حالات معينة؛ ما يؤدي إلى فقدان الأدلة بنسبة قد تصل إلى ١٠%.
- صعوبة جمع الأدلة عند وجودها على خوادم تقع خارج الحدود الوطنية، ما يستدعي تعاونًا دوليًا معقدًا[٨٩].
- اختلاف معايير قبول الأدلة الرقمية أمام المحاكم؛ ففي بعض النظم القانونية يُشترط إثبات أصالة الدليل باستخدام تقنيات مثل التوقيع الرقمي وختم الوقت وحساب قيمة التجزئة.

هذه العوامل تجعل من الضروري تطوير آليات تقنية وقانونية لضمان الحفاظ على الأدلة الرقمية وتحقيق العدالة في قضايا الجرائم السيبرانية.

---

[٨٨] بلغيث، عبد الله. (٢٠٢١). التصويت الإلكتروني في سياق الديمقراطية الرقمية السيبرانية: قراءة في المفاهيم والتساؤلات المرتبطة بها. مجلة حقوق الإنسان والحريات العامة، مج٦، ع٣، ٢٥– ٥٢.

[٨٩] مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١– ٢٧٣.

(ISSN: 2537- 0758)

ثانياً: إجراءات التحقيق والملاحقة في الجرائم السيبرانية:

تتطلب الجرائم السيبرانية اعتماد إجراءات تحقيق وملاحقة تختلف بشكل جذري عن الأساليب التقليدية، نظرًا لتعقيد الأدلة وطبيعة الجرائم العابرة للحدود. تعتمد الجهات الأمنية على مجموعة من التقنيات والإجراءات المتطورة، منها:

- **التفتيش الإلكتروني والضبط الرقمي:** تُستخدم برامج تحليل متطورة لاسترجاع البيانات دون الإخلال بسلامتها. كما يُمكن للسلطات إجراء نسخ احتياطي أو تجميد البيانات لمنع تعديلها خلال التحقيقات. وفي حالات معينة، يتم التفتيش عن بُعد على الأنظمة المستهدفة، ما يتطلب مراعاة الجوانب القانونية المتعلقة بسيادة الدول.
- **المراقبة الإلكترونية والإجراءات الاحترازية:** تُمنح السلطات صلاحيات متابعة النشاطات المشبوهة على الشبكات وفقًا لإجراءات قانونية صارمة، كما تُتخذ إجراءات احترازية مثل فصل الأجهزة عن الشبكات لمنع محو أو تغيير البيانات[٩٠].
- **التعاون الدولي في التحقيق:** تُعتبر آليات المساعدة القانونية المتبادلة من الأسس التي يعتمد عليها تبادل الأدلة والمعلومات بين الدول، حيث تمكِّن هذه الآليات من تقصير مدة التحقيقات بنسبة قد تصل إلى ٤٠% في بعض الحالات. كما يعتمد نظام تسليم المجرمين على مبدأ "إما التسليم أو المحاكمة "استنادًا إلى ازدواجية التجريم[٩١].
- **دور الخبراء الفنيين:** يشكل الخبراء في مجال الطب الشرعي الرقمي جسرًا حيويًا بين التقنيات الحديثة والمحاكم، حيث يتم إعداد تقارير فنية تشرح تفاصيل الأدلة بلغة مبسطة؛ ما يسهم في رفع نسبة قبول الأدلة الرقمية أمام القضاء.

ثالثاً: آليات مكافحة الجرائم السيبرانية:

تأتي آليات مكافحة الجرائم السيبرانية في إطار شامل يهدف إلى الوقاية، والكشف، والاستجابة السريعة للهجمات. **ويمكن تقسيم هذه الآليات إلى ثلاثة محاور رئيسة:**

أ. الآليات الوقائية والأمنية:

تتضمن الإجراءات الوقائية ما يلي:

---

[٩٠] ناصر، محمد عبدالرضا، والسرياوي، حيدر كاظم عبد علي. (٢٠١٨). وسائل القتال الحديثة: دراسة في ضوء أحكام القانون الدولي الإنساني. مجلة الكلية الإسلامية الجامعة، ع٤٥، ١٩٧– ٢٢٤.

[٩١] أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢– ٣١.

- **التدابير التقنية:** تعتمد المؤسسات على استخدام جدران الحماية وبرامج مكافحة الفيروسات وأنظمة كشف ومنع الاختراق. كما تُطبق تقنيات التشفير لحماية البيانات الحساسة، ويُستخدم التحقق متعدد العوامل في إدارة الهوية لتقليل مخاطر الاختراق.
- **التدابير التنظيمية:** تُعد سياسات الأمن السيبراني والهياكل التنظيمية المتخصصة داخل المؤسسات ضرورية لتطبيق الإجراءات الأمنية بفعالية. يُجرى تقييم دوري للمخاطر مع الالتزام بمعايير دولية مثل ISO؛ ما يسهم في تقليل الفجوات الأمنية[٩٢].
- **التدابير التوعوية والتثقيفية:** تُنظم حملات توعية عامة ودورات تدريبية متخصصة لتعزيز الوعي بمخاطر الجرائم السيبرانية. كما يتم إدراج موضوعات الأمن السيبراني في المناهج التعليمية وتطوير منصات إلكترونية للإبلاغ عن الحوادث ونشر التحذيرات[٩٣].

ب. التعاون الدولي في مكافحة الجرائم السيبرانية:

يُعتبر التعاون الدولي ركيزة أساسية في مواجهة الجرائم العابرة للحدود، ويشمل:

- **التعاون القانوني والقضائي:** يتم تبادل المعلومات والأدلة بين الدول وفق اتفاقيات تعاون قانوني، ويُعتمد نظام تسليم المجرمين بناءً على ازدواجية التجريم، كما يُعترف بالأحكام القضائية المتبادلة.
- **التعاون الفني والتقني:** يتبادل الخبراء المعلومات والتقنيات الحديثة، ويُجرى بحث مشترك لتطوير أدوات الكشف عن الجرائم السيبرانية، بالإضافة إلى تنسيق فرق الاستجابة للحوادث بين الدول.
- **بناء القدرات:** تُنظم ورش عمل ودورات تدريبية متخصصة لتأهيل الكوادر الفنية والقانونية، ويتم تقديم الدعم الفني والمادي للدول النامية لنقل التكنولوجيا والمعرفة وتطوير التشريعات[٩٤].

---

[٩٢] عباس، سعيدة، وبولعويدات، حورية. (٢٠١٩). وسائل الإعلام ودورها الاستراتيجي في السياق الثقافي: رؤية تحليلية مقارنة بين منظور عزي عبد الرحمان- إدغار موران- أبراهام موليس- ماكلوهان. مجلة العلوم القانونية والاجتماعية، مج٤، ع٤، ٥٦١- ٥٧١.

[٩٣] د. سقلاب فريدة، محاضرات في منهجية العلوم القانونية، جامعة عبد الرحمن ميره، بجايه- الجزائر ٢٠١٧- ٢٠١٨

[٩٤] القضيب، نورة بنت عبد الرحمن، الفوزان، نورة بنت محمد، والدوسري، نوف بنت حسن. (٢٠٢٣). التورط في الجرائم السيبرانية وعلاقته بسلوك المخاطرة لدى عينة من طلبة المرحلتين الثانوية والجامعية بمدينة الرياض. مجلة جامعة الأميرة نورة بنت عبد الرحمن للعلوم التربوية والنفسية، ع١، ١- ٣٢. مسترجع من http://search.mandumah.com/Record/1447409

(ISSN: 2537- 0758)

ج. دور الأجهزة الأمنية المتخصصة:

تلعب الأجهزة الأمنية المتخصصة دورًا محوريًا في مكافحة الجرائم السيبرانية، وتتضمن:

- **أنواع الأجهزة:** تشمل وحدات الشرطة المتخصصة، وهيئات الأمن السيبراني الوطنية، ومراكز الاستجابة للحوادث (CERT/CSIRT)، ووحدات الاستخبارات، والنيابة العامة المتخصصة.
- **المهام والصلاحيات:** تتولى هذه الأجهزة الكشف والتحري وجمع الأدلة الرقمية، وإجراء عمليات التفتيش والضبط، وتنظيم برامج الوقاية والتوعية. كما تسهم في التعاون الدولي من خلال تبادل المعلومات مع الجهات الأمنية الأجنبية.
- **التحديات التي تواجهها:** تعاني هذه الأجهزة تحديات تقنية نتيجة للتطور المستمر في أساليب الجرائم، بالإضافة إلى صعوبات قانونية ونقص في الموارد والكوادر المؤهلة. كما يواجه العمل تنسيقًا محدودًا بين الجهات المحلية والدولية.

رابعاً: تحديات وآفاق مستقبلية في مكافحة الجرائم السيبرانية:

تشهد مكافحة الجرائم السيبرانية تطورًا مستمرًا في ظل ظهور تقنيات جديدة وأساليب هجومية متطورة، ما يستدعي مواكبة التحديات التقنية والقانونية الحالية من خلال تبني آفاق مستقبلية شاملة:

أ. التحديات التقنية:

تتمثل التحديات التقنية في استخدام المجرمين لتقنيات متقدمة لإخفاء الهوية والتشفير؛ ما يعقد عملية جمع الأدلة. كما يُشكل انتشار الحوسبة السحابية وخدمات الاستضافة الخارجية تحديات من حيث تحديد موقع البيانات، في حين يسهم انتشار أجهزة إنترنت الأشياء في زيادة عدد النقاط الضعيفة في النظم الأمنية. تُظهر بعض الدراسات أن حوالي ٦٠% من الهجمات السيبرانية تعتمد على تقنيات إخفاء الهوية والتشفير[٩٥].

ب. التحديات القانونية:

يواجه صانعو السياسات تحديات قانونية تتمثل في اختلاف التشريعات بين الدول؛ ما يؤدي إلى تفاوت في تعريف الجرائم والعقوبات المقررة، بالإضافة إلى صعوبة تحقيق التوازن بين مكافحة الجرائم وحماية الحقوق الأساسية مثل الخصوصية وحرية التعبير.

[٩٥] د. جابر جاد نصار، أصول وفنون البحث العلمي، الطبعة الأولى، دار النهضة العربية بالقاهرة.

كما يُشكّل تباطؤ الإجراءات القانونية الدولية عقبة أمام سرعة تبادل المعلومات وتسليم المجرمين.

ج. آفاق التطور المستقبلية:

تستلزم مواجهة هذه التحديات تبني نهج استباقي يشمل:

- تحديث التشريعات الوطنية والدولية بشكل دوري لتواكب التطورات التقنية.
- زيادة الاستثمارات في البحث والتطوير في مجال الطب الشرعي الرقمي، حيث يمكن أن تُسهم هذه الاستثمارات في خفض نسب الفجوات الأمنية بنسبة تصل إلى ٢٠%.
- تطوير برامج تدريبية متخصصة لتأهيل الكوادر الفنية والقانونية، ما يضمن استجابة أسرع وأكثر كفاءة في مواجهة الجرائم السيبرانية.
- تعزيز التعاون الدولي وتنسيق الجهود بين الجهات المختصة لتقليص مدة التحقيقات وتسليم المجرمين.

الخاتمة

تمثل الجرائم السيبرانية أحد أبرز التحديات التي تواجه البنية القانونية التقليدية، إذ إنها تتميز بطابعها غير المادي، وسرعة انتشارها، وتعقيد أدواتها، إضافة إلى كونها لا تعرف الحدود الجغرافية أو السيادية. لقد أظهرت الإحصائيات الصادرة عن منظمات دولية، مثل **الاتحاد الدولي للاتصالات** و**الشرطة الجنائية الدولية (الإنتربول)**، أن الجرائم الإلكترونية سجلت معدلات نمو غير مسبوقة خلال العقد الأخير، مستهدفة الأفراد والمؤسسات والدول على حد سواء. هذا التوسع في حجم التهديدات يتطلب تطويرًا حقيقيًا وشاملًا للمنظومة التشريعية والجنائية بما يتلاءم مع طبيعة البيئة الرقمية، خاصة في ظل ظهور أنواع جديدة من الجرائم مثل استخدام الذكاء الاصطناعي في تنفيذ الهجمات، أو التلاعب بالمعلومات عبر تقنيات التزييف العميق (deepfake). وهو ما يُبرز الحاجة إلى إعادة النظر في القوانين الجنائية التقليدية من حيث المفاهيم، والنطاق، والأدوات الإجرائية، لتشمل جوانب مثل **تعريف الجريمة السيبرانية، والأدلة الرقمية، والاختصاص القضائي العابر للحدود، وآليات الإنفاذ.**

في ظل الطابع العابر للحدود الذي تتصف به الجريمة السيبرانية، يصبح التعاون الدولي عنصرًا محوريًا في التصدي لها. فمرتكبو هذه الجرائم قد ينفذون هجماتهم من دول لا تربطها اتفاقيات تعاون قضائي أو أمني مع الدولة المتضررة؛ ما يعوق عمليات التحقيق والملاحقة. ولهذا، فإن فعالية مكافحة الجرائم السيبرانية ترتبط ارتباطًا وثيقًا بمدى وجود **اتفاقيات دولية وإقليمية فعالة**، وبمدى التزام الدول بتطبيقها. ومن هنا تبرز

(ISSN: 2537- 0758)

الحاجة إلى تطوير اتفاقيات ذات نطاق أوسع وأكثر شمولية، مثل اتفاقية بودابست، ودعم الدول النامية فنيًا وتشريعيًا لتتمكن من الوفاء بالتزاماتها في هذا المجال. كما أن التكامل المؤسسي على المستوى الوطني يلعب دورًا جوهريًا، إذ يتطلب الأمر وجود أجهزة متخصصة قادرة على التعامل مع التقنيات الحديثة، إلى جانب قضاء مدرَّب ومطلع على مستجدات البيئة الرقمية. وفي هذا السياق، يجب توسيع برامج التدريب للقضاة وأعضاء النيابة وضباط الشرطة، وتحديث البنية التحتية الرقمية للجهات العدلية والأمنية، لتواكب طبيعة هذه الجرائم وآليات ارتكابها.

بالإضافة إلى الإطار القانوني والمؤسسي، فإن الوعي المجتمعي يمثل خط الدفاع الأول في مواجهة الجرائم السيبرانية، إذ تُعد الغالبية العظمى من هذه الجرائم ممكنة بفضل ثغرات سلوكية، مثل مشاركة كلمات المرور، أو التعامل غير الآمن مع الروابط الإلكترونية، أو ضعف الوعي بخطورة التطبيقات المشبوهة. لذلك، فإن بناء مجتمع رقمي آمن يبدأ من الفرد، ويتطلب تنفيذ **حملات توعية شاملة ومستدامة** تستهدف فئات المجتمع المختلفة، خصوصًا الشباب والأطفال، وتعزز من ثقافة الأمن السيبراني. ويجب أن تتضمن هذه الحملات محاور متعددة، منها الاستخدام الآمن للإنترنت، وطرق الوقاية من الابتزاز والاحتيال الإلكتروني، وآليات التبليغ الفوري. من جهة أخرى، فإن الرؤية المستقبلية الفعالة لمكافحة الجرائم السيبرانية تستلزم الجمع بين **التطور التكنولوجي والمرونة القانونية**، بحيث تُوضع تشريعات ذات طابع استباقي، تعتمد على تحليل المخاطر الرقمية المستقبلية، وتُدمج مفاهيم مثل الذكاء الاصطناعي، وسلاسل الكتل (blockchain)، وتشفير البيانات ضمن التشريعات. وبذلك، يمكن بناء منظومة متماسكة توازن بين ضرورات الأمن السيبراني، وحماية الحقوق الأساسية كحرية التعبير وخصوصية البيانات، ما يسهم في ترسيخ دعائم مجتمع رقمي آمن، متماسك، وعادل.

النتائج:

- أثبتت الدراسة أن الجرائم السيبرانية أصبحت تتخذ أشكالًا متعددة ومعقدة، مثل الاحتيال الإلكتروني، وسرقة الهوية، والتجسس الرقمي، والابتزاز، بل وتصل إلى الهجمات الموجهة ضد البنى التحتية للدول.
- تبين أن أغلب التشريعات الوطنية لم تعد قادرة على مواكبة تطور هذه الجرائم من حيث المفاهيم، والأدلة، وآليات التحقيق؛ ما أدى إلى فجوات قانونية واضحة يمكن للمجرمين استغلالها.

- أظهرت الدراسة أن هناك تفاوتًا كبيرًا في مدى التزام الدول بتنفيذ الاتفاقيات الدولية المتعلقة بالأمن السيبراني؛ ما يحد من فعاليتها في مواجهة الجرائم العابرة للحدود.
- تشير النتائج إلى أن العديد من الجهات الأمنية والقضائية تفتقر إلى التدريب المتخصص في التعامل مع الأدلة الرقمية؛ ما يؤثر سلبًا على كفاءة التحقيقات والمحاكمات.
- توضح الدراسة أن الرقمنة المتزايدة للخدمات العامة والخاصة زادت من حساسية المجتمعات تجاه الهجمات السيبرانية التي قد تعطل هذه الخدمات أو تهدد خصوصية الأفراد.
- لوحظ وجود ضعف كبير في مستوى الوعي المجتمعي بمخاطر الجرائم السيبرانية، خاصة بين فئات الشباب والمراهقين؛ ما يجعلهم عرضة أكبر للاستهداف الإلكتروني.
- كشفت الدراسة عن تباين كبير بين الاتفاقيات الدولية في تعريف الجريمة السيبرانية وآليات العقاب؛ ما يعوق التعاون الفعال بين الدول لملاحقة المجرمين الإلكترونيين.

التوصيات:

- يوصى بضرورة تحديث القوانين الجنائية لتشمل صراحةً الجرائم المرتكبة عبر الوسائط الرقمية، مع توضيح مفهوم الجريمة السيبرانية وتحديد أركانها بشكل دقيق.
- ينبغي على الحكومات إنشاء وحدات أمنية وقضائية متخصصة في الجرائم السيبرانية، مزودة بموارد بشرية وتقنية عالية الكفاءة.
- توصي الدراسة بتفعيل الاتفاقيات الدولية القائمة، وتوسيع دائرة الانضمام لها، وتوحيد آليات تسليم المجرمين وتبادل المعلومات بين الدول.
- ضرورة تنظيم حملات توعوية دورية في المدارس، والجامعات، والمؤسسات الحكومية والخاصة، حول وسائل الوقاية من التهديدات السيبرانية وطرق الإبلاغ عنها.
- يجب تنظيم برامج تدريب مستمرة للقضاة وأعضاء النيابة العامة وضباط الشرطة في مجال تحليل الأدلة الرقمية وتقنيات التتبع الإلكتروني.
- تشجيع الحكومات على تعزيز الأمن السيبراني في شبكاتها الحكومية ومرافقها الحيوية، من خلال اعتماد أنظمة حماية وتشفير متقدمة.
- يوصى بإعداد سياسة وطنية واضحة تتضمن رؤية متكاملة لمواجهة التحديات المستقبلية للجريمة السيبرانية، وتشمل التشريع، والتقنية، والتوعية، والتعاون الدولي.

(ISSN: 2537- 0758)

المراجع:

١. نعمة، أحمد عبيس، وكلنتر، زهراء عماد محمد. (٢٠٢٠). تكييف الهجمات السيبرانية في ضوء القانون الدولى. مجلة الكوفة للعلوم القانونية والسياسية، مج١٣، ع٤٤، ٤٩- ٧٤.

٢. الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية:ما بين التأصيل والتأويل.مجلة جامعة الاستقلال للأبحاث،مج٦، ع١، ١٢٩- ١٥٢.

٣. د. مصطفى البنداري أبو سعده، المنهجية القانونية بين القواعد النظرية والمهارات التطبيقية، دار النهضة العربية بالقاهرة، الطبعة الأولى، ٢٠٢٢- ٢٠٢٣

٤. معاذ سليمان راشد محمد الملا الملا. (٢٠٢٤). الجرائم السيبرانية في عصر الثورة الصناعية الرابعة: الواقع والمأمول "دراسة وصفية تحليلية استشرافية في حقل القانون الجنائي". مجلة الدراسات الفقهية والقانونية، ١٩(ملحق خاص يوليو)، ٢٨-٢٨.

٥. بونيف، & عبد القادر. (٢٠٢٥). موقف القانون الجزائري من الاتفاق الجنائي في الجرائم السيبرانية. مجلة البحوث القانونية والاقتصادية، ٨(١)، ٨٥٩-٨٧٤.

٦. سليمان، & مروة. (٢٠٢٢). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوكية، ٦(٦)، ١١٤-١٣٠.

٧. بوسام وصال، & بوناب آية. (٢٠٢٥). الجريمة السيبرانية في القانون الجنائي الجزائري (مكتبة كلية الحقوق والعلوم السياسية جامعة محمد البشير الابراهيمي برج بوعريريج).

٨. نعمة، أحمد عبيس، وكلنتر، زهراء عماد محمد. (٢٠٢٠). تكييف الهجمات السيبرانية في ضوء القانون الدولى. مجلة الكوفة للعلوم القانونية والسياسية، مج١٣، ع٤٤، ٤٩- ٧٤.

٩. مشوش، مراد. (٢٠١٩). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج١٢، ع٢، ٧٠٣- ٧٢٦.

١٠. مصطفى، حميل. (٢٠٢٢). الحرب السيبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج٦، ع٢، ٢٦١- ٢٧٣.

١١. بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة. مجلة العلوم القانونية والاجتماعية، مج٧، ع٤، ٨١٠- ٨٢٧.

١٢. بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢- ٣٥٥.

١٣. حيمد، محمد مسعد، ومصفى، مصطفى جاد الحق. (٢٠١٩). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. المجلة العربية الدولية للمعلوماتية، مج٧، ع١٢، ٨٣- ١٠٠.

١٤. ابن داود، عبد العزيز بن فهد بن محمد. (٢٠٢٠). الجرائم السيبرانية: دراسة تأصيلية مقارنة. مجلة الاجتهاد للدراسات القانونية والاقتصادية، مج٩، ع٣، ١٤٤- ١٦٦.

١٥. حسنين، سعد عاطف عبد المطلب. (٢٠١٩). دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي: دراسة مقارنة. مجلة بحوث كلية الآداب، ج١١٨، ٤٨١- ٥٨٧.
١٦. الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية:ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث،مج٦،ع١، ١٢٩-١٥٢.
١٧. مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١- ١٢٥.
١٨. بهلول، سمية. (٢٠٢١). الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. مجلة العلوم القانونية والاجتماعية، مج٦، ع٤، ٢٨٦- ٣٢٤.
١٩. مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١- ١٢٥.
٢٠. عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها علي الأمن القومي الاقتصادي: دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠١، ١٨- ٢٥.
٢١. عبد الحميد، عماد الدين محمد كامل. (٢٠٢٢). الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج٤٢، ع٥٠٠، ٢٤- ٣٣.
٢٢. معروف، كريم. (٢٠٢٢). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج٤، ع٢، ١٥٨- ١٦٦.
٢٣. عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.
٢٤. أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.
٢٥. الفتلاوي، أحمد عبيس نعمة، والخزعلي، بهاء عبد الحسين عبد علي. (٢٠٢٣). الأدلة غير المباشرة ودورها في إثبات جرائم السيبرانية: دراسة قانونية تحليلية في ضوء الاجتهاد القضائي للمحاكم الدولية. مجلة الكوفة للعلوم القانونية والسياسية، مج١٦، ع٥٦، ١١٨- ١٢٨.
٢٦. Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج٩، ع١، ١٧٥٢-١٧٦٥. مسترجع من http://search.mandumah.com/Record/1484671
٢٧. مهدي، رضا. (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج٦، ع٢، ١١١- ١٢٥.
٢٨. الحجار، عدنان إبراهيم، وبشير، فايز خضر محمد. (٢٠٢١). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج٦، ع١، ١٢٩-١٥٢.

(ISSN: 2537- 0758)

٢٩. عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.
٣٠. أحمد، أيمن عطا عبدالماجد محمد. (٢٠٢٢). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع١٤، ١٢- ٣١.
٣١. عبد الرازق، رانا مصباح عبد المحسن. (٢٠٢٣). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج١٥، ع٥، ١٣٥٩- ١٣٩٨.
٣٢. بوطلاعة، وداد، وبوكورو، منال. (٢٠٢٢). الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج٧، ع٢، ٣٢٢- ٣٥٥.
٣٣. عباس، سعيدة، وبولعويدات، حورية. (٢٠١٩). وسائل الإعلام ودورها الاستراتيجي في السياق الثقافي: رؤية تحليلية مقارنة بين منظور عزي عبد الرحمان- إدغار موران- أبراهام موليس- ماكلوهان. مجلة العلوم القانونية والاجتماعية، مج٤، ع٤، ٥٦١- ٥٧١.
٣٤. الأسدي، عبدالرسول عبدالرضا، و الكرعاوي، نصيف جاسم محمد. (٢٠٢١). دور تقنية التأمين لمواجهة المخاطر والأضرار في ظل انتشار جائحة كورونا. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج١٣، ع٤، ٨١٤- ٨٤٣.
٣٥. بلغيث، عبد الله. (٢٠٢١). التصويت الإلكتروني في سياق الديمقراطية الرقمية السيبرانية: قراءة في المفاهيم والتساؤلات المرتبطة بها. مجلة حقوق الإنسان والحريات العامة، مج٦، ع٣، ٢٥- ٥٢.
٣٦. ناصر، محمد عبدالرضا، و السرياوي، حيدر كاظم عبد علي. (٢٠١٨). وسائل القتال الحديثة: دراسة في ضوء أحكام القانون الدولي الإنساني. مجلة الكلية الإسلامية الجامعة، ع٤٥، ١٩٧- ٢٢٤.
٣٧. د جابر جاد نصار، أصول وفنون البحث العلمي، الطبعة الأولى، دار النهضة العربية بالقاهرة.
٣٨. د. سقلاب فريدة، محاضرات في منهجية العلوم القانونية، جامعة عبد الرحمن ميره، بجايه- الجزائر ٢٠١٧- ٢٠١٨
٣٩. د. محمد عادل عسكر، د. أكمل يوسف السعيد، القواعد الأساسية لأصول البحث القانوني مطبعة جامعة المنصوؤة، بدون تاريخ
٤٠. القضيب، نورة بنت عبد الرحمن، الفوزان، نورة بنت محمد، والدوسري، نوف بنت حسن. (٢٠٢٣). التورط في الجرائم السيبرانية وعلاقته بسلوك المخاطرة لدى عينة من طلبة المرحلتين الثانوية والجامعية بمدينة الرياض. مجلة جامعة الأميرة نورة بنت عبد الرحمن للعلوم التربوية والنفسية، ع١، ١- ٣٢. مسترجع من http://search.mandumah.com/Record/1447409