Ways to combat cybersecurity crimes

Assistant Professor Salah Mahmoud Khader*, Assistant Professor Ali Sami Hassan*

Lecturer at Al-Amal Private College/Department of Law*, University of Diyala / College of Law and Political Science*

Salahhdhdjj253@gmail.com, ali.sami@uodiyala.edu.iq

https://orcid.org/0000-0001-5366-8002

Abstract:

Cyberspace is a digital environment reliant on information technology, dealing with elements of informational networks and data processing at an extraordinary speed. Cyber power can be used to launch cyberattacks against critical infrastructure, whether civilian or military. Cyberwarfare represents a modern means and method of armed conflict, embodied in cyber operations whose effects mirror those of traditional armed conflicts or accompany hostile actions within the context of armed conflicts. A notable example is the recent cyberattack in Lebanon, which involved disabling paging devices ("pagers") in accordance with the objectives of international humanitarian law. Cyberwarfare is intrinsically linked to the nature of cybersecurity, which aims to protect information and electronic systems from various cyber threats. This protection includes implementing a set of measures and techniques to prevent such threats and manage them when they occur, involving international system actors in today's world—not only states and international organizations but also non-state actors. Thus, examining the extent to which domestic laws and international humanitarian law principles can be applied to cyberwarfare becomes essential. The increasing reliance of states on cyberattacks in their conflicts has subjected the rules of international humanitarian law to a real and complex test. This challenge revolves around whether these long-established international rules, codified decades ago, can apply to cyberattacks, which have emerged within the past decade. The difficulty of applying international rules to cyberattacks and subjecting them to the authority of these principles intersects with another issue: the lack of clarity surrounding the concept of direct participation in hostilities under international humanitarian law. The involvement of a significant number of individuals—both combatants and civilians—in modern hostilities has blurred the boundaries of the concept of direct participation to the extent that it has become difficult to clearly distinguish between direct and indirect participants in such operations. The

convergence of cyberattacks with direct participation has exacerbated and complicated the challenges related to the application of international humanitarian rules. This is particularly true when direct participants in cyberattacks belong to the category of civilians. In such cases, international humanitarian rules protecting civilians overlap with those related to combatants who directly engage in hostilities, along with the principles concerning their targeting. Direct participation in this context represents the core challenge to the proper application of international humanitarian law and its principles.

Keywords: Cyber attacks, cyber security, cyber crimes, electronic systems.

سُبل مكافحة جرائم الأمن السيبراني

المدرس المساعد صلاح محمود خضير، المدرس المساعد علي سامي حسن

تدريسي في كلية الآمال الأهلية/قسم القانون، جامعة ديالى /كلية القانون والعلوم السياسية

, ali.sami@uodiyala.edu.iq Salahhdhdjj253@gmail.com

https://orcid.org/0000-0001-5366-8002

المستخلص:

يُعد الفضاء السيبراني بيئة رقمية تعتمد التقنية المعلوماتية، وتتعامل مع مفردات الشبكات المعلوماتية ومعالجات البيانات بسرعة فائقة، ويمكن إستخدام القوة السيبرانية لتوجيه الهجمات السيبرانية ضد البنى التحتية الحيوية، سواء المدنية أم العسكرية. إنّ الحرب السيبرانية هي وسائل وأساليب حديثة للنزاعات المسلحة، تتمثل في العمليات السيبرانية التي تشابه آثارها ما تخلفه النزاعات المسلحة، أو هي عمليات سيبرانية ترافق العمليات العدائية التي تجري في سياق النزاعات المسلّحة، ولعل خير مثال ما حصل في لبنان مؤخراً من هجوم سيبراني وتفجير لأجهزة النداء "البيجر"، ووفقاً لمقاصد القانون الدولي الإنساني. وترتبط الحرب السيبرانية بشكل وثيق بطبيعة الأمن السيبراني، لأنه يهدف إلى حماية المعلومات والأنظمة الألكترونية من التهديدات السيبرانية المختلفة، ويتضمن تطبيق مجموعة من الإجراءات والتقنيات للوقاية من هذه التهديدات والتعامل معها عند حدوثها بواسطة فواعل النظام الدولي في عالم اليوم، التي لا تقتصر على الدول والمنظمات الدولية فقط، بل شملت فواعل من غير الدول. لذلك كان البحث في مدى إمكانية تطبيق القوانين الداخلية ومباديء القانون الدولي الإنساني على الحرب السيبرانية. حيث إن اللجوء المتزايد للدول إلى استخدام الهجمات السيبرانية في نزاعاتها، جعل قواعد القانون الدولي الإنساني أمام اختبار حقيقي ومعقد يدور حول مدى إمكانية تطبيق تلك القواعد الدولية التي قننت قبل عقود من الزمن على الهجمات السيبرانية، التي لم يتجاوز عمرها أكثر من عقد من الزمن. وصعوبة تطبيق القواعد الدولية على الهجمات السيبرانية وإخضاع هذه الهجمات لسلطان هذه المبادئ يلتقي بمشكلة أخرى، هي عدم وضوح معالم ومفهوم المشاركة المباشرة في العمليات العدائية في إطار القانون الدولي الإنساني، إذ إن مشاركة فئة كبيرة جداً من الأشخاص المقاتلين والمدنيين في العمليات العدائية الحديثة، جعل حدود مفهوم المشاركة المباشرة في العمليات العدائية يتلاشى بالصورة التي لا يمكن وضع الفوارق والتمييز الدقيق بين المشارك المباشر والمشارك غير المباشر في هذه العمليات. وإن التقاء الهجمات السيبرانية مع المشاركة المباشرة أدى إلى تزايد وتعقيد الصعوبات المتعلقة بتطبيق القواعد الإنسانية الدولية وإخضاع

المشاركة المباشرة في الهجمات السيبرانية إلى قواعد وقوانين الحروب وتتزايد هذه الصعوبات عندما يكون المشارك المباشر في الهجوم السيبراني من فئة المدنيين، حيث في هذه الحالة تتداخل القواعد الدولية الإنسانية المقننة لحماية المدنيين مع تلك القواعد المتعلقة بالمقاتلين الذين يشاركون مباشرة في العمليات العدائية والمبادئ المتعلقة باستهدافهم. وتمثل المشاركة المباشرة في هذه الحالة المشكلة الحقيقية أمام التطبيق السليم لقواعد القانون الدولي الإنساني ومبادئه.

الكلمات المفتاحية: الهجمات السيبرانية، الأمن السيبراني، الجرائم الإلكترونية، الأنظمة الإلكترونية.

المقدمة

يوفر التعاون الدولي لمكافحة الجرائم السيبرانية مسألتين أساسيتين، يقع اختصاصهما في نطاق الدولة وعلى المستوى الوطني: المسألة الأولى، تتطلب معالجة الجرائم بقوانين موضوعية تنسجم على موائمة القوانين الوطنية مع الأنماط الدولية والإقليمية، وهدف تحقيق تعاون نشط في مكافحة الجرائم السيبرانية، ويجب موائمة القوانين وتطوير الأطر القانونية الذي يمكن من خلالها طلب وتقديم التعاون الدولي، وهذا مكمل ضروري، فالإطار القانوني الدولي الذي قد يكون متعددة الأطراف أو ثنائي أو حتى في حالات محددة، يوفر أساساً قانونياً ضرورياً، للقيام بأي تعاون دولي، وتحتاج هذه الأطر القانونية إلى تعديل القانون الدولي ليناسب مع الطبيعة العابرة للحدود التي تتميز بها الجريمة السيبرانية[١].

إن انتشار المنظمات الدولية والإقليمية، ودمج أنشطة هذه المنظمات في معظم مجالات الحياة الدولية، أصبح سمة بارزة وأساسية للمجتمع الدولي، كما أسهم تمتع المنظمات الدولية بالشخصية القانونية وتمتعها بإرادة ذاتية ومستقلة، في المجتمع الدولي تم إثبات أهليتها للدخول في علاقات دولية مختلفة وإنشاء نوع من التنسيق والربط بين المنظمات الدولية، ذات الأنشطة المتخصصة والمنظمات العامة. هذا التنسيق والاتصال ضروريان في مكافحة الجرائم السيبرانية، إذ أن الأطر القانونية الوطنية لا تكون ذات تأثير ما لم يكن هنالك تعاون دولي على أكبر قدر من التنسيق والتعاون، فالطبيعة العابرة للحدود تحتم المواجهة الدولية، ويمكن القول إن الاتفاقيات والمعاهدات الدولية، هي أهم أشكال التعاون الدولي بشكل عام، وفي مجال الجرائم السيبرانية بشكل خاص[٢].

أولاً: أهمية البحث:

تكتسب دراسة "سبل مكافحة جرائم الأمن السيبراني" أهمية كبيرة في ظل التطور التكنولوجي المتسارع وزيادة الاعتماد على الشبكات الرقمية في مختلف جوانب الحياة، سواء على المستوى الفردي أو المؤسسي أو الحكومي. وفيما يلي أبرز الجوانب التي تبرز أهمية هذا البحث:

١. زيادة انتشار الجرائم السيبرانية:

مع تزايد استخدام الإنترنت والتقنيات الرقمية، أصبحت الجرائم السيبرانية تهديدًا عالميًا يؤثر على الأفراد والشركات والحكومات. لذا، يهدف البحث إلى فهم طبيعة هذه الجرائم وسبل مواجهتها بشكل فعال.

---

[١] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦، ص ٦.

[٢] سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ٢٠١٣، ص ١١.

٢. حماية البيانات والمعلومات:

تعد البيانات أحد أهم الأصول في العصر الرقمي، وتعرضها للاختراق أو السرقة قد يؤدي إلى خسائر مادية ومعنوية جسيمة. يساهم البحث في تحديد أفضل الممارسات لحماية المعلومات الحساسة من التهديدات السيبرانية.

٣. تعزيز الأمن القومي:

تشكل الجرائم السيبرانية تهديدًا للأمن القومي للدول، حيث يمكن أن تستهدف البنية التحتية الحيوية مثل أنظمة الطاقة والاتصالات والخدمات المالية. يقدم البحث رؤى حول كيفية تعزيز الأمن السيبراني لحماية هذه المرافق.

٤. تطوير التشريعات والسياسات:

يقدم البحث توصيات لتطوير التشريعات والقوانين التي تعالج الجرائم السيبرانية، مما يساعد في إنشاء إطار قانوني فعال لمكافحتها.

٥. تعزيز التعاون الدولي:

الجرائم السيبرانية لا تعترف بالحدود الجغرافية، لذا يبرز البحث أهمية التعاون بين الدول والمنظمات الدولية لمكافحة هذه الجرائم بشكل مشترك.

ثانياً: إشكالية البحث:

في ظل التطور التكنولوجي المتسارع وزيادة الاعتماد على الشبكات الرقمية في جميع مناحي الحياة، أصبحت جرائم الأمن السيبراني تهديدًا عالميًا لا يقتصر تأثيره على الأفراد فحسب، بل يمتد ليشمل المؤسسات والحكومات. ومع تزايد حدة هذه الجرائم وتعقيد أساليبها، تبرز تساؤلات حول مدى فعالية الجهود الحالية في مواجهتها. فما هي السبل الفعالة لمكافحة جرائم الأمن السيبراني في ظل التحديات المتزايدة التي تشمل تطور أساليب الجرائم، ونقص الوعي الأمني، وعدم كفاية التشريعات، وعدم توفر الموارد الكافية وذلك على الصعيدين الدولي والوطني، لذلك فإن الإشكالية الرئيسة التي يثيرها موضوع البحث تتمثل في السؤال التالي:

إلى أي مدى نجحت الجهود الدولية والإقليمية في الحد من انتشار الجرائم السيبرانية؟

ويتفرع عن هذا السؤال الرئيسي عدد من الأسئلة الفرعية لعل أهمها:

١. ما هي التحديات الرئيسية التي تواجه الدول والمؤسسات في مكافحة الجرائم السيبرانية؟

٢. ما هو دور التشريعات والقوانين في الحد من جرائم الأمن السيبراني، وكيف يمكن تطويرها لمواكبة التحديات الجديدة؟

٣. كيف يمكن تعزيز التعاون الدولي لمكافحة الجرائم السيبرانية التي تتجاوز الحدود الجغرافية؟

ثالثاً: أهداف البحث:

يسعى هذا البحث إلى تقديم فهم معمّق لجرائم الأمن السيبراني من خلال استعراض وتحليل أشكالها المختلفة، وتأثيراتها المتعددة على الأفراد والمؤسسات والدول. يتناول البحث الأطر القانونية والتشريعية الوطنية والدولية التي تتصدى لهذه الجرائم، بهدف تقييم مدى فاعليتها في تحقيق الردع والحماية في الفضاء الإلكتروني.

كما يركز البحث على الأدوات والتقنيات الحديثة المستخدمة في مكافحة الجرائم السيبرانية، مثل الذكاء الاصطناعي، التشفير، وأمن الشبكات، حيث يقيّم مدى كفاءتها ويبرز التحديات التي تواجه تطبيقها. ويستكشف البحث العقبات القانونية والتقنية والإجرائية التي تعترض جهود أجهزة إنفاذ القانون والمؤسسات في مواجهة هذه التهديدات، مسلطًا الضوء على ضرورة تذليلها لتعزيز فاعلية المكافحة.

وفي سياق التعاون الدولي، يبحث البحث في أهمية تضافر الجهود بين الدول والمؤسسات الأمنية لمواجهة التهديدات السيبرانية العابرة للحدود، مع تقييم المبادرات الدولية الرامية لتعزيز الأمن السيبراني على المستوى العالمي.

يخلص البحث إلى اقتراح مجموعة من الاستراتيجيات الوقائية والعلاجية لتعزيز الأمن السيبراني، تتضمن تطوير السياسات الأمنية، وتعزيز البنية التحتية الرقمية، ورفع مستوى الوعي لدى الأفراد والمؤسسات. كما يناقش دور الأفراد والشركات في تطبيق معايير الأمن السيبراني واتخاذ التدابير الوقائية المناسبة.

من خلال هذا الطرح المتكامل، يأمل البحث أن يسهم في تقديم رؤى جديدة ومبتكرة لمكافحة جرائم الأمن السيبراني، بما يعزز الحماية الرقمية ويقلل من المخاطر السيبرانية على المستويين المحلي والدولي.

رابعاً: فرضية البحث:

يقوم هذا البحث على فرضية أساسية مفادها أن جرائم الأمن السيبراني تشكل تهديدًا متزايدًا للأفراد والمؤسسات والدول، وأن مواجهتها بفعالية تتطلب تكاملاً بين الأطر القانونية والتشريعية، والتقنيات الحديثة، والتعاون الدولي.

وتنطلق هذه الفرضية من التساؤل الرئيس حول مدى كفاءة وملاءمة الوسائل القانونية والتقنية المستخدمة حاليًا في التصدي لهذه الجرائم، وما إذا كانت هناك حاجة إلى تطوير استراتيجيات أكثر شمولًا ومرونة لمواكبة التطور المتسارع في أساليب الجرائم السيبرانية.

خامساً: مناهج البحث:

نظرا لأهمية موضوع البحث في الوقت الراهن، فقد تزامن مع تزايد الاعتماد على تكنولوجيا المعلومات، لذلك تم التعويل على عدة مناهج علمية بهدف الإلمام بكافة جوانب البحث وذلك على النحو التالي:

المنهج التحليلي: حيث يسعى الباحث إلى وصف وتشخيص موضوع الدراسة من مختلف جوانبه الدولية والإقليمية والوطنية للوصول إلى الحلول المناسبة للإشكاليات المطروحة واستعراض الآراء الفقهية والقواعد القانونية المختلفة المتعلقة بالموضوع.

المنهج المقارن: وذلك لمقارنة الجهود الدولية والإقليمية في مكافحة الجرائم السيبرانية. ومقارنة أدوار المنظمات الدولية مثل الأمم المتحدة مع المنظمات الإقليمية مثل جامعة الدول العربية في مواجهة الجرائم السيبرانية.

سادساً: هيكلية البحث:

للإجابة على الإشكالية التي يثيرها موضوع البحث فقد اعتمدنا التقسيم الثنائي، حيث قسمنا البحث إلى مبحثين وكل مبحث إلى مطلبين كالآتي:

المبحث الأول: الجهود الدولية في مكافحة الجرائم السيبرانية.

المطلب الأول: دور منظمة الأمم المتحدة في مكافحة الجرائم السيبرانية.

المطلب الثاني: دور المنظمات والوكالات الدولية في مكافحة الجرائم السيبرانية.

المبحث الثاني: الجهود القانونية وأنشطة المنظمات الإقليمية.

المطلب الأول: الجهود الأوروبية في مواجهة الجرائم السيبرانية

المطلب الثاني: الجهود العربية في مواجهة الجرائم السيبرانية.

المبحث الأول

الجهود الدولية في مكافحة الجرائم السيبرانية

أصبح انتشار المنظمات الدولية والإقليمية، وشمول نشاط هذه المنظمات لمعظم ميادين الحياة الدولية، السمة البارزة والأساسية المميزة للمجتمع الدولي، كما أسهم تمتع المنظمات الدولية بالشخصية القانونية وتمتعها بإرادة ذاتية ومستقلة في المجتمع الدولي في ثبوت أهليتها للدخول في علاقات دولية مختلفة وقيام نوع من التنسيق والارتباط بين المنظمات الدولية ذات النشاط المتخصص والمنظمات العامة[١].

وبناء على ما تقدم سنقوم بتقسيم هذا المبحث إلى مطلبين، حيث سنتناول في المطلب الأول دور منظمة الأمم المتحدة في مكافحة الجرائم السيبرانية، أما في المطلب الثاني سنتناول دور المنظمات والوكالات الدولية في مكافحة الجرائم السيبرانية.

المطلب الأول

دور منظمة الأمم المتحدة في مكافحة الجرائم السيبرانية

إن البعد الدولي للإنترنت والسلامة والثقة في الفضاء السيبراني، يتطلب استجابة جماعية على نطاق دولي، فالتنازع المتصور بين عالمية الجريمة وبين إقليمية تطبيق النصوص القانونية، واقتصار البعض منها على نطاق دولة معينة، أمر يفرض استجابة دولية، فقد جرى نقاش في أكثر من مرة حول تبني اتفاقية دولية من قبل الأمم المتحدة لمكافحة الجريمة السيبرانية، من خلال وضع صك دولي جديد، منها مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية الذي انعقد في بانكوك ٢٠٠٥، لما للإطار العالمي الموحد من أهمية في مكافحة تلك الجرائم، فضلاً عن مستوى التمثيل، والإلزام للقواعد القانونية إن انطلقت من منصة الأمم المتحدة، إلا إن الدعوات لنص عالمي جوبهت بالرفض للأسباب التالية[٢]:

– إن وضع نص دولي يستغرق وقتاً طويلاً والجريمة السيبرانية تتطلب مواجهة عاجلة وليست آجلة لما تمثله من تهديد على الصعيد العالمي.

– وجود اتفاقية متعددة الأطراف اعتمدتها لجنة وزراء مجلس أوربا اتفاقية بودابست، وهي بحاجة إلى مزيد من الوقت لتقييم فوائدها.

---

[١] كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، الطبعة الأولى، منشورات الحلبي الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠٢١، ص ٣٣.

[٢] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٨، ص ٤٣.

– إن التدابير العملية للحد من الجريمة وتعزيز التعاون الدولي هي من يجب أن تولى الأولوية العليا في الوقت الحاضر[١].

فإن الفجوة الرقمية بين البلدان النامية والبلدان المتطورة تكنولوجيا، تقف عائقاً حول تبني صكاً دولياً وما يتبع ذلك من إمكانيات أجهزة إنفاذ القانون وتشريعات قانونية تواكب التطور التقني، وعلى ضوء ذلك سنتطرق الى قرارات الجمعية العامة المعنية بالجرائم السيبرانية في الفرع الاول وجهود المجلس الاقتصادي والاجتماعي للأمم المتحدة في مواجهة الجرائم السيبرانية في الفرع الثاني :

الفرع الاول: قرارات الجمعية العامة المعنية بالجرائم السيبرانية

أنشأت الأمم المتحدة أول مكتب لها لمكافحة الجريمة الدولية في ١٩٤٨، أما اليوم فتتمتع الأمم المتحدة بمكانة جيدة للغاية للعب دور منظمة محايدة يمكن لجميع بلدان العالم، أن تعمل بها في معالجة المشاكل العابرة للحدود ذات الأهمية المتزايدة، مثل تلك التي تمثلها الجريمة المنظمة عبر الوطنية، على مستوى الأمم المتحدة، صدرت عدة قرارات من منظمة الأمم المتحدة في مجالات متعددة تتعلق بإساءة استخدام التكنولوجيا والتقنيات، نظراً لتشعب الجريمة السيبرانية وصلاتها بجرائم أخرى كالإرهاب والاتجار بالبشر، وسنتناول أهم القرارات الصادرة من الجمعية العامة في مواجهة الجرائم السيبرانية على النحو الآتي[٢]:

١_ قرار الجمعية العامة للأمم المتحدة ١٢١/٤٥:

صدر قرار الجمعية العامة بعد المؤتمر الثامن المعني بمنع الجريمة ومعاملة المجرمين الذي عقد في كوبا/هافانا في عام ١٩٩٠، إذ اعتمدت قرار يدعو الحكومات إلى الاسترشاد بالسياسات الذي عقد في وقت سابق من ذلك العام، ودعى القرار الدول الأعضاء في الأمم المتحدة إلى التأكد من أن قوانينها الجنائية كافية للتعامل مع الجريمة السيبرانية[٣].

٢_ قرار الجمعية العامة للأمم المتحدة ٦٣/٥٥:

في عام ٢٠٠٠، اعتمدت الجمعية العامة للأمم المتحدة قراراً بشأن إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، وفيه شيء من التماثل مع المبادئ العشرة التي أعلنتها مجموعة السبعة G7 عام

---

[١] جيل برعام، تأثير تطور التكنولوجيا الحرب السبرانية على بناء القوة في إسرائيل، مؤسسة الدراسات الفلسطينية، فلسطين، ٢٠١٣، ص ٥٥.

[٢] سليم عبدالله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ص٧٥.

[٣] قرار الجمعية العامة للأمم المتحدة، رقم ١٢١/٤٥، أنظر الوثيقة رقم A/RES/121/45، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٢٠٢٤/١/٢

١٩٩٨، وقد حدد القرار عدداً من التدابير الرامية إلى منع إساءة استعمال التكنولوجيا في الفقرة (١) وهي:

أ- ينبغي للدول، أن تكفل عدم توفير قوانينها وممارساتها ملاذاً أمناً للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية، ينبغي أن تنسق جميع الدول المعنية التعاون في مجال إنفاذ القانون، لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية[١].

ب-ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها، في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وينبغي تدريب العاملين في مجال إنفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

ج-ينبغي للنظم القانونية أن تحمي سرية البيانات، ونظم الحواسيب وسلامتها وتوافرها، من أي عرقلة غير مأذون بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية، ينبغي للنظم القانونية أن تسمح بحفظ البيانات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعان الحصول عليها، وينبغي لنظم المساعدة المتبادلة أن تضمن التحقيق في الوقت المناسب، في إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

د- جمع الأدلة في مثل هذه الحالات وتبادلها في الوقت المناسب، ويتوجب عليه توعية عامة الناس بضرورة منع إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية ومكافحتها، ينبغي قدر الإمكان، تصميم تكنولوجيا المعلومات بطريقة تساعد على منع إساءة الاستعمال والكشف عنها، وتعقب المجرمين وجمع الأدلة، وتقتضي مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وضع حلول تأخذ في الاعتبار حماية حريات الأفراد.

ثانياً_ قرار الجمعية العامة للأمم المتحدة ١٢١/٥٦:

في عام ٢٠٠٢، اعتمدت الجمعية العامة للأمم المتحدة قراراً آخراً بشأن إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، ويشير القرار إلى النهج الدولي وحلول متنوعة لمكافحة الجرائم السيبرانية، ويؤكد على ضرورة التعاون بين الدول لمكافحة الجرائم، كما إن القرار يسلط الضوء على دور الأمم المتحدة والمنظمات الدولية والإقليمية في مكافحة هذه الجرائم[٢].

---

[١] عبدالله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧، ص ٢٤.

[٢] قرار الجمعية العامة للأمم المتحدة، رقم ١٢١/٥٦، أنظر الوثيقة رقم A/RES/121/56، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٢٠٢٤/١/٣.

ثالثاً_ قرار الجمعية العامة للأمم المتحدة ٢٣٩/٥٧:

في عام ٢٠٠٢ اعتمدت الجمعية العامة قراراً آخراً يهدف القرار إلى إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي، فقد ورد فيه[١]:

أ– تحيط علماً بالعناصر المرفقة بهذا القرار بهدف إنشاء ثقافة عالمية لأمن الفضاء الحاسوبي.

ب– تدعو جميع المنظمات الدولية ذات الصلة أن تراعي من جملة أمور، هذه العناصر المتعلقة بإنشاء، مثل هذه الثقافة في أية أعمال مقبلة بشأن أمن الفضاء الحاسوبي.

ج– تدعو الدول الأعضاء إلى أن تراعي من جملة أمور، هذه العناصر في جهودها المبذولة لتنمية ثقافة أمن الفضاء الحاسوبي في تطبيق واستخدام تكنولوجيا المعلومات، على صعيد المجتمع بكامله.

رابعاً_ قرار الجمعية العامة للأمم المتحدة ١٩٩/٥٨:

في عام ٢٠٠٣ اعتمدت الجمعية العامة للأمم المتحدة هذا القرار[٢]، والذي جاء كسابقة دون التطرق إلى الجريمة السيبرانية، وتمركز حول إرساء ثقافة عالمية لحماية الفضاء السيبراني وحماية الهياكل الأساسية للمعلومات، ويدعو الدول والمنظمات الدولية للحفاظ على العناصر الأساسية لحماية الهياكل الأساسية للمعلومات في أي إعمال مستقبلية تتعلق بأمن الفضاء السيبراني.

خامساً_ قرار الجمعية العامة للأمم المتحدة ١٧٧/٦٠:

صدر في بانكوك بتايلاند، واعتمد إعلان بانكوك الذي سلط الضوء على ضرورة تنسيق القوانين لمكافحة الجرائم السيبرانية. وقد جاء القرار ٦٠/١٧٧ يؤيد هذا الإعلان، الذي شجع الجهود المبذولة من قبل المجتمع الدولي الرامية إلى تعزيز التعاون القائم لمنع الجرائم السيبرانية، ودعا إلى مواصلة تقديم المساعدة إلى الدول الأعضاء في مجال مواجهة الجرائم السيبرانية تحت مظلة الأمم المتحدة وبشراكة منظمات مشابه[٣].

سادساً: قرار الجمعية العامة للأمم المتحدة ٢١١/٦٤:

---

[١] قرار الجمعية العامة للأمم المتحدة، رقم ٢٣٩/٥٧، أنظر الوثيقة A/RES/239/57 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٣/١/ ٢٠٢٤.

[٢] قرار الجمعية العامة للأمم المتحدة، رقم ١٩٩/٥٨، انظر الوثيقة رقم A/RES/199/58، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٤/١/ ٢٠٢٤.

[٣] قرار الجمعية العامة للأمم المتحدة، رقم ١٧٧/٦٠، انظر الوثيقة رقم A/RES/177/60 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٤/١/٢٠٢٤

في عام ٢٠١٠ أصدرت الجمعية العامة للأمم المتحدة[١]، قرار جديد لإرساء ثقافة عالمية للأمن السيبراني ودعى البلدان إلى استعراض وتحديث الهيئات والقوانين المتعلقة بالجرائم السيبرانية، وحماية البيانات والخصوصية والقانون التجاري، والتوقيع الرقمي والتشفير.

سابعاً_ قرار الجمعية العامة للأمم المتحدة ١٧٠/٧٠ والقرار ١٠٩/٧١:

في عام٢٠١٥ و٢٠١٦ على التوالي، اعتمدت الجمعية العامة للأمم المتحدة قرارين حول مؤتمر الأمم المتحدة لمنع الجريمة وتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية لاسيما قدراته في مجال التعاون التقني، كما أثنت على جهود الفريق الدولي المفتوح حول دراسة مشكلة الجرائم السيبرانية والتدابير الذي يتخذها المجتمع الدولي والقطاع الخاص لمواجهتها وطلب من الدول الأعضاء توفير بيئة إلكترونية متينة وأمينة لمنع ومكافحة الأنشطة الإجرامية على الإنترنت[٢].

الفرع الثاني: جهود المجلس الاقتصادي والاجتماعي للأمم المتحدة في مواجهة الجرائم السيبرانية

لعب المجلس الاقتصادي والاجتماعي دوراً في مجال مواجهة الجرائم السيبرانية، من خلال الوظائف المشار إليها في المادة (٦٢) من الميثاق، التي خولته إجراء الدراسات فيما يتعلق بالاقتصاد الدولي وكذلك التوصيات الخاصة بتعزيز احترام ومراعاة حقوق الإنسان الأساسية، فضلاً عن صياغة الاتفاقات فيما يدخل ضمن نطاق اختصاصه وعقد المؤتمرات الدولية، وسنتناول أهم المؤتمرات التي تناولت الجريمة السيبرانية، باعتبار هذه المؤتمرات من مسؤولية برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، وهذه المؤتمرات هي:

١_ مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين:

جرت وقائع المؤتمر في فيينا عام ٢٠٠٠، وقد أثير موضوع الجرائم المتصلة بالأنترنت في ورشة عمل خاصة، وقد ركزت النقاشات على فئات الجريمة والتحري عنها عبر الحدود والاستجابة القانونية لها، وقد تمخض عن ورشة العمل استنتاجات مهمة وأساسية في معالجة الجريمة السيبرانية، وتتلخص بالآتي ضرورة وضع قواعد تشريعية تجرم الأفعال السيبرانية ولابد إلى جانب التشريعات الموضوعية وجود تشريعات إجرائية توازيها، وسلط الضوء على ضرورة بناء قدرات لمكافحة الجريمة[٣].

---

[١] قرار الجمعية العامة للأمم المتحدة، رقم ٢١١/٦٤، انظر الوثيقة رقم A/RES/211/64 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/ تاريخ الزيارة ٢٠٢٣/١/٤ .

[٢] قرار الجمعية العامة للأمم المتحدة، رقم ١٧٠/٧٠، أنظر الوثيقة رقم A/RES/170/70، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/. تاريخ الزيارة ٢٠٢٤/١/٥.

[٣] علي محمد علي كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، لبنان، ٢٠١٩، ص ١١٢.

٢_ مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية:

في عام ٢٠١٠، وفي البرازيل تحديداً تم مناقشة الجرائم السيبرانية، ودعت الاجتماعات التحضيرية الإقليمية الأربعة للمؤتمر والخاصة بأمريكا اللاتينية ومنطقة غرب آسيا ومنطقة آسيا والمحيط الهادي وإفريقيا، فضلاً عن أوساط أكاديمية، إلى عقد اتفاقية دولية لمكافحة الجرائم السيبرانية[١].

٣_ مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية:

في عام ٢٠١٥ عقد في الدوحة المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية، وقد أكد هذا المؤتمر الدعوات في الاجتماعات التحضيرية الأربعة، لاتفاقية دولية والمناقشات التي جرت بشأن الجريمة السيبرانية.

نستخلص مما تقدم: إن تقدم التكنولوجيا والاتصالات الدولية لها تأثير كبير في تطور القانون الدولي، من خلال نشر اعمال المنظمات الدولية والقرارات والمؤتمرات، فالمؤتمرات التي تعقدها الأمم المتحدة لها أثار مهمة في تطور قواعد القانون الدولي، وإضفاء الطابع العالمي عليها.

المطلب الثاني

دور المنظمات والوكالات الدولية في مكافحة الجرائم السيبرانية

تنشط العديد من المنظمات والوكالات الدولية في مكافحة الجرائم السيبرانية، وانسجاماً مع خطة البحث سيتم تناول جهود منظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للاتصالات في الفرع الاول و المنظمة العالمية للملكية الفكرية في الفرع الثاني [٢]:

الفرع الاول: منظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للاتصالات:

تعتبر هذه المنظمة أول منظمة تطلق تحقيقاً شاملاً بشأن مشاكل الجرائم السيبرانية في الساحة الدولية والمنظمة لا تعمل بشكل مباشر على الجريمة السيبرانية في حد ذاتها، بل تركز بشكل أكبر على الأمن السيبراني، وتعزل نهجا سياسيا منسقا عالميا لبناء الثقة في الفضاء السيبراني، إذ يقوم فريق عمل منظمة التعاون الاقتصادي والتنمية (OECD) المعني بالمعلومات والخصوصية (WISP) بتطوير المبادئ التوجيهية الدولية.

---

[١] محمود مدين عبد الرحمن، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧، ص ١٠٧.

[٢] محمود مدين عبد الرحمن، الجريمة الإلكترونية وتحديات الأمن القومي، المرجع السابق نفسه، ص ١١٠.

يشمل نطاق الإرشادات الأشخاص الطبيعيين فقط، وينطبق على كل من القطاعين الخاص والعام ويتضمن معالجة البيانات الآلية وغير الآلية، إذ تتعلق النقاط الثمانية الرئيسية للمبادئ التوجيهية بمبادئ الحد من التحميل وجودة البيانات، ومواصفات الأغراض، والحد من الاستخدام، والضمانات الأمنية والانفتاح والمشاركة الفردية، والمساءلة فيما يتعلق بالتطبيق الدولي القوانين الخصوصية، إن المبادئ التوجيهية وقد أيدت جميع الدول الأعضاء في المنظمة هذه المبادئ التوجيهية في الميدان الاقتصادي[١].

قد قامت منظمة التعاون الاقتصادي والتنمية، بتأليف مجموعة من الخبراء لمناقشة القضايا القانونية التي طرحتها الجريمة السيبرانية، واستنادا إلى نتائج هذا الاجتماع، تم تكليف الخبراء بإعداد دراسة لمدة عامين، مع التركيز على إمكانية التنسيق وتدويل القوانين الوطنية للجرائم السيبرانية، في عام ١٩٨٦ أصدرت منظمة التعاون الاقتصادي والتنمية تقرير يلخص نتائج الدراسة بعنوان الجرائم المتعلقة بالحاسوب و تحليل السياسة القانونية، بالرغم من إن التقرير قد حدد الحد الأدنى من جرائم الحاسوب التي تضر الدول، إلا انه غير ملزم، وتكمن أهميته في انه يمنح الدول الوقت لاعتماد سياسة جديدة وتطويع قوانينها بإرادتها لكي تتقيد فيها الدول، في محاولة لفرض قواعد دولية بدون استياء وردود فعل فيما لو فرض عليهم بشكل ملزم.

إن النهج الذي اتبعته منظمة التعاون الاقتصادي والتنمية في هذه المبادرة، هو نفس النهج الذي أتبعته الجهود الأوروبية الأخرى لمكافحة الجريمة عبر الوطنية، من خلال التأكد من أن أكبر عدد ممكن من الدول يحظر مجموعة أساسية من الجرائم السيبرانية، وقد اعتمدت منظمة التعاون والتنمية في الميدان الاقتصادي، في عام ٢٠٠٢، ومبادئ توجيهية جديدة لأمن نظم وشبكات المعلومات نحو ثقافة الأمن وهذا النهج لحماية البنية التحتية للمعلومات الهامة في مبدأ توجيهي غير ملزم للدول الأعضاء[٢].

كذلك تعاونت منظمة التعاون والتنمية في الميدان الاقتصادي والبنك الدولي، في تنظيم ورشة عمل بشأن ترابط السياسات في تطبيق تكنولوجيا المعلومات والاتصالات لأغراض التنمية، وفيما يتعلق بالاستنتاج الرئيس للاعتبارات الأمنية، بينت ورشة العمل أن التحديات الرئيسة تتضمن نهجاً وطنياً منسقاً، ونقصاً في تنفيذ أفضل الممارسات القائمة ونقص التعاون عبر الحدود، وتطول قائمة جهود منظمة التعاون الاقتصادي والتنمية في مكافحة الجريمة السيبرانية، والتي كان آخرها مؤتمرا في شباط ٢٠١٨، الذي تم

---

[١] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، المرجع السابق، ٧٥.

[٢] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠، ص٨٢.

فيه مناقشة المعوقات التي تعيق سوق التأمين السيبراني، وورشة عمل حول الأمن الرقمي والمرونة في البنية التحتية الحيوية والخدمات الأساسية[١].

من كل ما تقدم يتضح، بأن منظمة التعاون الاقتصادي والتنمية تشتهر بقانونها الناعم، وهي عبارة عن أدوات غير ملزمة، حول مجموعة متنوعة من قضايا السياسة العامة الصعبة التي لها تأثير عالمي، ومنها مواجهة إساءة استخدام الفضاء السيبراني، وتهدف في أعمالها إلى توليد إجماعاً سريعاً على القضايا السياسية والتنظيمية الصعبة مثل تلك المتعلقة بالتشفير، الخصوصية، حماية البيانات، حماية المستهلك، وأمن أنظمة المعلومات، وبالرغم من أن نشاط المنظمة لا ينصب بشكل مباشر على الجريمة السيبرانية إلا إنها تدعم الأمن السيبراني وتعزز حماية الخصوصية والبيانات الشخصية، الأمر الذي يبلور مواقف وسياسات عالمية موحدة في مواجهة الجريمة السيبرانية.

الاتحاد الدولي للاتصالات:

في القمة العالمية لمجتمع المعلومات الذي عقد على مرحلتين في جنيف في بسويسرا عام ٢٠٠٣، وفي تونس عام ٢٠٠٥، كلف رؤساء الدول وزعماء العالم الاتحاد الدولي للاتصالات، بتنفيذ خطة عمل جنيف الرامية إلى مكافحة الجريمة السيبرانية، التي وردت في الفقرة (٥) المتعلقة ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وتم معالجة الجريمة السيبرانية في القمة العالمية لمجتمع المعلومات في تونس ٢٠٠٥، من خلال التأكيد على ضرورة التعاون الدولي في مكافحة الجريمة السيبرانية، فقد أطلق الاتحاد في عام ٢٠٠٧، البرنامج العالمي للأمن السيبراني كإطار للتعاون الدولي في هذا المجال، وعلى وجه الخصوص هذا البرنامج على سبعة أهداف، هي[٢]:

١ـ وضع استراتيجية لتطوير تشريعات نموذجية للجريمة السيبرانية، تكون قابله للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية والوطنية والدولية المعتمدة، وإنشاء وإقرار نموذج سياسة عامة واستراتيجيات وطنية لتطوير هياكل وطنية وإقليمية مناسبة للتعامل مع الجريمة السيبرانية.

٢ـ وضع استراتيجية لتحديد الحد الأدنى المقبول عالمياً، في موضوع معايير الأمن ونظم تطبيقات الأنظمة والبرامج، مع وضع إطار عمل للمراقبة والتحذير والاستجابة للحوادث[٣].

---

[١] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ٢٠٠٠، ص٩١.

[٢] يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص١٩٢.

[٣] منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٥، ص ٢٤٢.

٣-إنشاء وإقرار إطار عام عالمي لنظام هوية رقمية وتطبيقه، وتحديد هياكل لضمان الاعتراف بالوثائق الرقمية للإفراد عبر الحدود الجغرافية، وتطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية، والقدرات المؤسسية، لتعزيز المعرفة والدراية في جميع القطاعات وفي جميع المجالات المعلوماتية.

ومن أجل وضع استراتيجيات بشأن الأهداف السبعة البرنامج العالي للأمن السيبراني، شكل الأمين العام للاتحاد مجموعة من الخبراء رفيعي المستوى متخصصين في الأمن السيبراني، ويقدم هذا التقرير لمحة عامة عن الأساليب الإقليمية والدولية لمكافحة الجريمة السيبرانية، وفكرة عامة عن أحكام القوانين الجنائية والمسائل الإجرائية واللوائح التي تحدد مسؤولية موردي خدمات الانترنت والحقوق الأساسية لمستخدمي الانترنت[١].

وقد اعتمد الاتحاد الدولي العديد من القرارات بشأن الأمن السيبراني وذات صلة بنفس الوقت بالجريمة السيبرانية، منها: القرار ١٤٩ في انطاليا، ٢٠٠٦، بشان دراسة التعريفات والمصطلحات المتعلقة بالأمن السيبراني، والقرار ٤٥ الدوحة ٢٠٠٦، للمؤتمر الخاصة بتنمية الاتصالات العالمي بشان تعزيز التعاون في مجال الأمن السيبراني، والقرار ٥٠ جوهانسبرغ ٢٠٠٨، للجمعية العالمية لتقييس الاتصالات بشأن الأمن السيبراني، والقرار ٥٢ جوهانسبرغ ٢٠٠٨، لنفس الجمعية بخصوص الرسائل الاقتحامية، والقرار ٥٨ جوهانسبرغ ٢٠٠٨ بشأن تشجيع انشاء فرق استجابة وطنية للحوادث السيبرانية[٢].

وهذه القرارات ليست بمستوى المعاهدات، لذلك فهي لا تلزم الدول الأعضاء كما تفعل المعاهدة، ويمكن للقرارات، من حيث المبدأ، أن تلزم الدول الأعضاء إذا نص حكم تعاهدي على أن القرار ملزم، أو إذا كان القرار يتعلق بمسائل إجرائية داخلية للاتحاد الدولي للاتصالات (مثل المواعيد النهائية لتقديم الوثائق)، هذا وقد وقع الاتحاد الدولي للاتصالات ومكتب الأمم المتحدة المعني بالمخدرات والجريمة على مذكرة تفاهم بشأن الجريمة السيبرانية في عام ٢٠١١، لغرض بناء القدرات والمساعدة التقنية والتدريب وورش العمل المشتركة.

الفرع الثاني: المنظمة العالمية للملكية الفكرية

---

[١] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١١، ص ٢٥٤.

[٢] علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، ايتراك للنشر والتوزيع، القاهرة، ٢٠١٥، ص٢٦١.

تعمل المنظمة العالمية للملكية الفكرية على حماية الحقوق الفردية الملكية الفكرية، ومن المهم الوقوف على بعض الاتفاقيات الدولية، بمناسبة الحديث عن الجهد العالمي المتعلق بحماية حقوق الملكية الفكرية، إذ توجد ثلاث معاهدات دولية وهي[١]:

١-معاهدة برن:

تعد معاهدة برن لحماية المصنفات الأدبية والفنية لعام ١٩٧١، الحجر الأساس لحماية حق المؤلف، إذ تمنح للمؤلف حقا استئثارياً بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان، فضلاً عن ترخيص أو منع أي ترجمة او اقتباس أو بث أو توصيل إلى الجمهور، كذلك تلزم الاتفاقية بتوقيع جزاءات سواء كان المعتدى عليه وطنياً أم أجنبياً، وتستند هذه الاتفاقية، في مجملها إلى اتفاقية برن لحماية المصنفات الأدبية والفنية التي أبرمت في ١٨٨٦، واتفاقية المجالات المتعلقة بالتجارة في حقوق الملكية الفكرية هي أهم الاتفاقيات الثمانية والعشرين التي وقعت عليها الدول الموقعة على اتفاقية الجات[٢].

٢-معاهدة تربس:

تصيغ معاهدة تريبس ١٩٩٤، أيضاً الحماية على الملكية الفكرية، خصوصاً مع انتشار عمليات السطو الإلكتروني على الأعمال الفنية دون ترخيص من مالكيها، وفيها العديد من التدابير والمعالجات، ومنها على سبيل المثال: إعطاء الحق للسلطات في إصدار أوامر لشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة، والتحفظ على أدوات ارتكاب الجرائم، فضلاً عن فرض عقوبات جنائية، ويمكن القول أن اتفاقية تريس أضفت حماية دولية جنائية لبرامج الحاسوب والملكية الفكرية.

٣-معاهدة الويبو:

تعتبر اتفاقية الويبو بشأن حق المؤلف ١٩٩٦، اتفاقاً خاصاً في إطار اتفاقية برن وتحديداً لها، وقد دخلت حيز النفاذ في عام ٢٠٠٢، وقد قامت المنظمة العالمية للملكية الفكرية بإصدارها لتسهيل التطبيقات العالية للاتصالات الرقمية المباشرة عبر البنية الأساسية العالمية للمعلومات، وتتيح احكام الاتفاقية للأعضاء نقل القيود والاستثناءات الواردة، في قوانينهم الوطنية التي تعتبر مقبولة بموجب اتفاقية بيرن إلى الفضاء السيبراني.

---

[١] محمد علي العريان، الجرائم المعلوماتية، المرجع السابق، ص ٢٥٨.

[٢] منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، المرجع السابق، ص ٢٤٤.

يتضح مما تقدم: إن اتفاقية الويبو، تضفي الحماية على برامج الحاسوب وقواعد البيانات، والمصنفات الفنية والأدبية، وتحمي حقوق المؤلف فيها، من خلال إلزام الدول الأعضاء بتشريع قوانين تحوي على جزاءات فعالة لأي تعدي على هذه المصنفات، سواء كان هذا التعدي باستخدام التعامل للاستفادة من هذه المصنفات، أو حذف أو تغيير أو توزيع أو إذاعة المصنفات أو نقلها إلى الجمهور، مما يخلق موجة تشريعية دولية تجاه هذا النوع من الجرائم خصوصاً إذا ما علمنا بانضمام ٩٨ دولة إلى هذه الاتفاقية

المبحث الثاني

الجهود القانونية وأنشطة المنظمات الإقليمية

تتميز الجهود التشريعية الإقليمية المتعلقة بمختلف القضايا ومنها الجرائم السيبرانية بالوضوح ورسم الأطر والسياسات الدولية بطريقة أسرع، بسبب كونها تشمل نطاقاً جغرافياً معيناً محدوداً من الدول، متصلة بالعلاقات الدولية، نتيجة لذلك المسافة ووحدة التهديدات والشواغل، وفي بعض الأحيان قد تستفيد الدول في بعض أجزاء العالم من عضوية صكوك دولية ملزمة معنية بمكافحة الجرائم السيبرانية، بما في ذلك عضوية بعض الدول في أكثر من اتفاقية دولية[١].

وبناء على ما تقدم سنقوم بتقسيم هذا المبحث إلى مطلبين، حيث سنتناول في المطلب الأول الجهود الأوروبية في مواجهة الجرائم السيبرانية، أما في المطلب الثاني سنتناول الجهود العربية في مواجهة الجرائم السيبرانية.

المطلب الأول

الجهود الأوروبية في مواجهة الجرائم السيبرانية

تلعب المنظمات الدولية دوراً مهماً على المستوى العالمي، فضلاً عن عدد من المنظمات الإقليمية التي تركز عملها على مناطق محددة، باستثناء أن عدداً منها لديها أنشطة تتعامل مع القضايا المتعلقة بالجريمة السيبرانية، ويعد المجلس الأوربي، من أقدم المنظمات السياسية الأوربية، وفي عملها يغطي جميع المجالات السياسية عدا الدفاع، أما الاتحاد، فلديه قدرة محدودة على التشريع في مجال القانون الجنائي، والذي بعد رمزاً لسيادة الدولة، ولأن الاتحاد منظمة تجارية، وبالنظر إلى أن الجريمة السيبرانية تقف كعقبة أمام التجارة بين الدول الأعضاء، يتخذ الاتحاد الأطر القانونية لمواجهتها، ووعليه سنبحث الجهود الأوربية في مواجهة الجرائم السيبرانية في فرعين سنتطرق الى اتفاقية المجلس الاوربي بودابست

[١] كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، مرجع سابق، ص٤٢.

٢٠٠١ في الفرع الاول و قرارات الاتحاد الأوربي ذات الصلة بمكافحة الجرائم السيبرانية في الفرع الثاني.[١]:

الفرع الاول: اتفاقية المجلس الأوروبي بودابست ٢٠٠١

اتفاقية بودابست لعام ٢٠٠١ أهم صك دولي في مكافحة الجرائم السيبرانية، على مستوى العالم، وفي أوربا على وجه الخصوص، والسبب في إبرام الاتفاقية، يتمثل في الحاجة إلى اتخاذ تدابير قانونية تشريعية لمكافحة الجرائم السيبرانية في ظل الاعتماد على تكنولوجيا المعلومات والنمو الحاصل في أنظمة الحاسوب وتدفق المعلومات، فضلاً عن أهمية مكافحة الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الحاسوب وهي سرية وسلامة المحتوى وتوفر المعلومات والنظم[٢]، وسنتحدث عن واقع الاتفاقية على النحو الاتي:

اولاً: نبذة تاريخية عن أنشطة مجلس أوربا

إن من المهم اخذ لمحة عامة عن أنشطة المجلس في أوربا، في مواجهة الجرائم السيبرانية، ففي عام ١٩٧٦، عقد مجلس أوربا مؤتمراً تناول فيه الطبيعة الدولية لجرائم الحاسوب، وقد ناقشها بشكل مستمر في جدول الإعمال، وفي عام ١٩٩٦ قررت اللجنة الأوربية لمشكلات الجريمة إنشاء لجنة لمعالجة الجرائم السيبرانية، وخلال ثلاثة أعوام عقدت هذه اللجان عشرات الاجتماعات، تكللت باعتماد الجمعية مشروع اتفاقية بودابست في نيسان عام ٢٠٠١، والذي فتح باب التوقيع عليها في تشرين الثاني من نفس العام[٣].

ثانياً: أحكام اتفاقية بودابست

تعد معاهدة بودابست هي أبرز مثال على التعاون في الفضاء السيبراني لمواجهة التهديدات والجرائم السيبرانية، إنها الاتفاقية الدولية الملزمة المتعددة الأطراف في مجال مكافحة الجريمة السيبرانية، تم فتحه للتوقيع عليها في عام ٢٠٠١ ودخلت حيز التنفيذ عام ٢٠٠٤، إذ بدأت حتى الآن ٥٠ دولة، من داخل وخارج الاتحاد الأوربي بالاتفاق عليها، وصدقت من قبل ٤٠ دولة، من بينها الولايات المتحدة الأمريكية وكندا واليابان، وقد أسهمت هذه الاتفاقية في وضع أطر تشريعية لمكافحة الجرائم السيبرانية[٤]، وفي نفس

---

[١] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مرجع سابق، ص٩٤.

[٢] علي محمد علي كاظم الموسوعي، المشاركة المباشرة في الهجمات السيبرانية، المرجع السابق، ص١٢٨.

[٣] عبدالله عبد الكريم عبدالله، جرائم المعلوماتية والأنترنت، المرجع السابق، ص ١٠٩.

[٤] نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية، الطبعة الأولى، المكتب العربي للمعارف، القاهرة، ٢٠١٦، ص٣٧.

الوقت أظهرت مدى إدراك الدول لتهديدات الجريمة على الأمن السيبراني، وضرورة التصدي لأبرز التهديدات وإشكالها[١].

حيث أن أهداف الاتفاقية، واضحة من ديباجاتها، حيث ركزت على حماية المجتمع من الجرائم السيبرانية، وضرورة وقاية المصالح العامة المشروعة عند استعمال وتبلور تكنولوجيا المعلومات، كذلك ضمان التوازن بين مصالح إنفاذ القانون واحترام حقوق الأساسيات، ومنها الحق في الخصوصية والحق في حرية التعبير، من خلال اعتماد التشريعات المناسبة لمنع الأعمال الموجهة ضد سرية وسلامة وتوفر نظم الحاسوب، والشبكات والبيانات ودعم وتعزيز التعاون الدولي في المسائل الجنائية.

ثالثاً: البروتوكول الإضافي الأول بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق نظام الحاسوب

وتبين خلال المفاوضات إن تجريم العنصرية وتوزيع المواد المعادية للأجانب، من القضايا المثيرة للجدل، فيما يتعلق بحرية التعبير، حيث تتمتع في بعض الدول يحظى بحماية قوية، الأمر الذي أثار مخاوف من عدم انضمام بعض الدول، لذلك بعد الاتفاقية، تم وضع البروتوكول الإضافي الأول في عام ٢٠٠٣، واتفاقية بشأن حماية الأطفال من الاستغلال الجنسي في عام ٢٠٠٧.

رابعاً: الاستنتاجات

رغم أهمية الاتفاقية على المستوى الإقليمي والدولي، باعتبارها عملاً دولياً يقوم على إيجاد لغة فهم مشتركه للجرائم السيبرانية، عبر إنشاء شكل كحد أدنى مشابه لهذه الجرائم، إلا ان المعاهدة غير ملزمة لكل دول الاتحاد الأوربي بشأن الموافقة على المعاهدة وتنفيذها، ويرى المجلس الأوربي ذاته أن المعاهدة صارت قديمة، اذ لم يكن هناك استعمال الارهابين للأنترنت، والهجمات الروبوتية، والتصيد الاحتيالي عند إنشاء المعاهدة، إلا أن المعاهدة تعتبر الكيان الأساسي لأي عمل دولي تلاها، ومثال تشريعي يؤخذ به عند إنشاء أي تشريع وطني غايته مكافحة الجرائم السيبرانية، للمضمون الذي يعكس عملاً دولياً و حوارات خبراء مختصين في مواضيع الأمن والجريمة في الفضاء السيبراني[٢].

الفرع الثاني: قرارات الاتحاد الأوربي ذات الصلة بمكافحة الجرائم السيبرانية

---

[١] حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الأولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٧، ص ٤٩.

[٢] بهاء شاهين، شبكة الأنترنت، الطبعة الثانية، العربية لعلوم الحاسبات، القاهرة، ٢٠٠١، ص ٥٣.

إن الاحكام المتضمنة عمل تشريعي ينبثق من الاتحاد الأوربي في نطاق التشارك الجنائي والقضائي في القضايا الجنائية، وهي ايضاً تجبر الأعضاء بتحقيق الخلاصة، دون أن تعطيهم وسائل إنجازها وطنياً، وليس لها أثر مباشر على الدول الأعضاء، أما بالنسبة للقرارات التي صدرت في نطاق أوربا فيما يهم الجريمة السيبرانية فهي التالية:

اولاً: القرار الإطاري للمجلس بشأن مكافحة استغلال الأطفال على الأنترنت في المواد الإباحية ٢٠٠٤

في عام ٢٠٠٤، تبنى المجلس القرار (٢٠٠٤/٦٨)، للتصدي لاستغلال الأطفال على شبكة الانترنت وقد تضمن أحكاماً تمنع تبادل الصور الخاصة عبر الأنترنت، وقد سبق للمجلس الأوربي في عام ٢٠٠٠، أن تبنى القرار (٢٠٠٠/٣٧٥)، للتصدي لاستغلال الأطفال على شبكة الأنترنت، وفي وقت سابق في عام ١٩٩٦ صدر بيان بخصوص المضمون الغير قانوني والضار على شبكة الحاسوب، علماً انه تم تغير القرار بتوجيه (٢٠١١/٩٢)، بخصوص استغلال الأطفال في المواد الإباحية ٢٠١١.

ثانياً: القرار الخاص بمكافحة الاحتيال

في عام ٢٠٠١، تبنى المجلس الأوربي قراراً يواجه الجريمة السيبرانية بصورة مباشرة، عبر القرار الإطاري (٢٠٠١/٤١٣)، بشأن مكافحة الاحتيال وتزوير وسائل الدفع غير النقدية، فقد فرض المجلس مهام بشأن تنسيق القانون الجنائي فيما يهم أطراف معينة من الاحتيال المتصل بالحاسوب والبرامج الخاصة بالحاسوب، التي تستخدم لارتكاب الجرائم المشار عليها في القرار الإطاري[١].

ثالثاً: القرار بشأن الهجمات ضد أنظمة المعلومات ٢٠٠٥

تبنى المجلس في عام ٢٠٠٥، قراراً بخصوص الهجمات ضد أنظمة المعلومات، وهو ليس إعادة لما أتى في معاهدة بودابست لعام ٢٠١١، بل جاء ليكون مشتركاً مع المعاهدة، ويركز القرار على تنسيق الأحكام الجوهرية للقانون الجنائي وكذلك المرتبطة بالتعاون الدولي[٢].

رابعاً: القرار الخاص بمكافحة الإرهاب

غير المجلس الأوربي في عام ٢٠٠٨، القرار الإطاري بالإرهاب الذي وحد تعريف الجرائم الإرهابية في كافة دول الاتحاد الأوربي، وبنى أسساً لملاحقة قضائية فعالة لهذه الجرائم، وقد أتى هذا القرار فارغاً من تجريم استعمال الإرهابين للأنترنت في نشر الدعاية وخبراتهم في صنع القنابل، لذلك صدر القرار

---

[١] جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، مكتبة السنهوري، بغداد، ٢٠١٢، ص ٦٨.

[٢] أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٥، ص ٨٧.

الإطاري (٢٠٠٨/٩١٩)، لاتخاذ إجراءات لإغلاق هذه المشاكل وتقرب التشريعات الأوربية لإيقاف الإرهاب وجعل الأنظمة متناسبة مع معاهدة بودابست لعام ٢٠٠١، ويضم على وجه الخصوص الأحكام على الاستفزاز العام لارتكاب جريمة إرهابية[١].

خامساً:القرارات التوجيهية للاتحاد الأوربي ذات الصلة بالجرائم السيبرانية

عرفت التوصيات بأنها فئة من التدابير غير المرغمة الصادرة من منظمة دولية والموجهة إلى الدول الأعضاء بصدد قضية معينة، وبمعنى آخر إنها خطوط عامة توجه الدول الأطراف بشأن تنفيذ مهامها، ولكن في مجال الاتحاد الأوربي تضع التوجيهات تأثيراً مباشراً على الدول الأطراف، فهي ترغم الأعضاء بإنجاز المهام، وتترك لهم الطرق والوسائل طبقاً للأنظمة الداخلية للدول الأطراف.

أما بخصوص التوجيهات الصادرة من الاتحاد الأوربي، بخصوص السيبرانية وهي كالتالي:

أ_ التوجيه بشأن التجارة الإلكترونية عام ٢٠٠٠:

إن التوجيه (٢٠٠٠/٣١)، يعالج مسؤولية مورد خدمة الانترنت عن أعمال تقترفها أطراف ثالثة، ليتم إنشاء معايير قانونية لتأمين إطار، لأجل التنمية العامة لمجتمع المعلومات ودعم التنمية الاقتصادية بوجه عام، وكذلك أجهزة إنفاذ القانون[٢].

ب_ التوجيه بشأن الخصوصية:

هذا التوجيه تم تغيره لملاحقة التطورات في قضايا الخصوصية، الذي كانت الغاية منه وقاية خصوصية الاتصالات الإلكترونية، كما تضمن أمن الخدمات وسرية معلومات العميل، وقد تم مراجعته في عام ٢٠١٧، وتم طرح فكرة استبداله بقانون أفضل احتراماً للحياة الخاصة، وحماية البيانات الشخصية في البيانات الإلكترونية.

٦_ التوجيه بشأن الاحتفاظ بالبيانات عام ٢٠٠٦:

هذا التوجيه (٢٠٠٦/٢٤)، يشمل واجباً على موردي خدمات الانترنت، بحفظ بعض البيانات المتنقلة على شبكة الأنترنت، بغاية البحث عن مواقع الجناة في الفضاء السيبراني، وقد أثار هذا التوجيه مشكلة بخصوص وقاية الحق في الخصوصية، وقدم طعن بصدده إلى محكمة العدل الأوربية، والتي الغته منذ دخوله حيز التنفيذ.

---

[١] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص ٩٥.

[٢] عادل عبد صادق، أسلحة الفضاء الإلكتروني في ضوء القون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، ٢٠١٦، ص ١٠٣.

٧_ التوجيه بشأن الهجمات ضد نظم المعلومات:

يهدف هذا التوجيه (٢٠١٣/٤٠)، لحل الهجمات السيبرانية واسعة المجال عبر مطالبة الدول الأطراف بتعزيز القوانين الوطنية المتعلقة بجرائم الأنترنت، وتطبيق عقوبات جنائية أكثر صرامة[١].

٨_ التوجيه بشأن حماية البيانات الشخصية في ٢٠١٦:

ويهدف هذا التوجيه (٢٠١٦/٦٧٩)، إلى وقاية الأشخاص الطبيعيين، بما يتعلق بحل البيانات الشخصية، إذ بموجبه تم إلغاء التوجيه (٤٦/٩٥)، بالإضافة إلى تعزيز حرية نقل هذه البيانات ويهدف هذا التوجيه بالمساهمة في تحقيق نطاق من الحرية والأمن[٢].

مما تقدم يتبين تعدد الأدوات التشريعية في القارة الاوربية، فالاتفاقيات التي تصدر من مجلس الاتحاد في القضايا الجنائية والقرارات الإطارية والتوجيهات، التي تأتي من الاتحاد الأوربي، تعمل بأكملها على رسم سياسة جنائية وأطر قانونية في مواجهة الجرائم السيبرانية المنطوية، في مجلس أوربا والاتحاد الأوربي على حد سواء، الأمر الذي يدل على نضج المستوى التشريعي وتطوره ويوفر الأطر القانونية لمواجهة الجريمة السيبرانية إقليميا على مستوى القارة الأوربية، فضلاً عن أي استخدام غير مشروع للفضاء السيبراني، وقد استحدث القرار الإطاري جرائماً جديدة فيما يتعلق بالسلوكيات التي قد تؤدي إلى إعمال إرهابية، ووفر سنداً قانونياً لملاحقة نشر الدعاية الإرهابية، وتطوير المهارات الفنية للإرهابيين لصنع القنابل على شبكة الانترنت.

---

[١] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية للنشر والتوزيع، القاهرة، ٢٠٠٢، ص ١٠٩.

[٢] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١، ص ١٤٣.

المطلب الثاني

الجهود العربية في مواجهة الجرائم السيبرانية

إن تبلور الجريمة بشكل عام والجريمة السيبرانية بشكل خاص، آخذ في الازدياد على مستوى العالم، ومن الواضح أن مواجهة هذه الظاهرة بكفاءة وفعالية من أصعب الأمور في البلدان النامية، والبلدان التي في طور الانتقال[١]، والتي غالباً ما كانت عرضة للتغيرات السياسية والاجتماعية والاقتصادية سريعة مثل الدول العربية، وسنركز على الجهود الإقليمية في المجال التشريعي لمواجهة الجرائم السيبرانية في الوطن العربي على أهم الأطر التشريعية على النحو التالي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠ في الفرع الاول وسنتطرق الى التشريعات العربية الداخلية لمكافحة الجرائم السيبرانية في الفرع الثاني [٢]

الفرع الاول: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠

إن الاتفاقية العربية للحد من جرائم تقنية المعلومات ٢٠١٠، وجدت لهدف تطوير التعاون بين الدول العربية، بغاية مكافحة الجرائم السيبرانية، وسوف نتكلم عن هذه الاتفاقية العربية على الشكل التالي:

اولاً: نبذة تاريخية عن أنشطة الجامعة العربية

إن التعاون الأمني في نطاق جامعة الدول العربية يعود إلى وقت مبكر منذ توقيع ميثاق جامعة الدول العربية في ١٩٤٥، وفي مجال مكافحة الجريمة بشكل عام في ١٩٥٠، بإنشاء مكتب مكافحة المخدرات في جامعة الدول العربية، وقد تم دعم هذا التعاون بإنشاء المنظمة العربية للدفاع الاجتماعي عام ١٩٦٠ التي كان الغرض من إنشائها مكافحة الجريمة وتأمين التعاون المتبادل بين أجهزة إنفاذ القانون[٣].

أما في مجال مكافحة الجرائم السيبرانية، فقد أصدر مجلس وزراء الداخلية العرب، مجموعة من التوصيات عن هذه الجرائم في المؤتمر المنعقد في تونس ١٩٩٨، وقد دعا فيها الدول الأعضاء إلى تشكيل لجنة وطنية تتولى دراسة جوانب استخدام الحاسوب والانترنت لغرض وضع التدابير لسلامة استخدامها، ووضع النصوص الكفيلة بتجريم إساءة استخدام الحاسوب والانترنت، وفرض عقوبات بحق مرتكبيها.

ثانياً: أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

---

[١] عادل عبد صادق، أسلحة الفضاء الإلكتروني في ضوء القون الدولي الإنساني، المرجع السابق، ص ١٠٧.

[٢] ريتشارد كلارك، حرب الفضاء الإلكتروني، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، ٢٠١٢، ص ١٥٦.

[٣] زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، ص ١٦٢.

أعلنت الجامعة العربية في نهاية ٢٠١٠، عن اتفاقية عربية لمكافحة جرائم تقنية المعلومات في اجتماع وزراء الداخلية في القاهرة، وتزامن مع ذلك توقيع أربع اتفاقيات أخرى، تتكون الاتفاقية من خمسة فصول تضمنت (٤٣)، مادة.

ثالثاً: الأهداف العامة من الاتفاقية

تشير الديباجة إلى إن الهدف من الاتفاقية في المادة الأولى، هو رغبة الدول في تعزيز التعاون لمواجهة جرائم تقنية المعلومات، لحماية المجتمع العربي وأمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، من خلال تبني سياسة جنائية موحدة تجاه هذا النوع من الجرائم، فضلاً عن الالتزام بحماية واحترام وضمان حقوق الإنسان الأساسية، استرشاداً بالمبادئ الدينية والأخلاقية السامية، وبالأخص الشريعة الإسلامية التي تنبذ كل أشكال الجريمة[١].

رابعاً: أحكام مشروع بناء الثقة في الفضاء السيبراني

في هذه المبادرة تهدف إلى ضمان أمن وسلامة الفضاء السيبراني في المنطقة العربية، وقد رعاها مركز البحوث والدراسات القانونية والقضائية الجامعة العربية، وانصب في مشروع (بناء الثقة في الفضاء السيبراني)، وهو جهد جدير بالاهتمام لكونه يؤسس لحماية الفضاء السيبراني عبر قواعد قانونية، في غياب أطر قانونية واضحة وشاملة في المنطقة العربية[٢].

خامساً: الاستنتاجات

راعت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات خصوصية المنطقة العربية، وذلك كان واضحاً من خلال الديباجة من خلال الإشارة إلى مراعاة النظام العام في كل دولة، والأخذ بالمبادئ الدينية والأخلاقية لاسيما الشريعة الإسلامية، اما الانتقادات الموجهة إلى الاتفاقية، استخدامها لألفاظ فضفاضة وواسعة كمصطلح (تقنية المعلومات)، على سبيل المثال، كذلك لم تنص الاتفاقية على معايير محددة للحفاظ على خصوصية المستخدم وحماية بياناته، فضلاً عن شمولها طائفة واسعة من الجرائم على عكس اتفاقية بودابست، ولعل السبب في ذلك يرجع إلى وجود أدوات تشريعية للمنظمات الفاعلة في المنطقة الأوربية

---

[١] سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، مرجع سابق، ص ١٧٧.

[٢] سيد شوربجي عبد المولى، مواجهة الجرائم الاقتصادية في الدول العربية، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٦، ص ١٨٦.

غير الاتفاقيات تسمح لها بالتأثير على قوانين الدول الأعضاء، أن اقتصار التجريم على مسائل بعينها تتعلق بالولوج إلى الحاسوب وإساءة استخدام البرامج وغير ذلك التي احتوتها اتفاقية بودابست[١].

الفرع الثاني: التشريعات العربية الداخلية لمكافحة الجرائم السيبرانية

شهد الوطن العربي حركة تشريعية بداية القرن الحالي لضبط المعاملات الإلكترونية ومواجهة الجرائم السيبرانية، إذ صدر قانون التجارة والمبادلات الالكترونية التونسي عام ٢٠٠٠، وبعد عامين أصدرت إمارة دبي بشأن التجارة الالكترونية، وعقب ذلك صدر القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات، والذي وضع القواعد الأساسية التي ينبغي على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجرائم[٢].

اولاً: قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات ٢٠٠٣

في عام ٢٠٠٣، تم مناقشة مشروعين أحدهما لمكافحة الجرائم السيبرانية والآخر يخص التجارة الالكترونية، وما يهمنا بهذا الخصوص القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية المعلومات، اذ تم إقراره من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر، ومجلس وزراء الداخلية العرب في الدورة الحادية والعشرين، فضلاً عن تحقيق التقارب الإداري والتنظيمي بين أجهزة الأمن، لتوفير وحدة الأسلوب والممارسة الأمنية المبنية على وحدة القواعد، كذلك تبادل المعلومات عن حالة الجريمة المنظمة عبر الدول، فضلاً عن توسيع نطاق المعرفة بالتنظيمات الإجرامية ومصادر تمويلها، والتنسيق بين القدرات البشرية والخبرات التكنولوجية وتحديد سبل التدريب والتعاون التقني ولقانون الإمارات الاسترشادي أحكام واستنتاجات:

- **أحكام قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات:**

حيث جاء القانون في (٢٧) مادة، لم تتضمن النصوص القانونية عقوبات محددة، وهذا مسلك محمود، باعتبار إن تقدير مدة العقوبة إلى الدول الأعضاء، يتيح لهم الحرية في تقدير العقوبات طبقاً للبنية الثقافية والاجتماعية والسياسية للدولة العضو، وتضمن نصوصاً وأحكام موضوعية تجرم الدخول غير المشروع[٣].

- **الاستنتاجات:**

---

[١] ضياء يحيى السادات، مبادئ استخدام الحاسب الآلي والأنترنت وجهود مكافحة الجرائم الناشئة عنها، المرجع السابق، ص ١٩٦.

[٢] فاروق سعد، قانون الفضاء الكوني، الطبعة الثالثة، مطبعة صادر الحقوقية، بيروت، ٢٠٠٤، ص ٢٠٣.

[٣] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٢٢٣.

أن الشمول الذي احتوته النصوص القانونية يمكن الدولة من إصدار التشريع الكامل لمواجهة الجرائم السيبرانية، ويمكن الإضافة على النصوص التي لدى الدولة العضو، إذ لا يوجد ما يمنع ان تقوم الدولة العضو بتحديث النصوص التشريعية كل على حده لتتماشي مع القانون النموذجي، ويعتبر صدور هذا القانون في عام ٢٠٠٣، قد مهد للانضمام إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، ومقارنة باتفاقية بودابست ٢٠٠١، يحتوي القانون النموذجي العربي على عدد واسع من الجرائم التي تضمنت بالمقابل عدد محدود وقليل نسبياً، من الجرائم ذات الصلة بالحاسوب بشكل خاص والجرائم السيبرانية بشكل عام[١].

ثانياً: وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات في دول مجلس التعاون لدول الخليج العربي ٢٠١٣

أقر المجلس الأعلى لمجلس التعاون لدول الخليج العربي المنعقد في البحرين عام ٢٠١٢، النظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي، وهذا القانون يأتي في إطار سلسلة من القوانين والأنظمة الاسترشادية في مسائل التعاون العدلي والقضائي بين دول مجلس التعاون الخليجي، إذ يتجدد هذا النظام كل أربعة سنوات تلقائياً في حال عدم ورود ملاحظة عليه.

وقد سميت هذه الوثيقة ب (وثيقة الرياض للنظام القانوني الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي)، وتتكون من (٣٩) مادة قانونية صيغت من قبل خبراء ذوي اختصاص من الدول الأعضاء، بهدف محاربة الجرائم السيبرانية وفرض العقوبة على مرتكبيها، وتم تحديد الأفعال في هذه الوثيقة أما العقوبات فقد تركت للدول الأعضاء، وهناك احكام واستنتاجات لوثيقة الرياض لمكافحة جرائم تقنية المعلومات[٢].

-أحكام الوثيقة:

جاءت الوثيقة في المادة الأولى بالتعريفات، وفي المادة الثانية نصت على الاختصاص، ومن المادة (٣) إلى المادة (٣٠) نصت الوثيقة على الجوانب الموضوعية للجرائم، فقد جرمت الدخول غير المشروع وإتلاف المستندات المعلوماتية، والتزوير المعلوماتي، وكذلك الدخول إلى المواقع بشكل غير مشروع للقيام

---

[١] لورانس أوليفا، أمن تقنية المعلومات، المنظمة العربية للترجمة، ترجمة محمد مراياتي، بيروت، ٢٠١١، ص٢٣٦.

[٢] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص٢٥١.

بفعل غير مشروع، كذلك تجريم استخدام البطاقات الائتمانية بشكل غير مشروع، وتجريم الاستفادة من القنوات المسموعة والمرئية بشكل غير مشروع[١].

ولم تنشط دول مجلس التعاون للخليج العربي في مجال التشريع فقط، بل أيضاً عقدت العديد من المؤتمرات في مجال الأمن السيبراني برعاية ومشاركة دول مجلس التعاون الخليجي، ففي عام ٢٠٠٨ انعقد المؤتمر الثاني لجرائم تقنية المعلومات في أبو ظبي بدولة الإمارات العربية المتحدة، وفي عام ٢٠٠٩، انعقد المؤتمر الدولي الثالث أيضاً في أبو ظبي لبحث الجوانب الإجرائية، وفي عام ٢٠١٤ احتضنت أبو ظبي المؤتمر العالمي للأمن السيبراني، وكذلك مسقط بعمان إذ عقد مؤتمر الأمن السيبراني، وبالتعاون مع الاتحاد الدولي للاتصالات استضافت سلطنة عمان المؤتمر الإقليمي الثالث للأمن السيبراني، وترأس المؤتمر السنوي السادس للمراكز الوطنية للأمن السيبراني العماني بدول منطقة التعاون الإسلامي في برونای، ومؤتمر الأمن السيبراني في الدوحة بدولة قطر بمشاركة شركة تانجينت لينك البريطانية.

- **الاستنتاجات:**

عكس التشريعات على المستوى العربي المتمثلة بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أو القوانين النموذجية الاسترشادية على مستوى الجامعة العربية، أو منظمة دول مجلس التعاون لدول الخليج العربي ثلاث حقائق مهمة: مدى النضج والوعي العربي لظاهرة الجرائم السيبرانية وآثارها على المستوى الاقتصادي والاجتماعي والثقافي، كما أنها تصيغ تشريعات تشمل طائفة واسعة من الجرائم السيبرانية راعت النصوص، الخلفية الثقافية والدينية والعادات والتقاليد الخاصة بالمجتمعات العربية، كما أنها تكاتف الجهود العربية المحلية والإقليمية لمواجهة الجرائم السيبرانية عبر سن تشريعات موحدة، وعقد العديد من المؤتمرات الإقليمية لمواجهة التطورات في مجال مكافحة الجرائم السيبرانية، والسعي لتوحيد فهم عام لهذه الظاهرة وسبل مكافحتها[٢].

الخاتمة

أضحت التكنولوجيا جزءاً لا يتجزأ من الحياة اليومية للكثير من الأشخاص في إنحاء العالم، والشبكات والبيئة الرقمية والأنظمة تقدم مورداً حيوياً وتمثل بنى تحتية لا يمكن الاستغناء عنها في المجتمع الدولي

[١] كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، مرجع سابق، ص٧٤.
[٢] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص ٢٢٥.

المعاصر، هذه التكنولوجيا تربط مجتمعات بأكملها من خلال أنظمة معقدة ومتشابكة وتقدم حلولاً متطورة للكثير من المشكلات وتسهم في النمو الاقتصادي والإنساني.

هذا التطور في استخدامات الفضاء السيبراني رافقه سلوك غير مشروع لغايات متعددة ترتبط به وتستخدمه وتستغله بشكل أو بأخر، ونتيجة لكون نطاق الشبكة عالمي، الأمر الذي أثار عدة تحديات على مختلف المستويات الوطنية والدولية في مواجهة هذا السلوك غير المشروع الذي يمثل جريمة، هذه التحديات قانونية فنية، ونتيجة لعالمية السلوك وتأثيره في إقليم أكثر من دولة، ومع تنوع الأنظمة القانونية وقدرات الدول واعتمادها وتعاملها مع تكنولوجيا الاتصالات والمعلومات، فإن تنظيم السلوك هو مشكلة دولية ويحتاج إلى حلول دولية.

أولاً: النتائج:

١. الجرائم السيبرانية جرائم في غايه الخطوره لأنها جرائم لا تعترف بأي خصوصية أو سيادة للدول فهي تقع بين أكثر من دولة ولا تعترف بالحدود الجغرافية وعابرة للحدود.
٢. على جميع دول العالم بذل الجهود لمكافحتة الجريمة السيبرانية بكافه الطرق والأشكال وسبل التعاون الدولي بالإضافة إلى الدور الوطني والمجتمعي والأسري وبذلك يحد من أضرار ومخاطر هذه الجريمة.
٣. من شأن الهجمات السيبرانية أن تصل لمفهوم استخدام القوة في العلاقات الدولية التي من شأنه تفعيل حق الدفاع الشرعي واتخاذ التدابير المضادة، والقوة المقصود بها لا تشمل الاكراه غير العسكري على المستوى الواطئ، فينبغي أن يكون استخدام الاكراه والقوة بالدرجة التي تكفي لتقييد حرية تصرف الدولة التي يوجه ضدها هذا الاكراه، إذ من شأن أي صورة من صور الاكراه التي يترتب عليها التأثير وانتهاك واضح للأمن القومي لدولة أخرى استخداماً للقوة وبالتالي انتهاكاً لمبدأ عدم استخدام القوة في العلاقات الدولية، ولكن ليس أي إكراه واستخدام للقوة من شأنه تفعيل حق الدفاع الشرعي.
٤. إن عملية وضع تنظيم شامل لهذه الظاهرة الخطيرة تتسم بصعوبات شتى وذلك لأن المصالح الدولية للقوى العظمى تقف حجر عثرة أمامها، كالصعوبات التي واجهت المجتمع الدولي عند وضع اتفاقية بشأن الأسلحة النووية والجدل حول تقييدها أو حظر استخدامها كلياً.
٥. من المبادئ المستقرة في القانون الدولي العام أن استخدام القوة أو التهديد بها في العلاقات الدولية يعد عملا غير مشروع، إلا أن هناك مجموعة من العمليات السيبرانية تدور حول تفسير مصطلح القوة بين معيار يعتمد على العنصر الحركي للقوات المسلحة ولوجوستياتها، وآخر بشأن كافة صور استخدام القوة على ما ترتب عليها من انتهاك واضح للأمن القومي للدول.

٦. وعليه فإن استخدام التقنيات الإلكترونية ومنها الهجمات السيبرانية ويجب أن لا تقيم مقابل فكرة افتراضية بل يجب مقارنتها بالبشر في ضوء الظروف والالتباسات المحيطة أثناء المواجهة السيبرانية.

٧. بالنظر إلى قواعد القانون الدولي العام والتي يقع جزء كبير منها على التدابير الاحتياطية المستطاعة، تلك الاحتياطيات التي من الممكن التي يمكن أن تكون متاحة في الاستخدامات التقنية الحديثة لاسيما إذا ما تم تطويرها لتفوق كفاءة البشر في الامتثال لقواعد القانون الدولي الإنساني من خلال تقنية بحيث تكون قادرة على الحصول على المعلومات التي تشير إلى ضرورة وقف الهجوم السيبراني إذا ما بين أن تلك الهجمات تشكل انتهاكا لقواعد ذلك القانون وهي بذلك قد تحقق ميزة حتى على بعض الأسلحة التقليدية، ومنها عدم القدرة على إلغاء أو تأجيل هجوم تم بواسطة المدفعية أو القذائف بعد إطلاقها أي في اللحظات الأخيرة.

ثانياً: التوصيات:

١. يتوجب على الدول اتخاذ خطوات جدية لمكافحة الهجمات السيبرانية باعتماد تدريس الفضاء السيبراني والمخاطر الناشئة عنه لا سيما على المستوى الدولي في المؤسسات الأكاديمية، إرساء بنية تحتية في مجال البرمجيات، توفير وسائل وأدوات تقنية وتعظيم التعاون بين مؤسسات الدولة العسكرية والتكنولوجية على كافة الأصعدة، لتطوير القدرات العسكرية سواء الدفاعية منها أم الهجومية، للحفاظ على سرية المعلومات والبيانات العسكرية والتصدي للهجمات السيبرانية.

٢. السعي لاعتماد اتفاقية دولية لتنظيم الهجمات السيبرانية وإن كنت أعتقد أن هذا الأمر بعيد المنال في الوقت الحالي، وقد يستغرق وقت طويل من الزمن على غرار اتفاقية حظر الأسلحة النووية التي استغرق لدخولها حيز النفاذ في ٢٢ كانون الثاني عام ٢٠٢١ حوالي ٧٥ عام، وذلك بسبب تباين الآراء بين الدول وعزوف الدول من الانضمام إلى المعاهدات الدولية الملزمة، ولكن في حال كان هناك وعي من قبل المجتمع الدولي بخطورة هذه الهجمات هناك بصيص أمل باعتمادها.

٣. لحين إتمام الاتفاقية هنالك حاجة ماسة إلى إعادة تقييم الأطر القانونية التشريعات الدولية والإقليمية، وإجراء مراجعة شاملة لها وتحديثها عند الضرورة، لضمان كفاءتها وتحليل مدى تمكنها من مواجهة المستجدات التي يفرزها التقدم التكنولوجي، كالروبوتات المتطورة ذاتية التعلم والهجمات المؤتمتة.

٤. قيام منظمة الأمم المتحدة بإنشاء مركز خاص تحت تسمية "منظمة الأمن السيبراني" تتولى العمل على إصدار لوائح السلوك في الفضاء السيبراني، عقد الورش وتدريب المستشارين الدوليين والمحققين الدوليين بشأن التحقيق والكشف عن الانتهاكات التي تقع في إطار الفضاء السيبراني.

قائمة المصادر والمراجع

أولاً: الكتب القانونية:

١. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٨.

٢. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٥.

٣. بهاء شاهين، شبكة الأنترنت، الطبعة الثانية، العربية لعلوم الحاسبات، القاهرة، ٢٠٠١.

٤. جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، مكتبة السنهوري، بغداد، ٢٠١٢.

٥. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية للنشر والتوزيع، القاهرة، ٢٠٠٢.

٦. جيل برعام، تأثير تطور التكنولوجيا الحرب السبرانية على بناء القوة في إسرائيل، مؤسسة الدراسات الفلسطينية، فلسطين، ٢٠١٣.

٧. حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الأولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٧.

٨. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١.

٩. ريتشارد كلارك، حرب الفضاء الإلكتروني، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، ٢٠١٢.

١٠. زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر.

١١. سليم عبدالله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١١.

١٢. سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ٢٠١٣.

١٣. سيد شوربجي عبد المولى، مواجهة الجرائم الاقتصادية في الدول العربية، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٦.

١٤. عادل عبد صادق، أسلحة الفضاء الإلكتروني في ضوء القون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، ٢٠١٦.

١٥. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

١٦. عبدالله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧.

١٧. علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، ايتراك للنشر والتوزيع، القاهرة، ٢٠١٥.

١٨. علي محمد علي كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، لبنان، ٢٠١٩.

١٩. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤.

٢٠. فاروق سعد، قانون الفضاء الكوني، الطبعة الثالثة، مطبعة صادر الحقوقية، بيروت، ٢٠٠٤.

٢١. كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، الطبعة الأولى، منشورات الحلبي الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠٢١.

٢٢. لورانس أوليفا، أمن تقنية المعلومات، المنظمة العربية للترجمة، ترجمة محمد مراياتي، بيروت، ٢٠١١.

٢٣. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١١.

٢٤. محمود مدين عبد الرحمن، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧.

٢٥. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦.

٢٦. منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٥.

٢٧. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.

٢٨. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠.

٢٩. نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية، الطبعة الأولى، المكتب العربي للمعارف، القاهرة، ٢٠١٦.

٣٠. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ٢٠٠٠.

٣١. يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١.

ثانياً: قرارات الأمم المتحدة:

١. قرار الجمعية العامة للأمم المتحدة، رقم ١٢١/٤٥، أنظر الوثيقة رقم A/RES/121/45، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٢. قرار الجمعية العامة للأمم المتحدة، رقم ١٢١/٥٦، أنظر الوثيقة رقم A/RES/121/56، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٣. قرار الجمعية العامة للأمم المتحدة، رقم ٢٣٩/٥٧، أنظر الوثيقة A/RES/239/57 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٤. قرار الجمعية العامة للأمم المتحدة، رقم ١٩٩/٥٨، انظر الوثيقة رقم A/RES/199/58، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٥. قرار الجمعية العامة للأمم المتحدة، رقم ١٧٧/٦٠، انظر الوثيقة رقم A/RES/177/60 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٦. قرار الجمعية العامة للأمم المتحدة، رقم ٢١١/٦٤، انظر الوثيقة رقم A/RES/211/64 على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

٧. قرار الجمعية العامة للأمم المتحدة، رقم ١٧٠/٧٠، أنظر الوثيقة رقم A/RES/170/70، على الموقع الرسمي لمنظمة الأمم المتحدة: http://www.un.com/.

List of Sources and References

First: Legal Books

1. Ahmed Abis Neama Al-Fatlawi, *Cyber Attacks: A Legal Analytical Study on the Challenges of Contemporary Regulation*, Zain Legal Publications, Beirut, Lebanon, 2018.
2. Amir Faraj Youssef, *Combating Cyber Terrorism: Digital Terrorism under the Gulf Cooperation Council Convention on Combating Terrorism*, 1st edition, Dar Al-Kutub and Arab Studies, Alexandria, 2015.
3. Baha Shaheen, *The Internet Network*, 2nd edition, Arab Computer Sciences, Cairo, 2001.
4. Jamal Ibrahim Al-Haidari, *Cyber Crimes and Ways to Address Them*, Al-Sanhouri Library, Baghdad, 2012.
5. Jamil Abdel Baqi Al-Saghir, *Internet and Criminal Law*, Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Cairo, 2002.
6. Gil Baram, *The Impact of Technological Development and Cyber Warfare on Power Building in Israel*, Palestinian Studies Foundation, Palestine, 2013.
7. Hussein Mohammed Al-Ghoul, *Internet Crimes and the Criminal Liability Arising Therefrom*, 1st edition, Badran Legal Library for Publishing and Distribution, Beirut, Lebanon, 2017.
8. Rami Metwally Al-Qadi, *Combating Cyber Crimes in Comparative Legislation and in Light of International Conventions and Charters*, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo, 2011.
9. Richard Clarke, *Cyber War*, 1st edition, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2012.
10. Zabeekha Zidan, *Cyber Crime in Algerian and International Legislation*, Dar Al-Huda, Ain M'lila, Algeria.

11. Salim Abdullah Al-Jubouri, *Legal Protection of Internet Information*, Al-Halabi Legal Publications, Beirut, 2011.

12. Suleiman Ahmed Fadel, *Legislative and Security Confrontation of Crimes Arising from the Use of the International Information Network*, Dar Al-Nahda Al-Arabiya, Cairo, 2013.

13. Sayed Shorbaji Abdel-Moula, *Confronting Economic Crimes in Arab Countries*, 1st edition, Naif Arab University for Security Sciences, Riyadh, 2006.

14. Adel Abdel Sadiq, *Cyber Weapons in Light of International Humanitarian Law*, Bibliotheca Alexandrina, Alexandria, 2016.

15. Abdel Fattah Bayoumi Hegazy, *Combating Computer and Internet Crimes in the Model Arab Law*, 1st edition, Dar Al-Fikr Al-Jamii, Alexandria, 2006.

16. Abdullah Abdul Karim Abdullah, *Cyber and Internet Crimes*, 1st edition, Al-Halabi Legal Publications, Beirut, 2007.

17. Alaa Eldin Shehata, *International Cooperation in Crime Combatting*, Etrak for Publishing and Distribution, Cairo, 2015.

18. Ali Mohammed Ali Kazem Al-Mousawi, *Direct Participation in Cyber Attacks*, Modern Institution for Books, Beirut, Lebanon, 2019.

19. Omar Mohammed Abu Bakr bin Younis, *Crimes Arising from the Use of the Internet*, Dar Al-Nahda Al-Arabiya, Cairo, 2004.

20. Farouq Saad, *Space Law*, 3rd edition, Sader Legal Printing, Beirut, 2004.

21. Kamiran Aziz Hassan, *International Efforts in Confronting Cyber Crimes*, 1st edition, Al-Halabi Legal Publications for Publishing and Distribution, Beirut, Lebanon, 2021.

22. Laurence Oliva, *Information Technology Security*, Arab Organization for Translation, translated by Mohammed Marayati, Beirut, 2011.

23. Mohammed Ali Al-Arian, *Cyber Crimes*, New University House, Alexandria, 2011.

24. Mahmoud Medin Abdel Rahman, *Cyber Crime and National Security Challenges*, Egyptian Publishing and Distribution, Cairo, 2017.

25. Mamdouh Abdel Hamid Abdel Muttalib, *Digital Criminal Investigation in Computer and Internet Crimes*, Legal Books House, Cairo, 2006.

26. Munir Mohammed Al-Janabihi & Mamdouh Mohammed Al-Janabihi, *Electronic Information Security*, Dar Al-Fikr Al-Jamii, Alexandria, 2005.

27. Naeila Adel Mohammed Farid Qoura, *Economic Computer Crimes*, Al-Halabi Legal Publications, Beirut, 2005.

28. Nahla Abdel Qader Al-Moumani, *Cyber Crimes*, 2nd edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2010.

29. Nouran Shafiq, *The Impact of Cyber Threats on International Relations*, 1st edition, Arab Knowledge Office, Cairo, 2016.

30. Huda Hamed Qashqoush, *Computer Crimes in Comparative Legislation*, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

31. Youssef Hassan Youssef, *International Internet Crimes*, 1st edition, National Center for Legal Publications, Cairo, 2011.

Second: United Nations Resolutions

1. United Nations General Assembly Resolution No. 45/121, see document A/RES/121/45 on the official UN website: http://www.un.com/.
2. United Nations General Assembly Resolution No. 56/121, see document A/RES/121/56 on the official UN website: http://www.un.com/.

3. United Nations General Assembly Resolution No. 57/239, see document A/RES/239/57 on the official UN website: http://www.un.com/.
4. United Nations General Assembly Resolution No. 58/199, see document A/RES/199/58 on the official UN website: http://www.un.com/.
5. United Nations General Assembly Resolution No. 60/177, see document A/RES/177/60 on the official UN website: http://www.un.com/.
6. United Nations General Assembly Resolution No. 64/211, see document A/RES/211/64 on the official UN website: http://www.un.com/.
7. United Nations General Assembly Resolution No. 70/170, see document A/RES/170/70 on the official UN website: http://www.un.com/.