الآليات الدولية لمكافحة الجريمة الإلكترونية وتحدياتها

د. محمود محمد محمود ياسين

جامعة طنطا- مصر

ملخص البحث:

أصبحت التكنولوجيا في العصر الحالي جزءًا لا ينفصل عن المجتمعات الحديثة، وبناءً عليه اعتُبرت الجرائم الإلكترونية خطرًا شائعًا على المستوى العالمي، وذلك في ظل وجود أكثر من 4.5 مليار شخص متصلين بشبكة الإنترنت، الأمر الذي يجعل نصف سكان العالم معرضين بصورة محتملة لخطر الوقوع ضحية للجرائم الإلكترونية.

إذ تحوّل الفضاء الإعلامي والشبكة العنكبوتية إلى ميدان صراع يعتمد على العقول والتقنيات والفنيات والخبرات في المجال الإلكتروني، ولعل من أكثر الفئات نشاطًا وفاعلية التي تعرفنا عليها من خلال وسائل الإعلام والفضاء الافتراضي هي جماعات الهاكرز أو ما يُعرف بالتجسس التقني.

وقد شهد المجتمع الدولي خلال العقد الأخير موجة انتشار واسعة لتكنولوجيا الحواسيب والشبكات المعلوماتية، التي أحدثت تحولًا جذريًا في مختلف مجالات حياتنا، ويلاحظ أن لكل ظاهرة جانبها الإيجابي وجانبها السلبي، فعلى الرغم من التطور الكبير الذي صاحب ثورة المعلومات، إلا أنها في الوقت ذاته جعلت المجتمع الدولي يواجه أخطار جديدة ارتبطت بهذا التطور المتسارع.

ولا شك أن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسًا يقلق رجال القانون بصفة خاصة، لذلك بات من الضروري أن تتسع دائرة التعاون مع المتخصصين في التقنيات الرقمية، ورجال القانون، والمؤسسات الرسمية في الدولة، وكذلك على المستوى الدولي، من أجل سن قوانين وتشريعات فعالة تكافح مرتكبي تلك الجرائم، كما تتجلى أهمية هذا البحث من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية في منع الجريمة المعلوماتية وردع مرتكبيها، ومدى الحاجة إلى استحداث نصوص قانونية جديدة للحد من هذه الظاهرة.

الكلمات المفتاحية: الجريمة الإلكترونية؛ الآليات الدولية؛ الأمن السيبراني؛ التحديات القانونية؛ التعاون الدولي.

International mechanisms for combating cybercrime and its challenges

Dr. Mahmoud Mohamed Mahmoud Yassin

Abstract:
Technology has become an integral part of modern societies, and as a result, cybercrime is considered a common threat globally, given that more than 4.5 billion people are connected to the internet, which makes half of the world's population potentially at risk of becoming a victim of cybercrime.
The media space and the internet have turned into a battleground that relies on minds, technologies, techniques, and expertise in the electronic field. Perhaps one of the most active and effective groups that we have come to know through the media and virtual space is the hacker groups, or what is known as technical espionage.
During the last decade, the international community has witnessed a widespread wave of computer and information network technology, which has radically transformed various aspects of our lives. It is noted that every phenomenon has its positive and negative aspects. Despite the great development that accompanied the information revolution, it has at the same time made the international community face new risks associated with this rapid development.
There is no doubt that the issue of legal mechanisms to combat cybercrime has become a concern that worries legal professionals. Therefore, it has become necessary to expand the circle of cooperation with specialists in digital technologies, legal professionals, and official institutions in the country, as well as at the international level, to enact effective laws and legislation to combat the perpetrators of these crimes. The importance of this research is also evident from a theoretical standpoint in knowing the extent to which current legal texts are sufficient in preventing cybercrime and deterring its perpetrators, and the extent of the need to create new legal texts to reduce this phenomenon.
Keywords: Cybercrime; International mechanisms; Cybersecurity; Legal challenges; International cooperation.

المقدمة:

الحمد لله رب العالمين، وأشهد أن لا إله إلا الله وحده لا شريك له، وأشهد أن محمدًا عبده ورسوله، صلى الله عليه وعلى آله وصحبه أجمعين، ومن تبعهم بإحسان إلى يوم الدين. وبعد؛ فإن العلم نور يهدي الله به من يشاء من عباده، وهو وسيلة رفيعة لنهضة الأمم وتقدم المجتمعات، غير أن علم الإنسان – على سعته – يظل محدودًا أمام علم الله عز وجل، مصداقًا لقوله تعالى: ﴿وَمَا أُوتِيتُم مِّنَ الْعِلْمِ إِلَّا قَلِيلًا﴾ (الإسراء 85)، ومن هذا المنطلق تأتي هذه الدراسة لتسليط الضوء على موضوع الجريمة الإلكترونية، حيث تشكل في عصر الثورة الرقمية أحد أخطر التحديات التي تواجه المجتمع الدولي، نظرًا لطبيعتها العابرة للحدود واعتمادها على التطور التقني الهائل في مجالات الاتصال والمعلومات، وقد أفرزت هذه الجرائم صورًا جديدة من التهديدات شكلت خطورة على البنية التحتية للدول، والاقتصاد العالمي، وحقوق الأفراد، الأمر الذي فرض على المجتمع الدولي السعي نحو تبني آليات قانونية وأمنية وقضائية مشتركة لمواجهتها.

ورغم تعدد الجهود الدولية والإقليمية، لا تزال فعالية هذه الآليات محل جدل بسبب ما تعترضها من تحديات تتعلق بتباين التشريعات الوطنية، وضعف التعاون الدولي، وتسارع تطور أساليب الجريمة الإلكترونية. ومن هنا تأتي أهمية هذه الدراسة التي تسعى إلى بيان الإطار الدولي لمكافحة الجريمة الإلكترونية، وتحليل أبرز الآليات القائمة، والكشف عن التحديات التي تحد من فعاليتها، وصولًا إلى مقترحات عملية لتعزيز المواجهة الدولية لهذه الظاهرة.

1 – **أهمية الدراسة:**

تنبع أهمية هذه الدراسة من خطورة الجريمة الإلكترونية باعتبارها جريمة عابرة للحدود تهدد الأمن الدولي، وحقوق الأفراد، مما يجعل مواجهتها تتطلب تنسيقًا دوليًا فعالًا، وعليه تُبرز الدراسة أوجه القصور والتحديات التي تواجه الآليات الدولية.

2 – أهداف البحث: يهدف البحث إلى:

– بيان الإطار القانوني الدولي المنظم لمكافحة الجريمة الإلكترونية.

- تحليل أبرز الآليات الدولية (القانونية، الأمنية، القضائية) المطبقة في هذا المجال.
- الكشف عن التحديات والعقبات التي تحد من فعالية هذه الآليات.
- تقديم توصيات عملية لتعزيز التعاون الدولي والحد من انتشار الجريمة الإلكترونية.

3- منهج الدراسة:

اعتمدنا في هذا الدراسة على المنهج الوصفي التحليلي في تحديد ماهية الجريمة الإلكترونية، والتعرف على الآليات القانونية لمكافحتها.

4- مشكلة الدراسة:

تكمن مشكلة الدراسة في السؤال الرئيسي وهو إلى أي مدى تُعد الآليات الدولية الحالية كافية وفعّالة في مكافحة الجريمة الإلكترونية، وما هي أبرز التحديات التي تحد من تحقيق أهدافها؟

ويتفرع من هذا السؤال عدة تساؤلات فرعية:

ما هو الإطار القانوني الدولي المنظم لمكافحة الجريمة الإلكترونية؟

ما أبرز الآليات الدولية المتبعة في التصدي لهذه الجرائم؟

ما التحديات التي تواجه تلك الآليات على الصعيد القانوني والأمني والقضائي؟

6- خطة البحث:

المطلب التمهيدي: ماهية الجريمة السيبرانية.

المبحث الأول: الآليات القانونية لمكافحة الجريمة السيبرانية.

المطلب الأول: الآليات الأمنية لمكافحة الجريمة الإلكترونية الدولية.

المطلب الثاني: الآليات القضائية لمكافحة الجريمة الالكترونية الدولية.

المبحث الثاني: التحديات المواجهة لآليات مكافحة الجرائم الإلكترونية وطرق مواجهتها.

المطلب الأول: التحديات المواجهة لآليات مكافحة الجرائم الدولية.

المطلب الثاني: طرق مواجهة التحديات المواجهة لآليات مكافحة الجريمة الدولية.

المطلب التمهيدي
ماهية الجريمة السيبرانية

1- تعريف الجرائم السيبرانية:

استخدم مصطلح السيبرانية لأول مرة عام 1948 وهو عالم الرياضيات "Norbert wiener " وذلك أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فالجريمة السيبرانية رغم خصوصيتها فإنها ضاربة بجذورها في القدم، فقد وقعت أول جريمة إلكترونية مسجلة في عام 1820، بعد وقت قصير من قيام شركة (Joseph-Marie Jacquard) وهي شركة تصنيع نسيج في فرنسا، بإنتاج أول نول قابل للبرمجة، وقد كانت دوافع هذه الجريمة الأولى تتلخص في قلق موظفي الشركة من احتمالية تعرض وظائفهم التقليدية وسبل عيشهم للتهديد، مما أدى بهم إلى ارتكاب أعمالا تخريبية لإجبار الشركة على استخدام هذه التكنولوجيا الحديثة.

وجدير بالذكر فإن مصدر كلمة "Cyber" في المعاجم اللغوية فيتضح أنها يونانية الأصل وترجع إلى مصطلح "Kybernetes " الذي ظهر في مؤلفات الخيال العلمي، ويعني القيادة أو التحكم عن بعد.

أما في اللغة العربية فلا يوجد هناك مصطلح مقارب للسايبر "cyber" إذ جاء معنى هذه الكلمة في قاموس المورد الحديث بمصطلح "الكمبيوتري" أو "عصري جدا" كما ورد في مصطلح " cybernetics" بأنه "علم الضبط" (إسماعيل،2024، ص15)، وقد جاء في قاموس المعاني بمعنى "تخيلي" كما قد ترجم مصطلح الفضاء السيبراني "cyber space" إلى الفضاء المجازي أو الافتراضي، وهذا غير دقيق إذ ترجمة المجازي أو الافتراضي في اللغة الإنجليزية هي (virtual) ومن ناحية أخرى أن الفضاء السيبراني هو بيئة رقمية حقيقية وليس افتراضية.

وجدير بالذكر أنه لم يتفق الباحثون والمتخصصون في الدراسات القانونية المتعلقة بالجريمة المعلوماتية على مصطلح معين (Jürgen ،2021 ،p8)، فمنهم من يستخدم مصطلح

الجريمة المعلوماتية، والبعض يستخدم مصطلح جرائم الحاسب الآلي وجرائم الكمبيوتر، والجرائم الإلكترونية، وغيرها (محمد، 2006، ص69).

كما عرف قاموس الأمن المعلوماتي، مصطلح السيبرانية بأنه هجوم عبر إلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى محمية إلكترونيا لتعطيلها أو تدميرها أو الإضرار بها (اسماعيل، 2024، ص 16).

والجريمة السيبرانية تعرف بأنها "هي الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها، أو جريمة يكون الحاسب الآلي نفسه ضحيتها" (Jürgen، 2021، p10).

كما عرفتها الاتفاقية الأوروبية للجرائم السيبرانية (اتفاقية بودابست) بأنها كافة النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية (Esther، 2023، p12)، وصنفت هذه الاتفاقية الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها، والجرائم ذات الصلة بالكمبيوتر، والجرائم المتعلقة بمحتوى الكمبيوتر، والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية (انعقدت الاتفاقية الأوربية لجرائم الانترنت في بودابست بدولة المجر بتاريخ ٢٣/ 11/ 2001 وتعتبر هي الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الانترنت، وقد تم توقيعها من ٣٠ دولة أوروبية بالإضافة إلى أربع دول غير أعضاء في المجلس الأوروبي).

ولا شك أن الجريمة السيبرانية لا تشمل فقط الجرائم التي ترتكب عن طريق الكمبيوتر، بل تشمل أيضا أية جريمة تتضمن استخدام أو استهداف الكمبيوتر (إسراء، 2016)، وتأكيدا على ذلك ما جاء في إرشادات الإسكوا (ESCWA) للتشريعات السيبرانية في بيان مفهوم الجريمة السيبرانية إذ ذهب إلى أن "الجريمة السيبرانية تنقسم إلى نوعين أساسيين؛ أولهما هو أن يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة (Bénédicte، 2014، p2)، والنوع الثاني هو الذي يكون فيه جهاز الحاسوب

وشبكات الحواسيب وبرامجها موضوعا للجريمة، أي أن الفعل الجرمي ارتكب على هذا الجهاز (زين العابدين، 2018، ص48).

2- طبيعة الجرائم السيبرانية:

الجرائم السيبرانية في القانون الدولي هي أعمال عنف ضد الخصم سواء تم القيام بها على سبيل الهجوم أو الدفاع وبعيدا عن المنطقة التي تنفذ فيها تلك الأعمال، وهذا ما نص عليه البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977 في الفقرة الأولى من المادة 49 بأنها تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم (اللجنة الدولية للصليب الأحمر، 1997، ص 40).

وعلى وفق ما تقدم فإن التركيز على آثار النشاط السيبراني وجسامته سيبين أن وصف الهجوم متحقق فيه، فيمكن أن تستخدم الجرائم السيبرانية في تعطيل أو تدمير الأجهزة الإلكترونية المسؤولة عن تنظيم شبكة الكهرباء أو المياه والسدود أو المفاعلات النووية وأنظمة التحكم في الطائرات أو غيرها من المنشآت الحيوية مما قد يترتب عليها عرضة الكثير من المدنيين أو حياتهم للخطر.

3- صور الجرائم السيبرانية: يوجد العديد من الاتجاهات حول تقسيم الجرائم الإلكترونية ويمكن تقسيمها إلى: الجرائم الاقتصادية (Gulnaz،2025 ،p1)، الجرائم الأخلاقية، الجرائم الاجتماعية، الجرائم الثقافية، الجرائم السياسية، الجرائم الجنسية (بشري، ص72).

المبحث الأول

الآليات القانونية لمكافحة الجريمة السيبرانية

تعد الجريمة الإلكترونية من أسرع أشكال الجرائم نموا على الصعيدين الوطني والدولي Bénédicte،2014، (p1)، والأمم المتحدة منذ نشأتها عملت على رسم سياسة ناجحة في مجال منع الجريمة وتحقيق العدالة الجنائية، ولا شك أنها تلعب الدور الرئيسي في مكافحة الإجرام المنظم في جميع مظاهره، وبالنظر إلى طبيعة الجرائم الالكترونية ومرونتها واكتسابها بعدا دوليا متناميا، فإن التعاون الدولي لمكافحة هذه الجرائم أمر لا مناص منه (Jürgen،2021،p9)، وشرط هذا التعاون وجود تشريع داخلي متكامل وقضاء وطني فعال واتفاقيات دولية تتوافر على آليات التنفيذية قادرة على مساعدة الدول على التصدي للجرائم المنظمة وتفكيك الجماعات الإجرامية ومعاقبة وملاحقة العاملين فيها (محمد، محسن 1998، ص19).

ونظرا لتعدد الجرائم الالكترونية وتطورها تزايدت صورها (Esther،2023 ، p14)، مما أدى إلى ضرورة التعاون الدولي لمواجهتها، ومن ثم تكثيف الجهود الدولية وعقد الاتفاقيات والمؤتمرات الدولية لوضع استراتيجيات خاصة بمرحلتي الوقاية والمكافحة لهذه الجرائم، ونتناول المبحث على النحو الآتي:

المطلب الأول: الآليات الأمنية لمكافحة الجريمة الإلكترونية الدولية.

المطلب الثاني: الآليات القضائية لمكافحة الجريمة الالكترونية الدولية.

المطلب الأول: الآليات الأمنية لمكافحة الجريمة الالكترونية

نتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم، أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة (Jürgen،2021،p29)، وعليه هناك آليات على المستوى الدولي وأخرى الإقليمي، وذلك على النحو التالي:

أولا- الآليات الأمنية على المستوى الدولي (الإنتربول الدولي):

تهدف المنظمة الدولية للشرطة الجنائية (الإنتربول) إلى تعزيز وتشجيع التعاون الأمني الدولي (Marc،2025 ،p11)، أي مساعدة الأجهزة الأمنية في الدول الأعضاء على التعاون فيما بينها في مجال مكافحة الجريمة بأشكالها المختلفة، وبصفة خاصة الجرائم ذات الطابع عبر الوطني كالجرائم الإلكترونية (سامي، 2023، ص61)، دون التدخل في الشئون ذات الطابع السياسي أو العسكري أو الديني أو العرقي، أو ممارسة أي نشاط.

وتتمثل طريقة عملها في ملاحقة مرتكبي الجرائم الإلكترونية يستلزم القيام بإجراءات خارج حدود الدولة، حيث ارتكبت الجريمة، ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج وضبط الأقراص الصلبة، وتفتيش أنظمة الحاسب الآلى، وهذا كله يصطدم بمشاكل الحدود، ويتعذر على الدولة بمفردها القضاء على مثل هذه الجرائم الدولية؛ لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين خارج حدود الدولة، وقد مرت جهود منظمة الإنتربول في هذا المجال بمراحل عدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، ونيوزيلندا، ونيروبي، وأذربيجان وبوينس ايرس، بالإضافة إلى مكتب إقليمي فرعى في بانكوك، ونظرا لتنوع أنظمة الدول المختلفة.

فقد كان هناك خياران لأنظمة الاتصال داخل هذه الشبكة، أولهما، هو نموذج يخصص للدول المركزية، وتجرى الاتصالات الدولية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، وثانيهما، للدول اللامركزية وتجرى الاتصالات فيه مباشرة بين أجهزة الشرطة في الدول المختلفة حيث تقوم المنظمة من خلال

هذه المراكز بملاحقة مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، عن طريق تعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر للحدود المكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عما تحويه من معلومات وأدلة وبراهين على ارتكاب الجريمة الإلكترونية (سامي، 2023، ص67).

ثانيا- الآليات الأمنية على المستوى الإقليمي:

ارتفاع معدلات الجريمة الإلكترونية في عام 2013 تسبب في خسائر جسيمة نجمت عنها، وعليه قامت وكالة اليوروبول بإنشاء المركز الأوروبي للجرائم الإلكترونية الذي يهدف إلى مكافحة الجرائم الإلكترونية في الاتحاد الأوروبي، والعمل على حماية مواطني الاتحاد والحكومات والشركات من مخاطر جرائم الإنترنت (جميل، 2012، ص79)، ويختص المركز بالتالي:

- يعد محور مركزي للمعلومات والاستخبارات الجنائية.
- توفير قدرات دعم جنائية رقمية وتقنية عالية التخصص للتحقيقات والعمليات الأمنية.
- استضافة وتيسر مهام فرق العمل المشتركة لمكافحة الجرائم الإلكترونية.
- دعم التدريب وبناء القدرات، ولا سيما للسلطات المختصة في الدول الأعضاء(Esther،2023).
- تقديم مجموعة متنوعة من نتائج التحليل الاستراتيجي التي تمكن القادة من اتخاذ قرارات مستنيرة.
- المساهمة في تقديم أنشطة موحدة للوقاية من مخاطر الجرائم الإلكترونية، وإعداد حملات توعية في المجالات ذات الصلة بهذه الجرائم (سامي، 2023، ص69).

أما على المستوى العربي، فقد أنشأ المكتب العربي للشرطة الجنائية من قبل مجلس وزراء الداخلية والعدل العرب في سنة 2010، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء (سليمان، 2007، ص414).

وعليه ينبغي أن يتم اتخاذ نهجا واحدا بين كافة الدول المتعاونة فيما بينها لمكافحة الجرائم الدولية، لاسيما أنها مسؤولية مشتركة تعمل فيها الحكومة والمواطنون والشركات والمجتمع المدني معا لردع الجرائم الإلكترونية وكشفها وتعطيلها، فكلما كانت الرؤية أوضح كان من السهل على أصحاب المصلحة الرئيسيين ضمان اتباع نهج شامل ومتسق ومتماسك (This vision should ideally set a clear whole-of-government and whole-of-society approach for combating cybercrime، especially as it is a shared responsibility where government، citizens، businesses and civil society work together to deter، detect and disrupt cybercrime(Jürgen،2021، p30).

المطلب الثاني: الآليات القضائية لمكافحة الجريمة الإلكترونية

يهدف التعاون القضائي بين الدول إلى التنسيق بين السلطات القضائية فيما يتعلق بالإجراءات الجنائية من حيث إجراءات التحقيق والمحاكة إلى حين صدور الحكم، وعليه نقسم المطلب إلى فرعين أولهما المساعدة القضائية، والثاني، تنفيذ الأحكام القضائية الأجنبية وتسليم المجرمين، كما يلي:

الفرع الأول: المساعدة القضائية

يقتضي التعاون الدولي مساعدة الدول لبعضها قضائيا بسبب خصوصية الجرائم المعلوماتية المتمثلة في عبورها للحدود الوطنية، الأمر الذي يجعلنا نتعرف على المساعدة القضائية وأساليبها:

أولا: مفهوم المساعدة القضائية: يقصد بالمساعدة الفضائية الدولية كل إجراء قضائي تقوم به السلطات المختصة في الدولة المطلوب منها بناء على طلب الدولة الطالبة من شأنه تسهيل مهمة المحاكمة وكشف الحقيقة بصدد جريمة من الجرائم، وقد اصطلح عليها في بعض الصكوك الدولية المساعدة القانونية المتبادلة شأن اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، فملاحقة الدولة الواحدة للجريمة الإلكترونية لا يجدي نفعا في مكافحتها (سالم، 1997، ص425).

ثانيا- أساليب المساعدة القضائية: تقتضي المساعدة القضائية اتباع عدة أساليب، تبادل المعلومات، نقل الإجراءات، الإنابة القضائية نفصلها على النحو التالي:

1- تبادل المعلومات:

كان لهذه الصورة من صور المساعدة القضائية الدولية صدى كبير في الكثير من الاتفاقيات الدولية، كاتفاقية الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية، وأيضا اتفاقية الرياض العربية للتعاون القضائي.

ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أو أمنية أجنبية، متى كانت بصدد جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل أيضا السوابق القضائية للجناة، تتعرف من خلاله الجهات القضائية على الماضي الجنائي للفرد، لتقرير الاحكام الخاصة بالعود ووقف تنفيذ العقوبة وغيرها من الإجراءات (عبد الرحمن، 2011، ص528).

2- نقل الإجراءات:

وتتجسد هذه الصورة في قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الأخيرة، وذلك بتوافر شروط معينة كالتجريم المزدوج، وأن تؤدي الاجراءات المطلوب اتخاذها دورا مهما في الوصول إلى الحقيقة.

وعليه يمكن القول أن تبادل المعلومات حول مرتكبي الجرائم المعلوماتية يساهم في التعرف على الجناة وبالتالي إلقاء القبض عليهم والتخفيف من حدة انتشار هذا النوع من الجرائم، وفي المقابل نجد أن نقل الإجراءات تقيده شروط خاصة بالتجريم المزدوج وبشرعية الإجراءات لما ينقص من فعالية هذا الأسلوب في مكافحة الجرائم المعلوماتية، ولقد أقرت هذه الصورة من صور المساعدة القضائية العديد من الاتفاقيات كمعاهدة الأمم المتحدة النموذجية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999، وكذا المادة 16 من النموذج

الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003 (سالم، 1997، ص427).

3- الإنابة القضائية:

تعبر الإنابة القضائية عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن (Ismahane،2024 ، p9)، وتهدف إلى تذليل العقبات التي تعترض سير الإجراءات الجنائية في ظل ما تشهده الظواهر الإجرامية من تطور، بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كإجراء التفتيش والضبط والمعاينة (عمر، 2001، ص14).

وتجدر الإشارة إلى أنه تم إبرام العديد من الاتفاقيات المتعلقة بالإنابة القضائية، ومنها الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال، ونفس الشيء نجده في المادة (٢/ ٢٠) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام ١٩٩٩، والمادة (١٥) من اتفاقية الرياض العربية للتعاون القضائي لعام ١٩٨٣، والمادة (٥٣) من اتفاقية تشينجن لعام ١٩٩٠ بشأن استخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف والمادة (٤٦) من اتفاقية الأمم المتحدة لمكافحة الفساد العام ٢٠٠٤ (سامي2023، ص77).

كل هذه الإجراءات تساهم ولو بصورة نسبية في مكافحة الجريمة المعلوماتية، حيث تثبت فعاليتها من خلال التزام كل منظمة دولية بالتعاون مع باقي الدول في ظل العولمة والثورة التكنولوجية.

الفرع الثاني: تنفيذ الأحكام القضائية الأجنبية وتسليم المجرمين

تتميز الجريمة المعلوماتية بتخطيها للحدود الوطنية، حيث يكون الجاني في دولة ما ويمتد أثر الجريمة للمعلوماتية إلى دول أخرى بسبب سرعة تبادل المعلومات، الأمر الذي يستدعي التعاون الدولي عن طريق تنفيذ الأحكام القضائية الأجنبية ونظام تسليم المجرمين، وذلك على النحو الآتي:

أولا- تنفيذ الأحكام القضائية الأجنبية:

الحكم الأجنبي هو القرار الصادر من سلطة قضائية أجنبية لها ولاية الفصل في هذا الموضوع باسم سيادة دولة أجنبية بمقتضى ما لها من صلاحيات قضائية بصرف النظر عن مكان صدور الحكم أو القرار، وبصرف النظر عن جنسية القضاة الذين قاموا بإصداره.

وجدير بالذكر أن المادة 38 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية 2010 نصت على أن تلتزم كل دولة طرف، بتنفيذ أحكام هذه الاتفاقية وتحقيق الغاية منها أن تعترف بالأحكام الجزائية والمدنية الباتة الصادرة من محاكم دولة طرف أخرى.

ثانيا- تسليم المجرمين:

يعتبر نظام تسليم المجرمين من الأساليب الفعالة للتخفيف من حدة الجرائم المعلوماتية، وفيما يلي تتطرق لمفهومه وإجراءاته:

1- مفهوم تسليم المجرمين وشروطه:

عرفها الاتجاه الغالب في الفقه الدولي (سليمان 2007، ص7) بأنه "إجراء بمقتضاه تتخلى الدولة عن شخص موجود على إقليمها لسلطات دولة أخرى تطالب بتسليمه إليها لمحاكمته عن جريمة منسوب إليه ارتكابها، أو لتنفيذ عقوبة مقضي عليه بها من محاكم الدولة طالبة السليم" (حامد، 1962، ص400).

وقد نصت اتفاقية بودابست على إجراء تسليم المجرمين وفق المواد من 2 إلى 11 منها (عبد الغني 1991، ص 22)، كما تضمنت الاتفاقيات الدولية والتشريعات الوطنية شرط استبعاد بعض الجرائم والعقوبات من نطاق التسليم حيث كانت الجرائم السياسية

والعسكرية وأحيانا الجرائم المالية محلا لإجماع دولي قانوني يجيز أو يوجب أحيانا رفض التسليم بشأنها.

2- إجراءات تسليم المجرمين:

تتمثل إجراءات تسليم المجرمين في تقديم طلب التسليم، والرد عليه وتسليم المتهم وذلك كما يلي:

أ- تقديم طلب التسليم:

على الدولة الطالبة أن تتقدم إلى حكومة الدولة المتواجد بإقليمها الشخص المعني بطلب التسليم مشفوعا بكافة البيانات الخاصة بالمعني بالتسليم والمتضمن صورته الفوتوغرافية، هويته وأوصافه، فالتسليم عمل من أعمال السيادة لا تباشره إلا حكومة الدولة الطالبة.

ب- الرد على طلب التسليم إما بالموافقة أو الرفض:

بمجرد وصول الطلب إلى الدولة المطالبة تقوم سلطاتها المختصة بدراسة ملف الطلب والتحري عن الشخص المطلوب، وفي حالة الرفض تعلم الدولة للمطالبة الطرف الطالب بقرارها (عبدالرحيم 1982، ص104).

ج- نقل الشخص المطلوب تسليمه:

بعد صدور قرار التسليم يتم نقل الشخص المطلوب تسليمه من الدولة المُطالبة إلى الدولة الطالبة وفق ترتيبات تتفق عليها الدولتان في اتفاقية التسليم التي تربط الطرفان أو في تشريع الدولة المطالبة.

بناء على ما سبق يتضح أن الجهود الدولية المبذولة قصد التصدي للجريمة للمعلوماتية من خلال الاتفاقيات المبرمة بين الدول في مجال التسليم تعتبر نسبية بدليل الانتشار الواسع للجريمة المعلوماتية على اختلاف أشكالها وتخطيها للحدود الوطنية، كما أن هذه الجهود تواجه عدة تحديات وعراقيل من بينها احتجاج الدول بمبدأ السيادة في مجال الإنابة القضائية وتسليم الرعايا، ووجود شروط وضوابط لإعمال هذه الآليات ضمن

التشريعات الداخلية لكل دولة أو في الاتفاقيات، وفي حالة عدم التزام الدول بهذه الآليات يكون الحل الوحيد هو المعاملة بالمثل دون وجود أي مسؤولية.

المبحث الثاني

التحديات المواجهة لآليات مكافحة الجرائم الإلكترونية وطرق مواجهتها

تحول الفضاء الإعلامي والشبكة العنكبوتية إلى ساحة حرب عقول وتقنيات وفنيات وخبرات في المجال الإلكتروني، وعند التصدي للجرائم الإلكترونية يحدث تصادم بعدة عراقيل ومعوقات تتسبب في عرقلة المحاكمة عن هذه الجرائم، وعليه نستعرض المعوقات التي تعترض آليات مكافحة الجرائم الإلكترونية، وطرق مواجهتها، وذلك على النحو التالي:

المطلب الأول: التحديات المواجهة لآليات مكافحة الجرائم الدولية

مكافحة الجرائم المعلوماتية لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، وعلى ذلك نتناول المعوقات التي تعترض الآليات القانونية، ونقسمها إلى العوائق الخاصة بتحقيق التعاون الدولي، والمتعلقة بالجريمة الإلكترونية ذاتها، وأخيرا العوائق المرتبطة بالقضاء والسلطة التنفيذية والتشريعية:

أولا-التحديات الخاصة بتحقيق التعاون الدولي:

1- عدم وجود قانون موحد لجرائم الإنترنت:

من أكثر الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم الإلكترونية هي عدم وجود توافق بين الأنظمة القانونية في مختلف بلدان العالم حول نموذج موحد للنشاط الإجرامي المكون للجرائم الإلكترونية (Fátima،P90).

2- عدم وجود أجهزة فعالة لربط الأنظمة ببعضها:

ينبغي أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة.

3- مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت:

تعد الجرائم الإلكترونية، لما تتميز به من سمات وخصائص وكونها من الجرائم العابرة للحدود، من أكثر الجرائم التي يثار بشأنها تنازع الاختصاص القضائي بين الدول، الذي ينشأ نتيجة اختلاف التشريعات والنظم القانونية بين هذه الدول فيما يتعلق بالجرائم الإلكترونية (عبدالفتاح 2007، ص192).

4- تمسك الدول بمبدأ السيادة الوطنية:

الدولة هي السلطة العليا التي لا تعلوها سلطة في الداخل والخارج، بما يعنيه ذلك من استئثار جهة الحكم في الدولة بكافة اختصاصات السلطة ومظاهرها، دون أن تخضع في ذلك لأي جهة أعلى، وعليه قد تمتنع بعض الدول تنفيذ بعض الآليات لمكافحة الجرائم الإلكترونية، نظرا للمساس بسيادتها.

5- التجريم المزدوج في تسليم المجرمين:

يعد هذا الشرط في نظام تسليم المجرمين عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية لاسيما وأن معظم الدول لا تجرم هذه الجرائم، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة المجرمين.

6- المساعدات القضائية الدولية المتبادلة بالإنابة القضائية:

يوجد الكثير من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة كالتباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها (محمد، 2002، ص153).

7- عدم وجود معاهدات ثنائية أو جماعية بين الدول:

عدم وجود اتفاق تعاون بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حالة وجودها فإن هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم و برامج الحاسب الآلي و شبكة الإنترنت.

ثانيا- المعوقات المتعلقة بالجريمة الإلكترونية:

1- جرائم الإنترنت جرائم نظيفة وذلك لصعوبة اكتشاف دليل ثبوتها فلا أثر فيها لأي عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية.

٢- مهارة التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجردة.

٣- تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال، وسهولة محو الأدلة.

4- التكتم على الجرائم من قبل الجهات المجني عليها.

5- عدم وجود حملات إعلانية للتوعية بطرق النصب والخداع التي دائما تكون تطور مستمر (P 49،Esther 2023).

ثالثا- المعوقات المتعلقة بالقضاء والسلطة التنفيذية، والسلطة التشريعية:

1- وجود نقص كبير في المهارات داخل الشرطة والقضاء، فهذا النوع من الجرائم يحتاج إلى دراية كبيرة في الأدلة الإلكترونية والبرامج الضارة والبرمجيات والعملات المشفرة.

2- عدم وجود قضاة ورجال شرطة متخصصين في الجرائم الإلكترونية وغالبا ما يتعاملون مع هذه الجرائم بالطرق التقليدية، سواء في مرحلة القبض والتفتيش والتحفظ على الأدلة، أو عند التحقيق وتفقد وتمحيص الأدلة الإلكترونية، أو عند مرحلة المحاكمة والنطق بالحكم(Esther 2023،P47).

3- عدم الاهتمام بعلم الطب الشرعي الرقمي، وهو فرع من فروع الطب الشرعي ويتولى التركيز على تحديد البيانات المخزنة على الأجهزة الإلكترونية، والحصول عليها ومعالجتها، وتحليلها والإبلاغ عنها، حيث أصبحت الأدلة الإلكترونية عاملا في جميع التحقيقات الجنائية ودعما لإنفاذ القانون.

4- عدم تطوير التشريعات الداخلية بما يتوافق مع التطور التكنولوجي (Fátima، p90)، والنص على الجرائم الإلكترونية الحديثة، مما قد يتعارض مع مبدأ شرعية الجرائم

والعقوبات الذي قد يتسبب في عدم عقاب متهم ارتكب جريمة إلكترونية ولا يوجد نص في قانون العقوبات يجرمها (محمود 2025، ص25).

5- عدم تدريب القيادات الإدارية تعد من الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب، وعدم قابلية القيادات للتدريب على تكنولوجيا المعلومات، وكذلك ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين في مجال تكنولوجيا المعلومات وشبكات الاتصال (Esther 2023، P45).

المطلب الثاني: طرق مواجهة التحديات المواجهة لآليات مكافحة الجريمة الدولية

القضاء على الصعوبات التي تواجه آليات مكافحة الجرائم الدولية نجملها في التالي:

أولا- مواجهة المعوقات على المستوى التشريعي والقضائي:

- إنشاء واعداد لوائح قانونية وتشريع شامل للأمن السيبراني لأن هناك حاجة للائحة كاملة شاملة توفر الأساس القانوني لمكافحة الجرائم الالكترونية بطريقة تحترم الحقوق الأساسية.
- إنشاء وحدة مكافحة الجرائم الالكترونية، والتعاقد مع شركات عالمية مدربة.
- إنشاء دوائر قضائية متخصصة للنظر في قضايا الجرائم الإلكترونية لضمان سرعة ودقة الفصل.
- تعزيز التعاون القضائي الدولي في تسليم المتهمين وتبادل الأدلة الرقمية.
- اعتماد أدلة رقمية موحدة من حيث طرق الجمع والحفظ لضمان قبولها قضائيا.
- ينبغي أن يراعي رجال القضاة والشرطة الطبيعة الخاصة لهذه الجرائم في كافة مراحلها سواء في مرحلة القبض والتفتيش والتحفظ على الأدلة، وفي جمع الأدلة الإلكترونية، أو عند مرحلة المحاكمة والنطق بالحكم، ومراعاة الاتجاهات والتقنيات الحديثة (Esther 2023، P39).
- ضرورة تطوير القوانين الوطنية والإجراءات الاستباقية لمواجهة الجرائم الإلكترونية، على نحو أكثر شمولية ومرونة حتى تواكب حركة التشريع الدولية بشأن مكافحة الجريمة الإلكترونية.

- صياغة نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات، للتصدي للمنظمات الإجرامية التي تعمل بأسلوب علمي مدروس على تشتيت الأدلة والتخلص منها مما يستدعي تطوير التعاون القضائي في مختلف مراحله (محمود 2021، ص572).

- الاهتمام بتعيين خبراء الطب الشرعي الإلكتروني، ولا شك أنهم يعاونون القاضي في تتبع الأدلة وجمعها وتفسيرها لأنه في الغالب لم تكن له المهارة بالإلمام بهذه الشفرات والأرقام الإلكترونية (Esther 2023، P42).

ثانيا- مواجهة المعوقات على المستوى الأمني والتقني:

- توسيع مراكز الاستجابة للطوارئ الإلكترونية لرصد الهجمات والتعامل معها فورا.
- إنشاء قواعد بيانات وطنية للمجرمين الإلكترونيين وأساليبهم وربطها إقليميا ودوليا.
- استخدام تقنيات الذكاء الاصطناعي في تتبع الأنماط غير الطبيعية في المعاملات المالية أو أنشطة الإنترنت.
- توثيق التعاون فيما بين الأجهزة التنفيذية، وإنشاء أجهزة متخصصة لمواجهة الإجرام المنظم، وإنشاء قسم خاص بأقسام الشرطة متخصص في الجرائم الإلكترونية (Esther 2023، P50).
- التقريب بين الأجهزة والربط بين الإدارات والآليات الدولية المتخصصة أي تمكين المؤسسات المختصة من القيام بعملها دون أية عوائق.
- إنشاء ما يسمى بطوارئ الحاسب الآلي لسرعة الاستجابة، وعمل جهة اتصال واحدة تتعلق بالجرائم الإلكترونية وعدم استخدام الروتين العادي الخاص بجهات إنفاذ القانون.

ثالثا- مواجهة المعوقات على المستوى المؤسسي والتعليمي:

- التعاون بين مؤسسات الدولة بين القطاعين العام والخاص وخاصة بين البنوك وشركات الاتصالات لرصد عمليات الاحتيال.
- إدخال مناهج دراسية عن الأمن السيبراني في المراحل الجامعية والمدرسية.

– تنفذ أنشطة توعية على المستويات الفردية والمؤسسية والوطنية، أي في جميع أنحاء المجتمع وأفراده من نساء ورجال وأطفال وغيرهم من الأفراد الذي من الممكن أن يقعوا ضحية الجرائم الإلكترونية.

رابعا– مواجهة المعوقات على المستوى الدولي:

- الانضمام لاتفاقيات دولية مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية.
- إنشاء مركز إقليمي عربي لتبادل المعلومات والخبرات حول التهديدات الإلكترونية.
- تعزيز التعاون مع الإنتربول واليوروبول في تتبع الشبكات الإجرامية العابرة للحدود.
- حث الدول على إنشاء وتفعيل مصرف بيانات مشترك بشأن الإجرام المنظم وأعضائه وجمع المعلومات عن الأشخاص المحكوم عليهم، على أن يكفل الحماية القانونية للملفات الشخصية كما هو الحال بالنسبة للأحكام المحلية والدولية (Esther 2023، P51).
- تعيين سلطة مركزية تقوم بالاتصال مباشرة بالسلطات المركزية في سائر الدول الأطراف بغرض تقديم العون والمساعدة اللذين تنص عليهما هذه الاتفاقية.
- إقامة قنوات اتصال بين سلطات الدول وأجهزتها ودوائرها المختصة تسهيلا للأمان وسرعة تبادل المعلومات المتعلقة بجميع الجوانب المذكورة في هذه الاتفاقيات.
- القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين، حيث ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في الاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا (محمود 2021، 571).

الخاتمة والنتائج:

1- غياب إطار دولي موحد شامل لمكافحة الجرائم الإلكترونية، رغم وجود اتفاقية بودابست التي لم تنضم إليها جميع الدول.

2- تفاوت التشريعات الوطنية بين الدول أدى إلى عرقلة الملاحقة القضائية للمجرمين عابري الحدود.

3- ضعف التعاون القضائي الدولي في تبادل المعلومات وتسليم المجرمين الإلكترونيين.

4- صعوبة إثبات الجرائم الإلكترونية على الصعيد الدولي بسبب اختلاف معايير قبول الأدلة الرقمية.

5- غياب التوازن بين مكافحة الجريمة الإلكترونية وحماية حقوق الإنسان (خصوصاً الحق في الخصوصية).

6- تركز الجهود الدولية على البعد الأمني أكثر من الجانب القانوني والتنظيمي أدى إلى عرقلة التصدر للجرائم الدولية.

7- عدم الاهتمام بالجانب الإعلامي والتوعوي لأفراد المجتمع، للتوعية بطرق النصب والخداع التي دائما تكون تطور مستمر.

8- عدم وجود قضاة ورجال شرطة متخصصين في الجرائم الإلكترونية وغالبا ما يتعاملون مع هذه الجرائم بالطرق التقليدية.

9- استخدام الطرق التقليدية للكشف عن الجرائم الإلكترونية دون خبرة أو مهارة ، مما تسبب في عدم ملاحقة التطور في الإجرام السيبراني.

10- عدم الاهتمام بعلم الطب الشرعي الرقمي، أدى إلى غياب الدقة في التحفظ على الأدلة الإلكترونية، كذلك ضياع البيانات المخزنة التي من الممكن أن تعد الدليل الوحيد ضد المتهم.

11- التجريم المزدوج يعد عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية لاسيما وأن معظم الدول لا تجرم هذه الجرائم.

التوصيات:

1- العمل على صياغة اتفاقية دولية جديدة متطورة، تراعي مصالح الدول النامية والمتقدمة معاً، وتشتمل على كافة التطورات التكنولوجية الحديثة في الجرائم السيبرانية.

2- توحيد الحد الأدنى من القواعد الجنائية والإجرائية المتعلقة بالجرائم الإلكترونية بين الدول.

3- تعزيز آليات التعاون الدولي عبر قنوات رسمية وسريعة، مثل إنشاء منصات إلكترونية مشتركة بين الدول لتبادل الأدلة الرقمية، وصياغة نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات،

4- وضع معايير دولية موحَّدة للإثبات الإلكتروني تضمن حجية الأدلة الرقمية أمام المحاكم في مختلف الدول.

5- تضمين الاتفاقيات الدولية ضمانات قانونية تكفل حماية الخصوصية والبيانات الشخصية عند ملاحقة الجرائم الإلكترونية.

6- تعزيز الدور القانوني عبر إنشاء هيئات دولية متخصصة في وضع سياسات وتشريعات لمكافحة الجرائم الإلكترونية.

7- الاهتمام بالجانب الإعلامي عن طريق إدخال مناهج دراسية عن الأمن السيبراني في المراحل الجامعية والمدرسية، وأيضا تنفيذ أنشطة توعية على المستويات الفردية والمؤسسية والوطنية، أي في جميع أنحاء المجتمع وأفراده أن يقعوا ضحية الجرائم الالكترونية.

8- إنشاء دوائر قضائية متخصصة للنظر في قضايا الجرائم الإلكترونية لضمان سرعة ودقة الفصل.

9- استخدام تقنيات الذكاء الاصطناعي في تتبع الأنماط غير الطبيعية في المعاملات المالية أو أنشطة الإنترنت.

10- الاهتمام بتعيين خبراء الطب الشرعي الإلكتروني، ولا شك أنهم يعاونون القاضي في تتبع الأدلة وجمعها وتفسيرها لأنه في الغالب لم تكن له المهارة بالإلمام بهذه الشفرات والأرقام الإلكترونية.

11- القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين، حيث ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين.

المصادر والمراجع

أولا- المراجع العربية:

1- الكتب:

- د. إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود للنشر، 2024.

- د. بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر، الأردن.

- د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية لجرائم الإنترنت، دار النهضة العربية، القاهرة، 2012.

- د. حامد سلطان، القانون الدولي العام في وقت السلم، دار النهضة العربية، القاهرة، 1962.

- د. زين العابدين الكردي، جرائم الإرهاب المعلوماتي، منشورات الحلبي الحقوقية، ط 1، 2018.

- د. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة 2007.

- د. سليمان عبدالمنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين: دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

- د. عبدالرحمن فتحي سمعان، تسليم المجرمين في ظل قواعد القانون الدولي، دار النهضة العربية، القاهرة، 2011.

- د. عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دار النهضة العربية، 2001.

- د. محمد الأمين، د. محسن عبدالحميد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف للعلوم الأمنية بالرياض، الطبعة الأولى، 1998.

- د. محمد سامي عبدالحميد، التنظيم الدولي، دار المطبوعات الجامعية، الإسكندرية، 2002.

- د. محمد عبدالله أبو بكر سلامه، موسوعة الجرائم المعلوماتية جرائم الكمبيوتر والأنترنت، منشأة المعارف، الإسكندرية، 2006.

- د. محمود محمد محمود ياسين، شرعية الجرائم والعقوبات في النظام الأساسي للمحكمة الجنائية الدولية، دروب المعرفة لنتشر، ط1، 2025.

2- الرسائل:

د. سالم محمد الأوجلي، أحكام المسؤلية الجنائية عن الجرائم في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، القاهرة 1997.

3- الدوريات:

- د. إسراء جبريل رشاد مرعي، الجرائم الإلكترونية، المركز الديمقراطي العربي، تاريخ النشر 9/ 8/ 2016، https: //www.democraticac.de /?p=35426.
- د. سامي جاد واصل، التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد 3، العدد 1، إبريل 2023.
- د. عبدالرحيم صدقي، تسليم المجرمين في القانون الدولي، المجلة المصرية للقانون الدولي، المجلد 29، 1982.
- د. محمود محمد صفاء الدين، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مجلة البحوث القانونية والاقتصادية كلية الحقوق جامعة المنوفية، المجلد 54، العدد3، أكتوبر 2021.

ثانيا- المراجع الأجنبية:

1- المراجع الإنجليزية:

- **Gulnaz Aydin Rzayeva**، International Legal Mechanisms For Combating Cybercrime: The Economic Impact On Azerbaijan And Global Practices، Baltic Journal of Economic Studies، Vol. 11 No. 1، 2025.
- **Ismahane Kharmouche**، International Cooperation Mechanisms to Combat Cybercrime، Algerian Journal of Law And political Sciences، Vol 09، Issue 01، 2024.
- **Jürgen Stock**، JAIF، National cybercrime strategy Guidebook، Japan-Asia cooperation، april 2021.
- **Esther George**، Kemal Kumkumoğlu ، Michael Jameison، Preventing and Combatting Cybercrime: Key Findings And Recommendations For Türkiye، Council Of Europe، December 2023.

2- المراجع الفرنسية:

- **Bénédicte Graulle**، La lutte contre la cybercriminalité : un enjeu majeur pour les entreprises، Jones Day، 2014.
- **Fátima Roumate**، Les Mécanismes Légaux De Lutte Contre La Cybercriminalité Au Maroc، Jnifé com.
- **Marc Watin-Augouard**، L'ONU، la cybersécurité et la lutte contre la cybercriminalité : le difficile consensus، INCYBER AGORA، 2025.