مجلة النور للدراسات القانونية ، العدد (3) ، المجلد 1 ، اذار 2025
ISSN: 3007-3340 , https://doi.org/10.69513/jnfls.v1.i.3.a2 (65-24)

التحديات القانونيةُ المرتبطةُ بالجرائمِ الالكترونيةِ وآلياتِ مكافحتِها

م.م كرار براق طالب
جامعة ميسان / كلية الصيدلة
Karrar.burak @uomisan.edu.iq
ORCID: 0009-0007-5745-5689

تاريخ الاستلام: 2024/11/9 تاريخ القبول:2024/12/31
تاريخ النشر:2025/3/24

مستخلص
تناولت هذه الدراسةُ التحديات القانونية المرتبطة بالجرائم الإلكترونية وآليات مكافحتها، مع التركيز على القوانين الحالية وفعاليتها في مواجهة الظواهر المتزايدة في الفضاء الرقمي. أظهرت النتائج أن نقص التشريعات المتخصصة، والتحديات المرتبطة بالتعاون الدولي، وضعف الوعي العام تعد من العوامل الأساسية التي تعيق جهود مكافحة هذه الجرائم. كما قدمت الدراسة توصيات عملية تتضمن تحديث التشريعات، وتعزيز التعاون بين الدول، وزيادة الوعي المجتمعي لضمان بيئة رقمية آمنة. تعكس هذه الدراسة أهمية تطوير استراتيجيات قانونية شاملة تساهم في تحسين الأمان السيبراني وتعزيز الثقة في الفضاء الرقمي.

الكلمات المفتاحية: الجرائم الإلكترونية، التحديات القانونية، الأمن السيبراني

مجلة النور للدراسات القانونية ، العدد (3) ، المجلد 1 ، اذار 2025
ISSN: 3007-3340 , https://doi.org/10.69513/jnfls.v1.i.3.a2 (65-24)

Legal challenges associated with cybercrimes and mechanisms to combat them

Asst. Lect. Karrar buraq Talib
University of Maysan، College of Pharmacy
Karrar.burak @uomisan.edu.iq
ORCID: 0009-0007-5745-5689

Received :9/11/2024 Acceptance: 31/12/2024

Published:24/3/2025

Abstract

This study addressed the legal challenges associated with cybercrimes and the mechanisms to combat them، focusing on current laws and their effectiveness in confronting the growing phenomena in the digital space. The results showed that the lack of specialized legislation، challenges related to international cooperation، and weak public awareness are among the main factors that hinder efforts to combat these crimes. The study also provided practical recommendations that include updating legislation، enhancing cooperation between countries، and increasing community awareness to ensure a safe digital environment. This study reflects the importance of developing comprehensive legal strategies that contribute to improving cybersecurity and enhancing trust in the digital space.

Keywords: Cybercrime، Legal Challenges، Cybersecurity

المقدمة

في ظل التقدم التكنولوجي المتسارع، أصبح العالم أكثر اتصالًا من أي وقت مضى. لكن هذا التقدم لم يكن بلا تبعات، حيث ظهرت الجرائم الإلكترونية كأحد أبرز التحديات التي تواجه الأفراد والمجتمعات والدول. تعرّف الجرائم الإلكترونية بأنها الأنشطة الإجرامية التي تتم عبر الإنترنت أو باستخدام التكنولوجيا الرقمية، والتي تشمل مجموعة واسعة من الأفعال غير القانونية مثل الاحتيال المالي، سرقة الهوية، والجرائم المتعلقة بالمعلومات. تسببت هذه الجرائم في تكبد خسائر مالية كبيرة للأفراد والشركات، فضلاً عن تأثيراتها السلبية على الأمن الوطني.

تُظهر الإحصاءات أن الجرائم الإلكترونية في تزايد مستمر، مما يستدعي ضرورة التفكير في كيفية مواجهتها. تتمتع هذه الجرائم بسمات فريدة تجعلها أكثر تعقيدًا من الجرائم التقليدية. فعلى سبيل المثال، يمكن أن يتم تنفيذ هجوم سيبراني من أي مكان في العالم، مما يجعل من الصعب تحديد موقع الجاني أو حتى محاسبته. كما أن طبيعة الإنترنت تتيح للجاني إخفاء هويته، مما يزيد من التحديات القانونية المتعلقة بالتحقيق والملاحقة القضائية، وتعد التشريعات القانونية المعمول بها في معظم الدول غير كافية لمواجهة هذا النوع من الجرائم. إذ أن القوانين التقليدية غالبًا ما تفتقر إلى التكييف المناسب لمواجهة الظواهر الجديدة التي تطرأ على الفضاء الرقمي. وفي العديد من الحالات، تبقى القوانين عالقة في الماضي، مما يؤدي إلى وجود فجوات قانونية تُستغل من قبل المجرمين. هذا يشكل تحديًا كبيرًا ليس فقط للحكومات، ولكن أيضًا للقطاع الخاص والمجتمع المدني.

علاوة على ذلك، هناك تحديات إضافية تتعلق بالتعاون الدولي، لأن الجرائم الإلكترونية غالبًا ما تتجاوز الحدود الوطنية. تختلف التشريعات من دولة لأخرى، مما يُعقّد جهود التعاون في مكافحة هذه الجرائم. لذا، تبرز الحاجة الملحة إلى وضع أُطر قانونية دولية موحدة تُعزز من قدرة الدول على العمل سوياً لمواجهة هذه الظاهرة، وفي ضوء هذه التحديات، يصبح من الضروري التفكير في آليات فعّالة لمكافحة الجرائم الإلكترونية. يشمل ذلك تعزيز التشريعات القانونية، تطوير استراتيجيات تعليمية وتوعوية، وبناء شراكات بين القطاعين

العام والخاص، فضلا عن تعزيز التعاون الدولي في هذا المجال، وسيتناول هذا البحث التحديات القانونية المرتبطة بالجرائم الإلكترونية بمزيد من التفصيل، من خلال تحليل العوامل التي تساهم في تفشي هذه الظاهرة، وطرق مكافحتها، بما في ذلك الخطوات الواجب اتخاذها لتحسين الإطار القانوني وتعزيز إجراءات الأمان السيبراني. إن التصدي للجرائم الإلكترونية ليس مجرد مسألة قانونية، بل هو أيضًا مسؤولية جماعية تتطلب تضافر الجهود من جميع الأطراف المعنية، لضمان عالم رقمي أكثر أمانًا.

مشكلة البحث

تتجلى مشكلة البحث في تزايد الجرائم الإلكترونية بشكل متسارع، مما يؤدي إلى صعوبة في التصدي لها على الأصعدة القانونية والأمنية. تفتقر العديد من التشريعات الوطنية والدولية إلى التكيف مع طبيعة الجرائم الرقمية المتطورة، مما يسهل على المجرمين استغلال الثغرات القانونية. فضلا عن ذلك، تواجه المؤسسات القانونية تحديات في تطبيق القوانين القائمة بسبب ضعف التنسيق بين الدول وصعوبة تحقيق التعاون الدولي في مجال ملاحقة الجرائم التي تعبر الحدود. وعليه، يبقى السؤال الأهم وهو: كيف يمكن تحسين الأطر القانونية والتشريعات لمواجهة هذا النوع من الجرائم بفعالية؟

أهمية البحث

تكمن أهمية البحث في أنه يقدم تحليلاً معمقاً للتحديات القانونية التي تواجهها الدول في مكافحة الجرائم الإلكترونية، ويستعرض الطرق والأساليب الفعالة التي يمكن اعتمادها لتعزيز الأمن السيبراني. يعد البحث مهمًا أيضًا للمشرعين، حيث يسلط الضوء على الحاجة الماسة لتحديث التشريعات لتتناسب مع التطورات التكنولوجية، مما يساعد على تطوير سياسات وطنية ودولية فعالة لمكافحة الجرائم الرقمية. فضلًا عن ذلك، يمكن أن يسهم البحث في رفع الوعي العام حول مخاطر الجرائم الإلكترونية وسبل الحماية.

أهداف البحث

1. تحليل التحديات القانونية التي تواجه مكافحة الجرائم الإلكترونية على المستوى الوطني والدولي.

2. تقديم توصيات عملية لتحسين الأطر القانونية الحالية وتعزيز التعاون بين الدول في هذا المجال.
3. دراسة أثر التكنولوجيا الحديثة على الجرائم الإلكترونية وسبل مكافحتها.
4. تحليل دور المؤسسات الحكومية والقطاع الخاص في تحسين الأمن السيبراني والتصدي للجرائم الإلكترونية.
5. رفع مستوى الوعي لدى المجتمع حول أهمية حماية البيانات الشخصية ومخاطر الجرائم الإلكترونية.

فرضية البحث

"تزداد الجرائم الإلكترونية بشكل ملحوظ نتيجة لضعف الأطر القانونية الحالية وعدم توافقها مع طبيعة التطور التكنولوجي، مما يؤدي إلى تفشي هذه الجرائم في ظل عدم وجود تعاون دولي فعال."

منهجية البحث

تعتمد منهجية البحث على استخدام المنهج الوصفي التحليلي، حيث سيتم تحليل التحديات القانونية المرتبطة بالجرائم الإلكترونية وآليات مكافحتها من خلال استعراض الأدبيات القانونية والدراسات السابقة. سيتم أيضًا تطبيق المنهج المقارن لمقارنة التشريعات الوطنية والدولية، مما يساعد في تحديد الفجوات القانونية والفرص المتاحة لتحسينها. علاوة على ذلك، ستتضمن منهجية البحث دراسة حالات عملية للجرائم الإلكترونية، يسعى البحث إلى تقديم توصيات عملية لتحسين الاستجابة القانونية لهذه الجرائم المتزايدة.

المبحث الأول:

الإطار النظري للجرائم الإلكترونية

في هذا المبحث، سيتم استعراض الإطار النظري للجرائم الإلكترونية من خلال تعريف هذه الجرائم، وتسليط الضوء على الخصائص التي تميزها عن الجرائم التقليدية. كما سيتم التركيز على تطور هذه الجرائم في عصر الثورة التكنولوجية وكيفية تأثير الإنترنت والتكنولوجيا الحديثة على انتشارها. فضلا عن ذلك، سنناقش الأطر القانونية والأنظمة التشريعية التي تحكم مكافحة الجرائم الإلكترونية، مع توضيح التحديات التي تواجه مكافحة هذه الأنواع من الجرائم في ظل التقدم التكنولوجي السريع.

المطلب الأول: تعريف الجرائم الإلكترونية

تعد الجرائم الإلكترونية من أكثر التحديات الأمنية تعقيدًا في عصر التكنولوجيا الرقمية، حيث تتزايد عمليات الاحتيال والاعتداءات السيبرانية بطرق متنوعة ومبتكرة. ورغم وجود تعاريف متعددة لهذه الجرائم، إلا أن هناك اتفاقًا عامًّا على كونها تشمل جميع الأفعال الإجرامية التي تتم عبر الوسائل الإلكترونية والتي تستهدف المعلومات أو الشبكات أو الأنظمة الإلكترونية.

الجريمة الإلكترونية تُعرف لغويًّا بأنها "الاعتداء أو الإساءة" باستخدام الوسائل الرقمية، وغالبًا ما تكون عبر الإنترنت. أما من الناحية التقنية، فهي تشمل استخدام الحواسيب أو الشبكات لارتكاب أفعال تتعارض مع القانون، مثل القرصنة، التزوير الإلكتروني، والاحتيال السيبراني، بهدف إلحاق الضرر بالضحية.[1]

تُعرف الجرائم الإلكترونية قانونيًا بأنها الأنشطة التي تنطوي على استخدام التكنولوجيا الحديثة لارتكاب جريمة يعاقب عليها القانون. بعض التشريعات تصنفها على أنها أي نشاط يتم باستخدام الأجهزة الرقمية والشبكات لإلحاق الضرر بالأشخاص أو المؤسسات أو حتى الدول. يشمل هذا التعريف مجموعة واسعة من الجرائم، منها التعدي على حقوق الملكية الفكرية، اختراق الأنظمة، نشر البرمجيات الخبيثة، وجرائم الابتزاز الإلكتروني، ومن أهم خصائص الجرائم الإلكترونية:[2]

1. **النطاق الواسع:** تمتد الجريمة الإلكترونية إلى مناطق جغرافية بعيدة عن موقع الجاني، ما يجعل من الصعب تتبع الجناة وإخضاعهم للمساءلة القانونية.
2. **صعوبة التتبع:** تتيح التقنيات الحديثة إخفاء الهوية وتتبع خطوات المستخدمين، مما يجعل تعقب مرتكبي الجرائم الإلكترونية مهمة معقدة.
3. **الاعتماد على التكنولوجيا:** تعتمد الجرائم الإلكترونية بشكل كبير على الأدوات الرقمية والشبكات، وهذا يتطلب وجود متخصصين مؤهلين لفهم واكتشاف الأدلة الرقمية.

4. التأثير الكبير: قد تؤدي الجريمة الإلكترونية إلى خسائر مالية كبيرة وانتهاك الخصوصية، ما ينعكس على الأفراد والشركات والمجتمع ككل.

ويمكن تصنيف الجرائم الإلكترونية إلى عدة أنواع رئيسية على وفق طبيعة الجرائم أو نوع الأهداف، ومنها:[3]

- **القرصنة:** وتعني التسلل إلى الأنظمة أو الشبكات الخاصة دون إذن قانوني بقصد التخريب أو التجسس.
- **الاحتيال الإلكتروني:** ويتمثل في محاولات الخداع المالي عبر الإنترنت، مثل الاحتيال في التجارة الإلكترونية.
- **الهجمات التخريبية:** وتشمل نشر الفيروسات وبرامج التجسس والبرمجيات الخبيثة الأخرى التي تؤدي إلى تلف الأجهزة والبيانات.
- **التشهير والابتزاز الإلكتروني:** من خلال نشر أو تهديد بنشر معلومات حساسة عن الضحية للضغط عليها أو إجبارها على دفع مبالغ مالية.

مع تزايد الاعتماد على الإنترنت والأجهزة الذكية، تطورت تعريفات الجرائم الإلكترونية لتشمل أبعادًا جديدة. حيث لم تعد الجرائم محصورة بسرقة البيانات، بل امتدت إلى الاعتداءات على الخصوصية، التأثير في الرأي العام من خلال نشر الأخبار المضللة، وحتى التأثير في الأنظمة الاقتصادية للدول من خلال التلاعب بالأسواق الإلكترونية، وتتعدد التعريفات الأكاديمية التي تسعى إلى الإحاطة بمفهوم الجرائم الإلكترونية، ويلاحظ أن معظمها يرتكز على الفكرة الأساسية أن هذه الجرائم تتم عبر الإنترنت أو تعتمد على التكنولوجيا. أما في التعريفات القانونية، فتضع معظم التشريعات الحديثة قوانين صارمة لتجريم الأنشطة التي تندرج تحت هذه الجرائم، وتحدد العقوبات المناسبة لكل نوع منها.[4]

المطلب الثاني: أنواع الجرائم الإلكترونية

الجرائم الإلكترونية تمثل مجموعة واسعة من الأنشطة غير القانونية التي تتم عبر الوسائل الإلكترونية، سواء عبر الإنترنت أو باستخدام الأجهزة الرقمية. ومع تزايد الاستخدامات الرقمية، تطورت أساليب المجرمين في استغلال التكنولوجيا لارتكاب جرائم متعددة الأشكال

والأهداف. سنتناول فيما يلي أبرز أنواع الجرائم الإلكترونية، مع تسليط الضوء على طبيعة كل نوع وتأثيراته.

اولا: جرائم الاحتيال المالي الإلكتروني: تُعد جرائم الاحتيال المالي من أبرز الجرائم الإلكترونية، وهي تشمل محاولات لسرقة الأموال أو الاحتيال على الأفراد والشركات لتحقيق مكاسب مالية غير مشروعة. يمكن أن يحدث هذا النوع من الاحتيال من خلال:(5)

1. **التجارة الإلكترونية:** مثل الاحتيال عبر متاجر وهمية على الإنترنت أو إرسال عروض مغرية بهدف سرقة بيانات الحسابات المصرفية.
2. **التصيد الاحتيالي (Phishing):** إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من مصادر موثوقة، لكنها تهدف إلى خداع الضحايا للكشف عن معلوماتهم الشخصية أو المالية.
3. **احتيال بطاقات الائتمان:** يشمل سرقة بيانات بطاقات الائتمان واستخدامها للشراء أو التحويل المالي بشكل غير قانوني.

ثانيا: جرائم القرصنة والاختراق (Hacking): تشير الجرائم المرتبطة بالقرصنة إلى التسلل غير القانوني إلى أنظمة الحاسوب أو الشبكات أو قواعد البيانات بهدف الحصول على معلومات سرية أو تخريب الأنظمة. ومن أبرز هذه الأنواع:(6)

1. **التجسس الإلكتروني:** يقوم القراصنة بتسلل إلى شكات الشركات أو الحكومات للحصول على بيانات سرية، ويستهدف هذا النوع من الجرائم عادةً الأسرار التجارية أو المعلومات الحساسة.
2. **التخريب المعلوماتي:** يهدف إلى إتلاف أو حذف البيانات أو تعطيل الأنظمة، مما يتسبب في خسائر مادية أو تعطل عمليات العمل، كما هو الحال في الهجمات ضد البنية التحتية.
3. **الهجمات على الشبكات:** تشمل توزيع الفيروسات أو البرمجيات الخبيثة التي تتيح للمخترقين التحكم في الأنظمة المصابة وجمع المعلومات.

ثالثا: الجرائم المتعلقة بالبرمجيات الضارة (Malware): البرمجيات الضارة تشمل جميع أنواع البرمجيات التي صممت لإلحاق الضرر بالأجهزة أو الأنظمة أو سرقة المعلومات. ويشمل هذا النوع من الجرائم:(7)

1. **الفيروسات:** وهي برامج تتكاثر وتنتشر عبر الشبكات أو الملفات المصابة، وتسبب تلف الملفات أو تبطئ من أداء الأنظمة.
2. **الديدان الإلكترونية (Worms):** تُصمم هذه البرمجيات خصيصًا للانتشار في الشبكات، وعادةً ما تسبب زيادة الضغط على الشبكة وتعطلها.
3. **برمجيات التجسس (Spyware):** تجمع المعلومات عن المستخدم دون علمه وترسلها إلى جهة أخرى، غالبًا لأغراض تجارية أو لأعمال تجسس.
4. **البرمجيات الفدية (Ransomware):** تشفر البيانات على جهاز المستخدم وتطلب فدية لإعادة فك التشفير، مما يمثل تهديدًا كبيرًا للأفراد والمؤسسات.

رابعا: جرائم التشهير والابتزاز الإلكتروني: تشمل هذه الجرائم نشر معلومات ضارة أو تهديد بنشرها لابتزاز الضحية أو تشويه سمعتها. ويشمل ذلك:

1. **الابتزاز المالي:** يهدد المجرم بنشر معلومات شخصية أو صور خاصة للضحية، ويطالب بفدية مالية مقابل عدم النشر.
2. **التشهير الإلكتروني:** يتم عبر نشر معلومات كاذبة عن الضحية على مواقع التواصل الاجتماعي أو عبر الإنترنت بهدف الإضرار بسمعتها، سواء كانت شخصية أو مهنية.
3. **الملاحقة الإلكترونية:** متابعة أو مضايقة الضحية عبر الإنترنت بطرق تجعلها تشعر بعدم الأمان، ويتضمن ذلك إرسال رسائل تهديدية أو ملاحقتها عبر الشبكات الاجتماعية.

خامسا: الجرائم المتعلقة بالملكية الفكرية: تعد حماية حقوق الملكية الفكرية تحديًا كبيرًا في العالم الرقمي، حيث يسهل الوصول إلى الملفات والمعلومات ونشرها بطريقة غير قانونية. من أبرز جرائم الملكية الفكرية:[8]

1. **القرصنة الرقمية:** تتضمن توزيع المحتوى المحمي بحقوق الطبع والنشر، مثل الأفلام والموسيقى، دون إذن.
2. **سرقة البرمجيات:** من خلال تكرار أو بيع البرمجيات دون ترخيص أو إذن، مما يؤثر سلبًا على الشركات المنتجة للبرامج.

3. تزوير العلامات التجارية: إنشاء نسخ مقلدة من المنتجات أو العلامات التجارية الأصلية وبيعها بأسعار منخفضة، مما يؤدي إلى خسائر اقتصادية للشركات.

سادسا: الجرائم السيبرانية ضد البنية التحتية الوطنية: هذا النوع من الجرائم يستهدف البنية التحتية الحيوية للدول، مثل شبكات الطاقة، الماء، النقل، والاتصالات. تشمل هذه الجرائم:[9]

1. الهجمات على محطات الطاقة: يمكن أن يؤدي تعطيل محطات الطاقة إلى انقطاع الكهرباء عن مناطق واسعة، مما يؤثر على الخدمات الأساسية.

2. التلاعب في أنظمة النقل: من خلال اختراق أنظمة النقل، يمكن إحداث فوضى وإلحاق الضرر بالبنية التحتية الحيوية.

3. تعطيل أنظمة الاتصالات: من خلال الهجمات الموجهة إلى أنظمة الاتصال الأساسية، مما يؤدي إلى انقطاع الاتصال وتأثر القطاعات الحكومية والأمنية.

توضح أنواع الجرائم الإلكترونية التنوع الكبير في أساليب الهجوم الإلكتروني التي تتطلب اهتمامًا خاصًا من الجهات القانونية والأمنية. وتستلزم هذه الجرائم إجراءات قانونية صارمة وتعاونًا دوليًا لمكافحة التهديدات المتزايدة، مع تعزيز وعي الأفراد بمخاطر هذه الأنشطة.

المطلب الثالث: تطور الجريمة الإلكترونية في العصر الحديث

شهد العالم تطورًا هائلًا في مجالات التكنولوجيا والاتصالات في العقود الأخيرة، مما أدى إلى تسارع وتيرة الاعتماد على الإنترنت في جميع جوانب الحياة، سواء في مجال الأعمال أو التعليم أو التواصل الاجتماعي. ورغم أن هذا التطور أدى إلى فوائد كبيرة، إلا أنه تسبب أيضًا في ظهور تحديات جديدة، على رأسها الجرائم الإلكترونية التي باتت تشكل تهديدًا حقيقيًا لأمن المعلومات والأشخاص والمؤسسات على حد سواء. هذا المطلب يسعى إلى توضيح كيفية تطور الجرائم الإلكترونية عبر الزمن، والعوامل التي ساهمت في ازديادها وتنوعها في العصر الحديث.

التطورات التاريخية للجرائم الإلكترونية:[10]

1. المرحلة الأولى - ظهور الجرائم الإلكترونية الأساسية (السبعينات والثمانينات): بدأت الجرائم الإلكترونية في السبعينات والثمانينات

بشكل بسيط ومحدود، وكان أبرزها قرصنة الأنظمة واختراق الشبكات في المؤسسات الكبرى أو الحكومية. ركز القراصنة حينها على استغلال الثغرات الأساسية في أنظمة الحواسيب لعرض مهاراتهم أو للوصول إلى بيانات معينة. كانت الهجمات في هذه المرحلة تقتصر على عدد محدود من الأفراد ذوي المعرفة التقنية العالية، ولم تكن بعد متطورة من حيث الأدوات أو التأثيرات الكبيرة.

2. المرحلة الثانية ـ تطور الجريمة مع انتشار الإنترنت (التسعينات): مع انتشار الإنترنت على نطاق أوسع في التسعينات، ازدادت الجرائم الإلكترونية وبدأت في الانتشار بين أوساط المستخدمين العاديين. تطورت الأدوات والأساليب المستخدمة في الهجمات، وظهرت أنواع جديدة من الجرائم، مثل الاحتيال عبر البريد الإلكتروني (Email Scams) وفيروسات الكمبيوتر التي كانت تنتشر عبر الملفات القابلة للتنزيل. كما بدأ القراصنة في استهداف الأفراد بشكل أوسع، مما أدى إلى ظهور أولى حالات سرقة المعلومات الشخصية وبيانات بطاقات الائتمان.

3. المرحلة الثالثة ـ طفرة في الجرائم الإلكترونية مع تطور التكنولوجيا (العقد الأول من القرن الحادي والعشرين): مع تطور التكنولوجيا وتزايد الاعتماد على الإنترنت في الحياة اليومية، شهد العالم طفرة في الجرائم الإلكترونية. ظهرت برمجيات التجسس (Spyware) والبرامج الخبيثة (Malware) وبدأت الجرائم الإلكترونية تأخذ منحى أكثر تنظيمًا. ظهرت أيضًا جماعات إجرامية متخصصة تتخذ من الإنترنت وسيلة للقيام بهجمات على البنوك والمؤسسات المالية الكبرى. أدى تطور الهواتف الذكية والأجهزة الذكية الأخرى إلى توسيع نطاق الهجمات ليشمل منصات وأجهزة جديدة، مما زاد من تعقيد الجريمة الإلكترونية وتنوع أشكالها.

التطورات التقنية والعوامل المؤثرة في الجرائم الإلكترونية:[11]

1. التطور السريع في التكنولوجيا الرقمية: مع تطور الأجهزة والأنظمة الرقمية وزيادة تعقيد التطبيقات والخدمات الإلكترونية، ظهرت تقنيات متقدمة مثل الذكاء الاصطناعي وتعلم الآلة، والتي استغلها مجرمو الإنترنت في تحسين طرق الهجوم. أدت هذه

التطورات إلى ظهور أدوات جديدة تساعد المجرمين على تجاوز أنظمة الأمان بسرعة وسهولة.

2. زيادة الاعتماد على الإنترنت في المعاملات اليومية: مع تزايد استخدام الإنترنت للقيام بعمليات الشراء، التصفح، وإدارة الحسابات المصرفية، ازدادت فرص مجرمي الإنترنت لاستهداف المستخدمين من خلال سرقة بياناتهم الشخصية والمالية، مما سهل عمليات الاحتيال والابتزاز.

3. ظهور الإنترنت المظلم (Dark Web): يعد الإنترنت المظلم بيئة مثالية لنشاطات الجريمة الإلكترونية، حيث توفر هذه الشبكة فضاءً آمنًا نسبيًا للمجرمين للتواصل وبيع المعلومات المسروقة، والأسلحة، والمخدرات، وحتى الخدمات الإجرامية مثل تأجير القراصنة أو توزيع البرامج الضارة. ساعد الإنترنت المظلم على تنظيم الجرائم الإلكترونية ورفع مستوى الاحترافية فيها.

الأساليب المتطورة المستخدمة في الجرائم الإلكترونية:

1. الهجمات المعقدة والمتعددة الأوجه: يتمتع المجرمون الإلكترونيون اليوم بقدرات متقدمة لتنفيذ هجمات معقدة تشمل مراحل متعددة. على سبيل المثال، تستخدم العديد من الهجمات اليوم تقنيات التصيد الاحتيالي كمرحلة أولى، تليها مراحل تضمن زرع البرمجيات الضارة في النظام المستهدف ثم سرقة البيانات.

2. هجمات برامج الفدية (Ransomware): أصبحت برامج الفدية من أخطر أنواع الهجمات الإلكترونية في العصر الحديث، حيث يقوم المهاجم بتشفير بيانات الضحية ويطلب فدية مالية مقابل فك التشفير. وانتشرت هذه الهجمات على نطاق واسع خلال السنوات الأخيرة، مستهدفةً شركات كبيرة وحتى مؤسسات حكومية، مما أضر بالكثير من الأنشطة والعمليات التجارية.

3. استخدام الذكاء الاصطناعي والتعلم الآلي: بات المهاجمون يعتمدون على تقنيات الذكاء الاصطناعي لتطوير طرق الهجوم وجعلها أكثر ذكاءً، حيث يمكن أن تتعلم هذه البرامج كيفية تجاوز أنظمة الأمان أو تحليل سلوك الضحية بهدف استهدافها بطرق أكثر دقة. يمكن لتقنيات الذكاء الاصطناعي اليوم خلق رسائل تصيد احتيالي

مخصصة وفقًا لسلوكيات الضحايا، مما يزيد من فعالية الهجمات الإلكترونية.

4. الهجمات على إنترنت الأشياء (IoT): مع انتشار الأجهزة الذكية المتصلة بالإنترنت، مثل الكاميرات، الأجهزة المنزلية، وأنظمة التحكم في السيارات، أصبحت هذه الأجهزة هدفًا جديدًا للقراصنة. يمكن اختراق أجهزة إنترنت الأشياء واستغلالها لشن هجمات واسعة النطاق على الأنظمة أو حتى استخدامها كجزء من شبكات "بوت نت" لتنفيذ هجمات الحرمان من الخدمة (DDoS).

تطورت الجريمة الإلكترونية بشكل ملحوظ في العصر الحديث، لتصبح ظاهرة متنامية تهدد الأفراد والمؤسسات والدول على حد سواء. ويستدعي هذا التطور السريع ضرورة تعزيز آليات الأمن السيبراني وزيادة الوعي لدى الأفراد حول سبل حماية بياناتهم ومعلوماتهم الشخصية. كما أن التعاون بين الدول وتحديث التشريعات الدولية يعد أمرًا ضروريًا للحد من انتشار الجرائم الإلكترونية ومواكبة التغيرات المستمرة في هذا المجال.[12]

المبحث الثاني:

التحديات القانونية المرتبطة بالجرائم الإلكترونية

يعد الفهم العميق للتحديات القانونية المرتبطة بالجرائم الإلكترونية من الأمور الأساسية لتحسين الإجراءات التشريعية والتقليل من تأثير هذه الجرائم على الأفراد والمجتمعات. في هذا المبحث، سيتم تسليط الضوء على التحديات التي تواجهها الأنظمة القانونية في مواجهة الجرائم الإلكترونية، التي تتسم بطبيعة معقدة ومتطورة بشكل مستمر. سيشمل البحث تحليل القيود القانونية الحالية، التحديات التقنية في إثبات الجرائم الإلكترونية، وقصور التشريعات الوطنية والدولية في التعامل مع هذه الجرائم. كما سيتم مناقشة أبرز المعوقات في التنسيق بين الدول لمكافحة الجرائم الإلكترونية عبر الحدود.

المطلب الأول: نقص التشريعات القانونية المتخصصة

تعد الجرائم الإلكترونية من أكثر التحديات القانونية تعقيدًا في العصر الحديث، إذ تتطور هذه الجرائم بشكل متسارع، مما يجعل التصدي لها مهمة صعبة أمام القوانين التقليدية. وفي ظل التطورات السريعة للتكنولوجيا، يواجه النظام القانوني نقصًا في التشريعات المتخصصة

التي تواكب هذه التطورات وتتيح التعامل الفعال مع الجرائم الإلكترونية. في هذا السياق، سنستعرض الأسباب وراء نقص هذه التشريعات، الأثر الناتج عنها، والسبل الممكنة للتغلب على هذه التحديات.[13]

1. التحديات المرتبطة بنقص التشريعات: تتسم الجرائم الإلكترونية بتغيراتها السريعة والمستمرة، حيث تظهر أساليب ووسائل جديدة بانتظام. على الرغم من أن بعض القوانين قد تكون قد تم إعدادها لمواجهة هذه الجرائم، فإن التقدم السريع في التكنولوجيا غالبًا ما يتجاوز قدرة التشريعات على التكيف. وهذا يؤدي إلى فجوات تشريعية حيث تظل الجرائم غير معرّفة بشكل دقيق، مما يعرقل قدرة السلطات القانونية على التعامل معها، وتختلف القوانين المتعلقة بالجرائم الإلكترونية من دولة لأخرى، مما يخلق تناقضات وصعوبات في تطبيق القانون. قد تكون هناك تشريعات في دولة معينة تعالج نوعًا معينًا من الجرائم الإلكترونية، بينما تفتقر دول أخرى إلى تلك القوانين. هذا النقص في التنسيق الدولي يزيد من تعقيد الأمور، حيث يمكن للمجرمين الاستفادة من هذه الفجوات بالتنقل بين البلدان لتجنب الملاحقة القانونية، وتفتقر العديد من التشريعات إلى تعريفات واضحة ومحددة لمفاهيم الجرائم الإلكترونية. فعلى سبيل المثال، قد لا تتضمن القوانين الحالية تصنيفات دقيقة مثل "الجرائم السيبرانية" أو "الاحتيال الإلكتروني"، مما يؤدي إلى صعوبة في تطبيق القوانين بشكل فعال. هذه الضبابية تترك مجالًا واسعًا للتفسيرات المتباينة، مما يمكن المجرمين من التهرب من المساءلة القانونية.[14]

2. الأثر الناتج عن نقص التشريعات: نقص التشريعات يؤدي إلى صعوبة في ملاحقة الجناة وتقديمهم للعدالة. فغياب القوانين المتخصصة يجعل من الصعب جمع الأدلة، وتحديد المسؤولية، وتطبيق العقوبات. هذا النقص يؤدي في كثير من الحالات إلى إحباط جهود سلطات إنفاذ القانون، مما يسمح للمجرمين بمواصلة أنشطتهم بحرية، ويمكن أن يؤدي نقص التشريعات المتخصصة إلى تقويض الثقة في النظام القانوني والجهات المسؤولة عن حماية المواطنين. عندما يشعر الأفراد بأن الجرائم الإلكترونية لا تعاقب بشكل كافٍ، قد يترددون في الإبلاغ عن تلك الجرائم أو طلب المساعدة، مما يزيد من

انتشار هذه الأنشطة الإجرامية، تعد الجرائم الإلكترونية تهديدًا خطيرًا للأمن الاقتصادي للدول. فقد تتسبب الهجمات الإلكترونية في خسائر مالية ضخمة للشركات والأفراد، مما يؤثر سلبًا على الاقتصاد ككل. وبما أن التشريعات غير كافية لحماية المؤسسات والأفراد، فإن ذلك قد يؤدي إلى تراجع الاستثمار وفقدان الثقة في الاقتصاد الرقمي.[15]

3. الجهود المبذولة لمواجهة نقص التشريعات: تسعى بعض الدول إلى تطوير قوانينها المحلية لمواكبة التغيرات السريعة في عالم الجرائم الإلكترونية. يجب أن تشمل هذه الجهود تحديث التعريفات القانونية، وتحديد الجرائم الإلكترونية بشكل دقيق، ووضع عقوبات رادعة للمخالفين. كما ينبغي أن تتضمن القوانين آليات لتسهيل ملاحقة الجرائم عبر الحدود، وتتطلب الجرائم الإلكترونية نهجًا تعاونيًا دوليًا لمواجهتها. يمكن تحقيق ذلك من خلال تبادل المعلومات والخبرات بين الدول وتطوير اتفاقيات دولية تنظم كيفية التعامل مع الجرائم الإلكترونية. فعلى سبيل المثال، يمكن أن تسهم الاتفاقيات الدولية في تسهيل الإجراءات القانونية وتوحيد التعريفات، مما يجعل من السهل ملاحقة الجناة عبر الحدود، ويجب على السلطات القانونية تعزيز الوعي حول الجرائم الإلكترونية وتوفير التدريب المناسب لرجال القانون والمحامين والقضاة. يجب أن يتضمن هذا التدريب المعلومات الحديثة حول أساليب الجرائم الإلكترونية، وكيفية جمع الأدلة، وتطبيق القوانين بشكل فعال. بزيادة المعرفة، يمكن للجهات المسؤولة أن تكون أكثر استعدادًا لمواجهة التحديات المرتبطة بالجرائم الإلكترونية.

إن نقص التشريعات القانونية المتخصصة لمواجهة الجرائم الإلكترونية يشكل تحديًا حقيقيًا للأمن القانوني والاقتصادي في العصر الحديث. يتطلب الأمر جهودًا متكاملة تشمل تطوير القوانين المحلية، وتعزيز التعاون الدولي، وزيادة الوعي والتدريب في هذا المجال. مع التحديات المتزايدة، فإن اتخاذ خطوات جادة نحو معالجة هذه الفجوات التشريعية أصبح أمرًا ضروريًا لضمان حماية الأفراد والمؤسسات من مخاطر الجرائم الإلكترونية وضمان تحقيق العدالة.[16]

المطلب الثاني: التحديات القضائية وأدلة الإثبات في الجرائم الإلكترونية

تعد الجرائم الإلكترونية من أكثر التحديات القانونية والقضائية التي تواجه النظام القانوني في العصر الحديث، نظرًا للتطور السريع في تكنولوجيا المعلومات والاتصالات. تواجه السلطات القضائية صعوبات كبيرة في تحقيق العدالة في هذا المجال بسبب طبيعة هذه الجرائم التي تتم غالبًا عبر الإنترنت وتكون غالبًا معقدة وغير مرئية. وفيما يلي، سوف نناقش التحديات القضائية وأدلة الإثبات المرتبطة بالجرائم الإلكترونية :[17]

أولاً: التحديات القضائية

تواجه المحاكم القضائية عدة تحديات في التعامل مع الجرائم الإلكترونية، ومن أبرز هذه التحديات:[18]

1. صعوبة تحديد الجاني: واحدة من أبرز التحديات في الجرائم الإلكترونية هي صعوبة تحديد هوية الجاني. غالبًا ما يتم ارتكاب هذه الجرائم باستخدام هويات مزيفة أو أسماء مستعارة، مما يجعل من الصعب تعقب المتهمين. يستخدم الجناة تقنيات مثل الشبكات الافتراضية الخاصة (VPN) للتخفي عن أنظار السلطات، مما يزيد من تعقيد عمليات التحقيق.

2. قوانين غير موحدة: تختلف القوانين التي تتعلق بالجرائم الإلكترونية من دولة إلى أخرى. يفتقر العديد من الدول إلى تشريعات شاملة تتعلق بالجرائم الإلكترونية، مما يؤدي إلى تحديات قانونية في محاكمة الجناة. هذا النقص في التشريعات الموحدة قد يؤدي إلى عدم فعالية العدالة، حيث يمكن أن يهرب الجناة من العقاب بسبب الفجوات القانونية.

3. تعقيد التكنولوجيا: تتطلب الجرائم الإلكترونية معرفة تقنية متقدمة لفهم الأدلة والبرامج المستخدمة. لذا، تحتاج المحاكم إلى خبراء في مجال تكنولوجيا المعلومات لفهم كيفية حدوث الجريمة وتحديد الأدلة بشكل دقيق. وقد تؤدي عدم القدرة على تفسير التقنيات المعقدة إلى ضعف الأدلة المقدمة أمام المحاكم.

4. التحقيقات المتقاطعة: قد تشمل الجرائم الإلكترونية أكثر من ولاية أو حتى دول. يتطلب ذلك تعاونًا دوليًا معقدًا وتنسيقًا بين مختلف

الوكالات القانونية، مما يمكن أن يبطئ من عملية العدالة. كما أن اختلاف القوانين والإجراءات بين الدول يمكن أن يعقد عملية التحقيق والملاحقة القانونية.

ثانيًا: أدلة الإثبات في الجرائم الإلكترونية

تتطلب الجرائم الإلكترونية نوعًا خاصًا من الأدلة قد لا يتوفر في الجرائم التقليدية. تشمل أدلة الإثبات في هذا السياق ما يلي:[19]

1. **البيانات الرقمية:** تعد البيانات الرقمية أحد أهم مصادر الأدلة في الجرائم الإلكترونية. تتضمن هذه البيانات السجلات الإلكترونية، رسائل البريد الإلكتروني، سجلات الشبكات الاجتماعية، وتاريخ التصفح. يمكن أن تساعد هذه الأدلة في إثبات أنشطة الجاني وأماكن تواجده، ولكن يجب جمعها بطريقة صحيحة للحفاظ على قوتها القانونية.
2. **التحليل الجنائي الرقمي:** يُعد التحليل الجنائي الرقمي تقنية متقدمة تستخدم لاستخراج وتحليل الأدلة من الأجهزة الإلكترونية مثل الهواتف المحمولة وأجهزة الكمبيوتر. يتطلب هذا النوع من الأدلة خبرة فنية متخصصة، حيث يجب على المحققين استخدام أدوات متطورة لاستخراج البيانات دون تغييرها، مما يضمن قبول الأدلة في المحكمة.
3. **الشهادات التقنية:** قد تُستخدم الشهادات التقنية من الخبراء في مجالات التكنولوجيا للمساعدة في تفسير الأدلة المقدمة. يجب أن يكون هؤلاء الخبراء قادرين على توضيح كيف تعمل التكنولوجيا المستخدمة في الجريمة، مما يساعد في دعم الادعاءات المقدمة في المحكمة.
4. **الأدلة المادية:** على الرغم من أن الجرائم الإلكترونية تحدث في الفضاء الرقمي، إلا أن الأدلة المادية قد تؤدي دوراً مهماً في القضايا. على سبيل المثال، يمكن أن تشمل الأجهزة المستخدمة في الجريمة، مثل أجهزة الكمبيوتر أو الهواتف، أدلة مادية تدعم القضية.
5. **البروتوكولات الأمنية:** تعد سجلات الدخول والخروج من الأنظمة والشبكات أيضًا من الأدلة الهامة. يمكن استخدام هذه السجلات لتحديد من قام بالدخول إلى النظام في وقت معين، مما يساعد في تحديد المسؤول عن الجريمة.

تعد التحديات القضائية وأدلة الإثبات في الجرائم الإلكترونية مسألة معقدة تتطلب تعاونًا متعدد التخصصات. يجب أن تتطور الأنظمة القانونية لمواكبة الابتكارات التكنولوجية وتقديم القوانين اللازمة لمكافحة الجرائم الإلكترونية. من المهم أيضًا تعزيز التعاون الدولي لمواجهة هذه التحديات، حيث إن الجرائم الإلكترونية لا تعرف حدودًا. على السلطات القضائية أن تكون مستعدة للتكيف مع هذا النوع من الجرائم والتعلم من التجارب السابقة لتوفير الحماية اللازمة للأفراد والمجتمع.

إن مواجهة التحديات القضائية في الجرائم الإلكترونية يتطلب جهدًا مشتركًا من جميع الأطراف المعنية، بما في ذلك الحكومات، والهيئات القانونية، وخبراء التكنولوجيا، والمجتمع المدني، لضمان تحقيق العدالة وحماية الحقوق الرقمية للأفراد.

المطلب الثالث: التحديات التقنية في تتبع الجرائم الإلكترونية ومكافحتها

تُعد الجرائم الإلكترونية من أكثر التحديات التقنية تعقيدًا في عصرنا الحالي، حيث تتجاوز تأثيراتها الحدود الجغرافية وتتطلب استراتيجيات مبتكرة للتعامل معها. إن الطبيعة المتطورة والغير مرئية للجرائم الإلكترونية تجعل من الصعب على السلطات الأمنية تتبع الجناة ومكافحة الأنشطة الإجرامية بفعالية. وفيما يلي، سنناقش التحديات التقنية التي تواجه مكافحة الجرائم الإلكترونية.[20]

أولاً: سرعة التطور التكنولوجي: تتغير التكنولوجيا بشكل سريع، مما يجعل من الصعب على الجهات الأمنية مواكبتها. فكلما تم تطوير تقنيات جديدة، يظهر معها أساليب جديدة للجرائم الإلكترونية. على سبيل المثال، قد تستفيد العصابات الإجرامية من أحدث تقنيات التشفير، مما يجعل من الصعب على المحققين الوصول إلى المعلومات الضرورية لتحديد هوية الجناة. تعد هذه الديناميكية تحديًا رئيسيًا، حيث يتطلب الأمر من الجهات الأمنية تحديث أدواتها ومعرفتها باستمرار لمواكبة التطورات السريعة في عالم التكنولوجيا.

ثانيًا: استخدام تقنيات التشفير: التشفير هو أداة أساسية لحماية المعلومات، لكنه في نفس الوقت يمكن أن يكون أداة تُستخدم من قبل المجرمين لإخفاء أنشطتهم. تُستخدم تقنيات التشفير لحماية البيانات من

الوصول غير المصرح به، مما يجعل من الصعب على السلطات الأمنية الحصول على الأدلة اللازمة لتتبع الجرائم الإلكترونية. يُعد التشفير القوي عائقًا أمام التحقيقات، حيث يصعب فك تشفير البيانات المشفرة من قبل الجناة. هذا التحدي يتطلب من السلطات الأمنية تطوير استراتيجيات جديدة للتعامل مع المعلومات المشفرة دون انتهاك الحقوق القانونية للأفراد.

ثالثًا: الشبكات المظلمة: تعد الشبكات المظلمة (Dark Web) بيئة خصبة للأنشطة الإجرامية، حيث يتم تداول المعلومات بشكل سري بعيدًا عن الأنظار العامة. توفر هذه الشبكات ملاذًا آمنًا للجناة الذين يرغبون في ارتكاب جرائم مثل بيع المخدرات، الأسلحة، والبيانات المسروقة. إن تعقب الأنشطة في الشبكات المظلمة يتطلب تقنيات خاصة ومعرفة عميقة بتلك البيئة، مما يجعل مهمة السلطات الأمنية أكثر صعوبة وتعقيدًا. علاوة على ذلك، يؤدي عدم وجود لوائح واضحة لتنظيم هذا النوع من النشاط إلى تحديات إضافية في مكافحة الجرائم.[21]

رابعًا: عدم القدرة على تحديد الهوية: تستخدم الجرائم الإلكترونية هويات مزيفة وتقنيات مختلفة للتخفي عن الأنظار، مثل استخدام الشبكات الافتراضية الخاصة (VPN) وعناوين IP مجهولة. تجعل هذه الأساليب من الصعب تحديد هوية الجاني أو مكانه الحقيقي. يُعد هذا الأمر تحديًا كبيرًا للجهات الأمنية، حيث يتطلب الأمر استراتيجيات متطورة لتحديد موقع الجناة وتفكيك الشبكات الإجرامية. علاوة على ذلك، قد يُستخدم الجناة تقنيات التلاعب بالأرقام والعناوين للتلاعب بالتحقيقات، مما يزيد من تعقيد عملية التعقب.

خامسًا: تحليلات البيانات الضخمة: تنتج الجرائم الإلكترونية كميات هائلة من البيانات التي يجب تحليلها لاستنتاج الأنماط والسلوكيات. لكن، تحليل البيانات الضخمة يتطلب أدوات وتقنيات متطورة، فضلا عن خبراء قادرين على فهم البيانات واستخراج المعلومات القيمة منها. يُعد عدم وجود الأدوات الصحيحة والموارد البشرية المناسبة عائقًا أمام فعالية التحقيقات. لذا، تحتاج السلطات الأمنية إلى الاستثمار في تقنيات الذكاء الاصطناعي وتعلم الآلة لتحسين قدراتها على تحليل البيانات بشكل سريع وفعال.

سادسًا: نقص الوعي العام: يُعد نقص الوعي العام حول الجرائم الإلكترونية وتداعياتها من التحديات التقنية الكبيرة. فالكثير من الأفراد والشركات لا يمتلكون المعرفة الكافية بخصوص كيفية حماية أنفسهم من المخاطر الرقمية، مما يجعلهم عرضة للاختراق والاحتيال. يتطلب ذلك جهودًا لتوعية المجتمع حول المخاطر والوسائل التي يمكن استخدامها لحماية البيانات الشخصية. إن تعزيز الوعي العام حول الأمن السيبراني يمكن أن يسهم بشكل كبير في الحد من الجرائم الإلكترونية وتعزيز الحماية للأفراد والمؤسسات.

تُظهر التحديات التقنية في تتبع الجرائم الإلكترونية ومكافحتها أن السلطات الأمنية تحتاج إلى استراتيجيات مبتكرة ومتعددة الأبعاد لمواجهة هذه الظاهرة المتطورة. إن مواجهة هذه التحديات يتطلب تعاونًا دوليًا وتبادل المعرفة والخبرات، فضلا عن استثمار مستدام في التكنولوجيا والتدريب. كما يجب تعزيز الوعي العام حول المخاطر الرقمية وتعزيز ثقافة الأمن السيبراني لحماية الأفراد والمجتمعات. في النهاية، فإن جهود مكافحة الجرائم الإلكترونية يجب أن تكون شاملة ومرنة لتكون قادرة على مواجهة التحديات المستمرة والمتطورة في هذا المجال.[22]

المبحث الثالث:

الآليات القانونية والتشريعية لمكافحة الجرائم الإلكترونية

في ظل تزايد الجرائم الإلكترونية وتعقيداتها، أصبح من الضروري تطوير آليات قانونية وتشريعية فعالة لمكافحتها. يهدف هذا المبحث إلى استعراض أبرز الآليات التي تبنتها الأنظمة القانونية والتشريعية في مواجهة الجرائم الإلكترونية، مع التركيز على التشريعات المحلية والدولية والإجراءات التي تم تبنيها لتعزيز مكافحة هذه الجرائم. سيتم تناول التحديات التي تواكب هذه الآليات، فضلا عن تقييم مدى فعاليتها في التصدي للجرائم الإلكترونية وتقديم حلول مستدامة.

المطلب الأول: تحليل القوانين الوطنية لمكافحة الجرائم الإلكترونية في بعض الدول

تعد الجرائم الإلكترونية من التحديات الكبرى التي تواجه الأنظمة القانونية في مختلف أنحاء العالم. مع تزايد الاعتماد على التكنولوجيا والإنترنت، تحتاج الدول إلى تطوير آليات قانونية فعّالة لمكافحة هذه

الأنشطة الإجرامية. في هذا السياق، يهدف هذا المطلب إلى تحليل القوانين الوطنية لمكافحة الجرائم الإلكترونية في عدد من الدول، مع التركيز على كيفية تناول هذه القوانين للجرائم الإلكترونية، ومدى فعاليتها، والآليات المعتمدة في تنفيذها.[23]

1. القوانين في الولايات المتحدة الأمريكية:

تعد الولايات المتحدة من الدول الرائدة في مجال تطوير التشريعات لمكافحة الجرائم الإلكترونية. فقد أُقرت العديد من القوانين الفيدرالية التي تعالج مختلف أنواع الجرائم الإلكترونية، مثل قانون جرائم الحاسوب (Computer Fraud and Abuse Act) الذي صدر عام 1986. يهدف هذا القانون إلى مكافحة الاستخدام غير المصرح به للأنظمة الحاسوبية. كما يتضمن أيضًا أحكامًا تتعلق بالجرائم التي تؤدي إلى خسائر مالية أو سرقة المعلومات، وفضلا عن ذلك، تمثل قوانين مثل قانون حماية المعلومات الشخصية (Gramm-Leach-Bliley Act) أهمية كبيرة، حيث تفرض على المؤسسات المالية ضرورة حماية بيانات العملاء. وفي عام 2016، عدل قانون حماية البيانات الشخصية ليشمل جوانب جديدة تتعلق بالأمن السيبراني، مما يعكس الاستجابة السريعة للتطورات في هذا المجال، وتتمثل إحدى نقاط القوة في النظام الأمريكي في وجود هيئات متعددة تعمل على تنفيذ القوانين، مثل مكتب التحقيقات الفيدرالي (FBI) ووكالة الأمن القومي (NSA). هذه الهيئات تتعاون مع السلطات المحلية والدولية لملاحقة الجرائم الإلكترونية، مما يعزز من فعالية التنفيذ القانوني.[24]

2. القوانين في الاتحاد الأوروبي:

يُعد الاتحاد الأوروبي مثالًا آخر على جهود التنسيق القانوني لمكافحة الجرائم الإلكترونية. في عام 2013، أُقرت توجيهات الاتحاد الأوروبي بشأن مكافحة الجرائم الإلكترونية (Directive on Attacks against Information Systems)، والتي تهدف إلى وضع إطار قانوني شامل لمكافحة الهجمات الإلكترونية عبر الحدود. تتطلب هذه التوجيهات من الدول الأعضاء في الاتحاد تعزيز التعاون القضائي وتبادل المعلومات حول الجرائم الإلكترونية، وتشمل قوانين الاتحاد الأوروبي أيضًا اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في عام 2018. هذه اللائحة تضع متطلبات صارمة

لحماية بيانات الأفراد، مما يزيد من المساءلة القانونية للمؤسسات والشركات. تتضمن اللائحة أيضًا عقوبات مالية كبيرة على المخالفين، مما يعكس أهمية حماية البيانات في إطار الجرائم الإلكترونية، ومع ذلك، فإن التحديات لا تزال قائمة في تنفيذ هذه القوانين، حيث تختلف التشريعات الوطنية من دولة لأخرى، مما يعوق التنسيق الفعال في معالجة الجرائم الإلكترونية.[25]

3. القوانين في الهند:

تتضمن الهند نظامًا قانونيًا فريدًا لمكافحة الجرائم الإلكترونية، حيث تم إصدار قانون تكنولوجيا المعلومات (Information Technology Act) عام 2000 كاستجابة للتحديات المتزايدة المرتبطة بالتكنولوجيا. يُعد هذا القانون الإطار القانوني الرئيسي لمكافحة الجرائم الإلكترونية في الهند، حيث يغطي مجموعة من الأنشطة الإجرامية، بما في ذلك القرصنة والاحتيال الإلكتروني.

في عام 2008، عُدِّل القانون لإدخال أحكام جديدة تتعلق بالأمن السيبراني، بما في ذلك إنشاء وكالات وطنية لتعزيز الأمان السيبراني والاستجابة للحوادث. يتمثل أحد الجوانب الإيجابية لهذا القانون في قدرته على التعامل مع الجرائم المرتبطة بتكنولوجيا المعلومات، مثل سرقة البيانات والاحتيال عبر الإنترنت، ومع ذلك، يواجه القانون الهندي تحديات تتعلق بالتنفيذ، حيث تفتقر العديد من الولايات إلى الموارد اللازمة لتنفيذ القوانين بفعالية. كما أن الوعي العام حول حقوق الأفراد وحماية البيانات ما يزال منخفضًا، مما يزيد من صعوبة مكافحة الجرائم الإلكترونية.[26]

4. القوانين في الدول العربية:

في العالم العربي، تختلف التشريعات المتعلقة بالجرائم الإلكترونية بشكل كبير بين الدول. على سبيل المثال، أصدرت بعض الدول مثل الإمارات العربية المتحدة والمملكة العربية السعودية قوانين شاملة لمكافحة الجرائم الإلكترونية. في الإمارات، يُعد قانون مكافحة الجرائم الإلكترونية (Federal Decree Law No. 5 of 2012) من القوانين الرائدة، حيث يتناول جميع أنواع الجرائم الإلكترونية ويحدد العقوبات المناسبة للمخالفين، وكما تهدف هذه القوانين إلى حماية الخصوصية والبيانات الشخصية، وتعزيز التعاون بين المؤسسات

الحكومية لمكافحة الجرائم الإلكترونية. ومع ذلك، يواجه تنفيذ هذه القوانين تحديات تتعلق بالموارد، والوعي العام، وضرورة تطوير آليات رصد الجرائم الإلكترونية وتحليلها بشكل فعّال، وفي المقابل، ما تزال بعض الدول العربية تفتقر إلى تشريعات محددة لمكافحة الجرائم الإلكترونية، مما يعيق قدرتها على مواجهة هذه التحديات. وفي هذه الحالة، يعتمد الوضع القانوني على القوانين التقليدية التي قد لا تتناسب مع طبيعة الجرائم الإلكترونية.

تعكس قوانين مكافحة الجرائم الإلكترونية في الدول المختلفة مجموعة من الاستجابات المتنوعة لهذه الظاهرة العالمية. في حين نجحت بعض الدول في تطوير تشريعات فعّالة تعزز من الأمن السيبراني وتسمح بملاحقة الجناة، لا تزال دول أخرى تواجه تحديات كبيرة تتعلق بنقص التشريعات والتنسيق القانوني. من الضروري أن تتعاون الدول فيما بينها لتبادل الخبرات وتطوير أطر قانونية موحدة لمكافحة الجرائم الإلكترونية، مما يسهم في تعزيز الأمن والعدالة في العالم الرقمي.[27]

المطلب الثاني: استعراض جهود التعاون الدولي في مجال الأمن السيبراني.

تعد الجرائم الإلكترونية تحديًا عالميًا يتطلب استجابة منسقة من جميع الدول، حيث لا تعترف الحدود الجغرافية بالهجمات السيبرانية. في ظل تزايد التهديدات السيبرانية التي تواجه الأفراد والمؤسسات والدول، أصبحت الحاجة إلى التعاون الدولي في مجال الأمن السيبراني أكثر أهمية من أي وقت مضى. يهدف هذا المطلب إلى استعراض الجهود المبذولة على الصعيد الدولي لتعزيز التعاون في مجال الأمن السيبراني، مع التركيز على الاتفاقيات الدولية، والمنظمات المعنية، ومبادرات التعاون الإقليمي والدولي.[28]

1. الاتفاقيات الدولية:

أ. اتفاقية بودابست: تعد اتفاقية بودابست (Budapest Convention on Cybercrime) واحدة من أبرز الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية. تبناها مجلس أوروبا في عام 2001، وتهدف إلى تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية من خلال توحيد القوانين والإجراءات بين الدول الأعضاء. تتضمن الاتفاقية أحكامًا تتعلق بتبادل المعلومات بين الدول،

وتحديد إجراءات التحقيق والملاحقة القضائية، وتسعى الاتفاقية إلى تقديم إطار قانوني موحد يساعد الدول في التعامل مع الجرائم السيبرانية بشكل فعّال، مما يعزز من القدرة على محاكمة الجناة عبر الحدود. وقد حظيت الاتفاقية بتأييد واسع، حيث انضمت إليها العديد من الدول من خارج أوروبا، مما يعكس أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية.

ب. مبادرات الأمم المتحدة: تعمل الأمم المتحدة أيضًا على تعزيز التعاون الدولي في مجال الأمن السيبراني من خلال عدد من المبادرات. في عام 2013، أُنشئت مجموعة العمل الحكومية الدولية للأمن السيبراني، التي تهدف إلى تعزيز الحوار بين الدول بشأن القضايا المتعلقة بالأمن السيبراني وتطوير استراتيجيات مشتركة لمواجهتها، وكما يتم تنظيم مؤتمرات وندوات دولية تحت إشراف الأمم المتحدة لتعزيز الوعي بمخاطر الأمن السيبراني وتبادل الخبرات بين الدول. تُعَدُّ هذه المبادرات جزءًا من الجهود العالمية الرامية إلى بناء إطار عمل شامل يعزز من استجابة الدول تجاه التهديدات السيبرانية.[29]

2. المنظمات الدولية:

أ. منظمة التعاون والتنمية الاقتصادية (OECD): تلعب منظمة التعاون والتنمية الاقتصادية دورًا بارزًا في تعزيز التعاون الدولي في مجال الأمن السيبراني. قامت المنظمة بإصدار مجموعة من التوصيات التي تهدف إلى تحسين الأمان السيبراني على المستوى الدولي، وتشمل هذه التوصيات تعزيز الشراكات بين القطاعين العام والخاص، وتطوير استراتيجيات وطنية للأمن السيبراني، وتحسين تبادل المعلومات بين الدول، وتسعى منظمة التعاون والتنمية الاقتصادية إلى توفير منصة للدول لتبادل المعرفة والخبرات، مما يسهم في تطوير استراتيجيات فعالة لمواجهة التهديدات السيبرانية.[30]

ب. الاتحاد الدولي للاتصالات (ITU): يعمل الاتحاد الدولي للاتصالات، وهو وكالة تابعة للأمم المتحدة، على تعزيز الأمن السيبراني من خلال تطوير معايير وتقنيات جديدة. يقوم الاتحاد بتقديم الدعم للدول النامية لتعزيز قدراتها في مجال الأمن السيبراني، من خلال ورش العمل والدورات التدريبية، وكما ينظم الاتحاد مؤتمرات

دولية لمناقشة التحديات الأمنية السيبرانية وتبادل المعلومات حول أحدث التطورات في هذا المجال. يُعَدُّ دور الاتحاد في تعزيز الأمن السيبراني عالميًا عنصرًا أساسيًا في التعاون الدولي لمكافحة الجرائم الإلكترونية.[31]

3. التعاون الإقليمي والدولي:

أ. الجهود الإقليمية:

تعمل العديد من الدول على تعزيز التعاون الإقليمي في مجال الأمن السيبراني. على سبيل المثال، أنشأ مجلس التعاون الخليجي (GCC) برنامجًا للأمن السيبراني يعزز من التنسيق بين الدول الأعضاء في مواجهة التهديدات السيبرانية. يتضمن البرنامج تبادل المعلومات والخبرات، وتطوير استراتيجيات مشتركة لمواجهة الهجمات الإلكترونية، وكما يتم تنظيم تدريبات وورش عمل في دول المجلس لتعزيز الوعي بالتهديدات السيبرانية وتطوير القدرات الوطنية في مجال الأمن السيبراني. تُعَدُّ هذه الجهود جزءًا من استراتيجية شاملة تهدف إلى حماية البنية التحتية الحيوية في المنطقة.[32]

ب. التعاون بين الدول: يُعد التعاون بين الدول عنصرًا أساسيًا في مواجهة التهديدات السيبرانية. تشارك الدول في مجموعة من المبادرات الثنائية والمتعددة الأطراف لتعزيز الأمن السيبراني. على سبيل المثال، أبرمت الولايات المتحدة اتفاقيات مع عدة دول لتبادل المعلومات حول التهديدات السيبرانية والتعاون في مجال التحقيقات، وتُعَدُّ هذه الشراكات ضرورية لتعزيز القدرة على الاستجابة السريعة للتهديدات السيبرانية، حيث تتيح تبادل المعلومات الحيوية وتعزيز التنسيق بين السلطات المختلفة.

4. التحديات والفرص:[33]

أ. التحديات: على الرغم من الجهود الكبيرة المبذولة لتعزيز التعاون الدولي في مجال الأمن السيبراني، إلا أن هناك العديد من التحديات التي تعيق هذه الجهود. من أبرز هذه التحديات الاختلافات في القوانين والتشريعات بين الدول، مما يؤثر على القدرة على تبادل المعلومات وملاحقة الجرائم عبر الحدود. كما أن عدم الوعي الكافي بالتهديدات السيبرانية في بعض الدول قد يعيق تنفيذ استراتيجيات فعالة لمواجهة هذه التحديات.

ب. الفرص: مع ذلك، توفر التهديدات السيبرانية أيضًا فرصًا لتعزيز التعاون الدولي. يُمكن أن تؤدي الحوارات المستمرة بين الدول إلى تطوير استراتيجيات مشتركة لمواجهة التهديدات. كما أن ازدياد الوعي العالمي حول أهمية الأمن السيبراني يعزز من أهمية التعاون الدولي.

تعد جهود التعاون الدولي في مجال الأمن السيبراني خطوة أساسية لمواجهة التهديدات المتزايدة التي تواجه الأفراد والدول. من خلال الاتفاقيات الدولية، والمنظمات المعنية، والتعاون الإقليمي والدولي، يمكن تحقيق نتائج إيجابية في تعزيز الأمن السيبراني. ومع ذلك، من الضروري مواجهة التحديات القائمة وتعزيز الوعي بأهمية الأمن السيبراني لضمان نجاح هذه الجهود. من خلال التعاون الفعّال، يمكن للدول أن تضع أسسًا قوية لمواجهة الجرائم الإلكترونية وتعزيز الأمن في العالم الرقمي.

المطلب الثالث: دور المؤسسات القانونية والشرطية في مكافحة الجرائم الإلكترونية

تتزايد الجرائم الإلكترونية بشكل مطرد في عصر التكنولوجيا الحديثة، مما يتطلب استجابة فعّالة من المؤسسات القانونية والشرطية في جميع أنحاء العالم. تعد هذه المؤسسات خط الدفاع الأول في مواجهة التهديدات السيبرانية وحماية الأفراد والمجتمعات من الأضرار المحتملة. يهدف هذا المطلب إلى استعراض دور المؤسسات القانونية والشرطية في مكافحة الجرائم الإلكترونية، بدءًا من التحقيقات والملاحقات القضائية وصولًا إلى التوعية والتعاون الدولي.(34)

1. دور المؤسسات القانونية: تعد المؤسسات القانونية المسؤولة عن وضع إطار قانوني متين لمكافحة الجرائم الإلكترونية. يتطلب ذلك تحديث القوانين القائمة لتشمل الجرائم الجديدة الناشئة عن التقدم التكنولوجي. على سبيل المثال، تتطلب الجرائم مثل الاحتيال الإلكتروني والقرصنة الإلكترونية تشريعات محددة تتناول طبيعة هذه الأنشطة الإجرامية.

تعمل المؤسسات القانونية أيضًا على تعزيز التعاون بين الدول لتطوير معايير قانونية دولية موحدة، مما يسهل ملاحقة الجرائم الإلكترونية عبر الحدود. يتطلب ذلك استجابة منسقة لضمان أن تكون القوانين

فعالة وملائمة للتحديات الحديثة، وبعد وقوع جريمة إلكترونية، تؤدي المؤسسات القانونية دورًا حاسمًا في تحقيق العدالة. يتضمن ذلك جمع الأدلة، وتحليل البيانات، والتنسيق مع السلطات المحلية والدولية. يجب أن تكون الإجراءات القانونية دقيقة لضمان عدم انتهاك حقوق المتهمين أو الضحايا، وتتطلب قضايا الجرائم الإلكترونية أيضًا تعاونًا مع خبراء في تكنولوجيا المعلومات لمساعدتهم في فهم الأساليب المستخدمة في الجرائم. يسهم ذلك في تحقيق نتائج أكثر دقة وفعالية في المحاكم.

2. دور المؤسسات الشرطية: تتولى المؤسسات الشرطية مسؤولية التحقيق في الجرائم الإلكترونية وتقديم الجناة إلى العدالة. تُشكل وحدات خاصة لمكافحة الجرائم الإلكترونية، تكون مدربة على التعامل مع التهديدات السيبرانية وتحليل الأدلة الرقمية، وتستخدم هذه الوحدات تقنيات متقدمة لرصد وتحليل الأنشطة المشبوهة، مثل تتبع السجلات الرقمية، وتحليل البيانات الضخمة، واستخدام تقنيات التعلم الآلي. يعزز ذلك من قدرتها على الكشف عن الجرائم قبل أن تتفاقم، وتواجه الجرائم الإلكترونية تحديات خاصة تتعلق بالحدود، مما يتطلب تعاونًا دوليًا قويًا. تشارك المؤسسات الشرطية في العديد من المنظمات الدولية مثل الشرطة الجنائية الدولية (الإنتربول) ومكتب الأمم المتحدة لمكافحة المخدرات والجريمة.[35]

تسهم هذه الشراكات في تبادل المعلومات والخبرات حول الجرائم الإلكترونية وتنسيق الجهود لمواجهة الجريمة عبر الحدود. تعد العمليات المشتركة التي تُنظمها المؤسسات الشرطية الدولية جزءًا أساسيًا من استراتيجيات مكافحة الجرائم الإلكترونية.

3. التوعية والتدريب: تؤدي المؤسسات القانونية والشرطية دورًا مهمًا في توعية الجمهور بمخاطر الجرائم الإلكترونية وكيفية حماية أنفسهم. يتم تنظيم حملات توعية وورش عمل لتعليم الأفراد والشركات كيفية التعامل مع التهديدات السيبرانية.

تسهم هذه الجهود في تعزيز الوعي بمفاهيم الأمن السيبراني وتوعية الناس حول كيفية تجنب الاحتيال الإلكتروني والحماية من هجمات الفيروسات. من المهم أن تكون المعلومات المقدمة سهلة الفهم وقابلة للتطبيق في الحياة اليومية، وتتطلب مكافحة الجرائم الإلكترونية

موظفين مؤهلين ومدربين بشكل جيد. تقدم المؤسسات القانونية والشرطية برامج تدريبية لموظفيها لمساعدتهم على فهم التهديدات الجديدة والتقنيات المستخدمة في الجرائم الإلكترونية، ويتضمن ذلك التدريب على كيفية استخدام الأدوات والتقنيات الحديثة في التحقيقات، وكذلك كيفية التعامل مع الأدلة الرقمية بشكل فعال. يسهم ذلك في بناء قدرات المؤسسات الشرطية والقضائية لمواجهة التحديات المتزايدة.[36]

4. استخدام التكنولوجيا الحديثة: تتطلب مكافحة الجرائم الإلكترونية استخدام أحدث التقنيات والأدوات. تعتمد المؤسسات الشرطية والقانونية على برمجيات متقدمة لتحليل البيانات ومراقبة الأنشطة المشبوهة، وتتضمن هذه التقنيات أنظمة الكشف عن التسلل (Intrusion Detection Systems) وأنظمة تحليل البيانات الكبيرة (Big Data Analytics)، والتي تساعد في تحديد الأنماط المشبوهة والتنبؤ بالتهديدات قبل حدوثها، وتسعى المؤسسات أيضًا إلى تطوير حلول رقمية لمواجهة الجرائم الإلكترونية، مثل إنشاء منصات لتقديم الشكاوى إلكترونيًا، مما يسهل على الضحايا تقديم البلاغات. تسهم هذه الحلول في تحسين فعالية الاستجابة للجرائم الإلكترونية.

تؤدي المؤسسات القانونية والشرطية دورًا حيويًا في مكافحة الجرائم الإلكترونية. من خلال تطوير التشريعات، وتنفيذ التحقيقات، والتوعية العامة، واستخدام التكنولوجيا الحديثة، يمكن لهذه المؤسسات تعزيز الأمان السيبراني وحماية المجتمع من التهديدات المتزايدة. ومع استمرار تطور التكنولوجيا، يجب على هذه المؤسسات التكيف مع التغيرات وتطوير استراتيجيات جديدة لمواجهة الجرائم الإلكترونية بفعالية. من خلال التعاون والتنسيق بين مختلف الجهات، يمكن تحقيق نتائج إيجابية في مجال مكافحة الجرائم الإلكترونية وضمان أمن المعلومات والبيانات في العالم الرقمي.[37]

المبحث الرابع:

آليات وقائية وتوصيات مستقبلية

يعد الوقاية من الجرائم الإلكترونية جزءًا أساسيًا من استراتيجية مكافحة هذه الجرائم، حيث يتطلب الأمر تبني سياسات فعالة لمواجهة الجريمة قبل وقوعها. في هذا المبحث، سيتم استعراض الآليات

الوقائية التي يمكن أن تساهم في تقليل فرص حدوث الجرائم الإلكترونية، مع تقديم توصيات مستقبلية لتحسين فعالية هذه الآليات. علاوة على ذلك، سنسلط الضوء على الدور المهم للتوعية المجتمعية والتطورات التكنولوجية في تعزيز الوقاية من الجرائم الإلكترونية. كما سيتم اقتراح مجموعة من الإجراءات المستقبلية التي يمكن أن تساهم في بناء بيئة آمنة ومستدامة في العالم الرقمي.

المطلب الأول: دور التوعية القانونية والتثقيف السيبراني

في عصر التكنولوجيا الحديثة، أصبحت الجرائم الإلكترونية تهديدًا متزايدًا يواجه الأفراد والشركات والدول. ولذلك، يُعد التوعية القانونية والتثقيف السيبراني من الأدوات الأساسية لمكافحة هذه الجرائم وحماية المستخدمين من التهديدات السيبرانية. يهدف هذا المطلب إلى استعراض دور التوعية القانونية والتثقيف السيبراني، وتقديم توصيات لتعزيز هذه الجهود في المستقبل.[38]

1. أهمية التوعية القانونية: تؤدي التوعية القانونية دورًا حيويًا في رفع وعي الأفراد بحقوقهم القانونية المتعلقة بالأمن السيبراني. من خلال تعليم الناس حول القوانين والتشريعات المتعلقة بالجرائم الإلكترونية، يصبحون أكثر قدرة على حماية أنفسهم ومعرفة حقوقهم عند التعرض لأي اعتداء سيبراني، وهذا الوعي يُساعد الأفراد في التعرف على أساليب الاحتيال المختلفة وكيفية التعامل معها. فضلا عن ذلك، يمكن أن يشمل ذلك كيفية تقديم الشكاوى القانونية والتواصل مع السلطات المختصة، والتوعية القانونية تسهم في تعزيز الثقافة القانونية في المجتمع، مما يساعد في خلق بيئة آمنة وأقل عرضة للجرائم الإلكترونية. عندما يكون لدى الناس فهم شامل للقوانين والسياسات المتعلقة بالأمن السيبراني، فإنهم يصبحون أكثر استعدادًا للإبلاغ عن الجرائم والأنشطة المشبوهة، وهذا الأمر يُعد جزءًا من بناء مجتمع يتمتع بوعي قانوني، حيث يتعاون الأفراد مع السلطات للتصدي للجرائم الإلكترونية.[39]

2. التثقيف السيبراني: يتضمن التثقيف السيبراني تعليم الأفراد المهارات الأساسية التي تساعدهم في استخدام التكنولوجيا بشكل آمن. يشمل ذلك كيفية حماية البيانات الشخصية، واستخدام كلمات مرور قوية، والتعرف على رسائل البريد الإلكتروني الاحتيالية، وتُعد هذه

المهارات ضرورية في ظل تزايد التهديدات السيبرانية. من خلال توفير ورش عمل ودورات تدريبية، يمكن للمنظمات تعزيز فهم الأفراد لكيفية حماية أنفسهم في الفضاء الرقمي، ويجب أن يكون التثقيف السيبراني جزءًا من المناهج الدراسية في المدارس. يجب تعليم الأطفال والشباب كيفية التعامل مع الإنترنت بأمان وفهم المخاطر المحتملة. يشمل ذلك توعية الطلاب بخصوص استخدام وسائل التواصل الاجتماعي بشكل آمن، وكيفية التعرف على المحتوى الضار، وعند تزويد الشباب بالمعرفة اللازمة، يمكن تقليل المخاطر المرتبطة بالجرائم الإلكترونية، مما يساهم في بناء جيل واعٍ قادر على التعامل مع التحديات السيبرانية.(40)

3. آليات تنفيذ التوعية والتثقيف: يمكن تنفيذ حملات توعية قانونية وسيبرانية على نطاق واسع من خلال وسائل الإعلام التقليدية والرقمية. تشمل هذه الحملات تنظيم ورش عمل، ندوات، ومحاضرات، فضلا عن إنشاء مواد تعليمية مثل الكتيبات والفيديوهات التثقيفية، وتستهدف هذه الحملات فئات مختلفة من المجتمع، بما في ذلك الأفراد، الأسر، والشركات. من خلال تقديم معلومات واضحة ومفيدة، يمكن تعزيز الوعي بالجرائم الإلكترونية، ويجب أن تتعاون المؤسسات القانونية والشرطية مع المؤسسات التعليمية لتعزيز التوعية القانونية والتثقيف السيبراني. يمكن أن تتضمن هذه الشراكات تطوير برامج تعليمية تتناول الأمان السيبراني وكيفية التعامل مع الجرائم الإلكترونية، ويمكن أن يسهم التعاون بين المدارس والجهات القانونية في تحسين فهم الطلبة للتهديدات السيبرانية، ويجب أن تشمل الأنشطة الزيارات الميدانية، والمحاضرات من قبل خبراء في المجال.(41)

4. التحديات المرتبطة بالتوعية والتثقيف: تُعد نقص الموارد المالية والبشرية أحد التحديات الكبيرة التي تواجه جهود التوعية القانونية والتثقيف السيبراني. قد تحتاج المنظمات إلى استثمارات كبيرة لتنفيذ برامج التوعية والتثقيف بشكل فعّال، وتتغير التكنولوجيا بسرعة، مما يتطلب تحديثًا مستمرًا للمعلومات والمواد التعليمية. يجب أن تكون البرامج متناسبة مع أحدث الاتجاهات والتحديات في مجال الأمن السيبراني.

5. توصيات مستقبلية: يجب على الحكومات والمنظمات تطوير استراتيجيات طويلة الأجل للتوعية القانونية والتثقيف السيبراني، تتضمن أهدافًا محددة ومؤشرات قياس الأداء، ويجب تشجيع استخدام التكنولوجيا في برامج التوعية والتثقيف، مثل تطبيقات الهواتف الذكية، المنصات الإلكترونية، والألعاب التعليمية التي تعزز الفهم حول الأمن السيبراني.

تُعد التوعية القانونية والتثقيف السيبراني أدوات أساسية في مكافحة الجرائم الإلكترونية. من خلال رفع الوعي وتعليم المهارات الأساسية، يمكن للأفراد حماية أنفسهم والمجتمع من التهديدات المتزايدة. يجب على المؤسسات القانونية والشرطية اتخاذ خطوات فعّالة لتعزيز هذه الجهود، من خلال التعاون مع جميع فئات المجتمع. يتطلب ذلك استجابة شاملة ومنسقة لضمان أن يكون الجميع مستعدًا لمواجهة التحديات السيبرانية في المستقبل.[42]

المطلب الثاني: تعزيز التعاون بين المؤسسات الحكومية والقطاع الخاص

تتزايد التهديدات السيبرانية في العصر الرقمي بشكل كبير، مما يتطلب استجابة فعّالة من جميع القطاعات. يُعد التعاون بين المؤسسات الحكومية والقطاع الخاص من العوامل الأساسية في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني. يتطلب هذا التعاون تنسيقًا فعالًا وتبادل المعلومات والخبرات بين الجانبين. يهدف هذا المطلب إلى استعراض أهمية هذا التعاون، والتحديات التي تواجهه، وطرق تعزيز هذا التعاون لمواجهة التحديات السيبرانية.[43]

1. أهمية التعاون بين المؤسسات الحكومية والقطاع الخاص: يمتلك القطاع الحكومي العديد من الموارد القانونية والهيكلية، في حين يمتلك القطاع الخاص الابتكار والتكنولوجيا المتقدمة. يُعزز التعاون بين الجانبين استخدام هذه الموارد بشكل أكثر فعالية. على سبيل المثال، يمكن للقطاع الخاص توفير حلول تكنولوجية متطورة تساعد الحكومة في تطوير استراتيجيات لمواجهة الجرائم الإلكترونية، وتتطلب الجرائم الإلكترونية استجابة سريعة للحد من الأضرار. يمكن أن يساهم التعاون بين المؤسسات الحكومية والقطاع الخاص في تعزيز سرعة وفعالية الاستجابة للتهديدات. عندما تتشارك الجهتان

المعلومات والموارد، يمكن تحقيق تنسيق أفضل في حالة حدوث هجمات سيبرانية.

2. تحديات التعاون: يمكن أن تختلف الأهداف والرؤى بين القطاعين العام والخاص. في حين تركز الحكومة على حماية الأمن القومي، قد تركز الشركات على حماية بيانات عملائها وزيادة الأرباح. هذا الاختلاف في الأولويات يمكن أن يعيق التعاون الفعّال. تواجه الشركات الخاصة تحديات تتعلق بالخصوصية والأمان عند مشاركة البيانات مع الحكومة. قد تكون هناك مخاوف من استغلال المعلومات أو انتهاك حقوق الأفراد، مما يؤثر سلبًا على ثقة الشركات في التعاون.

3. آليات تعزيز التعاون: يمكن أن تُسهم مذكرات التفاهم بين المؤسسات الحكومية والقطاع الخاص في تحديد الأهداف المشتركة وتعزيز الشراكة. يجب أن تتضمن هذه المذكرات بنودًا واضحة تتعلق بتبادل المعلومات، وتعزيز التعاون في مجال الأمن السيبراني، وتطوير منصات تبادل المعلومات يعد من الوسائل الفعالة لتعزيز التعاون. يمكن أن تشمل هذه المنصات قاعدة بيانات مشتركة تحتوي على معلومات حول التهديدات السيبرانية وأساليب الحماية المبتكرة.

تساعد هذه المنصات في تبادل المعرفة والخبرات بين القطاعين، مما يعزز الاستجابة للتهديدات السيبرانية.

4. تعزيز التدريب والتطوير المهني: يمكن تنظيم ورش عمل مشتركة بين المؤسسات الحكومية والقطاع الخاص لتدريب الموظفين على التعامل مع التهديدات السيبرانية. تُساعد هذه الورش على تبادل المعرفة وتعزيز مهارات الأفراد في القطاعين، ويمكن أن تُسهم برامج تبادل الموظفين بين القطاعين في تعزيز الفهم المتبادل والتعاون. يعمل موظفو الحكومة في الشركات الخاصة والعكس، مما يسهل تبادل الخبرات والتقنيات الجديدة.

5. التشجيع على الابتكار: يجب على الحكومة تشجيع الشركات على الابتكار من خلال تقديم حوافز، مثل تخفيضات ضريبية أو منح. يمكن أن تساهم هذه الحوافز في دفع الشركات لتطوير تقنيات جديدة لمكافحة الجرائم الإلكترونية، ويمكن تعزيز التعاون من خلال تشجيع البحث والتطوير المشترك بين الحكومة والشركات. يمكن أن تُؤدي المشاريع

المشتركة إلى تطوير تقنيات جديدة وتحسين استراتيجيات الأمن السيبراني.

6. تعزيز الثقة بين الجانبين: يجب أن تتسم العلاقة بين المؤسسات الحكومية والقطاع الخاص بالشفافية. من خلال مشاركة المعلومات بوضوح، يمكن تعزيز الثقة بين الجانبين، مما يسهل التعاون الفعّال، ويجب أن تحد المسؤوليات بوضوح لكل طرف في التعاون. يساعد ذلك في تجنب أي لبس أو سوء فهم، مما يسهم في تعزيز العلاقة بين المؤسسات.

يُعد تعزيز التعاون بين المؤسسات الحكومية والقطاع الخاص خطوة حيوية لمكافحة الجرائم الإلكترونية. من خلال تكامل الموارد والخبرات، يمكن تحقيق استجابة أكثر فعالية للتهديدات السيبرانية. وعلى الرغم من التحديات، فإن وجود آليات واضحة لتعزيز التعاون، مثل توقيع مذكرات التفاهم وتطوير منصات تبادل المعلومات، يمكن أن يؤدي إلى نتائج إيجابية. يتطلب الأمر أيضًا التزامًا من كلا الجانبين بتعزيز الثقة والتفاهم المتبادل، مما يساهم في بناء بيئة آمنة وحماية المجتمع من التهديدات السيبرانية المتزايدة.(44)

المطلب الثالث: توصيات لتحسين التشريعات والإجراءات القانونية

تعد التشريعات والإجراءات القانونية من العناصر الأساسية في مكافحة الجرائم الإلكترونية. ومع تطور هذه الجرائم بشكل متسارع، أصبح من الضروري مراجعة وتحديث الأطر القانونية المعمول بها لضمان فعاليتها. يهدف هذا المطلب إلى تقديم توصيات لتحسين التشريعات والإجراءات القانونية المتعلقة بالجرائم الإلكترونية، بما يعزز من قدرة الدول على التصدي لهذه الظاهرة.(45)

1. تحديث التشريعات الحالية: تحتاج التشريعات القانونية إلى تحديث دوري يتماشى مع التطورات السريعة في التكنولوجيا. يجب على المشرعين العمل على مراجعة القوانين القائمة لضمان أنها تعالج جميع أنواع الجرائم الإلكترونية المستحدثة، مثل الهجمات السيبرانية والاحتيال الرقمي، ومن المهم إدراج تعريفات دقيقة لمختلف أنواع الجرائم الإلكترونية ضمن النصوص القانونية، مما يسهل تطبيقها بشكل فعال. يجب أن تتضمن هذه التعريفات جميع الأنشطة التي تعد جرائم إلكترونية، مما يقلل من التفسير الضيق للنصوص القانونية.

2. تعزيز التعاون الدولي: ينبغي على الدول الانضمام إلى الاتفاقيات الدولية التي تتناول الجرائم الإلكترونية، مثل اتفاقية بودابست، لتعزيز التعاون عبر الحدود. تسهم هذه الاتفاقيات في توحيد المعايير القانونية وتسهيل تبادل المعلومات بين الدول. من المهم إنشاء آليات تعاون واضحة وفعّالة مع الدول الأخرى لمكافحة الجرائم الإلكترونية. يمكن أن تشمل هذه الآليات تبادل المعلومات، وتنظيم ورش عمل مشتركة، وتبادل الخبرات بين الجهات القضائية.

3. تحسين الإجراءات القانونية: يجب العمل على تبسيط الإجراءات القانونية المتعلقة بمكافحة الجرائم الإلكترونية. ينبغي أن تكون هناك إجراءات محددة وسريعة للتعامل مع هذه الجرائم، مما يسهل على الضحايا تقديم الشكاوى والجهات القانونية اتخاذ الإجراءات اللازمة، ويجب أن يكون هناك برامج تدريب مستمرة للقضاة والمحامين حول القضايا المتعلقة بالجرائم الإلكترونية. يُسهم ذلك في تحسين فهمهم للتقنيات المستخدمة في هذه الجرائم ويساعدهم في تطبيق القوانين بشكل صحيح.

4. زيادة العقوبات: ينبغي مراجعة نظام العقوبات المفروض على الجرائم الإلكترونية. يجب أن تكون العقوبات رادعة بما يكفي لتقليل الجرائم السيبرانية. قد يتطلب ذلك زيادة العقوبات المالية والسجن للأشخاص الذين يرتكبون هذه الجرائم، ويمكن التفكير في استحداث عقوبات جديدة تناسب طبيعة الجرائم الإلكترونية، مثل فرض عقوبات إضافية على الأفعال التي تؤدي إلى سرقة البيانات أو التلاعب بها.

5. تعزيز الأمن السيبراني في المؤسسات الحكومية: يجب على الحكومات تطوير سياسات أمنية صارمة لحماية البيانات والمعلومات الحساسة. يتطلب ذلك إنشاء هيئات مختصة بالأمن السيبراني داخل المؤسسات الحكومية لضمان تطبيق هذه السياسات بشكل فعّال، ويجب أن يتم تدريب الموظفين في المؤسسات الحكومية على أهمية الأمن السيبراني وكيفية التعامل مع التهديدات المحتملة. يُساعد ذلك في تقليل المخاطر المرتبطة بالجرائم الإلكترونية.

6. نشر الوعي العام: من الضروري تنظيم حملات توعية شاملة حول الجرائم الإلكترونية وتأثيراتها، مع التركيز على توعية الجمهور بحقوقهم وكيفية حماية أنفسهم. ينبغي أن تكون هذه الحملات مدعومة

من قبل الحكومة وتستهدف جميع فئات المجتمع، ويمكن أن تُسهم تطوير مواد تعليمية، مثل الكتيبات والبرامج التلفزيونية والرقمية، في تعزيز الوعي حول كيفية حماية المعلومات الشخصية وسبل التعامل مع الجرائم الإلكترونية.

7. تشجيع الابتكار في التقنيات القانونية: يجب استخدام التكنولوجيا لتعزيز الكفاءة في الإجراءات القانونية. يمكن تطوير أنظمة إلكترونية لتقديم الشكاوى وتتبع القضايا المتعلقة بالجرائم الإلكترونية بشكل أسهل وأسرع، ويمكن تشجيع الابتكار من خلال تطوير تطبيقات مبتكرة تُساعد الأفراد على الإبلاغ عن الجرائم الإلكترونية بشكل مباشر وسريع، مما يعزز من قدرة السلطات على الرد الفوري.

تُعد تحسين التشريعات والإجراءات القانونية في مجال مكافحة الجرائم الإلكترونية خطوة ضرورية لمواجهة التحديات المتزايدة في هذا المجال. من خلال تحديث القوانين، وتعزيز التعاون الدولي، وتبسيط الإجراءات القانونية، وزيادة الوعي العام، يمكن للدول تعزيز قدرتها على التصدي للجرائم الإلكترونية. يجب أن يتم العمل بشكل شامل ومنسق بين جميع الجهات المعنية لضمان فعالية هذه الجهود وتحقيق نتائج ملموسة.[46]

الخاتمة:

في ختام هذا البحث، توصلنا إلى عدد من الاستنتاجات والتوصيات التي تسلط الضوء على التحديات التي تواجه مكافحة الجرائم الإلكترونية وآليات التصدي لها. لقد أظهرت الدراسة أن الجرائم الإلكترونية تمثل تهديدًا متزايدًا يتطلب استجابة قانونية فورية وفعالة، وأن الأطر القانونية الحالية غير كافية لمواكبة التطورات التكنولوجية المتسارعة. كما تبين أن هناك حاجة ملحة لتحديث التشريعات وتعزيز التعاون الدولي في هذا المجال.

من خلال هذا البحث، أكدنا على أهمية تبني سياسات وقوانين متطورة تتماشى مع التقدم التكنولوجي، وتحسين التعاون بين الدول في إطار مكافحة الجرائم الرقمية. وأوصينا بضرورة تعزيز الأمن السيبراني عبر تطوير آليات وقائية مبتكرة وزيادة الوعي المجتمعي. كما شددنا على ضرورة توفير بيئة قانونية وتشريعية فعالة ومستدامة للحد من

هذه الجرائم، مما يساهم في حماية الأفراد والمجتمعات من تهديدات العصر الرقمي.

الاستنتاجات

1. هناك زيادة ملحوظة في أنواع الجرائم الإلكترونية، مما يستدعي تدخلاً عاجلاً.
2. تعاني العديد من الدول من نقص في التشريعات القانونية المتخصصة لمواجهة الجرائم الإلكترونية.
3. يعوق عدم توافق القوانين الوطنية جهود التعاون الدولي في ملاحقة الجرائم السيبرانية.
4. عدم كفاية التوعية والتثقيف بشأن مخاطر الجرائم الإلكترونية يساهم في تفشيها.
5. تحتاج الأنظمة القانونية إلى الابتكار لتكون قادرة على مواجهة التحديات الجديدة في الفضاء السيبراني.

التوصيات

1. نوصي المشرع العراقي بالعمل على تحديث قوانينه لتكون أكثر توافقًا مع التطورات التكنولوجية الحديثة، بما يعزز قدرة النظام القانوني على مواجهة الجرائم الإلكترونية.
2. نحث السلطة التشريعية على تبني قوانين جديدة تتعامل مع الجرائم الإلكترونية بشكل أكثر فعالية، بما يتناسب مع التحديات التكنولوجية الحالية.
3. ندعو المشرع العراقي إلى إنشاء أُطر قانونية دولية موحدة للتعاون بين العراق والدول الأخرى في مكافحة الجرائم الإلكترونية، بما يسهم في تحسين التنسيق الدولي في هذا المجال.
4. نوصي الحكومة العراقية بتنفيذ حملات توعية شاملة لتثقيف المجتمع حول مخاطر الجرائم الإلكترونية وسبل الحماية منها، وذلك عبر وسائل الإعلام والمؤسسات التعليمية.
5. نحث الجهات المعنية على توفير برامج تدريبية متخصصة للجهات القانونية والأمنية لتمكينها من مواجهة الجرائم الإلكترونية بكفاءة، من خلال التعاون مع مؤسسات دولية متخصصة.

6. نوصي الحكومة العراقية باستثمار الموارد في تطوير تقنيات جديدة للأمن السيبراني، بما يعزز قدرة البلاد على التصدي للتهديدات الرقمية ويحسن مستوى الأمان في النظام الرقمي.

المصادر

1. أحمد جمال زين العابدين، "الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية: دراسة مقارنة"، الطبعة الأولى، مجلة مستقبل العلوم الاجتماعية، الجزائر، 2021.
2. إمام حسنين خليل عطا الله، "جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية"، الطبعة الأولى، المجلة الدولية للبحوث والدراسات، الإمارات، 2022.
3. أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة الاقتصاد والقانون، القاهرة، 2021.
4. بافان دوجال، "جلسة حول قانون الإنترنت والجرائم الإلكترونية والأمن السيبراني"، الاتحاد الدولي للاتصالات، جنيف، 2020.
5. جعفر حسن جاسم الطائي، "جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة"، الطبعة الأولى، دار البداية، 2010.
6. خالد حسن أحمد لطفي، "الإرهاب الإلكتروني: آفة العصر الحديث والآليات القانونية للمواجهة"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2018.
7. رامي متولّي القاضي، "مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية"، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.
8. سليمان أحمد فضل، "المواجهة التشريعية الناشئة عن استخدام معلومات الإنترنت"، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007.
9. عباس أبو شامة عبد المحمود، "عولمة الجريمة الاقتصادية"، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2009.

10. عبد العال الديربي محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية، الطبعة الثانية، دار الثقافة، عمّان، 2020.
11. عبد الفتاح بيومي حجازي، "مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
12. عبد الله القرني، الأمن السيبراني في الوطن العربي: دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، الرياض، 2016.
13. عبد الله عبد الكريم عبد الله، "جرائم المعلوماتية والإنترنت (الجرائم المعلوماتية)"، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.
14. علي الدليمي، قوانين الجرائم الإلكترونية في الدول العربية، مركز الدراسات القانونية، بغداد، 2021.
15. علي جبار الحسيناوي، "جرائم الحاسوب والإنترنت"، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمّان، 2018.
16. عمر بن يونس، "الجرائم الإلكترونية بين التعريف الضيق والواسع"، ضمن مجلة المنارة، 2019.
17. عيسى غسان الربطي، "القواعد الخاصة بالتوقيع الإلكتروني"، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمّان، 2009،
18. فايز شموط، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، الطبعة الأولى، دار عمار، بيروت، 2018.
19. كليات الشرق العربي، "تقنيات الأدلة الجنائية في مكافحة الجرائم السيبرانية"، المؤتمر الدولي الثاني لعلوم الأدلة الجنائية والطب الشرعي، السعودية، 2019.
20. لينده شرا بشة، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى، المجلد 4، العدد 4، الجزائر، 2022.
21. مركز الدراسات الأمنية، "إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية"، الطبعة الأولى، مجلة النبأ، العراق، 2023.

22.نهـلا المـومني، جـرائم الاعتـداء علـى الشـبكة المعلوماتيـة فـي التشـريعات العربية، دار الثقافة، عمّان، 2019.
23.نهـى الحسـن، التحقيـق فـي الجـرائم الإلكترونيـة وإثباتهـا فـي فلسـطين، مجلة جامعة بيرزيت، رام الله، 2018.

Sources:

1. Al-Abidin، A. J. Z. (2021). Judicial jurisdiction and investigation procedures in cyber crimes: A comparative study. Journal of Future Social Sciences، 1. Algeria.

2. Atta Allah، I. H. K. (2022). Crimes of attack on information networks in Arab legislation. International Journal for Research and Studies، 1. UAE.

3. Fikri، A. A. (2021). Cyber crimes: A comparative study in Arab and foreign legislation. Library of Economics and Law.

4. Duggal، P. (2020). Session on internet law، cyber crimes، and cybersecurity. International Telecommunication Union. Geneva.

5. Al-Taie، J. H. J. (2010). Information technology crimes: A new perspective on modern crime. Dar Al-Bidaya.

6. Lotfi، K. H. A. (2018). Cyber terrorism: The modern age plague and legal mechanisms for confrontation. Dar Al-Fikr Al-Jami'i.

7. Al-Qadi، R. M. (2011). Combating cyber crimes in comparative legislation and in light of international agreements and charters. Dar Al-Nahda Al-Arabiya.

8. Fadl، S. A. (2007). Legislative challenges arising from the use of internet information. Dar Al-Nahda Al-Arabiya.

9. Abd Al-Mahmood، A. A. (2009). Globalization of economic crime. Naif Arab Academy for Security Sciences.

10. Al-Dairbi، A. A. M. S. (2020). Cyber crimes: A legal judicial comparative study with the latest Arab legislation (2nd ed.). Dar Al-Thaqafa.

11. Hegazi، A. F. B. (2006). Combating computer and internet crimes in the model Arab law. Dar Al-Fikr Al-Jami'i.

12. Al-Qarni، A. (2016). Cybersecurity in the Arab world: A case study of Saudi Arabia. Arab Center for Research and Studies.

13. Abdullah، A. A. K. (2007). Cyber crimes and the internet. Halabi Legal Publications.

14. Al-Dulaimi، A. (2021). Laws on cyber crimes in Arab countries. Legal Studies Center.

15. Al-Husseini، A. J. (2018). Computer and internet crimes. Al-Yazuri Scientific Publishing and Distribution.

16. Younis، O. B. (2019). Cyber crimes between narrow and broad definitions. Al-Manarah Journal.

17. Al-Rabti، I. G. (2009). Special rules for electronic signatures. Dar Al-Thaqafa for Publishing and Distribution.

18. Shamout، F. (2018). Investigation procedures and evidence collection in cyber crimes. Dar Ammar.

19. Arab East Colleges. (2019). Forensic evidence techniques in combating cyber crimes. In Proceedings of the Second International Conference on Forensic Sciences and Forensic Medicine.

20. Sharabasha، L. (2022). Combating cyber crimes between national legislation and international agreements. Al-Sada Journal، 4(4).

21. Security Studies Center. (2023). Investigation procedures and evidence collection in cyber crimes. Al-Nabaa Journal.

22. Al-Momani، N. (2019). Crimes of attack on information networks in Arab legislation. Dar Al-Thaqafa.

23. Al-Hassan، N. (2018). Investigation and proving of cyber crimes in Palestine. Birzeit University Journal.

الهوامش

(1) عبد الفتاح بيومي حجازي، "مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006, ص88.
(2) عبد الفتاح بيومي حجازي، مصدر سبق ذكره, ص43.
(3) خالد حسن أحمد لطفي، "الإرهاب الإلكتروني: آفة العصر الحديث والآليات القانونية للمواجهة"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2018،ص 41.
(4) سليمان أحمد فضل، "المواجهة التشريعية الناشئة عن استخدام معلومات الإنترنت"، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007، 56.
(5) سليمان أحمد فضل، مصدر سبق ذكره, ص 85.
(6) خالد حسن أحمد لطفي، مصدر سبق ذكره، ص 22.
(7) خالد حسن أحمد لطفي، مصدر سبق ذكره، ص 79.
(8) علي جبار الحسيناوي، "جرائم الحاسوب والإنترنت"، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمّان، 2018،ص 196.
(9) علي جبار الحسيناوي، مصدر سبق ذكره, 2018،ص 98.
(10) جعفر حسن جاسم الطائي، "جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة"، الطبعة الأولى، دار البداية، 2010،ص29.
(11) علي جبار الحسيناوي، مصدر سبق ذكره, 2018،ص 38.
(12) علي جبار الحسيناوي، مصدر سبق ذكره, 2018،ص 27.
(13) عيسى غسان الربطي، "القواعد الخاصة بالتوقيع الإلكتروني"، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمّان، 2009،ص190.
(14) عيسى غسان الربطي، مصدر سبق ذكره ،ص 75.
(15) عمر بن يونس، "الجرائم الإلكترونية بين التعريف الضيق والواسع"، ضمن مجلة المنارة، دار النشر غير متوفرة، مكان الطبع غير متوفر، 2019.
(16) عيسى غسان الربطي، مصدر سبق ذكره ،ص 48.
(17) بافان دوجال، "جلسة حول قانون الإنترنت والجرائم الإلكترونية والأمن السيبراني"، الاتحاد الدولي للاتصالات، جنيف، 2020.
(18) عيسى غسان الربطي، مصدر سبق ذكره ،ص 69.
(19) إمام حسنين خليل عطا الله، "جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية"، الطبعة الأولى، المجلة الدولية للبحوث والدراسات، الإمارات، 2022.
(20) أحمد جمال زين العابدين، "الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية: دراسة مقارنة"، الطبعة الأولى، مجلة مستقبل العلوم الاجتماعية، الجزائر، 2021، الصفحات 65-134.
(21) عيسى غسان الربطي، مصدر سبق ذكره ،ص 19.
(22) علي جبار الحسيناوي، "جرائم الحاسوب والإنترنت"، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمّان، 2018, ص33.
(23) رامي متولّي القاضي، "مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية"، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011, ص78.
(24) خالد حسن أحمد لطفي، مصدر سبق ذكره، ص 42.
(25) مركز الدراسات الأمنية، "إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية"، الطبعة الأولى، مجلة النبأ، العراق، 2023, ص39.

(26) خالد حسن أحمد لطفي، مصدر سبق ذكره، ص 72.
(27) خالد حسن أحمد لطفي، "الإرهاب الإلكتروني: آفة العصر الحديث والآليات القانونية للمواجهة"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2018, ص73.
(28) رامي متولّي القاضي، مصدر سبق ذكره 2011, ص49.
(29) عبد الله القرني، الأمن السيبراني في الوطن العربي: دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، الرياض، 2016، ص 65-75 .
(30) عبد الله عبد الكريم عبد الله، "جرائم المعلوماتية والإنترنت (الجرائم المعلوماتية)"، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007, ص27.
(31) عبد الله القرني، مصدر سبق ذكره، ص 88.
(32) رامي متولّي القاضي، مصدر سبق ذكره 2011, ص74.
(33) كليات الشرق العربي، "تقنيات الأدلة الجنائية في مكافحة الجرائم السيبرانية"، المؤتمر الدولي الثاني لعلوم الأدلة الجنائية والطب الشرعي، السعودية، 2019, ص 27.
(34) رامي متولّي القاضي، مصدر سبق ذكره 2011, ص99.
(35) أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة الاقتصاد والقانون، القاهرة، 2021، ص 45-60 .
(36) رامي متولّي القاضي، مصدر سبق ذكره 2011, ص90.
(37) عباس أبو شامة عبد المحمود، "عولمة الجريمة الاقتصادية"، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2009.
(38) عبد العال الديربي محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية، الطبعة الثانية، دار الثقافة، عمّان، 2020، ص 80-95 .
(39) رامي متولّي القاضي، مصدر سبق ذكره 2011, ص41.
(40) نهلا المومني، جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية، دار الثقافة، عمّان، 2019، ص 23-30 .
(41) عبد الله القرني، مصدر سبق ذكره، ص 33.
(42) نهى الحسن، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين، مجلة جامعة بيرزيت، رام الله، 2018، ص 45-55 .
(43) ليندة شرا بشة، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى، المجلد 4، العدد 4، الجزائر، 2022، ص 241-253 .
(44) فايز شموط، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، الطبعة الأولى، دار عمار، بيروت، 2018، ص 110-120.
(45)45 عبد الله القرني، مصدر سبق ذكره، ص 82.
(46) علي الدليمي، قوانين الجرائم الإلكترونية في الدول العربية، مركز الدراسات القانونية، بغداد، 2021، ص 200-215 .