مجلة الباحث العربي
Arab Researcher Journal
ISSN: 2709 – 0647/DOI: 10.57072

مجلد 6 عدد 4 (2025)

المسؤولية الدولية الناتجة عن الجرائم السيبرانية

International liability arising from cybercrimes

الأستاذ تامر أحمد سعيد أحمد، حاصل على دكتوراه في القانون الدولي العام – كلية الحقوق– جامعه بني سويف
Mr. Tamer Ahmed Said Ahmed, Holder of a PhD in Public International Law – Faculty of Law, Beni-Suef University

https://doi.org/10.57072/ar.v6i4.176

نشر في 2025/12/15

المستخلص:

يهدف البحث الي التعرف علي موقف القانون الدولي من موضوع الجرائم السيبرانية، ومعرفة مدى إمكانية إقرار المسؤولية الدولية عن الجرائم السيبرانية،ويتناول هذا البحث مطلبين هما: التعريف بالجرائم السيبرانية، والمطلب الثاني: التكييف القانوني للجرائم السيبرانية، وقد توصل البحث إلي أن الجرائم السيبرانية تعد أحد أحدث صور الجرائم التي ظهرت في الآونة الأخيرة، وتتميز بأنها تكتسب خصوصيتها من أركانها وأساسها، وأنه عمل غير مشروع فهي بحد ذاتها تنتهك أحكام وقواعد القانون الدولي، فيترتب عليها اختراق أسرار ووثائق الدول، وهي تستهدف مصالح الدولة، وتعمل على اختلاق قضايا دولية جديدة لم تعرفها الدول في زمن الحروب التقليدية، ويوصي البحث بالعمل علي تحقيق الأمن السيبراني ومكافحة الجرائم السيبرانية، وكذلك حفظ الحقوق الناتجة عن الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

الكلمات الافتتاحية: المسؤولية الدولية – الجرائم السيبرانية– التكييف القانوني– الأمن السيبراني.

Abstract:

The research aims to identify the position of international law on the subject of cybercrimes, and to know the extent of the possibility of establishing international responsibility for cybercrimes. This research addresses two requirements: defining cybercrimes, and the second requirement: the legal classification of cybercrimes. The research concluded that cybercrimes are one of the latest forms of crimes that have emerged recently, and are characterized by the fact that they acquire their specificity from their pillars and foundations, and that they are an illegal act in themselves, violating the provisions and rules of international law, resulting in the penetration of state secrets and documents, and targeting the interests of the state, and working to invent new international issues that states did not know in the era of traditional wars. The research recommends working to achieve cybersecurity and combat cybercrimes, as well as preserving the rights resulting from the legitimate use of computers and information networks.

Keywords: International Responsibility – Cybercrimes – Legal Classification – Cybersecurity

مقدمة:

تعتبر الجريمة السيبرانية ثمرة من ثمار التقدم السريع الذي حدث مؤخراً في تكنولوجيا المعلومات، إذ أنها تعد من أهم وأخطر الصعوبات والتحديات الأمنية التي تواجه كافة المجتمعات العالمية في الوقت الحالي، خاصة في مجالات تقنية الاتصالات والمعلومات، ففي ضوء هذا التقدم السريع في مجال العلوم والتقنية واستخداماتها في خدمة البشرية، فقد حدث تطور في مجال الجريمة السيبرانية، فأخذت صُوراً عديدة كجرائم الاحتيال المعلوماتي وكذلك سرقة الهويات والتعدي على بطاقات الائتمان والأرصدة البنكية وجرائم التزوير وجرائم الاختلاس، وكذلك سرقة حقوق الملكية الفكرية والتعدي والاستغلال الجسدي للأطفال، وكذلك نشر الأفكار الإرهابية المتطرفة.

استلم البحث في 2025/09/19 قبل للنشر في 2025/11/27

لم يقتصر نطاق الجريمة السيبرانية فقط على التعدي على أنظمة الأفراد الإلكترونية، بل شمل مجالها كذلك التعدي على الأنظمة المادية والمعنوية التي تمتلكها الدول، فقد رأينا تعدي على الأنظمة المعلوماتية العسكرية والاقتصادية للدول، هذا التعدي قامت به بعض الدول والجماعات الإرهابية، وكذلك بعض الأشخاص العاديين، مما يعني قيام المسؤولية الدولية عن تلك الجرائم.

إن طبيعة الجريمة الدولية بوصفها جريمة تتم في الفضاء الخارجي باستخدام تكنولوجيا عصرية متقدمة، قد سهلت ارتكابها والتعدي بتلك الجرائم على المعطيات المادية والمعنوية للدول والأفراد، فالجاني يستطيع الإفلات من المسؤولية، للصعوبات التي تواجه الكشف عنه، كما أن الدول قد تقوم بتسهيل عملية الإجرام السيبراني، كما في التجسس والتعدي على الأنظمة الاقتصادية والسياسية.

مما يستدعي قيام المسؤولية الدولية عن تلك الجرائم، والمسؤولية الدولية عن الجرائم السيبرانية تتطلب الوقوف على ماهية تلك الجرائم، من حيث المقصود بها وتكييفها، وتحديد موقف القانون الدولي منها، ومعرفة الوثائق الدولية التي قامت بتجريم تلك الأفعال والوثائق الدولية التي تناولتها.

إشكالية البحث:

مشكلة البحث متمثلة في إمكانية قيام المسؤولية الدولية عن الجرائم السيبرانية، فهناك الكثير من الدول قد أصابتها الهجمات السيبرانية بالكثير من الاضرار، قامت بها دول أخرى بهدف التعدي وتعطيل الأنظمة العسكرية والاقتصادية للدولة المعتدى عليها، ومن أوجه القصور في المعايير الدولية هي عدم القدرة على المساءلة عن الهجمات السيبرانية الخبيثة، فالواقع يشير إلي أن التوصل إلي اتفاق دولي لمواجهة الأنشطة الإلكترونية الخبيثة أمراً محدوداً للغاية، وذلك لأن المجتمع الدولي يتحرك فقط عندما تُستخدم القوة، وهو أمرٌ غير متوفر في الهجمات الإلكترونية، فلم يحدث أن تسبب هجوم إلكتروني في وفاة أحد الأشخاص، وللتغلب على هذه المشكلة، يرى الباحث ضرورة إعداد قائمة من الإجراءات المتسقة مع القانون الدولي والمعايير المتفق عليها، وذلك عن طريق إقامة خطة استراتيجية دبلوماسية جماعية من أجل خلق المساءلة الدولية لمواجهة الهجمات الإلكترونية باعتبارها قضايا خطيرة.

المنهجية:

استخدم المنهج الوصفي، وذلك للوصف القانوني لإجلاء المسؤولية الدولية الناتجة عن الجرائم السيبرانية وذلك من منظور القانون الدولي لها.

أهمية الدراسة:

إن لدارسة المسؤولية الدولية الناتجة عن الجرائم السيبرانية أهمية نظرية وأخرى عملية:

- **الأهمية النظرية:** تظهر أهمية الدراسة في تقييم موقف القانون الدولي من الجرائم السيبرانية، ومدى كفاية الوثائق الدولية، لتجريم هذه الفئة المستحدثَة من الأفعال الإجرامية، ومعرفة موقف القانون الدولي من طبيعة تلك الجرائم، وأساس بناء المسؤولية الدولية طِبقاً لقواعد القانون الدولي.
- **الأهمية العملية:** الأهمية العمليّة للدراسة، معرفة الإجراءات التي تلتزم الدولة باتخاذها في تشريعاتها الوطنية، لكي تكون متماثلة مع قواعد القانون الدولي في مجال الجريمة المعلوماتية، من حيث الجرائم التي تنص عليها في تشريعاتها العقابية وكذلك العقوبات التي ترصدها لها.

تساؤلات الدراسة:

سيقوم الباحث من خلال الدراسة بالإجابة على التساؤلات الآتية:

- ما المقصود بالجرائم السيبرانية؟
- ما هو التكييف القانوني للجرائم السيبرانية؟
- ما هي أركان وأساس قيام المسؤولية الدولية عن الجرائم السيبرانية؟
- ما هو دور القانون الدولي في مكافحة الجرائم السيبرانية؟

أهداف الدراسة:

ترمي الدراسة لمعرفة موقف القانون الدولي من موضوع الجرائم السيبرانية، وهذا لا نقاش فيه، حيث أن الجريمة السيبرانية تتطلب تضافر الجهود الدولية لمواجهتها بحسب طبيعتها ووصفها كجريمة لا تعترف بالحدود الجغرافية للدول،

فالمسؤولية الدولية عن تلك الجرائم هي محور العقاب والمواجهة.

الهدف الرئيسي: يتمثل في معرفة مدى إمكانية إقرار المسؤولية الدولية عن الجرائم السيبرانية.

الأهداف الفرعية:

- بيان ماهية الجرائم السيبرانية.
- التكييف القانوني للجرائم السيبرانية.
- تحديد أركان وأُسس المسؤوليّة الدولية عن الجرائم السيبرانية.
- بيان الاتجاهات الدولية في مكافحة الجرائم السيبرانية.

الدراسات السابقة:

- **الدراسة الأولى:** للباحثة قطاف سليمان وبوقرين عبد الحليم، تحت عنوان "**الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**"، منشورةٌ بالمجلة الأكاديمية للبحوث القانونية والسياسية، المجلد (6)، العدد (1)، السنة 2022، تناولت الدراسة موضوع آليات مواجهة الجرائم السيبرانية في ظل اتفاقية بودابست والقانون الجزائري، وتتناول تلك الدراسة، دراسة شاملة عن اتفاقية بودابست، وتختلف عن دراستنا في أنها لم تتناول تحديد ماهية الجريمة الإلكترونية، كما أنها لم تعرض للمسؤولية الدولية فقد اقتصرت على القانون الجزائري، كما أنها لم تتناول موضوع الجريمة السيبرانية في دليل تالين.
- **الدراسة الثانية:** دراسة صديقي سامية تحت عنوان "**المسؤولية الدولية المترتبة على الهجوم السيبراني في منظور القانون الدولي**"، منشورة في مجلة البحوث القانونية والاقتصادية، المجلد (6)، العدد (1)، سنة 2023، وقد تناولت الدراسة، موضوع الهجمات السيبرانية من خلال اتجاه القانون الدولي، وتتفق تلك الدراسة مع دراستنا في أنها تناولت موضوع تأسيس المسؤولية الدولية، وتختلف عن دراستنا في أنها لم تحدد ذاتية الجريمة السيبرانية، ولم تتناول موضع أركان الجريمة السيبرانية، إضافة الى أنها لم تتطرق لموضوع المواجهة الدولية للجريمة السيبرانية.

خطة البحث:

المبحث الأول: ماهية الجرائم السيبرانية

المبحث الثاني: تحديد المسؤولية الدولية الناتجة عن الجرائم السيبرانية

المبحث الأول:
ماهية الجرائم السيبرانية

تمهيد وتقسيم:

تُعدّ الجريمة السيبرانية ظاهرة إجرامية حديثة النشأة، حيث أن ظهورها قد ارتبط بالتكنولوجيا الحديثة، ونتج عن حداثتها أن أحيط بها الكثير من الغموض، وقد أصبحت تقنية المعلومات من أساسيات الحياة في العصر الحالي، إلا أنها على الرغم من ذلك فهي تُستغلُّ في أغراض غير مشروعة، ولذلك فقد أصبح الحاسب الآلي بشكل عامّ وشبكة الإنترنت بشكل خاصّ محلا لارتكاب الجريمة بمفهومها الحديث، ونتيجة لذلك فقد احترف بعض الجناة ارتكاب العديد من الجرائم بواسطة الحاسب الآلي وشبكة الإنترنت.

وفي ضوء ذلك تتميز هذه الجريمة بأن ليس لها حدود جغرافية، مما يكسبها طابعاً دولياً، ونتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات فقد أصبحت تلك الظاهرة من الإجرام تؤرق العديد من الدول، وذلك لآثارها الخطيرة على مكانة تلك الدول، وتعد من المواضيع الحديثة والخطيرة التي تشغل اهتمامات رجال القانون والفقهاء.

وتتم الجريمة السيبرانية في الفضاء الخارجي بواسطة الوسائل الإلكترونية، وقد أثيرت التساؤلات المختلفة، حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى اختلاف الرؤية لهذه الطائفة من الجرائم، حيث ظهرت عدة آراء فقهية لفهم المقصود بالجريمة الإلكترونية، وتحديد تعريف لها مع بيان طبيعتها القانونية.

وقسمت الدراسة في هذا المبحث إلى مطلبين على النحو التالي:

المطلب الأول: التعريف بالجرائم السيبرانية

المطلب الثاني: التكييف القانوني للجرائم السيبرانية

المطلب الأول:

التعريف بالجرائم السيبرانية

ماهية الجريمة الإلكترونية يحتاج لإلمام بالجانب الموضوعي والإجرائي لها، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة، والإحاطة بالأمور الفنية لها عن طريق بيان خصائصها.

ونتناول هنا التعريف بالجرائم السيبرانية عن طريق بيان مفهوم الجريمة الإلكترونية، ثم بيان الخصائص التي تتمتع بها الجرائم السيبرانية، وذلك على النحو الآتي:

الفرع الأول: مفهوم الجرائم السيبرانية

الفرع الثاني: خصائص الجرائم السيبرانية

الفرع الأول: مفهوم الجرائم السيبرانية

اختلف الفقهاء في وضع مفهوم شامل للجريمة الإلكترونية، وسبب ذلك عدم تواجد نظام دولي موحد عالميا على هذه الجريمة وعدم تشريع دولي[1]، في بلدان العالم وحداثة نشأتها مقارنة بغيرها من الجرائم، ونتيجة لغياب التعريف القانوني لمثل هذا النوع من الإجرام المستحدث في غالبية النظم القانونية، بالإضافة إلى عدم وجود مصطلح قانوني موحد للتعريف بماهية الجرائم الإلكترونية.

إن الفقه قد انقسم بدوره إلى اتجاهين رئيسيين، ومن ناحية المنطلقات التي ينظر بها لذلك النوع من الجرائم، حيث أن الاتجاه الأول يضيق مفهوم الجريمة السيبرانية، أما الاتجاه الثاني فقد حاول التوسع في تعريف الجريمة السيبرانية.

أولاً: التعريف الضيق للجريمة السيبرانية:

ذهب هذا الاتجاه إلى حصر الجرائم السيبرانية في الأحوال التي تحتاج للعديد من المعرفة بشؤون تقنية تكنولوجية المعلومات الحديثة، فالجرائم التي لا تصل لهذه الدرجة من المعرفة تعتبر جرائم تقليدية عادية تعكف على دراستها نصوص القوانين العقابية التقليدية.

أوضح جانب من الفقه تعريفها بأنها "الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دوراً هاماً، أو هي كل نشاط إجرامي مستخدم فيه الحاسب الآلي، في ارتكابه كمحور رئيسي"[2].

كما عرّفها جانب آخر بأنها " كل سلوك غير مشروع، أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات، أو نقل هذه البيانات"[3].

كما قال عنها آخر بأنها "هي جرائم تمر بمراحل ومن ضمن مراحلها حدوث بعض العمليات الفعلية داخل الحاسوب"[4].

ومن الفقه الأجنبي ذهب أحد الفقهاء إلى أن الجريمة السيبرانية" كل نشاط إجرامي يلحق الضرر بأجهزة الكمبيوتر أو الشبكات أو الأنظمة الخاصة بالشركات وتتم من قبل قراصنة الإنترنت مجهولي الهوية[5].

ولذلك فالتعريفات السابقة قاصرة عن الإلمام بأوجه الجريمة السيبرانية، فأنصار هذا الاتجاه قد صبُّوا تركيزهم على موضوع الجريمة فقط، كما أن منهم من ركز على طريقة ارتكابها، ولكن لم يوجد تعريف تناول الظاهرة من مختلف الجوانب.

ثانياً: التعريف الواسع للجريمة السيبرانية:

ذهب جانب إلى تعريف الجريمة السيبرانية بأنها " كل عمل أو امتناع عن عمل يأتيه الإنسان إضراراً بمكونات جهاز الحاسب الآلي سواء كانت مادية أو معنوية أو شبكة الاتصال

---

(1) Richard Kissel Glassory of Information Security Terms, National Institute of Standers and technology, U.s Department of Commerce, (2013), p96.

(2) من أنصار هذا الجانب راجع د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص: 25.

(3) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر، ص: 25.

(4) د. باطلي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص: 15.

(5) MERWA(VANDER), COMPUTER CRIMES AND OTHER CRIMES AGAINST INFORMATION TECHNOLOGY IN SOUTH AFRICA, R.I.D.P 1993, P 554.

الخاصة بهذا الجهاز، وذلك باعتبارها من القيم والمصالح التي يحميها القانون"[1].

تناول رأي آخر من الفقه تعريف الجريمة الإلكترونية بأنها: "عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقاباً"[2].

كما عُرفت الجريمة الإلكترونية في إطار المنظمة الأوربية للتعاون والتنمية الاقتصادية بأنها: "كل فعل، أو عدم فعل من إثارة، من خلاله يحدث اعتداء على الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة بسبب تدخل التقنية المعلوماتية الإلكترونية"[3].

وجاء تعريف الجريمة الإلكترونية في توصيات منظمة مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة مقترفين الجريمة المُنعقد في فيينا، سنة 2000م بأنها: "يقصد بالجريمة الإلكترونية أيَّ جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[4].

كما عرفها أخر بأنه كل فعل إجرامي يتم في محيط جهاز الحاسب الآلي[5].

وفي النهاية نقول: أن هذا الاتجاه قد توسع كثيراً في مفهوم الجريمة السيبرانية، كما يؤخذ على هذا التوسع في التعريف أن من شأنه أن يطلق وصف الجريمة الإلكترونية على أفعال قد لا تدخل في طائفة الجرائم السيبرانية، وذلك لمجرد استخدام الحاسوب الآلي في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي، أو الأقراص مثلاً، فلا يمكن إعطاؤها وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محلاً لفعل الاختلاس.

ومن هنا فالجريمة السيبرانية: "هي كل فعل غير مشروع، يتم ارتكابه بواسطة تقنيات التكنولوجيا الحديثة، بهدف التعدي على الأموال المادية والمعنوية التي يمتلكها المعتدى عليه".

الفرع الثاني: خصائص الجرائم السيبرانية

نتج عن ارتباط الجريمة السيبرانية بجهاز الحاسب الآلي وشبكة الإنترنت إلى إضفاء عدة خصائص لهذه الجريمة تفرّقها عن الجريمة التقليدية، فهي جريمة عابرة للحدود، تتم في الفضاء الخارجي، كما تتميز بصعوبة الإثبات، وتلك الخصائص نوجزها كالتالي:

أولاً: الجريمة السيبرانية جريمة عابرة للحدود:

تتميز الجريمة السيبرانية بأنها جريمة تتعدى حدود الدولة الواحدة؛ وذلك لاتصالها بعالم الإنترنت وهو عالم لا يعرف الحدود الجغرافية للدول[6]، وينتج عن ذلك أن هناك دول تتأثر بهذه الجريمة بسبب سرعة التنفيذ، فيمكن أن تقع تلك الجريمة من طرف الجاني في مكان، والمجني عليه في مكان أخر.

نتج عن كثرة استخدام الحاسب الآلي وخصوصاً مع كثرة انتشار تكنولوجيا الإنترنت ربط أعداد كبيرة للحواسيب في أماكن جغرافية مختلفة بهذه الشبكة، فقد أصبح الاتصال بين تلك الأجهزة سهلاً، فيمكن الوصل للمرسل إليه بمجرد معرفة عنوانه، وسواء تم ذلك الاتصال بطرق مباحة أو غير مباحة، ويمكن أن نطلق على جرائم المعلومات التقنية بأنها جرائم

---

[1] د. محمد أمين الشوابكة، جرائم الحاسب والإنترنت، دار الثقافة، الأردن، 2011، ص 9.

[2] د. طارق إبراهيم الدسوقي، عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009، ص 158.

[3] U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication as amended through Feb, (2012). p128.

[4] د. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 28.

[5] Roden (Adrian), computer crime and the law, c, l, j.,1991, vol.15, p.399.

[6] Richard Kissel Glassory of Information Security Terms, National Institute of Standers and technology, U.s Department of Commerce, (2013), p258.

عابرة لحدود الدول، فغالباً ما نجد المعتدي في بلد والمعتدى عليه في بلد آخر، كما قد يقع الضرر عن الجريمة في بلد ثالث، وعليه تُعد الجريمة السيبرانية من الجرائم العابرة للحدود الجغرافية للدولة الواحدة[1].

وخلاصة ذلك أن الجريمة السيبرانية من الجرائم ذات النطاق الدولي التي ليس لها نطاق إقليمي، تقف عنده، إنما تمر على النطاق الاقليمي العالمي.

ثانياً: الجريمة السيبرانية تتم في الفضاء الخارجي:

يعتبر محل الجريمة السيبرانية هو الفضاء السيبراني فهي تَصرّف واقعي يتم في عالم افتراضي[2]، هذا العالم قائمٌ على استخدام بيانات رقمية ووسائل اتصال إلكترونية، ومن نتائج هذا التعريف أن أصبح نطاق الجريمة السيبرانية واسعاً يقوم على تحقيق عدة أهداف ملموسة، وذلك نتيجة القيام باختراق موقع إلكتروني ذو حساسية عالية، عادة ما تقوم تلك المواقع بوظائف ذات أولوية مثل محطات الطاقة النووية، أو المحطات الكهربائية، أو المطارات، أو وسائل النقل[3].

ثالثاً: صعوبة الاكتشاف والإثبات:

نظراً للطبيعة الخاصة الذي تتميز بها الجريمة السيبرانية، فإن إثباتها يكتنفه الكثير من الصعوبات، تتمثل في صعوبة الكشف عنها، فهي لا تترك أثراً في العالم الخارجي، فالجريمة السيبرانية لا تقوم على العنف، فلا أثر لاقتحام في السرقة المعلوماتية مثلاً، ولكنها أرقام وبيانات تُمحى أو يتم تغييرها أو تزويرها من السجلات المخزّنة، فلا أثر خارجي لها، فالجريمة السيبرانية تعد جريمة فنّية هادئة تقوم على العنف.

وبالرغم من تلك الخاصيّة إلا أن هناك بعض الفقهاء من يعتبر الجريمة السيبرانية من جرائم العنف، مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالأمم المتحدة، بدافع تشابه دوافع المتعدّين على أنظمة الحاسوب الآلي مع دوافع مرتكبي جرائم العنف[4].

المطلب الثاني:
التكييف القانوني للجرائم السيبرانية

يتعدد مستعملو تكنولوجيا الاتصالات الحديثة، فهناك أكثر من مائة مليون فرد على مستوى العالم يستخدمون الإنترنت، فبفعل الثورة التكنولوجية أصبحت الدول والمجتمعات غير الحكومية، والأعمال التجارية والأوساط الأكاديمية والأفراد مترابطة إلى حد لا يمكن تخيُّله من قبل، وفي الوقت نفسه ازداد الاعتماد العسكري على أنظمة الحواسيب وشبكاتها زيادة هائلة، مما ألقى بظلاله على بيان طبيعة الجرائم السيبرانية، فهناك من يعتبرها جرائم من نوع جديد، وهناك من نظر إليها علي أنها نوع جديد من الحروب، يُمثل امتداداً للحروب التي تتم باستخدام الأسلحة.

ولقد اختلف الفقه في تكييف طبيعة الجرائم السيبرانية إلى فريقين: الفريق الأول يرى أن الجرائم السيبرانية تعد حرباً دولية، بينما يرى الفريق الثاني أن الجرائم السيبرانية من ضمن نطاق الجرائم الدولية، هذا ما نتناوله في هذا المطلب في فرعين على النحو الآتي.

الفرع الأول: تكييف الجرائم السيبرانية كحرب دولية

الفرع الثاني: تكييف الجرائم السيبرانية كإجرام دولي

الفرع الأول: تكييف الجرائم السيبرانية كحرب دولية

---

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2014، ص 93.

[2] يعرف الفضاء السيبراني بأنه عالم افتراضي مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نظم الكمبيوتر وشبكات الإنترنت والمخزون الهائل من المعلومات والبيانات، حيث يتم الاتصال بشبكات الإنترنت عبر الحواسيب أو الهواتف أو غيرها من الأجهزة دون تقيد بالحدود الجغرافية.

[3] محمود محارب، قراءات في كتاب حرب الفضاء الإلكتروني، اتجاهات تأثيرات على إسرائيل، المركز القومي للأبحاث ودراسة السياسات، الدوحة، 2011، ص 132.

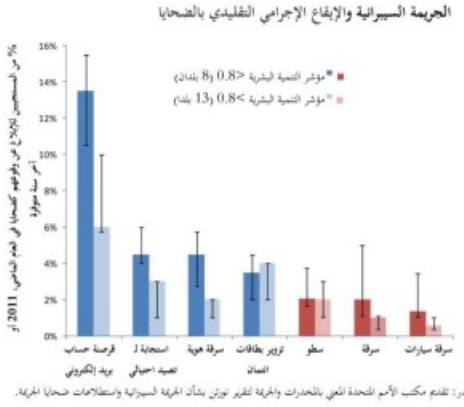
[4] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004، ص 53.

جانب من الفقه ذهب إلى أن الجريمة السيبرانية: هي نوع جديد من أنواع الحروب، الجرائم السيبرانية يشمل نطاقها ليس الدول فقط وإنما الاشخاص أيضاً، بما فيهم الاشخاص المعنوية والانظمة المعلوماتية، فالجرائم السيبرانية تهدد الأمن القومي والاقتصاد القومي للدولة، وأيضا تهدد الأفراد عن طريق سرقة المعلومات الشخصية واستخدامها ضد الشخص، وانتهاك حقوق النشر، ويصل الحد أيضا إلى التعرض لسرقة المعلومات وبيانات الشركة والمؤسسة[1]، فقد تم توجيه الهجمات السيبرانية في الآونة الأخيرة على الدول بحد ذاتها.

فلقد لعب الفضاء الإلكتروني دوراً هاماً في الاستحواذ على عناصر الجريمة السيبرانية في العلاقات بين الدول، حيث أضحى التقدم في محور الإلكترونيات عاملاً حيوياً في القيام بعمليات ذات فعاليّة، عن طريق القدرة على القتال في الفضاء الخارجي، وهذا الأمر يستدعي بالضرورة تغيير في مفهوم القوة، فقد بات بالإمكان تعريفها بأنها مجموعة الطاقات والإمكانيّات الماديّة وكذلك غير الماديَّة التي تحوزها إحدى الدول وتستخدمها في مهمة إصدار القرار للقيام بفعل مؤثّر، بما ينتج عنه تحقيق مصالح الدولة، والتأثير في سلوك الوحدات السياسية في الوقت نفسه[2].

فقد انتقلت عناصر القوة من نظام الحروب الكلاسيكية القائمة على احتلال أرض الخصم والاستيلاء على ثرواته بعد القيام بتدمير أرضه، إلى نمطٍ جديدٍ من الحروب، قوامهُ الاستحواذ على التكنولوجيا وسرقة الأسرار والابتكارات العلمية والتحكم بالمعلومات، وكذلك العمل على إختراق الأمن القومي للدولة بدون أسلحة، أو حتى القيام بالتعدّي على الحدود، وبدون عمليات التجسُّس، فذلك النوع الجديد من القوة له آثارُ تفوقِ الحرب التقليديّة.

ففي الحرب السيبرانية يكون مجال الحرب هو الفضاء الإلكتروني، فهو الساحة التي يتم فيها الصراع، ففي تلك الساحة يتم التأثير على النواحي الثقافية والاقتصادية والاجتماعية للدولة المعتدى عليها، وإن كان مجال ذلك النوع الجديد من الحروب ضيق فلا تتطور إلى القوة



المصدر: تقديم مكتب الأمم المتحدة المعني بالمخدرات والجريمة لتقرير تورتن بشأن الجريمة السيبرانية واستطلاعات ضحايا الجريمة.

المسلحة، ومن الصور التي قد تأخذها تلك الحروب الاختراقات المتعمدة للأنظمة، وكذلك عمليات التجسّس، وكذا سرقة المعلومات، كما يمتد نطاق الحروب السيبرانية إلي شن الحرب الفكرية[3].

وتمثل استبيانات الإيذاء الإجرامي أساسا أسلم للمقارنة. وتُظهر هذه الاستبيانات أن حالات التأذي الفردية من الجريمة السيبرانية هي أكثر بكثير من حالات التأذّي من أشكال الجرائم "التقليدية". وتتراوح معدلات التأذّي من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت، والوقوع ضحية محاولات تصيُّدٍ احتيالي ومحاولات اطلاع دون إذنٍ على حسابات البريد الإلكتروني بين 1 و17 بالمائة من نسبة السكان الذين يستخدمون الإنترنت في 21 بلداً في كل دول العالم، مقارنة بمعدلات التأذّي من السطو والسلب وسرقة السيارات التقليدية التي تقل عن 5 % بالمائة من نسبة السكان في هذه الدول نفسها، وكانت معدلات الإيذاء بسبب الجريمة السيبرانية أعلى

---

(1) عبد الصمد سرحان، التعاون الدولي الأمني في مكافحة الجرائم المعاصرة، القاهرة، مطابع كلية الشرطة،2010، ص 160.

(2) د. جوزيف ناي، المنازعات الدولية مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، 2011، ص 82.

(3) Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, P 33.

في البلدان التي تشهد مستويات نمو منخفضة، مما يُظهر الحاجة إلي تدعيم جهود منع الجرائم في هذه الدول[1].

وبناءً على ذلك، فالجريمة السيبرانية هي حربٌ دولية وساحتها هي الفضاء الالكتروني، حيث يتم اختراق كافة الأنظمة للدولة المعتدى عليها مع تدميرها بعد والتجسس عليها، وبنفس الاسلوب يستهدف الأشخاص من خلال التجسس كذلك على بياناتهم الشخصية طبعاً للإضرار بهم.

الفرع الثاني: تكييف الجرائم السيبرانية كإجرام دولي

ذهب جانب من الفقه إلى أن الجريمة السيبرانية تدخل في نطاق الجرائم الدولية.

ذهب جانب من الفقه إلى أن الجريمة الدولية تتمثل في كل مخالفة لقواعد القانون الدولي، تقع من أجل الإضرار بالأفراد أو حتى بالمجتمع الدولي كله[2]، سواء كان يمنعها القانون الوطني أو يُبيحها، وقد تُرتكب تلك الجريمة بفعلٍ أو بامتناعٍ من شخص يتمتّع بحُريَّته في الاختيار وذلك إضراراً بالأفراد والمجتمع[3].

الجريمة الدولية "هي فعل غير مشروع في القانون الدولي، صادرٌ من شخص ذي إرادة معتبرة قانوناً، ومتصل على نحوٍ معين بالعلاقة بين دولتين أو أكثر، وله عقوبة تُوقَّع من أجله"، من خلال هذا التعريف يتضح أن الجريمة الدولية لها أربعة أركان تقوم عليها، تتمثل في الركن المادي والركن المعنوي والركن الشرعي والركن الدولي[4].

وقد عرفها الدكتور فتوح عبد الله الشاذلي بقوله: "هي سلوك إنساني غير مشروع، هذا السلوك صادر عن إرادة إجرامية يقوم به الفرد باسم أحد الدول أو برضاها، وينطوي هذا السلوك على انتهاك لمصلحة أحد الدول والتي يقرر لها القانون الدولي حماية جنائية"[5].

في حين عَرفَّها أحد الفقهاء بأنها: "سلوك إرادي يصدر عن فرد باسم الدولة أو بتشجيعها أو برضاها غير المشروع، ينطوي على المساس بمصلحة أحد الدول تكون محمية قانوناً"[6].

هذا الجانب من الفقه، ذهب إلى أن أهم مزايا الجريمة الدولية، وهو الركن الرابع المتمثَل في الركن الدولي، وهذا الركن هو خاصية تتميز به الجرائم السيبرانية، فهي بطبيعتها جريمة عابرة للحدود، فهي بذلك جريمة دولية[7].

وعلى هذ النحو فأن تكييف الجريمة السيبرانية بوصفها جريمةً وليست حرباً هو الأقرب للصواب، حيث أن الجريمة السيبرانية تعد من الجرائم بالرغم من خطورتها، كما تنطبق عليها أوصاف الجريمة الدولية والتي تتميز بركنها الدولي، كون السلوك الإجرامي في دولة والنتيجة الإجرامية في دولة أخرى.

---

(1) راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، 2018، ص 26.

(2) Clay Wilson, Cyber Crime. In Franklin D. Kramer et al (eds), Cyber power and National Security, Potomac Book, (2009), p197.

(3) د. أحمد بشارة موسى، المسؤولية الجنائية الدولية للفرد، دار هومة للنشر والتوزيع، الجزائر، 2009، ص 13.

(4) د. عبد الفتاح بيومي حجازي، المحكمة الجنائية الدولية دراسة متخصصة في القانون الجنائي الدولي، دار الفكر الجامعي، الإسكندرية، 2004، ص 97.

(5) د. فتوح عبد الله الشاذلي، القانون الدولي الجنائي، أولويات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، الطبعة الثانية، دار النهضة العربية للنشر والتوزيع، 2016، ص 207.

(6) د. حسنين إبراهيم صالح عبيد، الجريمة الدولية، دراسة تحليلية تطبيقية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1979، ص 123.

(7) شريف محمد، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة، القاهرة،2012، ص 85.

المبحث الثاني:

تحديد المسؤولية الدولية الناتجة عن الجرائم السيبرانية

تُعدّ المسؤولية الدولية الناتجة عن الجرائم السيبرانية من أهم الموضوعات التي يتناولها القانون الدولي في الآونة الأخيرة، فبالنظر إلى التطورات الحديثة في مجال التكنولوجيا نجد أنها قد أثّرت بشكل كبير على العلاقة بين الدول، فقد ظهرت عدة إشكاليات لم يتناولها القانون الدولي بالتنظيم، مما استدعى معالجة وحلّ تلك الإشكاليّات بطريقة تتفق مع طبيعتها الخاصة.

ولا تختلف الجرائم السيبرانية عن مثيلاتها من الجرائم من حيث اشتراط توافر أركانها وأساسها، ومعرفة موقف القانون الدولي من مكافحتها والتصدي لها، وعليه سيتم التطرق إلى تحديد المسؤوليّة الدوليّة الناتجة عن الجرائم السيبرانية من خلال المطلبيْن الآتييّن:

المطلب الأول: أركان وأساس المسؤولية الدولية عن الجرائم السيبرانية

المطلب الثاني: الاتجاهات الدولية في مكافحة الجرائم السيبرانية

المطلب الأول:

أركان وأساس المسؤولية الدولية عن الجرائم السيبرانية

دخل العالم في الآونة الأخيرة مرحلة جديدة، فقد أصبح قرية صغيرة وظهر مسمّى القرية الكونية، ويرجع السبب في ذلك للتطور الكبير الذي كان في عالم تكنولوجيا الاتّصال، فقد استحدثت طرقٌ جديدة للتعامل بين الدول، ولكن مع هذا التطور الهائل في التكنولوجيا ظهرت العديد من التهديدات الجديدة داخل هذا الفضاء مُتمثّلة في الجرائم السيبرانية بمختلف أنواعها من القرصنة، التجسس، السرقة، والإرهاب الإلكترونية، لكن المجتمع الدّولي وضع العديد من الاستراتيجيات لمواجهتها، وذلك للتقليل من أضرار هذه الجرائم، والتي استلزم الأمر تحديد أركان وأساس المسؤولية الدولية عن تلك الجرائم.

هذا ما نتناوله في هذا المطلب من خلال الفرعين التاليين:

الفرع الأول: أركان المسؤولية الدولية عن الجرائم السيبرانية

الفرع الثاني: أساس المسؤولية الدولية عن الجرائم السيبرانية

الفرع الأول: أركان المسؤولية الدولية عن الجرائم السيبرانية

ثمة تشابه بين الانظمة القانونية الدولية والانظمة القانونية الداخليّة، فالفرد هو محور شخص النظام القانوني الدّاخلي، وكذلك الـ حال النظام القانوني الدولي الذي له أشخاصه والمتمثلون في الدول، حيث يفرض النظام القانوني الدولي على الدول عدة التزامات، كما يُرتّب للدول عدة حقوق، فإذا قامت الدولة بأي عمل مخالف لقواعد القانون الدولي، ونتج عن هذا العمل إحداث ثمة ضرر أصاب دولة أخرى فإن قواعد القانون الدولي تُحمِّلها نتيجة ذلك الضرر، فالإجرام السيبراني الذي تقوم به الدولة بوصفها من أشخاص القانون الدولي وينتج عنه أضرار تصيب دولة أخرى من أشخاص القانون الدولي يُرتّب المسؤولية الدولية للدولة المعتدية[1].

من متطلبات قيام المسؤولية الدولية للدولة المعتدية، أن تكون أفراد القانون الدولي، وإن تأتي بأفعال غير مشروعة تدخل في نطاق الإجرام السيبراني، وأن ينتج عن تلك الأفعال ضررٌ يصيب الدولة المعتدى عليها.

أولاً: نسبة الجريمة السيبرانية إلى أحد أشخاص القانون الدولي:

يلزم لقيام المسؤولية الدولية عن الجرائم السيبرانية أن يكون العمل غير مشروع، بل يلزم أن إسناد هذا العمل إلى دولة من شخصيات القانون الدولي، فلا يكفي أن يكون العمل منسوباً إلى دولة محددة، بل يلزم كذلك أن تكون تلك الدولة ذات

[1] د. زياد البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، 2003، ص 116.

سيادة، وينتج عن ذلك أن الدولة ناقصة السيادة لا تسأل عن أعمالها، فهي لا تمارس حقوق الدولة كاملة السيادة[1].

وبالتطبيق علي الجرائم السيبرانية نجد أن ركن الضرر يقوم بمجرد وقوع هجمات سيبرانية، حيث أن الهجمات السيبرانية تهدف الي السيطرة على بنية الدولة التحتية، ويتسبب في إحداث أضرارٍ تصيب الدولة المعتدى عليها، والدولة المعتدية هي بالقطع من دولٍ متقدمةٍ تمتلك القوة الإلكترونية الهائلة التي تُمكّنها من إتيان هذه الهجمات، كما قد تقوم بتلك الهجمات عناصر أخرى، فعلى سبيل المثال قد تُرتكب الجرائم السيبرانية من الجماعات الإرهابية والجماعات المتمردة، وكذلك حركات التحرر الوطني، فهؤلاء ينطبق عليهم الركن الأول المتمثل في نسبة الفعل إلى الدولة[2].

ثانياً: أن تكون الجريمة السيبرانية غير مشروعة:

يعتبر الفعل غير المشروع دولياً متى شكّل انتهاكاً لقواعد القانون الدولي، فالفعل غير المشروع طبقاً لقواعد القانون الدولي يتمثل في الإتيان بفعلٍ أو امتناعٍ عن الإتيان به مما يشكل مخالفةً لأحد الالتزامات الملقاة على الدولة، فمعيار عدم المشروعية بصفة عامة هو معيار موضوعي مجرد، ولا عبرة في وصف الفعل بعدم المشروعيّة بمنشأ الالتزام، فقد تكون عدم المشروعية من فعل الدولة كما تكون من فعلٍ أتاه الفرد، ولا عبرة في وصف الفعل بعدم المشروعية بوصفه في القانون الداخلي، كما لا يعتد بالوسيلة التي يتحقق بها انتهاك قواعد القانون الدولي، سواءٌ أكان ذلك بفعلٍ إيجابيّ أم امتناعٍ عن فعلٍ بسلوكٍ سلبي[3].

وفي الجرائم السيبرانية نجد أنها قد تسبب أضراراً بشريّة وماديّة، وهذا ما يشكّل مخالفةً لميثاق الأمم المتحدة، ومخالفةً لقواعد القانون الدّولي الإنساني.

ثالثاً: إن ينتج عن الجريمة السيبرانية ضرر:

يعتبر ركن الضرر أهم ركن من أركان المسؤولية الدولية عن الجرائم السيبرانية، لأنه متى انعدم الضرر انعدمت معه مسؤولية الدولة، ويأخذ الضرر عدة أوصاف، فهناك ضرر مباشر وضرر غير مباشر، وهناك الضرر المادي وهو كل تعدّي على حقٍ من حقوق الدولة، أو المساس بحقوق رعاياها، وهناك الضرر المعنوي ويتمثل في كل اعتداء أو حتى المساس بشرف الشخص الدّولي أو بأحد رعاياه[4].

وبالتطبيق على الجرائم السيبرانية نجد أن ركن الضرر متحقّق بكافّة أشكاله، سواء أكان القائم بالفعل دولةً كما حدث في الهجوم الفيروسي على البرنامج النووي الإيراني، كما يتحقق الضرر بفعل المنظّمات الإجرامية كما في فعل الهجمات التي يكون من هدفها سرقة المعلومات أو اختراق حسابات مصرفية، وكذلك سرقة أرقام بطاقات الوفاء والضمان[5].

الفرع الثاني: أساس المسؤولية الدولية عن الجرائم السيبرانية

تشكل الجهود التي سعت إليها الدول ومختلف المنظّمات العالمية وسيلةً لمواجهة الجرائم السيبرانية، وذلك من خلال التوفيق بين مختلف الوسائط التقنيّة والأكاديمية، وتكثيف آليّات الاتّصال والتعاون، من وضع استراتيجيّاتٍ دوليّة متنوعة، لمواجهة التهديدات السيبرانية في نطاق ومسؤوليّة كل طرفٍ، وضرورة مراقبة استخدام تكنولوجيا المعلومات والاتصالات في ظل انكشاف العالم على بعضه.

ولقد اختلف الفقه في تحديد أساس بناء المسؤولية الدولية عن الجرائم السيبرانية على فريقين، أحدهما أخذ بنظرية العمل غير المشروع، والاخر أخذ بنظرية المخاطر (المسؤوليّة الموضوعية).

---

(1) د. محمد عبدالله أبو بكر، جرائم الكمبيوتر والإنترنت، منشاة المعارف، الإسكندرية، 2006، ص 88.

(2) عبد الفتاح بيومي حجازي، الإثبات الجنائي "جرائم الكمبيوتر والإنترنت"، بدون ناشر، 2007، ص 324.

(3) صلاح الطائي، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديثة، القاهرة، 2009، ص 116.

(4) د. جميل عبد الباقي الصغير، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1998، ص 256.

(5) جانكارلو أ. باراليتا، النزاع السيبراني والاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، القاهرة، 2011، ص 18.

أولاً: المسؤوليّة الدوليّة عن الجرائم السيبرانية استناداً لنظريّة العمل غير المشروع:

تقوم نظرية الفعل غير المشروع عن الإخلال بالتزام دوليٍّ يستوجب مساءلة الدولة المعتديّة، ولا عبرة لمصدر هذا الإخلال فقد يكون صادراً من السلطة التشريعيّة، أو السلطة التنفيذيّة، أو السلطة القضائيّة، متى نتج عنه ضرراً بأحد الأجانب في شخصه أو أمواله وكان متواجداً بأراضيها[1].

تعتبر الهجمات السيبرانية الدوليّة عمل غير مشروع، وتخضع للمسؤوليّة الدوليّة على هذا الأساس إذا تَوفّر معيار الصِّفة الدوليّة، والمتمثِّل في صدور هذه الهجمات من قبَل دولة ما، أما المعيار الثاني أن تكون الهجمات السيبرانية خارقة لمعاهدة أو عُرفٍ دولي، فيجب أن يترتب على الهجمات السيبرانيّة ثمة ضررٌ بمصالح أحد أشخاص القانون الدُّولي، حيث يكون قد تم التعدي عليها من الناحية الاقتصاديّة أو من الناحيّة السيّاسيّة، أو تمس الهجمات السيبرانيّة بأحد المبادئ التّي كرّستها الأمم المتحدة من أجل حفظ السِّلم والأمن الدُّولي[2].

وقد تعرضت نظرية العمل غير المشروع للنقد من عدّة أوجه:

- إن عمليّة إسناد المسؤوليّة للدولة عن الأضرار الناتجة عن الجرائم السيبرانية التي تقوم عليها نظريّة العمل غير المشروع، تثير مشكلة تتعلَّق بصعوبة، ليبين إن كان هذا العمل منسوباً للدولة فعلا، وهذا الأمر مرتبط بالقدرة التكنولوجيّة للدولة المعتدى عليها، فيمكن للدولة منشأ التصرف (المعتدية) طمس هوية الفاعل[3].
- إن عملية نسبة العمل الدولية تزداد تعقيداً في الحالة التي لا تكون الشبكات السيبرانية هي المحور الذي تمت من خلاله هذه الهجمات، مثل عملية إرسال فيروسات توضع مباشرة في أجهزة الحاسوب الخاصّة بالدولة المعتدى عليها، أو في حالة استخدام الدولة المعتديّة إقليم دولة أخرى لتنفيذ الجرائم[4].

ثانياً: المسؤوليّة الدوليّة عن الجرائم السيبرانيّة استناداً لنظريّة المخاطر (المسؤوليّة الموضوعيّة):

ظهرت نظريّة المخاطر بعد الانتقادات التي وجَّهها الفقه لنظريّة الفعل غير المشروع، بعد أن أصبحت عاجزة عن مواكبة التطوُّر التكنولوجي والعلمي، فقد كان من نتاج هذا تطوير هذه النظرية وظهور ما يطلق علية العالم الافتراضي الذي أصبح مسرحاً تدار من خلاله شؤون الكثير من الدول في مختلف الاتجاهات، سواء أكانت سياسيّةً أو اجتماعيةةً أو اقتصاديّة، وتقوم نظريّة المخاطر على أساس مساءلة الدولة بوصفها شخص من أشخاص القانون الدُّولي متى قامت بارتكاب سلوكٍ مخالفٍ للقانون الدُّولي، وكان هذا السلوك على درجة عاليّة من الخطورة[5].

وهنا الكثير من الاتفاقيات الدوليّة التي أخذت بنظريّة المخاطر كأساس لتحديد المسؤوليّة الدوليّة، فنجد على سبيل المثال الاتفاقيّات الخاصة بالطاقة الذريّة، فهذه الاتفاقيات تُلزم الدولة متى قامت بأيّ نشاط ذرّيٍّ في وقت السّلم أن تقوم بدفع التعويض، عن كافة الأضرار الناجمة عن هذه الأنشطة،

---

[1] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد،23 مكتبة الإسكندرية، مصر، 2016، ص 65.

[2] لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة"، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، المملكة العربية السعودية، 2016، ص 19.

[3] رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، ديسمبر، 2018، ص 338.

[4] عباس بدران، الحروب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، 2010، ص 111.

[5] إيهاب خليفة، مجمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، ص 188.

وذلك بناء على قواعد المسؤوليَّة الموضوعيَّة دون أن تشترط أن يكون هناك أيُّ خطأ للدولة[1].

إن أغلب الأضرار التي تصيب دول أخرى، تكون نتيجة أعمال غير مشروعة للدُّول المتسبِّبة في تلك الأفعال أو عن طريق القيام بأنشطة مشروعة بناءً على أنظمة القانون الدُّولي، إلا أنه يتعذر إثبات عدم المشروعيّة، من هنا أقيمت المسؤوليّة الدُّوليّة على اعتبار توافر أركانها، وعلى هذا الأساس يجب أن نُبيِّن ما إذا كانت شروط المسؤوليّة الموضوعيّة تنطبق على الفضاء السيبراني:

أ. النشاط الخطر:

النشاط الخطِر، الذي يؤدِّي إلى اقتراف الجرائم السيبرانية، متمثّلٌ في نيَّةٍ لدى المجرم في إيذاء شخص ما، أو إلحاق ضرر بالشخص المعنوي إن كان مؤسّسةً أو شركةً أو دولة[2]، التي تمارسها الدُّول في هذا الفضاء تكون خطِرة على أمن الدُّول، وتهدِّد أو تُحدث إخلالاً بالسِّلم والأمن الدُّوليَّين، فنشاط الانترنت يندرج تحت بند المخاطر الدُّوليَّة التي تقع الدولة على أثرها في خانة المسؤوليَّة عند اتهامها في إحداث هجْمة سيبرانيّة دُوليّة[3].

ب. الضرر:

يتميز ركن الضَّرر في الجرائم السيبرانيّة بانّه عابرٌ للحدود، ولا يستطيع أحدٌ إنكار حقيقة أن الهجمات السيبرانيّة والأنشطة الضارّة التي تمارسها الدولة المعتديّة في الفضاء الإلكتروني تُلحق أضراراً بالدولة المعتدى عليها، إذ أن تبنِّي الدُّول الأنظمة الإلكترونية في تسيير شؤونها واتساع دائرة التعامل بوسائل التكنولوجيا والاتصال، نتج عنه أنْ أصبحت قواعد البيانات القوميّة غير سريَّة، مما عرَّضها إلى مخاطر هجمات الفضاء الإلكتروني[4].

ج. علاقة السببيّة:

من مُتطلّبات قيام المسؤوليّة الموضوعيّة، وجود علاقة سببيّة بين النشاط الخطِر والأضرار الناتجة عنها، لذا يجب إثبات أنَّ الأضرار التي لحقت الدُّول وأضرَّت أمنها القومي، ناتجٌ عن الهجمات السيبرانيّة التي قامت بها دولة أخرى(5).

فإذا تحققت الشروط السابقة في الفضاء الخارجي، تكون الدولة مسؤولةً موضوعياً لأن نشاط الدولة الخطِر هو نشاطٌ مشروعٌ لكن في الفضاء الافتراضي حتى لو تحققت تلك الشروط لا تُسأل الدولة على أساس نظريَّة المخاطر.

فإني أرى أن الأساس الذي تُبنى عليه المسؤوليّة الدوليّة عن الجريمة السيبرانيّة هو نظريّة المخاطر، لأن نشاط الدولة في الفضاء الافتراضي ليس فعلاً مشروعاً، فهو في وقت الحرب سيكون نزاعاً مسلّحاً، وفي وقت السِّلم يكون نشاطاً إجرامياً.

المطلب الثاني:

الاتجاهات الدوليّة في مكافحة الجرائم السيبرانيّة

لم يقف المجتمع الدُّولي مكفوفَ الأيدي حيال الجرائم السيبرانيّة، بل سارع الفقه والتشريع الدّولي إلى إقرار العديد من الاتفاقيّات الدوليّة للتصدِّي لتلك الظاهرة الإجراميّة الحديثة،

---

(1) د. صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، ط 1، دار الخلدونية للنشر والتوزيع، الجزائر، 2010، ص 174.

(2) شريف محمد، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة، القاهرة،2012، ص 109.

(3) عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر، 2006، ص 214.

(4) د. وسيم طعمة، السرقة المعلوماتية "دراسة مقارنة"، مجلة جامعة البحث، جامعة دمشق، العدد 68، سوريا، 2017، ص 176.

(5) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، 2016 ص 145.

فنجد دليل تالين[1] بوصفه مجموعة من الوصايا التي قدّمها الفقه الدّولي للتصدِّي للجريمة السيبرانيّة، وكذلك شرع المجتمع الدّولي اتفاقية بودابست بوصفها اتفاقية دولية لمكافحة الجريمة الدوليّة.

هذا ما نتناوله في هذا المطلب والذي قسمته إلى فرعين على النحو الآتي:

الفرع الأول: دور دليل تالين في مكافحة الجرائم السيبرانيّة

الفرع الثاني: دور اتفاقية بودابست في مكافحة الجرائم السيبرانيّة

الفرع الأول: دور دليل تالين في مكافحة الجرائم السيبرانيّة

متى تم تكْييف الجرائم السيبرانيّة على أنّها حروب، فإن دليل تالين قد تكفّل بها، فطبقاً للدليل نجد أن الجرائم السيبرانيّة تقوم بارتكابها دولة ضد دولة أخرى، وقد تم إعداد الدليل نتيجة لقصور قواعد القانون الدولي عن مواجهة هذا النوع المستحُدث من الجرائم وكذلك التشريعات الداخليّة، ومن جهة أخرى عدم وجود أيّ أساسٍ قانوني ينظم اللجوء إلى الحروب السيبرانيّة، وتم إبرام هذا الدليل من أجل دراسة مدى إمكانيّة مدى استخدام قواعد القانون الدولي الإنساني في الحروب السيبرانيّة بصفة عامة، وذلك إثر الهجوم السيبراني الشامل الذي شنّته روسيا ضد استونيا عام 2017[2].

يظهر دور دليل تالين في مواجهة الحرب السيبراني من خلال قيامه بتحديد أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية، كمفهوم نظام النزاع المسلح في إطار الحرب السيبرانية، ومفهوم الجيوش السيبرانيّة، وكيفية إدارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفة مقاتلو السيبراني، إضافة إلى إمكانية مراعاة القانون الدولي الإنساني المعروف كمبدأ التميز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكريّة كالطائرات العسكريّة بدون طيّار[3].

الفرع الثاني: دور اتفاقية بودابست في مكافحة الجرائم السيبرانيّة

إذا تم تكييف الجرائم السيبرانيّة على أنها أفعال إجرامية تنفِّذها الدّول ضدّ بعضها البعض، فقد تكفّلت اتفاقية بودابست (2011) بتحديد القانون الواجب التطبيق على تلك الجرائم، ولكن يلاحظ أنّ اتفاقية بودابست لم تتطرق للجرائم السيبرانيّة التي تشنُّها الدول ضد بعضها البعض، فقد تَحدّد نطاق الاتفاقية بالجرائم السيبرانية التي تُنَفَّذ من قبَل الأفراد ضدّ الأفراد الاخرين، ومن أسباب هذا أنّ الاتفاقية قد اعتبرَت الجرائم السيبرانيّة بأنّها جرائم وليست حروب.

ولقد تضمّنت الاتفاقية مجموعةً من القواعد التي إذا تمَّ اقترافها لابد من أنّ هذه الدول[4] تُجرِّم هذه الافعال في لوائحها الداخليّة، كما تضمَّنت العقوبات التي اشترطت أن تكون فعَّالة ورادعة ومناسبة لتلك الجرائم.

أولاً: الجرائم الواردة في اتفاقية بودابست:

عملت اتفاقية بودابست على توزيع الجرائم التي تُرتكب بواسطة الإنترنت على أربع مجموعات، تضمّ الأولى: الجرائم التي تتعرض لخصوصيّة وسلامة وتوفر الأنظمة والبيانات، مثل النفاذ غير الشرعي، والاعتراض غير الشرعي، وتشويه البيانات، وسلامة النظام. وتضم المجموعة الثانية: جرائم الاحتيال والتزوير. كما تضم المجموعة الثالثة: الجرائم المتّصلة بالمحتوى مثل إنتاج توزيع وحيازة مواد إباحيّة

---

[1] صدر دليل تالين (le manuel de Tallinn) عام 2013 المتعلق بقواعد القانون الدولي المطبقة على الحرب السيبرانية، قام بإعداد هذا الدليل مجموعة من خبراء القانون الدولي بدعوة من منظمة حلف شمال الأطلس (NATO) بحضور اللجنة الدولية للصليب الأحمر، ويتكون هذا الدليل من (95) مادة جاءت معظمها من ميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني.

[2] د. سعيد درويش ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1 ، العدد 29، ص 11.

[3] اللجنة الدولية للصليب الأحمر،" ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"، على الرابط:
http://accronline.com/article_detail.aspx?id=28958

[4] Micheal N. Schmitt,"Tallinn Manual on the International Law Applicable to Cyber Warfare ", Cambridge University press, first publishes, (2013), p117.

يُستخدم فيها الأطفال. وتضمُّ المجموعة الرابعة: جرائم الاعتداء على الملكيّة الفكريّة، والحقوق المجاورة[1].

واتفاقية بودابست تُلزم الدول الأعضاء باتخاذ التدابير التشريعيّة وكافّة الإجراءات التي تتناسب لتجريم عدد (9) الجرائم فيها، إذ تعد عماداً للجرائم السيبرانية وهي كالتالي:

- الدخول غير القانوني المتعمّد إلى أيّ نظام كمبيوتر أو جزء منه دون حقٍّ أو إذنٍ، سواء أكان هذا الدخول بنيّة انتهاك وسائل الأمن أو حتى بنيّة الحصول على معطيات الكمبيوتر، أو لأيّة نيّةٍ أخرى غير مباحة.
- الاعتراض غير القانوني المتعمّد ودون حقٍّ بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامّة إلى أو من نظام كمبيوتر، وكذلك اعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أيّ نظام كمبيوتر يحمل مثل هذه المعطيات.
- التدخل عمداً أو إرادياً في المعطيات، بالتدمير أو التشويه أو الحذف والإفساد أو تبديلها أو التعطيل، أو التعديل أو الإلغاء.
- التدخل عن عمد في أنظمة التكنولوجيا.
- سوء استعمال الأجهزة.
- التزوير المتعمَّد باستخدام جهاز الكمبيوتر: كذلك بإدخال أيٌّ حذف أو تعديل أو إخفاء بيانات الحاسب الآلي، على نحوٍ يُظهر بيانات غير البيانات الأصليَّة لتكون متوافقة قانونا، وكأنها بيانات أصليّة، وذلك بصرف النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة، ويحقُّ للدولة أن تشترط نية أو قصد الغش لقيام المسؤوليّة الجنائيّة.
- الاحتيال المتعمد باستخدام أجهزة الكمبيوتر.
- الجرائم المرتبطة باستخدام دعارة الأطفال.
- الجرائم المرتبطة بحق الملكيّة الفكريّة والمؤلِّف.

ثانياً: العقوبات الواردة في اتفاقية بودابست:

ربطت اتفاقية بودابست بين الجرائم والعقوبات، فتحدّد مختلف الجرائم السيبرانيّة أو الجرائم المتّصلة بالكمبيوتر التي ينبغي أن يعاقب عليها المقترف الجنائي، وفقاً للالتزامات التي تفرضها تلك المواد، يلزم هذا الحكم الأطراف المتعاقدة باستخلاص العواقب من الطبيعة الخطيرة لهذه الجرائم من خلال النص على عقوبات جنائيّة" فعّالة ومتناسبة ورادعة"، تشمل فيما يتعلّق بالأشخاص الطبيعيّين إمكانيّة فرض عقوبات بالسجن[2].

وقد أقرت الاتفاقية مبدأ مسؤولية الشخص غير الطبيعي أي المعنوي، عن الجريمة السيبرانيّة، حيث نصَّت المادة (12) على ما يلى: وأن الدول تتبنّى سيّاسة إجراءات تشريعية وأيّ تدابير أخرى، وذلك لضمان قيام مسؤولية الأشخاص المعنوية عن أيّ جريمة موصوفة في هذه المعاهدة، إذا ما ارتكبت لصالح الشخص المعنوي بواسطة شخص طبيعي ارتكبها بشكل منفرد أو بوصفه جزءً من جهاز تابع للشخص المعنوي ويتبوأ منصباً قيادياً داخله، وذلك علي أساس: أ- سلطة اتخاذ قرارات لصالح الشخص المعنوي "سلطة تمثيليّة".، ب- تفويض قانوني من الشخص المعنوي.، ج- سلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوي[3].

الخاتمة:

تُعدّ الجرائم السيبرانيّة، أحد أحدث صور الفعل غير القانوني، التي ظهرت في الآونة الأخيرة، فهي جريمة محلّها الفضاء الخارجي، وتتم باستخدام التكنولوجيا الحديثة، لذلك أرتبط مفهومها بجهاز الحاسب الآلي، فهي جريمة يكون الحاسب الآلي العامل الأساسي في ارتكابها، وتقع أضراراً

---

[1] د. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 2017، ص 105.

[2] د. وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، قطاع التشريع بوزارة العدل، مصر، بدون سنة نشر، ص 23 وما بعدها.

[3] د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001)، والبروتوكول الملحق بها، لأول مرة باللغة العربية، دار النهضة العربية، القاهرة، 2009، ص 22.

بمكوّنات الحاسب والنّظُم المعلوماتية، وتتميز تلك الجريمة بعدّة خصائص، فهي جريمة عابرة للحدود، حيث أن محلّها الفضاء الخارجي، كما أن الجريمة السيبرانية جريمة صعبة الإثبات والاكتشاف.

اختلف الفقه في ماهيّة الطبيعة القانونيّة للجريمة السيبرانيّة، فذهب اتجاه إلى أنها نوع جديد من الحروب الدوليّة، تستهدف به الدولة المعتديّة التجسس والإضرار بالنّظم التكنولوجيّة العسكريّة والاقتصادية للدولة المعتدى عليها، بينما ذهب جانب آخر إلى أنها تدخل في نطاق الجرائم الدوليّة.

تتميز الجرائم السيبرانيّة بأنها تكتسب خصوصيتها من أركانها وأساسها، فأركان المسؤوليّة الدوليّة تتمثّل في نسبة الفعل إلى دولة وليس إلى شخص من أشخاص القانون الخاص، فالدولة المعتديّة تقوم بأفعال غير مشروعة ينتج عنها ضرر يصيب الدولة المعتدى عليها.

يمكن بناء المسؤوليّة الدوليّة عن الجريمة السيبرانيّة إلى نظريّة المخاطر حيث أنها الأنسب، فهي تقوم على أساس المسؤوليّة الموضوعيّة المفترضة، مما يسهل على المضرور إثبات عناصر الجريمة، أما نظريّة العمل غير المشروع فلا تتماشى مع طبيعة الجريمة السيبرانيّة، فمن الصعوبة نسبة الجريمة إلى فاعل.

سارع المجتمع الدّولي إلى مواجهة الجرائم السيبرانيّة لإدراكه التام بخطورتها، فقدّم الفقه الدولي دليل تالين، والذّي يتمثّل في مجموعة توصيّات تَقدّم بها خبراء القانون الدّولي، والتي ترمي إلى تحديد مفهوم الجرائم السيبرانية وكيفية إدارة الاشتباكات الإلكترونيّة، كما وضع المجتمع الدولي اتفاقية بودابست، والتي تشمل مجموعةً من القواعد الموضوعيّة، متمثّلة في أفعالٍ إجرامية، تقوم الدولة بتجريمها في تشريعاتها الداخليّة، ووضع العقوبات المناسبة لها، وكما تضمنت الاتفاقية بعض العقوبات، واشترطت علي الدّول أن تكون العقوبات فعّالة ومتناسبة ورادعة، كما أقرّت الاتفاقية مبدأ مسؤوليّة الشخص المعنوي عن الجرائم السيبرانيّة.

النتائج:

- إن تنصيب الهجمات السيبرانيّة في المحور القانوني الدّولي القائم على أمرٍ بالغ الأهمية، وذلك لطبيعته الخاصة إضافة إلى عدم وجود نظامٍ قانوني رسمي ونهائي متفقٌ عليه بشأن هذه الظاهرة.
- إن هناك سباقاً للتسلح السيبراني والإلكتروني بين الدول، وذلك لرغبة الدّول المتزايدة في تعزيز دفاعاتها ضدّ خطر التعرض للهجمات السيبرانيّة.
- إن هناك جهوداً دوليّة، وإقليميّة، لمواجهة هذه الظاهرة، وذلك من خلال المؤتمرات والاتفاقيّات الدوليّة، لمنع الجريمة السيبرانيّة ومعاملة المجرمين السيبرانيّين.
- إن الجرائم السيبرانيّة بوصفها جرائم عالميّة عابرة للحدود لا تتحقّق مكافحتها إلا من خلال التعاون الدّولي على المستوى الإجرائي الجنائي.
- إن الجرائم السيبرانيّة تُعدّ عملاً غير مشروع، فهي بحد ذاتها تنتهك أحكاماً وقواعد القانون الدولي، فيترتّب عليها اختراق أسرار ووثائق الدّول، وهي تستهدف مصالح الدولة، وتعمل على اختلاق قضايا دوليّة جديدة لم تعرفها الدّول في زمن الحروب التقليديّة.
- أن بناء المسؤوليّة الدوليّة عن الهجمات السيبرانيّة في سياق نظريّة العمل غير المشروع قد لا تحقّق أهدافها، والسبب هو صعوبة تحديد هويّة المهاجم السيبراني، وهذا بحد ذاته يُعدّ عائقاً أمام تحقيق أهداف القانون الدّولي باعتباره يُنظّم قواعد المسؤولية المتعلّقة بانتهاكات القانون الدّولي العام والقانون الدّولي الإنساني.
- تعدّ اتفاقية بودابست من أهم الوثائق الدوليّة لمكافحة الجرائم السيبرانيّة، وتبدو أهميّتها في إقرارها إجراءات وقواعد تلتزم الدول المنظّمة بإدراجها في تشريعاتها الداخليّة والتي تهدف إلى حفظ بيانات الاتّصال وتحديد مصدرها.
- وضعت اتفاقية بودابست قواعد من الأفعال الإجراميّة، التي كان من الجدير بالدولة تجريمها عند وضع قانون لمواجهة الجرائم السيبرانيّة، كما تُرك تحديد العقوبات للتشريعات الجنائيّة، على أن تكون العقوبات متناسبة مع الأفعال الإجرامية.

التوصيات:

- لابد من تحقيق الأمن السيبراني، وحفظ الحقوق المترتّبة على الاستخدام المشروع للحاسبات الآليّة، والشبكات المعلوماتيّة.
- سدّ الفراغ التشريعي في مجال مكافحة الجريمة السيبرانيّة، وضرورة سنّ التشريعات التي تغطي هذا الفراغ، من أجل الوصول إلى فضاء سيبراني آمن.
- تطوير اللوائح التشريعيّة الجنائيّة الداخليّة، بما يتماشى مع الجهود الدوليّة في مكافحة الجرائم السيبرانيّة.
- تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية والأمنية المتبادلة في مجال مكافحة الجرائم السيبرانية.
- يوصي الباحث بإنشاء شراكات بين القطاعين العام والخاص على المستوى الوطني والإقليمي والدولي لمكافحة الجرائم السيبرانيّة، وتبادل الخبرات وتحسين طرق مكافحتها بوصفها جرائم عابرة للحدود الوطنيّة.
- نوصي بالعمل على تحقيق الأمن السيبراني ومكافحة الجرائم السيبرانية، وكذلك حفظ الحقوق الناتجة عن الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتيّة.
- نوصي بتفعيل التعاون بين الدول بما ينتج عنه تعظيم دور المعاهدات الدولية، وبما يرمي إلى إقرار مبدأ المساعدة القضائية والقانونية والأمنية بين كافة الجهات في حقل مكافحة الجرائم السيبرانية.
- نوصي بتطوير بنية التشريعات العقابية الداخلية للدول، وذلك بما يتوافق مع الجهود التشريعية الدولية في مجال مكافحة الجريمة السيبرانية.
- العمل على تكثيف الدراسات، ووضع مشاريع، وابتكار تقنيات جديدة لمعرفة المهاجم السيبراني، وبها نتجاوز عقبة إخفاء الهوية للقائم بالهجوم الذي يُعدّ من الصعوبات الكبرى التي تواجه إثبات المسؤوليّة.

قائمة المراجع

أولاً: المراجع بالعربية:

- **الكتب:**

- د. أحمد بشارة موسى، المسؤولية الجنائية الدولية للفرد، دار هومة للنشر والتوزيع، الجزائر، 2009.
- أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2014.
- د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001)، والبروتوكول الملحق بها، لأول مرة باللغة العربية، دار النهضة العربية، القاهرة، 2009.
- إيهاب خليفة، مجمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة.
- د. باطلي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.
- جانكارلو أ. باراليتا، النزاع السيبراني والاستقرار الجيوسيبران، الاتحاد الدولي للاتصالات، القاهرة، 2011.
- د. جميل عبد الباقي الصغير، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1998.
- د. جوزيف ناي، المنازعات الدولية مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، 2011.
- د. حسنين إبراهيم صالح عبيد، الجريمة الدولية، دراسة تحليلية تطبيقية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1979.
- د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
- د. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011.

- د. زياد البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، 2003.
- د. صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، ط 1، دار الخلدونية للنشر والتوزيع، الجزائر، 2010.
- صلاح الطائي، حق الاسترداد في القانون الدولي، مكتبة الجامعة الحديثة، القاهرة، 2009.
- د. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.
- د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، 2016.
- عباس بدران، الحروب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، 2010.
- د. عبد الفتاح بيومي حجازي، المحكمة الجنائية الدولية دراسة متخصصة في القانون الجنائي الدولي، دار الفكر الجامعي، الإسكندرية، 2004.
- عبد الفتاح بيومي حجازي، الإثبات الجنائي "جرائم الكمبيوتر والإنترنت"، بدون ناشر، 2007.
- عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر، 2006.
- د. فتوح عبد الله الشاذلي، القانون الدولي الجنائي، أولويات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، الطبعة الثانية، دار النهضة العربية للنشر والتوزيع، 2016.
- د. محمد أمين الشوابكة، جرائم الحاسب والإنترنت، دار الثقافة، الأردن، 2011.
- د. محمد عبدالله أبو بكر، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، 2006.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004.
- محمود محارب، قراءات في كتاب حرب الفضاء الإلكتروني، اتجاهات تأثيرات على إسرائيل، المركز القومي للأبحاث ودراسة السياسات، الدوحة، 2011.
- د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر.
- محمد عبد الله، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، 2018.
- إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، الإسكندرية، مكتبة الإسكندرية، 2013.
- عبد الصمد سرحان، التعاون الدولي الأمني في مكافحة الجرائم المعاصرة، القاهرة، مطابع كلية الشرطة، 2010.
- جميل عبد الباقي، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2010.
- شريف محمد، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة، القاهرة، 2012.
- راشد محمد المري، الجرائم السيبرانية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، سنة 2018.
- عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد،23 مكتبة الإسكندرية، مصر، 2016.

- **الدوريات:**

- رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، ديسمبر، 2018.

- د. سعيد درويش، ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر 1، العدد 29.
- لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة "، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، المملكة العربية السعودية، 2016.
- د. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 2017.
- د. وسيم طعمة، السرقة المعلوماتية "دراسة مقارنة"، مجلة جامعة البحث، جامعة دمشق، العدد 68، سوريا، 2017.

ثانياً: الكتب باللغة الأجنبية:

- MERWA (VANDER), COMPUTER CRIMES AND OTHER CRIMES AGAINST INFORMATION TECHNOLOGY IN SOUTH AFRICA, R.I.D.P, 1993.
- Roden (Adrian), computer crime and the law, c, l, j.,1991, vol.15.
- Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008.
- Richard Kissel Glassory of Information Security Terms, National Institute of Standers and technology, U.s Department of Commerce, (2013).
- U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication as amended through Feb, (2012).
- Clay Wilson, Cyber Crime. In Franklin D. Kramer et al (eds), Cyber power and National Security, Potomac Book, (2009).

.