

بسم الله الرحمن الرحيم



المملكة العربية السعودية

جامعة ميدأوشن

وزارة التعليم

الجرائم السيبرانية في القانون الجنائي

إعداد الطالب :

يزيد صالح المحيميد

الرقم الجامعي : ٢٤٣٠٠٠٦٤٣

إشراف الدكتور :

العام الجامعي

1446 هـ / 2025 م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الإهداء/

(وَأَخِرُ دَعْوَاهُمْ أَنْ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ)

الحمد لله الذي ما نَجَحْنَا وما عَلُّونا وما تَفُوقْنَا إلا بِرِضَاهُ، الحمد لله عند الْبَدْءِ وعند الْخِتَامِ، فَمَا تَنَاهَى دَرْبُ، ولا خَتَمَ جُهْدُ، ولا تم سَعْيٌ إلا بِفَضْلِهِ، الْحَمْدُ لِلَّهِ حُبًّا وَشُكْرًا وَامْتِنَانًا.

لَمْ تَكُنْ الرِّحْلَةُ قَصِيرَةً وَلَا يَنْبَغِي لَهَا أَنْ تَكُونَ، وَلَمْ يَكُنْ الْحُلُمُ قَرِيبًا وَلَا الطَّرِيقُ كَانَ مُحْفُوفًا بِالتَّسْهِيلاتِ، لَكِنِّي بِالْعَزَمِ فَعَلْتُهَا وَبِالْإِصْرَارِ حَصَلْتُ عَلَى مُرَادِي، الْيَوْمُ أَتَوُجُّ اللَّحْظَاتِ الْأَخِيرَةَ فِي ذَلِكَ الطَّرِيقِ الَّذِي كَانَ يَحْمِلُ فِي بَاطِنِهِ الْعَثَرَاتِ وَالْأَشْوَكَ، وَرُغْمًا عَنْهَا ظَلَّتْ قَدَمِي تَخْطُو بِكُلِّ صَبْرٍ وَطُمُوحٍ وَعَزِيمَةٍ وَتَفَاوُلٍ وَحَسَنِ ظَنٍّ بِاللَّهِ، فَالْحَمْدُ لِلَّهِ الَّذِي أَكْرَمَنِي بُلُوغِ غَايَتِي الْعُظْمَى.

- أَهْدِي بِكُلِّ حُبٍّ هَذَا النِّجَاحَ لِنَفْسِي الْعَظِيمَةِ أَوَّلًا الَّتِي تَحَمَّلَتْ كُلَّ الْعَثَرَاتِ وَأَكْمَلَتْ رُغْمَ كُلِّ الصَّعُوبَاتِ،
- وَأَهْدِي هَذَا الْفَخْرَ الْمَهِيْبَ إِلَى مَنْ كَلَّلَهُ اللَّهُ بِالْمَهِيْبَةِ وَالْوَقَارِ، إِلَى مَنْ أَحْمَلُ اسْمَهُ بِكُلِّ فَخْرٍ، إِلَى مَنْ كَانَ الدَّاعِمِ الْأَوَّلَ لَتَحْقِيقِ طُمُوحَاتِي، إِلَى مَنْ آمَنَ بِأَنِّي أَسْتَطِيعُ النِّجَاحَ "والدي الحبيب"
- وَإِلَى مَنْ جَعَلَ اللَّهُ الْجَنَّةَ تَحْتَ قَدَمَيْهَا، إِلَى أَيْقُونَةِ الْحَنَانِ وَأَسَاسِ الْحُبِّ، إِلَى مَنْ سَهَرَتْ وَسَانَدَتْ، إِلَى مَنْ مَهَّدَتْ عَثَرَاتِ مَسِيرَتِي بِدُعَائِهَا، إِلَى مَنْ تَعَجَّرَ كُلُّ الْكَلِمَاتِ عَنْ وَصْفِهَا، إِلَى مَنْ كَانَتْ النُّورُ فِي عَتَمَتِي "والدتي الغالية"

- ثُمَّ إِلَى كُلِّ رُوحٍ وَعَقْلٍ وَقَلْبٍ كَانَ لَهَا ذَلِكَ التَّأْثِيرُ الْإِيجَابِيُّ عَلَى حَيَاتِي، وَعِلْمِي وَتَعْلُمِي،
- وَإِلَى كُلِّ رُوحٍ أَمْنَتْ بِي وَبِمَجْهُودِي، وَسَعَتْ لِأَنْ تُضِيءَ لِي السِّرَاجَ رُغْمَ كُلِّ التَّحْدِيَّاتِ.
- وَلَا أَنْسَى أَسَاتِذَتِي الْكَرَامَ الَّذِينَ لَمْ يَتَوَانَوْا أَبَدًا فِي مَدِيدِ الْعُونِ لِي فِي كُلِّ لَحْظَةٍ.

ها أَنَا أَصِلُ بَعْدَ لَيَالٍ طَوَالٍ قَضِيئُهَا فِي سَبِيلِ الْعِلْمِ،

لَمْ يَمْضِ يَوْمٌ لَمْ أَشْعُرْ فِيهِ بِالتَّعَبِ وَالْإِجْهَادِ، وَلَكِنْ بِالْعَزَائِمِ وَصَلْتُ عِنَانَ السَّمَاءِ وَعَانَقْتُ الْمَجْدَ فَخْرًا..
فَالْحَمْدُ لِلَّهِ عَلَى جُهْدِي وَاجْتِهَادِي الَّذِي مَنْحَنِي اسْمِي مَرَاتِبَ الشَّرَفِ .

فهارس المحتويات

رقم الصفحة	الموضوع
4	المقدمة
5	مشكلة الدراسة
6	أهمية الدراسة
7	أهداف الدراسة
8	الدراسات السابقة
20	المبحث الأول: مفهوم الجرائم السيبرانية وخصائصها وأنواعها
20	المطلب الأول: تعريف الجرائم السيبرانية وخصائصها وأركانها
22	المطلب الثاني: أنواع الجرائم السيبرانية وتصنيفاتها
28	المبحث الثاني: الإطار القانوني للجرائم السيبرانية
29	المطلب الأول: التشريعات الوطنية لمكافحة الجرائم السيبرانية
30	المطلب الثاني: الاتفاقيات الدولية والإقليمية لمكافحة الجرائم السيبرانية
34	المبحث الثالث: التحديات وآفاق مكافحة الجرائم السيبرانية
34	المطلب الأول: خصوصية الدليل الرقمي وإشكالياته
35	المطلب الثاني: إجراءات التحقيق والملاحقة في الجرائم السيبرانية
36	المطلب الثالث: تحديات وآفاق مستقبلية في مكافحة الجرائم السيبرانية
39	الخاتمة
40	المراجع

المقدمة

شهد العالم في العقود الأخيرة تطوراً تكنولوجياً هائلاً 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 مسرحاً لها، وهو ما يعرف بالجرائم السيبرانية أو الجرائم الإلكترونية (نعمة، 2020).

تمثل الجرائم السيبرانية تحدياً كبيراً للأنظمة القانونية التقليدية، نظراً لطبيعتها المتجاوزة للحدود الجغرافية وسرعة تطورها وصعوبة اكتشافها وإثباتها. فهي جرائم تتسم بالتعقيد والتطور المستمر، وتستهدف الأفراد والمؤسسات والدول على حد سواء، مما يجعل مكافحتها تحدياً يتطلب تضافر الجهود على المستويين الوطني والدولي (الحجار وبشير، 2021).

تعرف الجرائم السيبرانية بأنها "الأفعال غير المشروعة التي ترتكب بواسطة الحاسب الآلي أو شبكات الاتصال أو تكون موجهة ضدهما، وتشكل انتهاكاً للحقوق والمصالح المحمية قانوناً". 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 طبيعة هذه الجرائم. كما فرض هذا التطور تحديات إجرائية تتعلق بإثبات هذه الجرائم وجمع الأدلة الرقمية وتقديمها أمام المحاكم (مصطفى، 2023).

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

ومن المتوقع أن يساهم 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 عالمياً وتنوع أشكالها وأساليب ارتكابها، مما يشكل تحدياً كبيراً 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 تعقيداً وتشعباً؛ إذ يمكن أن تقف وراءها جهات متعددة، سواء كانت أفراداً أو جماعات منظمة، مما 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، مما يثير تساؤلات حول كفاية القوانين الجنائية الحالية في التعامل مع هذه الظاهرة المتجددة.

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

1. ما مدى كفاية القوانين الجنائية التقليدية في مواجهة الجرائم السيبرانية المستحدثة؟
2. ما هي التحديات التي تواجه تطبيق القانون الجنائي على الجرائم السيبرانية؟
3. كيف يمكن التغلب على الصعوبات المتعلقة بإثبات الجرائم السيبرانية وجمع الأدلة الرقمية؟
4. ما هي آليات التعاون الدولي الفعالة في مجال مكافحة الجرائم السيبرانية العابرة للحدود؟
5. ما هي 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 على مختلف جوانب الحياة. وتتمثل أهمية الدراسة في:

الأهمية النظرية:

1. تقديم إطار مفاهيمي متكامل: تساهم الدراسة في تقديم إطار مفاهيمي متكامل للجرائم السيبرانية، يشمل تعريفها وخصائصها وأركانها وأنواعها، مما يعزز الفهم النظري لهذه الظاهرة.
2. تحليل الإطار القانوني: تحلل الدراسة الإطار القانوني للجرائم السيبرانية على المستويين الوطني والدولي، وتقيم مدى كفايته في مواجهة هذه الجرائم.
3. دراسة التحديات الإجرائية: تتناول الدراسة التحديات الإجرائية المتعلقة بإثبات الجرائم السيبرانية وجمع الأدلة الرقمية، مما يساهم في تطوير الأطر النظرية في هذا المجال.
4. تحليل آليات المكافحة: تحلل الدراسة آليات مكافحة الجرائم السيبرانية، سواء على المستوى الوقائي أو العلاجي، مما يثري المكتبة القانونية في هذا المجال.

الأهمية التطبيقية:

1. تطوير المنظومة القانونية: تسهم الدراسة في تقديم مقترحات لتطوير المنظومة القانونية لمكافحة الجرائم السيبرانية، بما يتناسب مع طبيعتها المتغيرة.
 2. تعزيز التعاون الدولي: تساهم الدراسة في تقديم رؤية متكاملة لتعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية، مما يسهم في تطوير آليات التعاون العملية.
 3. تحسين إجراءات التحقيق: تقدم الدراسة مقترحات لتحسين إجراءات التحقيق في الجرائم السيبرانية وتطوير آليات جمع الأدلة الرقمية وحفظها وتقديمها أمام المحاكم.
 4. تعزيز الوعي المجتمعي: تسهم الدراسة في تعزيز الوعي المجتمعي بمخاطر الجرائم السيبرانية وسبل الوقاية منها، مما يعزز الأمن السيبراني للمجتمع.
 5. دعم صانعي القرار: توفر الدراسة معلومات وتحليلات تساعد صانعي القرار في وضع السياسات والاستراتيجيات الوطنية لمكافحة الجرائم السيبرانية.
 6. 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:

1. تحديد مفهوم الجرائم السيبرانية وخصائصها وأركانها وأنواعها من خلال تحليل التعريفات المختلفة في القوانين الوطنية والاتفاقيات الدولية
2. تحليل الإطار القانوني للجرائم السيبرانية عبر دراسة التشريعات الوطنية والاتفاقيات الدولية والإقليمية وتقييم مدى كفايتها وفعاليتها في مواجهة هذه الجرائم
3. دراسة التحديات الإجرائية في مكافحة الجرائم السيبرانية من خلال تحليل الصعوبات المتعلقة بإثبات الجرائم الرقمية وجمع الأدلة وحفظها وتقديمها أمام المحاكم

4. تحليل آليات مكافحة الجرائم السيبرانية عبر استعراض التدابير الوقائية والأمنية المتبعة وآليات التعاون الدولي ودور الأجهزة الأمنية المتخصصة
5. استشراف التحديات المستقبلية في مجال مكافحة الجرائم السيبرانية من خلال تحليل التطورات التقنية والقانونية وتأثيرها على المنظومة القانونية
6. تقديم مقترحات لتطوير المنظومة القانونية لمكافحة الجرائم السيبرانية وتعزيز الوعي المجتمعي بمخاطر الجرائم وسبل الوقاية منها

الدراسات السابقة

1. دراسة (نعمة، 2020) بعنوان : تكييف الهجمات السيبرانية في ضوء القانون الدولي. 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 التأثير على بعضها البعض عن طريق الهجوم على البنية التحتية الأساسية بكبسة زر واحدة ورغم ذلك إحداث آثار مدمرة سواء في الحجم الدمار البشري أو المادي. إن المعالم الدقيقة للهجمات السيبرانية لازالت غير محددة لذلك خصصنا هذه الدراسة للبحث في مفهوم الهجمات السيبرانية والموائمة بينها وبين قواعد القانون الدولي المكتوبة منها والعرفية.
2. دراسة (مشوش، 2019) بعنوان : الجهود الدولية لمكافحة الإجرام السيبراني. إن التعاون الدولي في مجال مكافحة الجريمة السيبرانية يأخذ مظهران، 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

3. دراسة (مصطفى، 2022) بعنوان : الحرب السبرانية الصينية الأمريكية. شهد الفضاء السبراني صراعات وحروب إلكترونية، بين الدول وحتى الفواعل الغير دولتية سعيا من كل طرف السيطرة على مصادر المعلومة، وفرض نفسها كقوة سبرانية 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 كقوتين سبرا نيتان، في هذا الفضاء، سعت كل واحدة إلى تطوير استراتيجيات وبرامج جوسسة وحتى تجنيد قراصنة الإنترنت من أجل السيطرة على بيانات الطرف الآخر، هذا الوضع المتأزم أدى بالقوتين إلى ضرورة التفكير في حوكمة الفضاء السبراني، من خلال منظمات دولية على غرار الأمم المتحدة من أجل تقنينه وتجريم الهجمات 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..

4. دراسة (بوطلاعة، 2022) بعنوان : صراع الفضاء السبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة. برز الفضاء السبراني كعنصر مؤثر في النظام الدولي نكشف عن أنماط جديدة من المخاطر والتهديدات السبرانية زاد من حدتها توظيفه لأغراض، عسكرية حتى أضحي مهددا رئيسيا 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 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.

5. دراسة (بوطلاعة، 2022) بعنوان : الهجمات السبرانية علي البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. تشكل الهجمات السبرانية تهديدا حقيقيا 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 نبحت في هذه الدراسة الحماية القانونية لهذه البنية التحتية الحرجة من الهجمات السبرانية في ظل القانون الدولي غير السبراني وتقييم مدى شمولية قواعده ومبادئه في ظل غياب قانون دولي سبراني متخصص ودقيق..

6. دراسة (حيمد، 2019) بعنوان : رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. هدف الدراسة إلى وضع رؤية إستراتيجية لمكافحة الجرائم السيبرانية، حيث تم تطبيقها

على أعضاء هيئة التدريس بأكاديمية الشرطة اليمنية وقطاع التأهيل والتدريب بالوزارة، عددهم 121 مفردة، وتم استخدام المنهج الوصفي التحليل، والاستبانة كأداة دراسة، ومن نتائج الدراسة أن واقع التطرف والإرهاب السيبراني: استغلال شبكة الأنترنت للتحريض على العنف والتطرف، أوجدت العولمة الرقمية فرصة للتشبيك بين الجماعات المتطرفة، بروز أدوات وأنماط حديثة لتجنيد المتطرفين عبر الأنترنت. وأن دور مكافحة الجرائم السيبرانية في تعزيز الأمن الإنساني: تنمية الوعي الاجتماعي بمخاطر ارتكاب الجرائم السيبرانية، تسهم في تحقيق أهداف الأمن الإنساني بأبعاده المختلفة، تعمل على تحقيق الوقاية المبكرة من الجرائم السيبرانية، رفع نسبة الكفاءة الوطنية والوسائل الأمنية المستخدمة لحماية البنية التحتية الوطنية، تعزز الحماية الشخصية على مستوى الفرد. توفير 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 الأنترنت. تدني نسبة الإبلاغ عن الجرائم السيبرانية لتجنب الإساءة للسمعة أو زعزعة ثقة العملاء. ومن أهم التوصيات: سرعة أعداد مشروع قانون يسمى (قانون الأمن السيبراني) يعزز مكافحة الجرائم السيبرانية، وحماية المجتمع اليمني سيبرانيا، 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-أفراداً ومؤسسات- بطرق الحماية من الجرائم السيبرانية.

7. دراسة (ابن داود، 2020) بعنوان : الجرائم السيبرانية: دراسة تأصيلية مقارنة. يعني هذا البحث ببيان الجرائم السيبرانية، وتأصيلها الفقهي، ومقارنتها بالنظام السعودي. بين 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 ختم 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 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

8. دراسة (حسنين، 2019) 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 والتي تستلزم وجود مناخ اقتصادي مستقر يعتمد على المنافسة الشريفة وتكافؤ الفرص، فضلاً عن تطور أنماط الجريمة بمختلف أشكالها باستخدام الحاسب الآلي، سواء التي تنال من الأشخاص أو الأموال أو المصلحة العامة. لقد هدفت الدراسة محل البحث إلى: النهوض بدور الشرطة في مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي أسوة بالتجارب الموجودة في الدول المتقدمة، من خلال دراسة تحليلية مقارنة. وانطلاقاً من أهمية موضوع الدراسة محل البحث، ونظراً لما عرضه الباحث سابقاً، وكضرورة تقتاضها 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 ثان، ثم يتناول دور جهاز الشرطة الدولية (الإنترپول) 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، انتهى الباحث إلى مجموعة من النتائج مقدماً عدة توصيات بشأن النهوض بدور الشرطة في مكافحة الجرائم السيبرانية المستحدثة ومن ثم تحقيق الأمن المعلوماتي وما ينعكس أثره على العلوم الإنسانية ومن ثم إثرائها.

9. دراسة (الحجار، 2021) 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، والذي أطلق عليه عدة مسميات مثل: الجريمة السيبرانية، أو الجريمة المعلوماتية، أو الجريمة الإلكترونية، ونظراً لأن إثبات الجريمة يتطلب دليلاً جنائياً 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 في 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.

10.دراسة (الطريف، 2020) بعنوان : اتجاهات الشباب السعودي نحو الجرائم السيبرانية وخطورتها: دراسة ميدانية. إن الوعي بالجرائم السيبرانية بين الشباب السعودي أمر هام، خاصة وأن استخدام الإنترنت أصبح نمط حياة اليوم. وبالتالي، يجب أن يكون الوعي بالجريمة السيبرانية جزءا 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 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، والتي جابت في المرتبة الأولى بنسبة ٩٦% ومتوسط حسابي 1.92، وهو ما يعكس حجم الخطر الذي يحيط بأفراد المجتمع نتيجة انتشار الجرائم السيبرانية وتزايد معدلاتها، كما أوضحت نتائج الدراسة أن الوسائل الأكثر تأثيرا في نشر الجريمة السيبرانية من وجهة نظر عينة الدراسة كان الاستخدام المستمر لمواقع التواصل الاجتماعي بنسبة 99.5% ومتوسط حسابي بلغ 1.97، وأن الشباب هم الفئة الأولى المستهدفة من الجرائم السيبرانية بنسبة 100% ومتوسط حسابي بلغ 2.0.

11.دراسة (بهلول، 2021) بعنوان : الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. تعتبر الجرائم السيبرانية من أخطر الجرائم التي يشهدها العالم اليوم، والتي 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 تهديدا ليس فقط للأفراد، بل حتى 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 التفتن 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.

12.دراسة (مهدي، 2021) بعنوان : الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. شهد العالم في الألفية الأخيرة تحولات عميقة على كل المستويات الاقتصادية والاجتماعية والثقافية وبخاصة التكنولوجية، حيث تحولت المجتمعات من مجتمعات استهلاكية إلى مجتمعات صناعية إلى مجتمعات إلكترونية سيبرانية بفضل ما قدمته التكنولوجيا الحديثة من خدمات رقمية سريعة قليلة التكاليف بدقة متناهية وبمردودية أكبر، وعلى الرغم من إيجابيات هذه التقنية والتكنولوجيا إلا أنها بالمقابل شكلت هاجسا لكل المجتمعات بسبب إفرازها لمجموعة من السلبيات أهمها ما يعرف بالجرائم السيبرانية. ونظرا لخصوصية هذه الجرائم باعتبار أنها جرائم عابرة للجغرافيا ولا تميز بين مجتمعات وأخرى، فإن الجزائر تعتبر هي الأخرى من الدول التي عرفت في السنوات الأخيرة ارتفاع مؤشر هذه الجرائم بشكل ملموس، حسب التقارير الأمنية والعلمية أيضا، 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

13.دراسة (عبد الحميد، 2022) بعنوان : الجرائم السيبرانية في زمن "كورونا" وآثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. سعت الورقة للتعرف الجرائم السيبرانية في زمن كورونا وآثارها على الأمن القومي. تطرقت إلى مفهوم الهجوم السيبراني، مشيراً إلى تزايد تلك الجرائم مع ظهور جائحة كوفيد (19). تناولت تحديد طبيعة كوفيد (19) تقييم أضراره الاقتصادية وتأثيره على الظاهرة الإجرامية. أوضح انحسار الجرائم التقليدية في زمن مرض فيروس كورونا. عرضت وسائل ارتكاب الجرائم السيبرانية وتقييم مشهدها في زمن كورونا. استعرضت تقرير جهاز الإنتربول الدولي (2020) يؤكد تزايد الجرائم السيبرانية في زمن كورونا. تناولت مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتزايد الجرائم السيبرانية في زمن كوفيد (19). أشارت إلى تزايد هجمات الإرهاب السيبراني على المؤسسات والمرافق الطبية في زمن كورونا. تطرقت إلى الجرائم السيبرانية والأمن الاقتصادي القومي في زمن كورونا ومدى تطور نظرية الأمن القومي للدول، مشيراً إلى مفهوم الأمن القومي الاقتصادي، كما أوضحت آثار الجرائم السيبرانية عليه. تناولت تحليل اقتصادي للأمم المتحدة بشأن الوضع الاقتصادي العالمي وآفاقه (2022). اختتمت الورقة بالإشارة إلى تقرير البنك الدولي عن الآفاق الاقتصادية الإقليمية عام (2022).

14.دراسة (عبد الحميد، 2022) بعنوان : الجرائم السيبرانية في زمن "كورونا" وآثارها علي الأمن القومي الاقتصادي: دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة. استعرض المقال الجرائم السيبرانية في زمن كورونا وآثارها على الأمن القومي الاقتصادي. يعد هذا الجزء الحلقة الثانية من البحث وتناول فيها استراتيجية الباحث لمواجهة الجرائم السيبرانية في زمن كوفيد (19) واشتملت على الإشكاليات التي فرضتها الدراسة واستوجبت استراتيجية لحلها ومنها أن مرافق ومؤسسات البنى التحتية لمختلف دول العالم المتقدم، بين المشهد العالمي هشاشة النظام الاقتصادي، طبيعة مرض فيروس كورونا، مخاطر العملات الرقمية المشفرة وآثارها على الأمن القومي الاقتصادي، تزايد ارتكاب الجرائم السيبرانية في زمن (كوفيد 19) وتطور وسائل ارتكابها، تحقيق الأمن السيبراني، تزايد هجمات الإرهاب السيبراني على المؤسسات والمرافق

الطبية في زمن كوفيد (19). 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 19)، ضرورة إنشاء جهاز لمكافحة الأوبئة والأمراض يتبع منظمة الصحة العالمية ويكون له فروع في المكاتب الإقليمية للمنظمة في مناطق دول العالم، سرعة إصدار العملات الرقمية للبنوك المركزية كأحد بدائل العملات الرقمية المسفرة لتفادي مخاطرها، تعزيز تدابير الأمن السيبراني في مجال العمل عن بعد، 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 (19)، 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.

15.دراسة (معروف، 2022) بعنوان : المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. نهدف من خلال دراستنا لهذا الموضوع إلى 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.

16.دراسة (عبدالرازق، 2023) 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 خطراً وتهديداً على أمن الفرد والمجتمع وعلى كافة 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، مما ترتب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، فظاهرة الجرائم السيبرانية تعتبر نتاج طبيعي لثورة الاتصالات والتكنولوجيا والتي أصبحت واسعة الانتشار، والتي تحدث عن طريق هجمات واختراقات وتسلسل داخل النظم المعلوماتية بهدف تدميرها أو الحصول على معلومات سرية سواء عسكرية أو 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 1439/٢/11هـ، لتكون هذه الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، ولحماية للمصالح 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.

17.دراسة (أحمد، 2022) بعنوان : مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. هدفت هذه الدراسة إلى معرفة الجريمة السيبرانية التي أصبحت خطراً على الفرد والمجتمع وعلى أمن الدولة، إذ أنها تتقدم بوتيرة سريعة باستخدام المجرمون أحدث التقنيات في تنفيذ

هجماتهم السيبرانية. هناء جاءت فكرة هذا البحث ليلقي مزيداً من الضوء على التطورات التكنولوجية والجريمة السيبرانية لإلقاء الضوء على مشاكلها وتقييمها، وذلك لتعظيم الاستفادة من مميزاتا وتفادي مخاطرها وسبل التعاون الإقليمي والدولي لمكافحتها، حيث انه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي والقضاء عليها ومحاكمة مرتكبيها. ولهذا أحببت أن أقدم هذه الورقة لإعطاء نظرة حول الجريمة السيبرانية في المبحث الأول، وتناول الاتفاقيات العربية والدولية في المبحث الثاني، ووضع النتائج والتوصيات في خاتمة البحث..

18.دراسة (الفتلاوي، 2023) 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، إلا أن موضوع الأدلة غير المباشرة لم يأخذ مكانه من الدراسة والتحليل، فأغلب الدراسات القانونية قد تعرضت لهذا موضوع 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. فضلا عن أهميتها الخاصة في عملية إثبات الجرائم الدولية بشكل عام، وجريمة السيبرانية على وجه الخصوص، وتكمن هذه الأهمية في الدور الذي تضطلع به الأدلة غير المباشرة في إثبات هذه الجرائم- جرائم السيبرانية- أمام المحاكم الدولية.

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

وأخيراً، 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 تطوراً كبيراً 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" (Kharmouche، 2024).

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" (مهدي، 2021).

تعريفات المنظمات الدولية:

1. منظمة الأمم المتحدة: عرّفت الجريمة السيبرانية في المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين (2000) بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو في نطاق نظام حاسوبي أو شبكة حاسوبية" (الحجار وبشير، 2021).
2. 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" (عبدالرازق، 2023).
3. اتفاقية بودابست لمكافحة جرائم الإنترنت (2001): لم تقدم تعريفاً محدداً 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 (أحمد، 2022).

التعريفات التشريعية:

1. التشريع المصري: عرّف قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 الجريمة السيبرانية بأنها "أي جريمة ترتكب باستخدام وسيلة أو أكثر من وسائل تقنية المعلومات أو أنظمة معلوماتية أو شبكة معلوماتية".
2. التشريع السعودي: عرّف نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8 هـ الجريمة السيبرانية بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" (عبدالرازق، 2023).
3. التشريع الإماراتي: عرّف المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الجريمة السيبرانية بأنها "الأفعال التي تشكل انتهاكاً للتشريعات النافذة، سواء بالدخول غير المشروع إلى الأنظمة المعلوماتية، أو إتلاف البيانات والمعلومات، أو تعطيل الشبكات".

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

الفرع الثاني: خصائص الجرائم السيبرانية

تتميز الجرائم السيبرانية بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، وتجعل من مكافحتها تحدياً كبيراً 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، مما يثير إشكاليات تتعلق بالاختصاص القضائي وتطبيق القانون (بوتلاعة وبوكورو، 2022).
- **السرعة والخفاء:** يمكن ارتكاب الجرائم السيبرانية بسرعة كبيرة وبشكل خفي، مما يصعب اكتشافها في الوقت المناسب. كما يمكن للجاني إخفاء هويته باستخدام تقنيات مختلفة، مثل تغيير عنوان IP، أو استخدام شبكات الهوية المجهولة (معروف، 2022).
- **التقنية العالية:** تتطلب الجرائم السيبرانية مهارات تقنية عالية، سواء في ارتكابها أو في التحقيق فيها وكشفها، مما يتطلب توفير كوادر متخصصة في مجال الأمن السيبراني والتحقيق الرقمي (الحجار وبشير، 2021).
- **الأثر الواسع:** يمكن أن تؤثر الجرائم السيبرانية على عدد كبير من الضحايا في وقت واحد، بل يمكن أن تستهدف بنية تحتية حيوية لدولة بأكملها، مما يزيد من خطورتها (بوتلاعة وبوكورو، 2022).
- **صعوبة الإثبات:** يصعب إثبات الجرائم السيبرانية نظراً لطبيعة الأدلة الرقمية التي يمكن محوها أو تعديلها بسهولة، وصعوبة ربط الجاني بالجريمة إذا استخدم تقنيات لإخفاء هويته (معروف، 2022).
- **التطور المستمر:** تتطور الجرائم السيبرانية باستمرار مع تطور التكنولوجيا، مما يتطلب تطويراً مستمراً للتشريعات وآليات المكافحة (مهدي، 2021).

- الطبيعة الاقتصادية: غالباً ما تكون الدوافع وراء ارتكاب الجرائم السيبرانية اقتصادية، مثل الاحتيال الإلكتروني، وسرقة البيانات المالية، والابتزاز الإلكتروني، مما يؤدي إلى خسائر اقتصادية كبيرة (عبد الحميد، 2022).

- استغلال الثغرات الأمنية: تعتمد الجرائم السيبرانية على استغلال الثغرات الأمنية في النظم المعلوماتية، مما يتطلب جهوداً مستمرة لتحديث هذه النظم وسد الثغرات (عبد الرزاق، 2023).

- تعدد الجهات الفاعلة: يمكن أن تقف وراء الجرائم السيبرانية جهات مختلفة، بدءاً من الأفراد، مروراً بالمنظمات الإجرامية، وصولاً إلى الدول التي يمكن أن تستخدم الهجمات السيبرانية كوسيلة للحرب الهجينة (مصطفى، 2022).

- انخفاض التكلفة: تتميز الجرائم السيبرانية بانخفاض تكلفة ارتكابها مقارنة بالجرائم التقليدية، فلا تتطلب سوى حاسب آلي متصل بالإنترنت ومهارات تقنية معينة (أحمد، 2022).

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.

أولاً: الركن المادي

يتمثل الركن المادي في السلوك الإجرامي الذي يقوم به الجاني، سواء كان إيجابياً (فعل) أو سلبياً (امتناع عن فعل)، والذي يترتب عليه نتيجة إجرامية، مع وجود علاقة سببية بين السلوك والنتيجة (عبد الرزاق، 2023).

ويتخذ السلوك الإجرامي في الجرائم السيبرانية أشكالاً 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، مما يجعل إثباته أكثر صعوبة، ويتطلب وسائل تقنية متطورة لجمع الأدلة الرقمية (الحجار وبشير، 2021).

ثانياً: الركن المعنوي

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

1. 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.
2. القصد الجنائي الخاص: ويتمثل في نية خاصة يتطلّبها القانون لقيام الجريمة، مثل نية الاحتيال في جرائم الاحتيال الإلكتروني، أو نية الإضرار في جرائم إتلاف البيانات.
3. الخطأ غير العمدى: وقد تقوم بعض الجرائم السيبرانية على أساس الخطأ غير العمدى، مثل التسبب في انتشار فيروس معلوماتي بسبب الإهمال في تأمين النظام المعلوماتي (مهدي، 2021).

ثالثاً: الركن القانوني

يتمثل الركن القانوني في النص القانوني الذي يجرّم الفعل ويحدد عقوبته، تطبيقاً 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، مما دفع العديد من الدول إلى إصدار تشريعات خاصة بالجرائم السيبرانية (أحمد، 2022).

رابعاً: الركن المعلوماتي (التقني)

يتمثل الركن المعلوماتي في استخدام تقنية المعلومات والاتصالات في ارتكاب الجريمة، سواء كانت هذه التقنية محلاً للاعتداء أو وسيلة لارتكاب الجريمة. وهذا الركن هو ما يميز الجرائم السيبرانية عن الجرائم التقليدية (عبدالرازق، 2023).

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 (الحجار وبشير، 2021).

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 نظراً لتطور التكنولوجيا وتعدد استخداماتها. ويمكن تصنيف الجرائم السيبرانية وفقاً لعدة معايير:

الفرع الأول: تصنيف الجرائم السيبرانية وفقاً لطبيعة الاعتداء

1. 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.

2. 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) (بوتلابة وبوكورو، 2022).

3. الجرائم التي تستهدف أموال الأفراد والمؤسسات:

- جرائم الاحتيال الإلكتروني.
- جرائم سرقة البطاقات الائتمانية والحسابات المصرفية.
- جرائم غسل الأموال الإلكتروني.
- جرائم القرصنة المالية (عبدالحميد، 2022).

4. 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 (بهلول، 2021).

5. 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 وفقاً لدور تكنولوجيا المعلومات في ارتكابها

1. الجرائم التي تكون فيها تكنولوجيا المعلومات محلاً للاعتداء: وهي الجرائم التي تستهدف النظم المعلوماتية والبيانات ذاتها، مثل جرائم الدخول غير المشروع إلى النظم المعلوماتية، وجرائم إتلاف البيانات والبرامج، وجرائم اعتراض البيانات (معروف، 2022).
2. الجرائم التي تكون فيها تكنولوجيا المعلومات وسيلة لارتكاب الجريمة: وهي الجرائم التي يتم فيها استخدام تكنولوجيا المعلومات كوسيلة لارتكاب جرائم تقليدية، مثل جرائم الاحتيال الإلكتروني، وجرائم الابتزاز الإلكتروني، وجرائم نشر المحتوى غير المشروع (عبدالرازق، 2023).

الفرع الثالث: تصنيف الجرائم السيبرانية وفقاً للتصنيف الوارد في الاتفاقيات الدولية

تصنف اتفاقية بودابست لمكافحة جرائم الإنترنت (2001) الجرائم السيبرانية إلى أربع فئات رئيسية:

1. الجرائم ضد سرية وسلامة وتوافر البيانات والأنظمة الحاسوبية:

- الدخول غير المشروع إلى النظم المعلوماتية.
- 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) (أحمد، 2022).

2. الجرائم المرتبطة بالحاسوب:

- التزوير المرتبط بالحاسوب.

○ الاحتيال المرتبط بالحاسوب (أحمد، 2022).

3. الجرائم المتعلقة بالمحتوى:

○ الجرائم المتعلقة بالمواد الإباحية للأطفال.

○ الجرائم المتعلقة بانتهاكات حقوق الملكية الفكرية (أحمد، 2022).

4. الجرائم المتعلقة بانتهاكات الخصوصية:

○ جمع البيانات الشخصية بطرق غير مشروعة.

○ معالجة البيانات الشخصية بطرق غير مشروعة.

○ تسريب البيانات الشخصية (أحمد، 2022).

الفرع الرابع: تصنيف الجرائم السيبرانية وفقاً للجهة المستهدفة

1. الجرائم السيبرانية ضد الأفراد: وهي الجرائم التي تستهدف الأفراد وتمس حقوقهم وحياتهم وممتلكاتهم، مثل جرائم الابتزاز الإلكتروني، وجرائم سرقة الهوية، وجرائم الاحتيال الإلكتروني (بهلول، 2021).

2. 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 (عبد الحميد، 2022).

3. 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 بدوافع الحصول على منافع مالية، مثل جرائم الاحتيال الإلكتروني، وجرائم سرقة البيانات المالية، وجرائم الابتزاز الإلكتروني (عبد الحميد، 2022).

❖ 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 (بهلول، 2021).

❖ الجرائم السيبرانية ذات الدوافع الإيديولوجية: وهي الجرائم التي ترتكب بدوافع إيديولوجية، مثل جرائم الإرهاب الإلكتروني، وجرائم نشر الكراهية والتطرف (حيمد ومصطفى، 2019).

المبحث الثاني: الإطار القانوني للجرائم السيبرانية

المطلب الأول: التشريعات الوطنية لمكافحة الجرائم السيبرانية

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

الفرع الأول: نماذج للتشريعات الوطنية في الدول العربية

1. المملكة العربية السعودية: أصدرت المملكة نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ، ثم تم تحديثه بالمرسوم الملكي رقم م/7 بتاريخ 1443/3/27هـ. 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 6801 بتاريخ 1439/2/11هـ، لتكون الجهة المختصة بالأمن السيبراني في المملكة (عبدالرازق، 2023).

2. جمهورية مصر العربية: أصدرت مصر قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، 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 405 لسنة 2020، ليكون الجهة المسؤولة عن وضع استراتيجية الأمن السيبراني في مصر (مشوش، 2019).

3. دولة الإمارات العربية المتحدة: أصدرت الإمارات المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، الذي تم تعديله بالمرسوم بقانون اتحادي رقم 34 لسنة 2021. 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 2 لسنة 2019، لتكون الجهة المسؤولة عن الأمن السيبراني في الدولة (ابن داود، 2020).
4. الجزائر: أصدرت الجزائر القانون رقم 04-09 المؤرخ في 5 أوت 2009 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 15-261 المؤرخ في 8 أكتوبر 2015

الفرع الثاني: نماذج للتشريعات الوطنية في الدول الأجنبية

1. الولايات المتحدة الأمريكية: تعتبر الولايات المتحدة من أوائل الدول التي أصدرت تشريعات لمكافحة الجرائم السيبرانية. ففي عام 1986، 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 1986، وقانون حماية الأطفال على الإنترنت (Children's Internet Protection Act) عام 2000 (Kharmouche، 2024).
2. المملكة المتحدة: أصدرت المملكة المتحدة قانون إساءة استخدام الحاسوب (Computer Misuse Act) عام 1990، الذي تم تعديله عدة مرات، آخرها في عام 2015. ويتضمن القانون تجريم الدخول غير المشروع إلى النظم المعلوماتية، وتعديل البيانات بدون تصريح، ونشر البرمجيات الخبيثة. كما تم إصدار قانون الاقتصاد الرقمي (Digital Economy Act) عام 2017، الذي يتضمن أحكاماً تتعلق بحماية البيانات الشخصية وحقوق الملكية الفكرية على الإنترنت (Kharmouche، 2024).

3. ألمانيا: قامت ألمانيا بتعديل قانون العقوبات في عام 1986 لإدخال جرائم الحاسب الآلي، مثل التجسس على البيانات، والاحتيايل الإلكتروني، وتغيير البيانات. ثم تم إصدار قانون خدمات الإعلام والاتصالات (Telemedia Act) عام 2007، الذي يتضمن أحكاماً تتعلق بحماية البيانات الشخصية والمسؤولية القانونية لمقدمي خدمات الإنترنت (أحمد، 2022).
4. فرنسا: أصدرت فرنسا قانون جوتي (Godfrain Law) عام 1988، الذي يجرم الدخول غير المشروع إلى النظم المعلوماتية وتعديل البيانات بدون تصريح. وتم دمج هذا القانون لاحقاً في قانون العقوبات الفرنسي. كما تم إصدار قانون الثقة في الاقتصاد الرقمي (Law for Trust in the Digital Economy) عام 2004، الذي يتضمن أحكاماً تتعلق بالمسؤولية القانونية لمقدمي خدمات الإنترنت والتجارة الإلكترونية (مشوش، 2019).

الفرع الثالث: تقييم التشريعات الوطنية لمكافحة الجرائم السيبرانية

تواجه التشريعات الوطنية لمكافحة الجرائم السيبرانية العديد من التحديات، منها:

- ❖ **تباين التشريعات بين الدول:** يؤدي تباين التشريعات بين الدول إلى صعوبات في التعاون الدولي لمكافحة الجرائم السيبرانية العابرة للحدود، مما قد يؤدي إلى وجود ملاذات آمنة لمرتكبي هذه الجرائم (مشوش، 2019).
- ❖ **صعوبة مواكبة التطور التكنولوجي:** تتطور التكنولوجيا بسرعة كبيرة، مما يجعل من الصعب على التشريعات مواكبة هذا التطور وتجريم الأفعال المستحدثة في البيئة الرقمية (بوظلاعة وبوكورو، 2022).
- ❖ **التوازن بين الأمن والحرية:** تواجه التشريعات تحدياً في تحقيق التوازن بين حماية الأمن السيبراني واحترام الحقوق والحريات الأساسية للأفراد، مثل الحق في الخصوصية وحرية التعبير (أحمد، 2022).
- ❖ **قصور القدرات التقنية:** قد تفتقر بعض الدول إلى القدرات التقنية اللازمة لتنفيذ التشريعات ومكافحة الجرائم السيبرانية بفعالية، مما يجعل هذه التشريعات غير فعالة في الواقع العملي (حيمد ومصفى، 2019).

ورغم هذه التحديات، تظل التشريعات الوطنية أداة مهمة في مكافحة الجرائم السيبرانية، خاصة إذا تم تطويرها باستمرار لمواكبة التطورات التكنولوجية، وتعزيز التعاون الدولي لسد الفجوات التي يمكن أن يستغلها مرتكبو هذه الجرائم (عبدالرازق، 2023).

المطلب الثاني: الاتفاقيات الدولية والإقليمية لمكافحة الجرائم السيبرانية

نظراً 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.

الفرع الأول: الاتفاقيات الدولية لمكافحة الجرائم السيبرانية

1. اتفاقية بودابست لمكافحة جرائم الإنترنت (2001): تعتبر اتفاقية بودابست من أهم الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية. تم اعتمادها من قبل مجلس أوروبا في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004. وتهدف الاتفاقية إلى:

- توحيد التشريعات الوطنية في مجال مكافحة الجرائم السيبرانية.
- وضع أسس للتعاون الدولي في التحقيق والملاحقة القضائية.
- 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 (أحمد، 2022).

2. بروتوكول بودابست الإضافي بشأن تجريم الأعمال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب بواسطة أنظمة الحاسب الآلي (2003): تم اعتماد هذا البروتوكول في 28 يناير 2003، ودخل حيز التنفيذ في 1 مارس 2006. ويهدف إلى تجريم نشر المواد العنصرية والمعادية للأجانب عبر شبكات الإنترنت (أحمد، 2022).

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

- القرار 63/55 بتاريخ 4 ديسمبر 2000 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات.
- القرار 121/56 بتاريخ 19 ديسمبر 2001 بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات.

- القرار 239/57 بتاريخ 20 ديسمبر 2002 بشأن إنشاء ثقافة عالمية للأمن السيبراني.
- القرار 199/58 بتاريخ 23 ديسمبر 2003 بشأن إنشاء ثقافة عالمية للأمن السيبراني وحماية البنى التحتية المعلوماتية الحيوية (مشوش، 2019).
- 4. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (2000): رغم أن هذه الاتفاقية لا تتعلق بشكل مباشر بالجرائم السيبرانية، إلا أنها توفر إطاراً قانونياً للتعاون الدولي في مكافحة الجريمة المنظمة، بما في ذلك الجرائم السيبرانية التي ترتكبها مجموعات إجرامية منظمة (Kharmouche، 2024).
- 5. المؤتمر الدولي الثالث عشر لمنع الجريمة والعدالة الجنائية (2015): أكد المؤتمر على أهمية تعزيز التعاون الدولي في مكافحة الجرائم السيبرانية، وتطوير قدرات الدول في هذا المجال، وتبادل المعلومات والخبرات (أحمد، 2022).

الفرع الثاني: الاتفاقيات الإقليمية لمكافحة الجرائم السيبرانية

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010): تم اعتماد هذه الاتفاقية من قبل مجلس وزراء الداخلية العرب في 21 ديسمبر 2010، ودخلت حيز التنفيذ في 7 أكتوبر 2014. 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 (أحمد، 2022).
2. اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (2014): تم اعتماد هذه الاتفاقية في 27 يونيو 2014، وتهدف إلى:
 - إنشاء إطار قانوني للأمن السيبراني وحماية البيانات الشخصية في أفريقيا.
 - تنظيم المعاملات الإلكترونية.
 - تعزيز الثقة في البيئة الرقمية.
 - مكافحة الجرائم السيبرانية (الفتلاوي والخزعلي، 2023).
3. اتفاقية منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات الدولي (2009): تم توقيع هذه الاتفاقية في 16 يونيو 2009، وتهدف إلى:

- تعزيز التعاون بين الدول الأعضاء في مجال أمن المعلومات.
- مكافحة الإرهاب المعلوماتي والجريمة المعلوماتية.
- حماية البنية التحتية المعلوماتية الحيوية (مصطفى، 2022).

4. اتفاقية مجلس أوروبا بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (اتفاقية 108) (1981): تعتبر هذه الاتفاقية من أقدم الاتفاقيات الدولية في مجال حماية البيانات الشخصية. تم اعتمادها في 28 يناير 1981، ودخلت حيز التنفيذ في 1 أكتوبر 1985. وتهدف إلى حماية الأفراد من إساءة استخدام البيانات الشخصية المعالجة آلياً (شرف، 2023).

5. توجيه الاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات (2013): تم اعتماد هذا التوجيه في 12 أغسطس 2013، 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 (بوطلاعة وبوكورو، 2022).

الفرع الثالث: تقييم الاتفاقيات الدولية والإقليمية لمكافحة الجرائم السيبرانية

رغم أهمية الاتفاقيات الدولية والإقليمية في مكافحة الجرائم السيبرانية، إلا أنها تواجه العديد من التحديات، منها:

1. عدم شمولية الانضمام: لم تنضم العديد من الدول إلى هذه الاتفاقيات، مما يحد من فعاليتها في مكافحة الجرائم السيبرانية العابرة للحدود (أحمد، 2022).
2. تباين التنفيذ: تختلف الدول في مدى التزامها بتنفيذ أحكام هذه الاتفاقيات، مما يؤدي إلى تباين في مستوى الحماية القانونية ضد الجرائم السيبرانية (مشوش، 2019).
3. التحديات السياسية: تؤثر العلاقات السياسية بين الدول على مستوى التعاون في مكافحة الجرائم السيبرانية، مما قد يؤدي إلى عدم فعالية الاتفاقيات في بعض الحالات (مصطفى، 2022).
4. التطور التكنولوجي: قد لا تواكب الاتفاقيات التطور السريع في التكنولوجيا والأساليب المستخدمة في ارتكاب الجرائم السيبرانية، مما يجعلها غير فعالة في مواجهة الأشكال الجديدة من هذه الجرائم (بوطلاعة وبوكورو، 2022).

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 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.

أولاً: 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 تحدياً كبيراً 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، مما يؤدي إلى فقدان الأدلة بنسبة قد تصل إلى 10%.
- صعوبة جمع الأدلة عند تواجدها على خوادم تقع خارج الحدود الوطنية، ما يستدعي تعاوناً دولياً معقداً (مصطفى، 2022).
- 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.

ثانياً: إجراءات التحقيق والملاحقة في الجرائم السيبرانية

تتطلب الجرائم السيبرانية اعتماد إجراءات تحقيق وملاحقة تختلف بشكل جذري عن الأساليب التقليدية، نظراً 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 وفقاً لإجراءات قانونية صارمة، كما تُتخذ إجراءات احترازية مثل فصل الأجهزة عن الشبكات لمنع محو أو تغيير البيانات.
- **التعاون الدولي في التحقيق:**
تُعتبر آليات المساعدة القانونية المتبادلة من الأسس التي يعتمد عليها تبادل الأدلة والمعلومات بين الدول، حيث تمكّن هذه الآليات من تقصير مدة التحقيقات بنسبة قد تصل إلى 40% في بعض الحالات. كما يعتمد نظام تسليم المجرمين على مبدأ "إما التسليم أو المحاكمة" استناداً إلى ازدواجية التجريم (أحمد، 2022).
- **دور الخبراء الفنيين:**
يشكل الخبراء في مجال الطب الشرعي الرقمي جسراً حيوياً بين التقنيات الحديثة والمحاكم، حيث يتم إعداد تقارير فنية تشرح تفاصيل الأدلة بلغة مبسطة، مما يساهم 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 رئيسية:

أ. الآليات الوقائية والأمنية

تتضمن الإجراءات الوقائية ما يلي:

• 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، مما يساهم في تقليل الفجوات الأمنية.

• 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.

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 المتبادل بالأحكام القضائية.

- **التعاون الفني والتقني:**
يُتبادل 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.

ج. دور الأجهزة الأمنية المتخصصة

تلعب الأجهزة الأمنية المتخصصة دوراً محورياً 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 تساهم في التعاون الدولي من خلال تبادل المعلومات مع الجهات الأمنية الأجنبية.
- **التحديات التي تواجهها:**
تعاني هذه الأجهزة من تحديات تقنية نتيجة للتطور المستمر في أساليب الجرائم، بالإضافة إلى صعوبات قانونية ونقص في الموارد والكوادر المؤهلة. كما يواجه العمل تنسيقاً محدوداً بين الجهات المحلية والدولية.

رابعاً: تحديات وآفاق مستقبلية في مكافحة الجرائم السيبرانية

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

أ. التحديات التقنية

تتمثل التحديات التقنية في استخدام المجرمين لتقنيات متقدمة لإخفاء الهوية والتشفير، مما يعقد عملية جمع الأدلة. كما يُشكل انتشار الحوسبة السحابية وخدمات الاستضافة الخارجية تحديات من حيث تحديد موقع البيانات، بينما يساهم انتشار أجهزة إنترنت الأشياء في زيادة عدد النقاط الضعيفة في النظم الأمنية. تُظهر بعض الدراسات أن حوالي 60% من الهجمات السيبرانية تعتمد على تقنيات إخفاء الهوية والتشفير.

ب. التحديات القانونية

يواجه صانعو السياسات تحديات قانونية تتمثل في اختلاف التشريعات بين الدول، مما يؤدي إلى تفاوت في تعريف الجرائم والعقوبات المقررة، بالإضافة إلى صعوبة تحقيق التوازن بين مكافحة الجرائم وحماية الحقوق الأساسية مثل الخصوصية وحرية التعبير. كما يُشكل 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 تُساهم هذه الاستثمارات في خفض نسب الفجوات الأمنية بنسبة تصل إلى 20%.
- 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 لتقليل مدة التحقيقات وتسليم المجرمين.

الخاتمة :

تشكل الجرائم السيبرانية تحدياً متجدداً للمنظومة القانونية الجنائية التقليدية، إذ يستدعي انتشارها المتسارع وتنوع أساليب ارتكابها إعادة النظر في الإطار القانوني والإجرائي لضمان تحقيق العدالة في ظل التقدم التكنولوجي المستمر. إذ تُظهر الدراسات أن نسب الجرائم الرقمية قد ارتفعت بنسبة ملحوظة خلال السنوات الأخيرة، مما يستدعي ضرورة تطوير تشريعات متكاملة تعالج خصوصيات الأدلة الرقمية وتضمن حماية الحقوق والحريات الأساسية في آن واحد. ومن هنا، تظهر أهمية تعزيز التعاون الدولي بين الدول لتبادل الخبرات وتوحيد المعايير القانونية، كما يجب التركيز على بناء القدرات الفنية للقضاء والجهات الأمنية للتعامل مع التحديات التقنية الناجمة عن استخدام تقنيات التشفير وإخفاء الهوية. وفي هذا السياق، يبرز الدور الحيوي للتوعية المجتمعية في تقليل فرص التعرض لهذه الجرائم عبر حملات توعوية ودورات تدريبية مستمرة، مما يساهم في رفع مستوى الأمن السيبراني بشكل عام. تبقى الحاجة ملحة إلى تبني رؤية استباقية تدمج بين التطور القانوني والتكنولوجي، بما يضمن تحقيق توازن فعال بين مكافحة الجرائم السيبرانية وحماية الحقوق الأساسية للأفراد، مما يعد خطوة محورية نحو بناء مجتمع رقمي آمن و متماسك.

المراجع :

1. نعمة، أحمد عبيس، و كلنتر، زهراء عماد محمد. (2020). تكييف الهجمات السيبرانية في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونية والسياسية، مج 13، ع 44، 49 - 74.

2. عباس، سعيدة، و بولعويديات، حورية. (2019). وسائل الإعلام ودورها الاستراتيجي في السياق الثقافي: رؤية تحليلية مقارنة بين منظور عزي عبدالرحمان - إدغار موران - أبراهام موليس - ماكلوهان. مجلة العلوم القانونية والاجتماعية، مج4، ع4، 561 - 571.
3. مشوش، مراد. (2019). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، مج12، ع2، 703 - 726.
4. الأسدي، عبدالرسول عبدالرضا، و الكرعاوي، نصيف جاسم محمد. (2021). دور تقنية التأمين لمواجهة المخاطر والأضرار في ظل انتشار جائحة كورونا. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج13، ع4، 814 - 843.
5. بلغيث، عبدالله. (2021). التصويت الإلكتروني في سياق الديمقراطية الرقمية السيبرانية: قراءة في المفاهيم والتساؤلات المرتبطة بها. مجلة حقوق الإنسان والحريات العامة، مج6، ع3، 25 - 52.
6. مصطفى، حميل. (2022). الحرب السبرانية الصينية الأمريكية. المجلة الأكاديمية للبحوث القانونية والسياسية، مج6، ع2، 261 - 273.
7. بوطلاعة، و داد، و بوكورو، منال. (2022). صراع الفضاء السبراني وتأثيره على السلم والأمن الدوليين: التحديات والتهديدات الجديدة وسبل المواجهة. مجلة العلوم القانونية والاجتماعية، مج7، ع4، 810 - 827.
8. بوطلاعة، و داد، و بوكورو، منال. (2022). الهجمات السبرانية علي البنية التحتية الحرجة: دراسة في ضوء القانون الدولي العام. مجلة حقوق الإنسان والحريات العامة، مج7، ع2، 322 - 355.
9. شرف، ياسين. (2023). الحماية الجنائية للمرأة في الفضاء الرقمي وفق مستجدات القانون 103.13. مجلة قانونك، ع15، 472 - 495.
10. ناصر، محمد عبدالرضا، و السرياوي، حيدر كاظم عبد علي. (2018). وسائل القتال الحديثة: دراسة في ضوء أحكام القانون الدولي الإنساني. مجلة الكلية الإسلامية الجامعة، ع45، 197 - 224.

11. حيمد، محمد مسعد، و مصطفى، مصطفى جاد الحق. (2019). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. المجلة العربية الدولية للمعلوماتية، مج7، ع12 ، 83 - 100.
12. د جابر جاد نصار، أصول وفنون البحث العلمي، الطبعة الأولى، دار النهضة العربية بالقاهرة .
13. د/ سقلاب فريدة، محاضرات في منهجية العلوم القانونية، جامعة عبد الرحمن ميره، بجاية - الجزائر 2017 - 2018
14. د. مصطفى البنداري أبو سعده، المنهجية القانونية بين القواعد النظرية والمهارات التطبيقية، دار النهضة العربية بالقاهرة، الطبعة الأولى، 2022 - 2023
15. ابن داود، عبدالعزيز بن فهد بن محمد. (2020). الجرائم السيبرانية: دراسة تأصيلية مقارنة. مجلة الاجتهاد للدراسات القانونية والاقتصادية، مج9، ع3 ، 144 - 166.
16. حسنين، سعد عاطف عبدالمطلب. (2019). دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي: دراسة مقارنة. مجلة بحوث كلية الآداب، ج118 ، 481 - 587.
17. الحجار، عدنان إبراهيم، و بشير، فايز خضر محمد. (2021). الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل. مجلة جامعة الاستقلال للأبحاث، مج6، ع1 ، 129 - 152.
18. د. محمد عادل عسكر، د/ أكمل يوسف السعيد، القواعد الأساسية لأصول البحث القانوني مطبعة جامعة المنصورة، بدون تاريخ
19. الطريف، عبدالرحمن بن سالم بن فهاد. (2020). اتجاهات الشباب السعودي نحو الجرائم السيبرانية وخطورتها: دراسة ميدانية. مجلة بحوث كلية الآداب، ع123، ج3 ، 1833 - 1883.
20. بهلول، سمية. (2021). الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها. مجلة العلوم القانونية والاجتماعية، مج6، ع4 ، 286 - 324.
21. مهدي، رضا. (2021). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري. مجلة إيليزا للبحوث والدراسات، مج6، ع2 ، 111 - 125.

22. عبدالحميد، عماد الدين محمد كامل. (2022). الجرائم السيبرانية في زمن "كورونا" وأثارها على الأمن القومي الاقتصادي: دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج42، ع500، 24 - 33.
23. عبدالحميد، عماد الدين محمد كامل. (2022). الجرائم السيبرانية في زمن "كورونا" وأثارها على الأمن القومي الاقتصادي: دراسة التحديات القانونية والاقتصادية واستراتيجية المواجهة. مجلة الاقتصاد الإسلامي، مج42، ع501، 18 - 25.
24. معروف، كريم. (2022). المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية. المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج4، ع2، 158 - 166.
25. عبدالرازق، رانا مصباح عبدالمحسن. (2023). آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. المجلة القانونية، مج15، ع5، 1359 - 1398.
26. أحمد، أيمن عطا عبدالماجد محمد. (2022). مكافحة الجرائم السيبرانية: الاتفاقيات العربية والدولية. مجلة ذخائر للعلوم الإنسانية، ع14، 12 - 31.
27. الفتلاوي، أحمد عبيس نعمة، و الخزعلي، بهاء عبدالحسين عبد علي. (2023). الأدلة غير المباشرة ودورها في إثبات جرائم السيبرانية: دراسة قانونية تحليلية في ضوء الاجتهاد القضائي للمحاكم الدولية. مجلة الكوفة للعلوم القانونية والسياسية، مج16، ع56، 118 - 128.
28. القضيب، نورة بنت عبدالرحمن، الفوزان، نورة بنت محمد، و الدوسري، نوف بنت حسن. (2023). 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، ع1، 1 - 32. مسترجع من <http://search.mandumah.com/Record/1447409>
29. Kharmouche, I. (2024). International Cooperation Mechanisms to Combat Cybercrime. المجلة الجزائرية للحقوق والعلوم السياسية، مج9، ع1، 1752 - 1765. مسترجع من <http://search.mandumah.com/Record/1484671>