IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة كلية الكوت الجامعة للعلوم الإنسانية
ISSN (E): 2707 – 5648 II ISSN (P): 2707 – 563x
www.kutcollegejournal1.alkutcollege.edu.iq
k.u.c.j.hum@alkutcollege.edu.iq
عدد خاص لبحوث المؤتمر العلمي الثالث لكلية القانون - جامعة واسط للمدة من 17 - 18 نيسان 2024

الموقف الدولي من الجرائم السيبرانية

م. د. محمد كريم علي [1] ، م. د. كرار رياض السيد [2]

المستخلص

شهد العالم تطورات سريعة في مجال تقنيات المعلومات والاتصالات فاتساع استخدام الحاسوب وما تبعه من استخدام الشبكة الدولية الإنترنت، وما نتجة عنه من انماط جديدة من السلوك الإجرامي حيث أصبحت الجرائم الالكترونية والهجمات السيبرانية تمثل خطراً كبيراً على امن الدول حيث أن هذه الجرائم لاتكون ضمن حدود الدولة ، بل تتخطى الحواجز والحدود جاعلة من العالم مسرحاً واحداً، وان حداثة الجريمة السيبرانية والسرعة في ارتكابها وتطورها، جعلت من الصعوبه مكافحتها من خلال القوانين الوطنية وهذا الأمر دفع الدول الى التعاون الدولي من خلال عدة وسائل دولية ومنها الاتفاقيات الدولية والمنظمات الدولية من اجل مكافحتها.

الكلمات المفتاحية : الموقف الدولي ، الجرائم، السيبرانية

انتساب الباحثين
[1] كلية المعلوماتية الطبية الحيوية، جامعة تكنولوجيا المعلومات والاتصالات،العراق، بغداد، 10069

[2] كلية القانون، جامعة ميسان، العراق، ميسان، 62001

[1] fintish.mk1990@gmail.com
[2] karar.alkhefe@gmail.com

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : كانون الثاني 2025

The International Position on Cybercime

Dr. Mohammed Karim Ali [1] , Dr. Karrar Riyadh Sayyid [2]

Abstract

The world has witnessed rapid developments in the field of information and communication technologies, the widespread use of computers, the subsequent use of the Internet, and the resulting new patterns of criminal behavior. Cybercrimes and cyberattacks have become a major threat to the security of states as these crimes are not within the borders of the state, but go beyond barriers and borders, making the world a single theater. The modernity, speed and development of cybercrime have made it difficult to combat it through national laws. This has prompted countries to cooperate internationally through several international means, including international agreements and organizations The international community in order to combat it.

Keywords: The International Position, Crimes, Cyber

Affiliation of Authors
[1] Biomedical Informatics College, University of Information and Communications Technology, Iraq, Baghdad, 10069

[2] College of Law, Maysan University, Iraq, Maysan, 62001

[1] fintish.mk1990@gmail.com
[2] karar.alkhefe@gmail.com

[1] **Corresponding Author**

Paper Info.
Published: Jan. 2025

المقدمة

في ضوء التطور الكبير في مجال تقنيات الاتصالات والمعلومات، حيث أصبحت شاملة لأغلب القطاعات والأنشطة الاقتصادية والاجتماعية، وهي تعد فرص جديدة للتنمية، إلا أنه مع هذا التطور قد نتجه عنه زيادة المخاطر الإلكترونية نتيجة الاستخدام السيئ لهذه التكنولوجيا، حيث إن أغلب التعاملات في الوقت الحاضر تتم إلكترونيا بالإضافة إلى تزايد أعداد مستخدمي الإنترنت، وما أدى إلى ظهور ما يسمى بالجرائم السيبرانية، وحول خطورة هذه الجرائم عملت الدول على سن تشريعات لمواجهة هذا النوع من الإجرام، وهذا ما لجأ آلية المجتمع الدولي على حد سواء، وذلك من خلال إصدار إعلانات دولية، وإبرام اتفاقيات التي تحد من هذه الجرائم حيث يرى المجتمع الدولي إلى أن مرتكبي الجرائم السيبرانية اصبحوا يبسطون نفوذهم على جميع أرجاء العالم، بفضل مايملكونه من قوة ونفوذ ودهاء، وصار هنا حتمية التعاون الدولي لمواجهه ازدياد ضراوة الإجرام، وظواهرة المختلفة في كل بلاد العالم، مما جعل الدول مهما بلغت درجتها من القوة والتطور لاتستغني عن الدخول في علاقات تعاونية متبادلة مع غيرها من

دول، ولم تعد جهودها الداخلية في المكافحة أو الملاحقة كافية لتحقيق منع الجريمة او تقليص حجمها، كونها قد قوبلت بالعديد من المصاعب لا سيما مع طبيعة المجرم الإلكتروني ومع الطبيعة المعقدة للجرائم في نظم المعلومات والتكنولوجيا والتي تختلف اختلافا جذريا عن الجرائم العادية الداخلية كما تختلف عن الجرائم العابرة للحدود ومع اتساع مسرح ارتكاب الجرائم السيبرانية الى دول العالم المختلفة، لجأ المجتمع الدولي لمكافحة هذه الجرائم عن طريق التعاون الدولي كاليه لتعزيز الأمن الدولي وذلك كونها تمثل تهديدا على جميع مفاصل الحياة.

أهمية البحث

إن دراسة موضوع الجرائم السيبرانية له أهمية للوقوف عليها كونها امتد تأثيرها على جميع مجالات الحياة ومع تزايد مخاطرها وانتشارها بصورة كبيرة في جميع دول العالم، وقد غدت تشكل خطرا يهدد الاستقرار الدولي والأمن الداخلي للدول وعلى هذا الأساس تعد محط اهتمام الدول الهيئات الدولية، وذلك لأن عالمية الإجرام تتطلب عالمية المواجهة، باعتبارها تمثل تحديا يواجه أجهزة إنفاذ القانون مما يجعل جميع الدول في حاجة ماسة إلى تفعيل التعاون الدولي في جميع المجالات التشريعية الأمنية والقضائية من خلال إبرام اتفاقيات معنية في مجال مكافحة الجرائم السيبرانية.

أهداف البحث

يرمي هذا البحث إلى الوقوف على طبيعة الجرائم السيبرانية، ومحاولة بيان بما تتميز به من خصائص، وإلقاء الضوء على أهم أشكال ووسائل التعاون الدولي في مجال مكافحتها، والتعرض لآليات التعاون بمختلف صورها القانونية ،والأمنية على المستوى الدولي.

إشكالية البحث

ما تتميز به الجرائم السيبرانية من التعقيد والغموض إذ يصعب وضع قواعد قانونية منضبطة تحكم جميع أنشطتها، ومناهج مكافحتها تثير عديدا من القضايا المتعلقة بالتعاون الدولي باعتبار أن هذا التعاون، قد يمس السيادة الوطنية للدول ومدى فاعلية الاتفاقيات الدولية المعنية بمكافحة الجرائم السيبرانية.

منهجية البحث

يعتمد هذا البحث منهجا وصفيا تحليليا من خلال تسليط الضوء على ما تتميز به الجرائم السيبرانية من خصائص، وبيان أهم الاتفاقيات والهيئات الدولية المعنية في مجال مكافحة الجرائم السيبرانية ،من خلال بيان النصوص الواردة في تلك الاتفاقيات وبيان مدى فاعليتها.

خطة البحث

سنتاول البحث من خلال مبحثين وهما : المبحث الأول: ماهية الجرائم السيبرانية ، ونتناول في هذا المبحث من خلال ثلاثة مطالب وهما المطلب الأول مفهوم الجرائم السيبرانية ،والمطلب الثاني خصائص الجرائم السيبرانية، و المطلب الثالث أركان الجريمة السيبرانية ،وأما المبحث الثاني دور القانون الدولي في مكافحة الجرائم السيبرانية، ونتناول في هذا المبحث مطلبين ،وهما المطلب الأول: دور الاتفاقيات في مجال مكافحة الجرائم السيبرانية ، والمطلب الثاني: موقف المنظمات الدولية من الجرائم السيبرانية.

المبحث الاول: ماهية الجرائم السيبرانية

في ضوء التطور الكبير في مجال تقنيات الاتصالات والمعلومات، حيث أصبحت شاملة لأغلب القطاعات والأنشطة الاقتصادية ،والاجتماعية وهي تعد فرص جديدة للتنمية ،إلا أنه مع هذا التطور قد نتجت عنه زيادة المخاطر الإلكترونية نتيجة الاستخدام السيئ لهذه التكنولوجيا ،حيث إن أغلب التعاملات في الوقت الحاضر تتم إلكترونيا، بالإضافة إلى تزايد أعداد مستخدمي الإنترنت وما أدى إلى ظهور ما يسمى بالجرائم السيبرانية ، ويشير مصطلح الجريمة السيبرانية إلى أي جريمة تتضمن الحاسوب أو الشبكات الحاسوبية، قد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو الهدف وحول خطورة هذه الجرائم عملت الدول إلى سن تشريعات لمواجهة هذا النوع من الإجرام. وعليه سنقسم هذا المبحث الى ثلاثة مطالب على النحو الآتي:

المطلب الاول: مفهوم الجرائم السيبرانية

إن مصطلح الجرائم السيبرانية (الإلكترونية) مصطلح يستخدم لوصف النشاط الإجرامي على نطاق واسع حيث تكون أجهزة الكمبيوتر أو شبكات الكمبيوتر أداة أو هدفا أو مكانا للنشاط الإجرامي وتشمل كل شيء من الاختراق الإلكتروني إلى هجمات، ويمكن للجرائم الإلكترونية أن توقف أي شي يتعلق بالمعلومات والاتصالات مثل وتوقف سكة خط حديد، أو مطار أو محطة

كهرباء وغيرها، وتعد الجرائم السيبرانية من أكثر الجرائم خطورة وانتشارا خلال السنوات الأخيرة، نظرا لاعتماد العديد من المؤسسات الحكومية والشركات على تقنيات المعلومات والاتصالات في تعاملاتها، والتي أصبحت جزءا لا يتجزأ في مجالات الحياة على الرغم من سهولة في السرعة والوصول والتواصل ونقل المعلومات إلا انها أصبحت وسيلة لارتكاب نوع جديد من الجرائم وهو ما يعرف بالجرائم السيبرانية. [1] وعلية سنبين في هذا المطلب الآتي:

اولا: التعريف اللغوي

في ما يلي تعريف كلمة سايبر في قواميس اللغوية العالمية: [2]

1- قاموس أكسفورد: كلمة يونانية الأصل وتعود إلى مصطلح (kybernetes) والذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بعد.
2- قاموس مصطلحات الأمن المعلوماتي السيبرانية: وهو هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونيا لتعطيلها وتدميرها أو الإضرار بها.

ثانيا: التعريف الاصطلاحي

تعددت تعريفات الجريمة السيبرانية فقد عرفها البعض بأنها "الجرائم التي تهدد الأمن السيبران والتورط فيها ويسمى (بالجريمة السيبرانية) وتتكون الجريمة السيبرانية من (cybercrime) من مقطعي هما: الجريمة (Crime) والتي تعني الأفعال الخارجة عن القانون، والسيبرانية (Cyber) تستخدم لوصف استخدام الحاسب الآلي في هذه الجرائم. [3]

وعرفها البعض الآخر بأنها" نشاط إجرامي تستخدم فيه التقنية الإلكترونية الرقمية (الحاسوب الآلي وشبكة الإنترنت) بطريقة مباشرة او غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف [4]."

ويتفق الأستاذ محمد أمين الشوابكة مع الأستاذ (middet) بأن الجريمة السيبرانية تسهل استخدام الحاسوب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به للحاسوب الآلي أو البيانات الرقمية لتشمل الاعتداءات المالية المادية [5]

وقد عرفت القيادة الإستراتيجية الأمريكية الجريمة السيبرانية: هو تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الإستخدام الفعال لها فضلا عن التسلل الى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها [6] وهذا التعريف يتفق مع ماجاء في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، في مضمون المادة (5) والتي نصت" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير اخرى لتجريم الفعل، التالي في قانونها الوطني اذ ما ارتكبت عمدا وبغير حق الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات كمبيوتر. [7]

وكماعرفها الفقيهان (Michel _ redo) بانها سوء استخدام الحاسب، ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به. [8]

وعليه نجد تعدد تعاريف الجرائم السيبرانية ، يرجع ذلك الى اختلاف الاراء في تبني مفهومها فهنالك من ينظر اليها من زاوية فنية وأخرى قانونية وهنالك جانب اخر ينظر الى وسيلة ارتكابها أو موضوعها .ويمكن أن نعرف الجريمة السيبرانية: بأنه كل فعل جرمة القانون ارتكب عن طريق استخدام وسائل الاتصال الانترنت بواسطة الحاسب الالي للولوج غير المصرح به للانظمة السيبرانية أو البيانات الالكترونية بهدف أحداث اضرار او تعطيل او سرقة المعلومات.

المطلب الثاني : خصائص الجريمة السيبرانية

إن الجريمة السيبرانية شكل متطور من أشكال الجريمة عبر الوطنية وهي بطبيعتها جرائم لا حدود جغرافية أو دولية واضحة لها حيث تتم باستخدام الحاسب الآلي وشبكة الإنترنت في ارتكابها ومن ثم من الصعوبة معرفة مرتكبي هذه الجرائم .ومن اهم خصائص الجريمة السيبرانية وهي:

1- الطبيعة الدولية للجريمة السيبرانية

تتميز الجريمة السيبرانية بكونها جريمة متجاوزة الحدود الوطنية وعابرة للدول والقارات اذ انها لا تخضع لنطاق إقليمي محدد إذ أعطى انتشار اجهزة الحاسوب في كل الدول وامكانية ربطها عبر الانترنت ضمن الشبكة العنكبوتية من غير أن تخضع للحدود والزمان والمكان ومن هنا لا بد من وجود تنظيم دولي يتلائم معها

لمكافحة هذا النوع من الجرائم وضبط مرتكبيها، وتظهر ايضا مشاكل عدة ومنها حول جهه صاحبة الاختصاص القضائي لهذه الجريمة واشكالات اخرى تتعلق بإجراءات الملاحقة القضائية وتتشابه هذه الجريمة مع الجرائم المنظمة. [9]

2- صعوبة الاكتشاف

لاتحتاج الجريمة السيبرانية الى اي عنف، او سفك الدماء أو اثار اقتحام لسرقة الاموال، انما هي أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزنة في ذاكرة الحاسب الالي حيث إنها لاتترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه ومما يزيد من صعوبة إثبات هذه الجرائم ايضا ارتكابها عادة في الخفاء وعدم وجود أي أثر كتابي عند تنفيذها وتعد الوسيلة المستخدمة لإرتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال اقل من ثانية واحدة وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بهدوء دون إحداث اي ضجة، وذلك على خلاف الكثير من الجرائم [10] إذ إن مجرمي الانترنيت هم أولئك الذين يتمتعون بامتيازات أكبر نسبيا ولديهم إمكانية الوصول الى الهدف المعنى ويتميزون بمستوى أعلى من مهارات الشخص العادي. [11] ويرجع صعوبة الاكتشاف الى عدة اسباب. [12]

- إنها كجريمة لاتترك اثرا بعد ارتكابها.
- صعوبة الاحتفاظ الفني باثارها إن وجدت.
- تحتاج الى خبرة فنية يصعب على المحقق التقليدي التعامل معها.
- تعتمد على الخداع في ارتكابها والتضليل في التعريف على مرتكبيها.
- تعتمد على الذكاء المرتفع في ارتكابها .

3- حداثة الجريمة السيبرانية

تتميز الجريمة السيبرانية بأنها من الجرائم المستحدثة، والتي تشكل خطرا في ظل العولمة التي طرأت على المجتمع الدولي، والثورة التكنولوجية في مجال المعلومات والاتصالات، حيث تتميز بالغرابة كون الوسيلة التي ترتكب فيها الجريمة بواسطة أجهزة الكمبيوتر، إذ إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة إذ يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها. [13]

وعليه نرى أن ما تتميز به الجريمة من خصائص جعلتها تختلف عن الجرائم التقليدية الأخرى، وهذا الأمر جعل من الصعوبة مكافحتها فلا بد من قيام الدول إلى تحديث تشريعاتها مع ما يتوافق مع هذه الجرائم. وإن للجرائم السيبرانية أهداف وهي ليست على سبيل الحصر ومنها:

1- التمكن من الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو الاطلاع عليها وحذفها.
2- التمكن من الوصول بواسطة الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات لتعطيلها أو التلاعب بمعطياتها.
3- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا، كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم إما لتحقيق هدف مادي أو سياسي.
4- الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات.

المطلب الثالث: أركان الجريمة السيبرانية

تتخذ الجريمة المرتكبة عبر الإنترنت من الفضاء مسرحا لها ،مما يجعلها تتميز بخصوصيات تنفرد بها ولا تختلف أركان الجريمة السيبرانية عن غيرها من الجرائم التقليدية، فهو لا بد من توافر الأركان العامة للجريمة بالإضافة إلى الركن الدولي في حالة ارتكابها من خارج الحدود فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل . وعليه سوف نبين أركان الجريمة السيبرانية على النحو الآتي:

أولا: الركن الشرعي (القانوني)

يقصد بالركن الشرعي (لا جريمة ولا عقوبة إلا بنص) وهذا يعد من المبادئ الراسخة في القانون الجنائي وعلي ذلك نصت المادة الأولى من قانون العقوبات العراقي على أنه (لا عقاب على فعل أو امتناع إلا بناء على قانون ينص على تجريمه وقت اقترافه ولا يجوز توقيع عقوبات أو تدابير لم ينص عليها القانون).

إلا أن هنالك أنماطا من السلوك جاءت نتيجة وسائل متقدمة تكنولوجيا لا يمكن أن ينطبق عليها النصوص العقابية وان تطبيقها سيولد مشكلة لأن ذلك يعد خروجا على مبدأ الشرعية الذي يتعين على القضاء أن يلتزم به هذا من جانب ومن جانب آخر أنه لا يمكن التوسع في تفسير النصوص لأن من شأنه سيوسع من دائرة التجريم وهذا الواقع يفرض تدخلا تشريعيا نظرا لغياب النصوص التي

تحكم الوقائع المعروضة وعدم انطباق النصوص التقليدية على هذه الوقائع .[14]

ثانيا: الركن المادي

لقد وضحت المادة (28) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل الركن المادي للجريمة بأنه " سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون " ويتكون الركن المادي من ثلاثة عناصر :

1- السلوك الإجرامي

السلوك الاجرامي وهو عبارة عن فعل أو نشاط يصدر من الجاني، ويتخذ مظاهر خارجية يسهل الاستدلال عليها [15] ويعد السلوك الإجرامي من أهم عناصر الركن المادي لأي جريمة ،لأنه يكشف عن سلوك مخالف لإرادة المشرع وقد يكون هذا السلوك ايجابي بصورة قول او فعل يجرمه القانون يصدرعن الجاني ،وهذا السلوك محظروا قانونا فهو يشكل جريمة، مثل السرقة او الضرب وغيرها اما السلوك الآخر، فهو السلبي أي الامتناع عن عمل أمر به القانون ،مثل امتناع الطبيب عن إسعاف المريض اي هنا أمتنع عن عمل يوجب عليه القانون .[16] إلا أننا نجد أن الجاني في الجرائم السيبرانية يختلف عن الجاني في الجرائم التقليدية، من حيث كونه ذو خبرة كافية في مجال استخدام تطبيقات أنظمة التقنيات المعلوماتية الحديثة، فإن السلوك الإجرامي الذي سيصدر منه في مجال ارتكاب الجريمة الإلكترونية حتما سيختلف عن الجاني التقليدي، ففي جريمة الإرهاب الإلكتروني، فإن السلوك الجرمي هنا، هو إطلاق صفحات ومواقع تدعو وتحرض على الإرهاب والتطرف والتكفير والانضمام إلى الجماعات المسلحة وغيرها من الأعمال الإرهابية.[17]

وعليه تعد الجرائم السيبرانية من الجرائم الإيجابية ويتمثل ذلك في النشاط الإرادي الخارجي الذي يستخدم فيه الجاني أعضاء جسمه لإحداث الأثر الخارجي المحسوس ويتجسد هذا الفعل بممارسة نشاط تقني والشروع فيه باستخدام الحاسب الآلي متصل بشبكة الإنترنت في بيئة رقمية .[18]

2- النتيجة الإجرامية

ويقصد به الأثر المادي الذي نتجه عن السلوك الإجرامي، سواء كان فعلا أم ترك للفعل ،وهو الأثر الخارجي الذي يتولد عن السلوك ويحدث تغيير يعتد به القانون، وذلك طبقا للتصور المادي للجريمة أما التصور الشرعي أو القانوني فهو الاعتداء على مصلحة يحميها القانون، وبالتالي تعتبر الأثر المباشر للسلوك الجرمي غير المشروع وأما النتيجة الجرمية في الجرائم الإلكترونية، يثور النقاش بشأنها فيما إذا كانت نتيجة الفعل الجرمي في العالم الافتراضي أم في العالم الحقيقي، وفي الحقيقة الفرضيتين محتملات الحدوث في الجرائم السيبرانية فالسلوك قد أحدث تغيرا ملموسا ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى. [19]

3- الرابطة السببية

تعد الرابطة السببية هي العلاقة التي تربط بين الفعل والنتيجة،وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وأهمية الرابطة السببية ترجع إلى أن إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، إذ لا يعد مسؤولا عن النتيجة التي تحققت إذا كانت الجريمة غير عمدية، فإن نفي الرابطة السببية يؤدي إلى انتفاء المسؤولية كليا عنه، ذلك أنه لا شروع في الجرائم غير العمدية. [20]

وعليه نجد أن تحديد الركن المادي في الجرائم المرتكبة عبر الإنترنت تثير جملة من الصعوبات كون الجريمة ارتكبت عن طريق الوسائل التقنية وهذا ما يميز ركنها المادي الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي بالإضافة إلى اتصالها بالإنترنت وهنا الصعوبة تكون تحديد بداية النشاط التقني أو الشروع فيه ومكان البداية واكتمال الركن المادي.

ثالثاً: الركن المعنوي

لقد وضحت المادة (33) من قانون العقوبات العراقي في فقرتها الأولى على أنه "القصد الجرمي هو توجيه الفاعل إرادته إلى ارتكاب الفعل المكون للجريمة هادفا إلى نتيجة الجريمة التي وقعت أو أي نتيجة جرمية أخرى." ويتضح من هذا التعريف أن للقصد الجنائي مقومين هما إرادة السلوك الإجرامي والنتيجة الجريمة والعلم بها.

وان الركن المعنوي يتمثل في القصد الجنائي العلم والإرادة ،وحتى يسأل الشخص عن الجريمة، ودون توافر هذا الركن إلى جانب الركن المادي والقانوني لا يمكن أن يسأل الشخص عن هذه الجريمة [21] ،ويقوم الركن المعنوي للجريمة الإلكترونية على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه

الإرادة إلى القيام بعمل غير مشروع جرمه القانون ،كانتحال شخصية مزود خدمة عبر الإنترنت وسرقة أرقام البطاقات الائتمانية فالجرائم الإلكترونية يختلف فيها الركن المعنوي من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى النظام الحاسب الآلي تتطلب قصدا جنائيا عاما- يتمثل في علم الجاني بعناصر الركن المادي للجريمة ،أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فإن الدخول إلى الحاسب الآلي خطا أو سهوا ونتج عنه أضرار للآخرين ينفي عنه القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي على الحاسب. [22]

رابعاً: الركن الدولي

إن تسمية الركن الدولي ناتجا من أن هذه الجريمة قد تكون عابرة للحدود الوطنية ومن المعلوم والثابت أن التقنية ووسائلها اخترعت لتسهيل حياة الناس ولكن تمت إساءة استخدامها من قبل المجرمين إذ إن تقنية شبكات المعلومات قد ساعدت المجتمعات المعاصرة على التواصل الحضاري والثقافي إلا أنها من الجانب الآخر أسهمت بشكل ملحوظ فيما يمكن تسميته ب (عولمة الجريمة)، وأصبحت تحديات الجريمة عابرة للحدود قضية تهدد الأمن الدولي .[23] وفي ضوء ما تقدم يمكن أن نبين شروط قيام الركن الدولي للجريمة السيبرانية: [24]

1- يجب أن تقع الجريمة السيبرانية إما بناء على خطة أي تدبير من دولة ضد دولة أخرى، أو عن طريق منظمات تابعة لها أو أشخاص تابعين لها، سواء أكان القيام بها سلوك مباشر أم بتشجيع منها، أم بقبول منها فإذا قام الجاني بارتكاب الجريمة عن طريق الحاسوب الحكومي فإنهم يسألون عنها، وذلك لأن القانون الدولي الجنائي يحرك مسؤوليتهم الجنائية، فالجاني هنا يعمل باسم الدولة ولحسابها ولا يشترط فيه أن يكون حاملا جنسيتها.
2- حتى تكون الجريمة متحققة يشترط أن يؤدي السلوك الإجرامي إلى إحداث ضرر بدولة ما ،أو أحد أفرادها أو مؤسساتها أو ملكيتها أو أموالها ،وأن تؤدي تلك الأفعال إلى إحداث ضرر بالعلاقات الدولية.
3- انعقاد الاختصاص للقضاء الجنائي الدولي في الفصل في النزاع القضائي القائم بمناسبة وقوع احدى صور الجرائم الدولية، مع الضرورة العمل بمبدأ التكامل الوارد في النظام الأساسي للمحكمة الجنائية الدولية، حيث تجدر الاشارة الى ان عدم توفر الركن الدولي يؤدي الى اعتبار الجريمة المرتكبة جريمة وطنية تخضع للقضاء الوطني لكل دولة.

وعليه نجد أن الركن الدولي يدور وجودا وعدما مع طبيعية الجرائم السيبرانية فإذا كانت الجريمة عابرة للحدود الوطنية فإن الركن الدولي للجريمة يتحقق مع توفر شروطه وأما في حالة ارتكبت الجريمة السيبرانية داخل الحدود الوطنية للدولة فإنه يشترط لقيامها تحقق الأركان العامة للجريمة دون الركن الدولي.

المبحث الثاني: دور القانون الدولي في مكافحة الجرائم السيبرانية

تشكل الجريمة السيبرانية تحديا خطيرا لأجهزة العدالة الجنائية، في كثير من بلدان العالم ولا سيما بعد أن أكتسب هذا النوع من الجريمة بعدا دوليا في ظل التطور التكنولوجي والتي شهدها العالم في العقد الأخير، مما يستلزم المبادرة للتصدي لهذه الظاهرة على الصعيد الدولي، حيث أدرك المجتمع الدولي أن مشكلة الجرائم السيبرانية هي ليست مشكلة فردية تهم دولة واحدة فحسب، بل تهم المجتمع الدولي برمته إذ إن المنظمات الإجرامية أصبحت تبسط نفوذها على جميع أرجاء العالم، بفضل ما تملكه من خبرة وسهولة اقتراف الجريمة وعليه لقد اتجهت الدول إلى عدة وسائل لغرض مكافحتها ومنها عقد الاتفاقيات الدولية وإقامة المؤتمرات لغرض الوقوف على أهمية مكافحة الجرائم السيبرانية لكونها تهدد الأمن القومي، ألا إنها على الرغم من الجهود التي بذلت من قبل المنظمات الدولية والإقليمية وما اعطتة من اهتمام ألا إنها أخفقت حتى الآن في تأسيس إطار قانوني صارم يحكم بفاعلية كل الهجمات السيبرانية. وعلية سنقسم هذا المبحث الى مطلبين على النحو الآتي :

المطلب الأول : دور الاتفاقيات الدولية في مكافحة الجرائم السيبرانية

إن ضمان الأمن والاستقرار غاية أساسية لأي تنظيم قانوني وطني أو دولي، على حد سواء وان الاهتمام الواضح دوليا بالحماية الإنسانية للإنسان سلما وحربا، ويتبلور ذلك في عشرات الوثائق الدولية التي تهدف إلى تأكيد كرامة الإنسان وآدميته، وتؤكد الكثير من أحكامها على الرابطة الوثيقة بين كفالة الأمن والاستقرار للإنسان من خلال احترام حقوقه، وان للاتفاقيات الدولية دور كبير في الحد من الجرائم السيبرانية من خلال وضع أحكام قانونية تضمنها العديد من الاتفاقيات الدولية، بغية الوصول إلى مرتكبي

هذه الجرائم، وحصولهم على جزاء رادع من خلال إلزام الدول بتجريم الأعمال السيبرانية وضمان تسليم مرتكبي الجرائم إلى الدول التي لأتملك الاختصاص القضائي لمحاكمتهم أو تقديمهم للمحاكمة في الدول التي ترفض تسليمهم. [25] وعليه سوف نبين أهم الاتفاقيات المعنية بمكافحة الجرائم السيبرانية على النحو الآتي:

الفرع الاول : اتفاقية بودابست لسنة 2001

نظراً للتطور الذي أحدثته تكنولوجيا المعلومات والاتصالات، واستمرار عولمة الشبكات الحاسوبية والقلق من أن شبكات الإنترنت والمعلومات الإلكترونية يمكن أن تستخدم لارتكاب الجرائم ،وبالنظر إلى أن هدف مجلس أوروبا هو تحقيق مزيد من الوحدة بين أعضائها في مجال مكافحة الجرائم المعلوماتية، من خلال وضع قواعد قانونية تكون أساسا للقانون المعلوماتي الوطني [26] ،وحرصا على حماية مصالح المواطنين وحقوقهم والجهة التي تتضرر، لقد سلكت هذه الاتفاقية إلى وضع تدابير تشريعية لضمان قيام مسؤولية الأشخاص الطبيعية عن جرائم الإنترنت، وكذلك الأشخاص المعنوية وإن قام الأشخاص الطبيعيون بارتكابها لمصلحة الأشخاص المعنويين [27] ولقد وقعت هذه الاتفاقية (26) دولة أوروبية على الرغم من أن هذه الاتفاقية هي في الأصل اتفاقية أوروبية المنشأ، إلا أنها اتفاقية ذات طابع عالمي، لكونها مفتوحة للدول الأخرى طالبة الانضمام من خارج أوروبا مما يجعلها إطارا دوليا مفيدا في مجال مكافحة الجرائم السيبرانية، وتهدف اتفاقية بودابست إلى توحيد الجهود الدولية في مجال مكافحة الجرائم السيبرانية، فهي تحدد أفضل الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت التي تعهدت الدول الموقعة عليها بالتعاون الوثيق من أجل محاربتها [28] **ومن أهداف هذه الاتفاقية.** [29]

1- توحيد عناصر القانون الجنائي الوطني مع الأحكام المتعلقة بالجرائم الإلكترونية، وتحديد أنواع معينة من السلوك كجرائم جنائية في التشريعات المحلية بنصوص تجريمية موضوعية.
2- توفير التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية _أي النصوص الإجرائية المتعلقة بتزويد سلطات العدالة الجنائية بالوسائل الفعالة للتحقيقات من خلال أدوات القانون الإجرائي.
3- تعيين نظام سريع وفعال للتعاون الدولي والإقليمي، واتخاذ تدابير دولية وإقليمية مشتركة وعاجلة. وكذلك التعاون بين جهات إنفاذ القانون والقضاء في مجال مكافحة هذا النوع من الجرائم.
4- الحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر، وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
5- ضرورة وضع خطط عمل مشتركة لمكافحة الأنشطة التي تستهدف سرية وسلامة المعلومات وأنظمة الكمبيوتر وشبكاته، وأنشطة إساءة استخدامها بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة بالنص في قانون الإجراءات الجنائية الوطني.

وقد نصت هذه الاتفاقية على تسمية مجموعة من الأعمال الإرهابية التي تقوم عبر الوسائل الإلكترونية بطرق غير المشرعة، وحث الدول الأعضاء فيها على تجريمها في تشريعاتها الداخلية [30]، وبالرجوع إلى المعايير التي اعتمدتها الاتفاقية نجدها بالأساس تقوم على فكرة دور الكمبيوتر بالجريمة كما تضمنت الاتفاقية عدة طوائف من الجرائم الإلكترونية: [31]

الطائفة الأولى: التي نصت عليها الاتفاقية، والتي أطلقت عليها الجرائم التي تستهدف سرية وسلامة، وتوفر المعلومات، وهي في الحقيقة الجرائم التي يلعب فيها الكمبيوتر دور الهدف أي الجرائم التي تستهدف الكمبيوتر والبيانات المسجلة عليه، بذاتها سواء لجهة الوصول إليها أو الاطلاع عليها أو إفشائها أو تحويرها أو إتلافها، وهي من المعطيات في مراحل المعالجة والتخزين والنقل بواسطة أجهزة الكمبيوتر ووسائل الاتصال وشبكات المعلومات.

الطائفة الثانية: وهي ما أطلقت عليها الاتفاقية الجرائم المرتبطة بالكمبيوتر ،وهي الجرائم التي يلعب فيها الكمبيوتر دور الوسيلة، أي الأداة المستخدمة لارتكاب جرم تقليدي كالاحتيال والتزوير.

الطائفة الثالثة: والتي أطلق عليها تعبير الجرائم المرتبطة بالمحتوى، فهي الجرائم التي يلعب فيها الكمبيوتر دور البيئة الجرمية، وقد حصرتها الاتفاقية بجرائم المواد اللاأخلاقية المتصلة بالأطفال أو المتعلقة بهم، ولا تنص الاتفاقية على بقية أنماط جرائم المحتوى.

الطائفة الرابعة: المتعلقة بجرائم الملكية الفكرية، فهو نص مكمل لقواعد الحماية الجزائية في هذا الحقل المقرر وطنيا ودوليا وفي نطاق التعاون الدولي لمكافحة الجرائم السيبرانية ،لقد وضعت الاتفاقية أحكاما تفصيلية باعتبار هذه الاتفاقية هي الأداة التشريعية الرئيسية التي تحكم مسائل التعاون الدولي في مجال مكافحة الجرائم المعلوماتية ،وأن أبرز ما ينطوي على مسائل التعاون

الدولي يتمثل بالقواعد المتعلقة بتسليم المجرمين، والانابات القضائية ومسائل الضبط والتفتيش وتحريز الأدلة خارج الحدود ولقد واجهت هذه الاتفاقية اعتراضا واسعا من عدة جهات، ومن الواضح أن جرائم الكمبيوتر تحديدا لا يمكن مواجهتها دون قواعد محددة تنظم المسائل المهمة والحساسة، أي القواعد التي تحمي السيادة الوطنية باعتبارها تنطبق على كافة الدول الأعضاء، ضمن المعايير الموضوعية المقررة في الاتفاقية، وبشكل قد يحول دون تدخلات لصالح طرف دون آخر في ظل اختلاف موازين القوى وسيادة إرادة المتحكمين بمصاير الشعوب والدول.[32]

وعليه نجد أن الاتفاقية في المادة (13/2)، تلزم الدول الأعضاء فيها وهي هنا الدول الأوروبية والدول الأخرى ،التي انضمت إليها من خارج مجموعة مجلس أوروبا، باتخاذ التدابير التشريعية والإجراءات الملاءمة لتجريم هذه الجرائم التي تناولتها هذه الاتفاقية.

وعلى الرغم من الإيجابيات التي تتمتع بها الاتفاقية ،إلا أنها تعرضت إلى انتقادات ومنها:[33]

أ- نطاقها محدود كون أن أكثر من ثلثي الدول لم تصادق على المعاهدات بالرغم من ان العديد من الدول استخدمت الاتفاقية كنموذج وصاغت أجزاء من تشريعاتها وفقا لأحكامها دون أن تنضم إليها رسميا.

ب- المساعدة القانونية التي نصت عليها المعاهدة في أحكامها معقدة وطويلة، مما يؤثر سلبا على كشف الجرائم ونسبتها إلى مرتكبيها ومقاضاتهم.

ت- انتهاكها المفترض لسيادة الدول، كما جاء في المادة (32) المثيرة للجدل المتعلقة "بالنفاذ العابر للحدود إلى بيانات الكمبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم".

ث- عدم تجاوبها مع المتغيرات الحديثة للأنشطة الإجرامية وأصبحت قديمة نسبيا حيث عندما وضعت الاتفاقية لم يكن استخدام الإنترنت متاح للإرهابيين ،ولم تعرف بعد الهجمات البرمجية الروبوتية الموجهة ،وكذلك التصعيد الاحتيالي، وعليه فانه لا بد أن يواكب القانون الجنائي التغير في السلوك الإجرامي.

الفرع الثاني: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)

في عام 2010 وافق مجلس الوزراء الداخلية والعدل العرب في اجتماعهم ،المشترك المنعقد في الأمانة العامة لجامعة الدول العربية بالقاهرة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث تحتوي هذه الاتفاقية على (43) مادة ودخلت حيز النفاذ اعتبارا في 2014/2/7، بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو إقرارها من سبع دول عربية أعمالا بالفقرة (3) من الأحكام الختامية للاتفاقية التي تنص "تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق والتصديق عليها أو قبولها أو إقرارها من سبع دول عربية .[34]

حيث جاءت في المادة الأولى من الاتفاقية" تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنيات المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية مصالحها وسلامة مجتمعاتها وأفرادها وحيث ورد في هذه الاتفاقية (21) مادة تجرم أفعال تقنيات المعلومات و (8) مواد إجرائية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية، ويكون الفصل الرابع من (14) مادة تنظم التعاون بين دول الأعضاء، في تبادل معلومات المستخدمين حيث يكون نطاق سريان هذه الاتفاقية على النطاق الإقليمي ،وقد تضمنت الاتفاقية الأحكام الموضوعية التي جرمت الأفعال المعلوماتية، وهي الاختراق، والاعتراض، والاعتداء على سلامة البيانات والملكية الفكرية، وإساءة استخدام وسائل التقنيات المعلومات، والتزوير والاحتيال، والإباحية والجرائم المتعلقة بالإرهاب الإلكتروني، وغسل الأموال والمخدرات والاتجار بالجنس البشري والأسلحة والاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية، فضلا عن تشديد العقوبات على الجرائم التقنية التي ترتكب بواسطة تقنية المعلومات. [35]وكذلك تضمن المادة (15) من الاتفاقية العربية لتقنية المعلومات على الجرائم الإرهابية المرتكبة بواسطة تقنية المعلومات ومنها ما يأتي:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في العمليات الإرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

ويتضح مما تقدم أن المادة (15) تعد من المواد الأساسية وكان مجلس الجامعة العربية موفقا بإيراد هذا النص بالإضافة إلى النصوص الأخرى التي تكافح الجرائم الواقعة عبر الوسائل الإلكترونية.

المطلب الثاني : موقف المنظمات الدولية من الجرائم السيبرانية

إن للمنظمات الدولية لها موقفا حول مكافحة الجرائم السيبرانية نظرا للخطر الكبير الذي تمثله الجرائم الإلكترونية، وهذا ما ذهبت إليه منظمة الأمم المتحدة والتي تعد من أهم المنظمات الدولية كوناً أحد أهدافها وهو حماية السلم والأمن الدوليين حيث تغيرت الطرق التي تجري فيها النزاعات المسلحة في السنوات الأخيرة إذ انتقلت المعارك من المجال المادي إلى الافتراضي الذي يسمى بالفضاء الساير أي الحروب السيبرانية التي تقع من خلاله.، وكذلك لمنظمة الشرطة الدولية (الإنتربول) لها دور كبير في العمل على مكافحة الجرائم من خلال إلقاء القبض على الجناة وتسليمهم إلى الدول صاحبه الاختصاص لمحاكمتهم.

الفرع الأول : دور منظمة الأمم المتحدة في مكافحة الجرائم السيبرانية

بالرغم من أن ميثاق الأمم المتحدة لم ينص صراحة على تجريم الأعمال المعلوماتية ،إلا أن الميثاق يتفق مع تجريم أي عمل يهدد السلم والأمن الدوليين وباعتبار أن الميثاق جاء لمكافحة النزاعات المسلحة، على اعتبار أن الجرائم السيبرانية واستخدام حرب المعلومات يقعان ضمن العدوان حيث إن هذا النوع من الجرائم يهدد العلاقات الدولية ، باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجهة آخر لا يتفق مع مقاصد الأمم المتحدة .[36]

وتوصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجراء الدولي لمواجهة جرائم الإنترنت يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص في : [37]

1- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة (التحقيق، قبول الأدلة) على نحو ملائم وإدخال التعديلات الضرورية.
2- مصادرة العائد والأصول من الأنشطة غير المشروعة.
3- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.
4- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة، على مكافحة هذا النوع من الجرائم بأهمية مكافحة هذه الجرائم ومحاكمة مرتكبيها.
5- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمن المناهج المدرسية وحماية مصالح الدولة وحقوق ضحايا جرائم الإنترنت.

ومع تزايد الجرائم المرتكبة عبر الإنترنت وماتثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنه 2000، حيث أكدت على الحاجة الى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية. [38]

وقد طلبت الجمعية في قرارها الى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقا للفقرة (42) من إعلان سلفادور، فريق خبراء حكوميا ودوليا من أجل إجراء دراسة شاملة لمشكلة الجرائم السيبرانية، والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية دراسة الاختيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم الالكترونية واقتراح تدابير جديدة في هذا الشأن، وعلاوة على ذلك أحاطت الجمعية العامة علما مع التقرير في قرارها 189/67 الخاص بفريق الخبراء الحكومي الدولي المفتوح العضوية المعنى بإجراء دراسة شاملة عن مشكلة الجرائم السيبرانية وأثرها على الامن المجتمعي.وقد ركز فريق الخبراء دراسته لهذا الموضوع على ظاهرة الجريمة السيبرانية بالتطرق الى مواضيع التالية:

تحليل ظاهرة الجريمة السيبرانية، جمع المعلومات والاحصائيات المتعلقة بالجريمة السيبرانية، وتحديات الجريمة السيبرانية، مدى مواءمة التشريعات للظاهرة الإجرامية السيبرانية، النص على الجرائم السيبرانية إجراءات التحقيق، التعاون الدولي، الأدلة الإلكترونية، مسؤولية متعهدي خدمات الإنترنت، التصدي للجريمة خارج دائرة التدابير القانونية، المساعدة التقنية الدولية، دور القطاع الخاص في الحد من الجريمة .[39]

وقد اتخذت الجمعية العامة في دورتها (173/74) لسنة 2019 قرارا يتناول التحديات التي تواجهها جميع الدول في مكافحة الجريمة الإلكترونية، ويشدد على ضرورة تعزيز المساعدة التقنية كما يلزم الدول الأعضاء على وضع وتنفيذ تدابير تكفل فعالية تحقيق والملاحقة القضائية على الصعيد الوطني في الجرائم الالكترونية والجرائم التي تكون فيها الأدلة الإلكترونية مهمة، على أن تضمن إمكانية الحصول على تعاون دولي فعال في هذا المجال، تماشيا مع القانون الوطني، وبما يتفق مع أحكام القانون الدولي كما يحث دول الأعضاء على تشجيع تدريب موظفي أجهزة إنفاذ القانون وسلطات التحقيق والنيابة العامة والقضاة على التعامل مع الجرائم مع الجريمة الإلكترونية.

الا انه بالرغم من الجهود التي تبذلها الامم المتحدة في مجال مكافحة الجرائم السيبرانية ،الا انها لاتتلائم مع حجم خطورتها، حيث إنه مع تفاقم مشكلة الاختصاص القضائي في ظل امتداد الملاحقة والتحري والضبط والتفتيش خارج الحدود، الامر الذي يستوجب وجود تعاون دولي يكفل مكافحة الجرائم السيبرانية من جهه وعدم انتهاك مبدأ سيادة الدول على إقليمها من جهة أخرى ،وبالرغم من ادراك الأمم المتحدة وكل افراد المجتمع الدولي بأهمية التعاون بين كل الأطراف من أجل مكافحة هذا النوع من الجرائم الذي بات يهدد الجميع، إلا أنها لم تحقق ماكانت تتطلع إليه من خلال كل مؤتمراتها وقراراتها ولعل من أهم الاسباب التي جعلت التعاون يصعب في هذا المجال ،وهو عدم وجود نموذج موحد متفق عليه فيما يتعلق بالنشاط الإجرامي، ويرجع ذلك الى عدم اتفاق الدول وأنظمتها على صور محددة يندرج ضمنها بما يعرف باساءة استخدام نظم المعلومات الواجب اتباعها ومن جهة أخرى عدم وجود تعريف محدد للنشاط المفروض أن يتفق على تجريمة. [40]

ومن خلال ماورد اعلاه نجد تحركات منظمة الامم المتحدة حول مواجهة الجرائم السيبرانية من خلال القرارات التي تصدرها، مؤكدة على وجوب تضافر جهود الدول والعمل المشترك والجماعي بهدف الحد من انتشار هذا النوع من الجرائم.

الفرع الثاني: جهود المنظمة الدولية للشرطة الجنائية " الانتربول" في مكافحة الجرائم السيبرانية

الإنتربول هو أكبر منظمة شرطية دولية حيث تم تأسيسها عام 1923 ، ومقرها مدينة ليون بفرنسا وأن هذه المنظمة تعد من قبيل المنظمات الدولية المتخصصة ، التي تهتم بالتعاون الدولي بين دول الأعضاء فيها ، في مجال مكافحة الجريمة وتعقب المجرمين الذي يستطيعون تجاوز حدود الدولة في ارتكاب جرائمهم[41]. وتتمثل مهام الأنتربول الأساسية في تجميع البيانات والمعلومات التي تساعد في الكشف عن الجريمة وتحديد الجاني والتعاون مع الدول في تتبع المجرمين الفارين والقبض عليهم ولاينحصر اختصاص المنظمة في إطار الجرائم التي ترتكب داخل حدود إقليم الدولة بل يتعداه الى الجرائم العادية التي تتعدى حدود اقليم الدولة الواحدة سواء من حيث الفعل المادي المكون للجريمة ولكن ايضاً من حيث التخطيط والتحريض الى جانب الحالات التي يرتكب فيها الجاني الجريمة في اقليم دولة وينتقل الى دولة أخرى أو أكثر [42] ويشترط في الجريمة محل طلب التسليم أن تكون على قدر معين من الجسامة ، حيث إن الجريمة التافهة لا تتناسب مع صعوبة إجراءات نظام تسليم المجرمين وتعقيداته.[43]

وطبقاً للمادة الثانية من ميثاق المنظمة تتمثل أهم أهدف هذه المنظمة في تحقيق الاتي:

1- جميع المعلومات المتعلقة بالجرائم والمجرمين ، وذلك عن طريق المعلومات التي تتسلمها المنظمة _ مكتب الرئيس في ليون_ من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء ، ويتم ذلك عبر شبكة اتصالات حديثة
2- التعاون مع دول الأعضاء في ضبط الهاربين والمطلوبين أيا كانت جنسياتهم والصادرة ضدهم أحكام قضائية ، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق .
3- دعم جهود الشرطة في مكافحة الإجرام العابر للحدود ، وتقديم الخدمات في مجال الأدلة الجنائية ، كبصمات الأصابع، والحمض النووي DNA.
4- إنشاء وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان .

وقد انشأت المنظمة الدولية للشرطة الجنائية (الإنتربول) خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا ، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى بوضع استراتيجية لمواجهة هذا النوع من الجرائم .وذلك من خلال : [44]

أ- إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار (24) ساعة (7) أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف.

ب- استخدام وسائل حديثة في المكافحة ، كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج Excalibur للتحليل والمقارنة الأوتوماتيكية لتلك الصور .

ت- تزويد شرطة دول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها .

نلخص من ذلك إلى أن هدف الإنتربول باختصار ، هو الوصول الى بلد عالمي مأمون وهكذا يتولى الإنتربول إقامة العلاقات بين الدول والمنظمة وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بالجرائم المتشعبة في عدة دول كتلك المتعلقة بالجرائم المعلوماتية والعمل على تسليم المجرمين من خارج الحدود الوطنية.

الخاتمة

اولاً: النتائج

1- عدم وجود إجماع على تعريف محدد للجرائم السيبرانية ويرجع ذلك إلى طريقة ارتكابها والجهة التي يتم استهدافها في الجريمة فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، واخرون يستندون الى الباعث لارتكاب الجريمة .

2- تتميز الجريمة السيبرانية بعدة خصائص تميزها عن الجرائم التقليدية فهي من الجرائم الناعمة لا تحتاج إلى مجهود بدني بل إلى المهارة والموهبة وهذا ما يتميز به المجرم السيبراني من ذكاء في ارتكابها وتعد الجرائم السيبرانية هي الأقرب إلى الجرائم المنظمة عبر الوطنية كونها تكون من الجرائم العابرة للحدود ، وبالإضافة إلى صعوبة اكتشافها.

3- عدم وجود اتفاقية دولية بالرغم من وجود اتفاقية بودابست الا انها غير كافية في مكافحة الجرائم السيبرانية في الوقت الحالي بسبب التطور الجرائم وظهور صور لها منها الجرائم الارهابية .

4- عدم توصل الامم المتحدة الى ابرام اتفاقية دولية موحدة في مجال مكافحة الجريمة السيبرانية رغم ايمانها بخطورتها.

5- ان المنظمة الدولية للشرطة الجنائية الأنتربول لها دور كبير في مكافحة الجرائم السيبرانية من خلال تسليم المجرمين من أجل محاكمتهم في حالة عدم توفر الاختصاص القضائي .

ثانياً :التوصيات

1- وضع تعريف محدد للجريمة السيبرانية ويكون ذلك من خلال اتفاقية او مؤتمر دولي بإشراف الأمم المتحدة.

2- توحيد الجهود الدولية لانشاء اتفاقية دولية لتعزيز التعاون الدولي في مواجهة الجرائم السيبرانية وحث الدول الى الانضمام الى الاتفاقية الخاصة بمكافحة الجرائم السيبرانية ولا سيما الاتفاقية الدولية لمكافحة جرائم المعلومات بوداست لسنة (2001).

3- تطوير القوانين الجنائية من الناحية الموضوعية والاجرائية المتعلقة بالجرائم السيبرانية والاحاطة بها من كل جوانبها وصورها واساليبها.

4- العمل على تنمية الكوادر البشرية العاملة في مجال مكافحة الجرائم السيبرانية .

5- زيادة التوعية بخطورة جرائم الاعتداء الإلكتروني وعدم التهوين من شانها .

6- دعم الدول التقدمة للدول النامية في مجال تكنولوجيا المعلومات والاتصالات من اجل مكافحة الجرائم السيبرانية.

7- تعاون الدول العربية بانشاء منظمة متخصصة مهمتها التنسيق مع الدول العربية في مواجهة الجرائم المعلوماتية عن طريق تبادل المعلومات والخبرات.

الهوامش

(1) _ Rao ، 2012.p202.

(2) العمري ، 2000م، ص16.

(3) عبد المحسن، ، 2023م، ص 1368.

(4) البشري ، محمد الأمين ،2000م، ص322.

(5) الشواكبة ، 2011م ، ص8.

(6) خضير ، ، 2021م، ص22.

(7) مادة (5) ، بودابست عام 2001.

(8) ادبيس، 2023، ص1239

(9) خضير ، مرجع سابق ، ص 23-24.

(10) بشير ، 2012م، ص8.

(11) _ Jahanakani, AL-Nemrat, hossinian-faJ 2014p.152.

(12) القرعان ، 2017م، ص40 .

(13) علي البلدوي، 2023م، ص308.

(14) عبد شكر ، 2023م، ص207.

(15) لطفي ، ، 2018م، ص124.

(16) بدير ،2019، ص96.

(17) هروال، ، 2007م، ص45.

(18) عبد المحسن ، مرجع سابق ، ص1382

(19) فليح ، 2024م، ص70.

(20) بدير ، مرجع سابق ، ص 97.

(21) حسني ، 1989م، ص 630.

(22) فليح ، مرجع سابق ، ص73.

(23) علي ، 2021م، ص31.

(24) خضير ، مرجع سابق ، ص 34.

(25)خضير، مرجع سابق ، ص131.

(26) عبد شكر ، مرجع سابق ، ص220.

(27) البلقي، 2010م ، ص24.

(28) بشير ، مرجع سابق ، ص 16.

(29) فليح، مرجع سابق ، ص179.

(30) Gervais ،2012.p.167.

(31) صالح ، 2015، ص439.

(32) الشوابكة، ، 2007، ص73.

(33) فليح، مرجع سابق، ص209_210

(34) شاكر، ص1055.

(35) القاضي ، 2011 ، ص7.

(36) علي ، 2023، ص315.

(37) عيد 2003، ص194.

(38) اتفاقية مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، 2000.

(39) اجتماع فريق الخبراء المعني بالجريمة السيبرانية .

(40) شرابشة، 2009، ص250.

(41)حمودة ، 2013، ص11.

(42) الحاملولى ، 2015، ص519.

(43) حمودة، مرجع سابق، ص203.

(44) هروال ، 2007، ص153 .

المصادر

اولاً: الكتب

- البلقي، هيثم عبد الرحمن ،الجرائم الالكترونية الواقعة على العرض ، بين الشريعة والقانون المقارن ، دار العلوم للنشر والتوزيع ، القاهرة ، 2010.
- ال جار الله ،عبد العزيز ، جرائم الانترنيت وعقوباتها وفقا نظام مكافحة جرائم المعلوماتية السعودي، دار الكتاب الجامعي للنشر والتوزيع ، الرياض ط1 ،2017 .
- الحامولى، حسين فتحي ، التعاون الدولي الأمني في تنفيذ الأحكام الجنائية ، دون نشر ، 2015.
- الشواكبة، محمد أمين ، جرائم الحاسوب الإنترنت، ط4، دار الثقافة للنشر والتوزيع، الاردن 2011.
- الشوابكة ، محمد أمين ، جرائم الحاسوب والإنترنت الجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ،ط1 ، الاصدار الثاني ، 2007.
- العمري، محمد محمود مدخل الى الأمن السيبراني، دار زهران ، مملكة الاردن الهاشمية ، 2000.
- القاضي ، رامي متولي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ،ط1، دار النهضة العربية ، القاهرة .2011.
- القرعان، محمود احمد ، الجرائم الالكترونية، دار وائل للنشر والتوزيع ، عمان ، الطبعة الاولى ، 2017 .
- بدير،محمد ممدوح ، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت دراسة مقارنة، مركز الدراسات العربية ،2019.
- حسني ،محمود نجيب ، شرح قانون العقوبات ، القسم العام ، ط6، دار النهضة العربية ، 1989.
- حمودة ، منتصر سعيد ، المنظمة الدولية للشرطة الجنائية الإنتربول ، دار الفكر الجامعي ، ط2، 2013.
- خضير، عمر عباس ، مكافحة الجرائم السيبرانية كآلية لتعزيز الامن الاقليمي ، مركز الدراسات العربية ، .2021
- صالح، مروة زين لعابدين ، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، بين القانون الدولي الاتفاقي والقانون الوطني ، مركز الدراسات العربية ، 2015، ص439.
- علي، محمد كريم ، مكافحة الجريمة المنظمة في ظل المعاهدات الدولية ، مركز الدراسات العربية ، 2021.
- عيد ، محمد فتحي ، الإنترنت ودورة في انتشار المخدرات ، أكاديمية نايف للعلوم ، الرياض 2003.
- فليح،أثير هلال ، القواعد الدولية لمكافحة الجرائم الإلكترونية والسيبرانية ، دراسة مقارنة ، مركز الدراسات العربية ، ط1، 2024.

- لطفي، خالد حسن أحمد ، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دراسة مقارنة ، دار الفكر الجامعي ، الإسكندرية ، 2018.
- هروال ، نبيلة هبة الجوانب الاجرائية لجرائم الانترنت ، ط1،دار الفكر الجامعي ، الاسكندرية ، 2007.
- هروال، نبيلة هبة ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، دار الفكر الجامعي ، 2007.

ثانياً: البحوث

- ادبيس،سعد فهد سعد، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية ، 16، العدد، 5، 2023.
- البشري ، محمد الأمين ، التحقيق في جرائ الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب ، المجلد 15، عدد30 ،2000.
- البلدوري، حامد محمد علي ، الحرب السيبرانية وموقف القانون الدولي الإنساني ، مجلة جامعة تكريت للحقوق المجلد (8) ، العدد(1) ، 2023.
- بشير ، هشام ، الاليات الدولية لمكافحة الجرائم الالكترونية ،المركز الدولي للدراسات المستقبلية والاستراتيجية ، العدد، العدد90، 2012.
- شاكر، هيرش فاضل ، المكافحة القانونية للجرائم السيبرانية ، دراسة تحليلية ، مجلة جامعة الانبار للعلوم القانونية والسياسية ، العدد 2، المجلد 13، 2023.
- شرابشة ، ليندة ، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية ، مجلة دراسات وأبحاث، جامعة الجلفة ، المجلد1، العدد 1، 2009.
- عبدالمحسن ، رنا مصباح، آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية ، المجلة القانونية،المجلد 15،العدد 5 ، 2023.
- عبد شكر، اياد ، الجريمة المعلوماتية في ظل التشريع الوطني والدولي ، مجلة الحقوق ، العدد 46، 2023.
- علي ، حامد محمد ، الحرب السيبرانية وموقف القانون الدولي الإنساني ، مجلة جامعة تكريت للحقوق ، المجلد 8، العدد 1، 2023.

ثالثاً: الاتفاقيات والوثائق

- اتفاقية بودابست عام 2001.
- اتفاقية مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (63/55) الصادرة عن هيئة الأمم المتحدة ، الجلسة العامة 81، ديسمبر 2000.
- اجتماع فريق الخبراء المعني بالجريمة السيبرانية ، مشروع المواضيع المطروحة لنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية والتدابير التصدي لها فيينا 17-21 يناير 2011 رقم UNODC/CCPCI/EG 2-2011-4 .
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010).
- ميثاق المنظمة الدولية للشرطة الجنائية الدولية الانتربول.

رابعاً: المصادر الاجنبية

- Hamid Jahanakani,Ameer AL-Nemrat,Amin hossinian-faJ Cybercrime classification andcharacteristics,2014.
- Michael Gervais, “cyber attacks and the laws of war” , Berkeley Journal of international law,Iss 2, vol. 30,2021.
- Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
- Yerra ,Shankar Rao،Hemraj ,Saini T.C.Panda / International Journal of ،Yerra Shankar Rao،Hemraj Saini ،Engineering Research and Applications (IJERA) ISSN: www.ijera.com Vol. 2.،Mar-، Issue 2.