وزارة التعليم العالي والبحث العلمي
جامعة يحي فارس – المدية
كلية الحقوق والعلوم السياسية

التعاون الدولي في مكافحة الجريمـــة السيبرانيـــة

مذكرة تخرج لنيل شهادة الماستر، تخصص: قانون دولي.

إعداد:

- سفيان خلفي.
- سفيان بن مطير.

إشراف:

– د/ سعاد شيكر

أعضاء المناقشة :

د. غربي أسامة .....رئيسا

د. شريد وسيلة .....مناقشا

السنة الجامعة: 2025/2024



الحمد لله الذي بحمده تتم الصالحات – الحمد لله على تمام النجاح والتوفيق

وعملا بما جاء في سنة نبينا محمد صلى الله عليه وسلم من لم يشكر الناس لم يشكره الله

وبعد صبر وقوة وعزيمة وفقنا الله في اتمام مشوارنا الدراسي والتعليمي

نتقدم بالشكر إلى الوالدين وأساتذتي الذين رافقوني في مسار الدراسي وإلى الأستاذة المشرفة والأساتذة المناقشين

إهداء

بكل الحب والامتنان أهدي هذا الجهد المتواضع الذي ما كان ليرى النور لولا فضل الله ثم دعم وسند من **أمي الحبيبة**، نبع الحنان والعطاء، وإلى **أبي الغالي**، سندي وقدوتي، كلمات الشكر لا توفيكما حقكما، فدعواتكما كانت زادي وطريقا لي نحو النجاح.

وإلى زوجتي التي كان لها الفضل في نجاحي وإلى أبنائي **عبد الباري** و**براءة** وإخوتي وأخواتي الأعزاء.

أتوجه إليكم بخالص الشكر لدعمكم اللامحدود وحبكم الصادق، وإلى أصدقائي ورفقاء دربي الذين شاركوني لحظات التعب والفرح، لكم مني فائق التقدير.

سفيان خلفي

أهدي عملي الى كل من يعرفني عن قريب او بعيد

سفيان **بن مطير**

المقدمة

المقدمة

يعاني المجتمع الدولي من ظاهرة خطيرة تتمثل في تزايد عصابات الجريمة السبيرانية وهذا لما أحدثته تكنولوجيا المعلومات والاتصالات في نسق الحياة العامة من تغيرات، بحيث صاحب ظهور الحاسب الألي وتوسع في استخدام الانترنت تزايد الجرائم وطنيا وإقليميا ودوليا، إذ أصبح من الضروري التعاون بين الدول للوقوف أمام هذه الجرائم.

وعليه فالتعاون الدولي في مجال مكافحة الجريمة السيبرانية يشكل عنصرا هاما في مواجهة هذه الجرائم أو الحد من انتشارها وأضرارها، بحيث لم تعد هذه الجرائم مقتصرة على دولة بعينها بل أصبحت تتجاوز الحدود الجغرافية، وقد فطن المجتمع الدولي إلى أن مرتكبوا الجرائم السبيرانية أصبحوا يبسطون نفوذهم على جميع أرجاء العالم، بفضل ما يملكونه من قوة ونفوذ ودهاء وتحكم الكبير في التكنولوجيا مما يصعب إثبات الجريمة ويعيق تحديد هوية مرتكبيها وحتى القبض عليهم، ولما لها من آثار على الدول في جانب حقوق الإنسان والجوانب السياسية الاقتصادية والاجتماعية والأمنية، تتأكد حتمية التعاون الدولي لمواجهة ازدياد ظاهرة الإجرام في كل بلاد العالم، حتى صارت كل دولة مهما بلغت درجتها من القوة والحضارة لا تستغني عن الدخول في علاقات تعاونية متبادلة مع غيرها من الدول، بوضع آليات قانونية وقضائية وأمنية لمواجهة هذه الجرائم، كل ذلك مع وجود تحديات وعوائق حادة ضد المواجهة والملاحقة، وهذا ما يؤكد ضرورة بل وحتمية تنسيق وتوجيه جهود الدول المختلفة بهدف مجابهة تلك التحديات والعمل على حلها والتغلب عليها.

أما أهمية هذا الموضوع يتمثل في تناوله أحد المواضيع بالغة الأهمية في الوقت الراهن، وتتجلى أهميته في النقاط متعددة منها، الطبيعة الخاصة للجرائم السبيرانية التي ميزتها عن الجرائم التقليدية سواء من حيث فاعلها أو محلها أو مسرح الجريمة وكونها من الجرائم عابرة الحدود فقد يكون فاعلها في دولة والضحية في دولة أخرى، لذلك فهي من الجرائم المستحدثة التي تعتمد على التقنيات الحديثة، التي ظهرت في مطلع القرن العشرين كما أن أهمية الموضوع تبرز من خلال خطورة هذه الجرائم وآثارها السلبية على الأفراد والدول، خصوصا مع ما أظهرته الدراسات العلمية التي اثبتت ازدياد إنتشارها بشكل مطرد، واتساع مجالاتها ليشمل أمور حساسة تتعلق بأمن وسلم الدول ،بالإضافة الى صعوبة المتابعة الجنائية وفقا للقواعد العامة بسبب اختلاف البيئة (المكان الزمان) ارتكاب هذه الجرائم ،كما تهدف هذه الدراسة إلى التعرف على الجريمة السيبرانية بشكل مفصل، واستكشاف آثارها على الصعيد الدولي . وتسليط الضوء على الجهود المبذولة لمواجهة الجريمة السيبرانية، وتحليل الصعوبات التي تواجه هذه الجهود الدولية في القضاء عليها. وأخيرًا، تهدف الدراسة إلى اقتراح سبل لتعزيز التعاون الدولي في هذا المجال الحيوي.

من الأسباب الموضوعية الدافعة لاختيار الموضوع حداثة الموضوع وارتباطه بالواقع ولأنها من الجرائم العابرة للحدود تتطلب تظافر الجميع أفرادا ودولا لما لها من آثار وانعكاسات ضارة على الأفراد والدول، ومن هنا كان لا بد أن يثار هذا الموضوع الحساس بكل أبعاده وتداعياته اهتماما خاصا لدينا، هما يدفعنا إلى التعمق ورصد مستجداته، خصوصا مع الإزدياد متسارع للجرائم السبيرانية في ظل الثورة التكنولوجية الهائلة وفي ظل قصور التشريعات الوطنية في مكافحة الجرائم المعلوماتية ،كما أنه من الاسباب الموضوعية لاختيار الموضوع والرغبة في الدراسة الاكاديمية بمضمون المكافحة للجرائم السبيرانية المقررة بموجب الاتفاقيات الدولية والإقليمية والوقوف على أوجه القصور ومحاولة إيجاد حلول تعزز المكافحة الدولية للجرائم المعلوماتية.

كما أنه هناك أسباب ذاتية دفعتنا لاختيار هذا الموضوع الرغبة الشخصية في التعرف على صورة من صور الجرائم المترتبة عن التطور الحاصل في مجال التكنولوجي، وابراز خصوصيتها عن الجرائم التقليدية والرغبة في معرفة مدى التعاون الدولي في مجال مكافحة الجرائم السبيرانية، وأهم مجالاته بين الدول، والوقوف على مدى تطبيق قواعد القانون الدولي وقواعد مكافحتها خاصة في أرض الواقع مقارنة بالنصوص القانونية و أهم الاليات المتعلقة بمكافحتها.

وعليه فإذا كان التطور التكنولوجي في مجال المعلوماتية وزيادة الربط بالأنترنت اعتبر أحد العوامل التي سهلت حياة الافراد يمكنها بالمقابل عرضتها لمخاطر ذات طبيعة خاصة باعتبارها كانت ايضا البيئة المناسبة لنشأة وتطور بعض الجرائم ومنها الجريمة السبيرانية التي انتشرت بوتيرة سريعة مستعينة بالتطور الحصل في تكنولوجيا المعلومات والاتصال .

وعليه فإن الاشكالية التي يطرحها الموضوع دراستنا إلى أي مدى يمكن للتعاون الدولي مكافحة الجريمة السبيرانية والحد منها في ظل التزايد المطرد في ربط المجتمعات بالأنترنت ؟

وللإجابة على الإشكالية السابقة اعتمدنا المنهج الوصفي لبيان مفهوم الجريمة السبيرانية وسبل التعاون لمكافحتها واعتمدنا منهج تحليل المحتوى لدراسة وتحليل النصوص القانونية ذات الصلة .

ومن الصعوبات التي واجهناها في بحثنا هذا ضيق الوقت لأن هذا موضوع متشعب ويأخذ أبعاد كثيرة كان لابد من إعطائه متسع من الوقت لتعمق فيه وإحاطته من كل الجوانب اكثر من هذا.

ولدراسة الموضوع قسمنا بحثنا الى فصلين تضمن الاول منها ، "الإطار المفاهيمي للجريمة السيبرانية ،وأما الفصل الثاني، "آليات مواجهة المجتمع الدولي للجريمة السيبرانية

الفصل الأول

الإطار المفاهيمي للجريمة السبيرانية

الفصل الأول : الإطار المفاهيمي للجريمة السبيرانية

في عصرنا الحالي، ومع التطور التكنولوجي الهائل والانتشار الواسع للإنترنت، أصبحت المجتمعات تعتمد بشكل متزايد على الفضاء السبيراني في شتى مناحي الحياة، من التواصل الشخصي إلى المعاملات التجارية والخدمات الحكومية. ورغم الإيجابيات الكبيرة التي جلبها هذا التطور، إلا أنه فتح الباب أيضًا أمام تحديات جديدة ومخاطر متنامية، أبرزها الجريمة السبرانية .هذه الظاهرة المعقدة لم تعد مجرد تهديد تقني محدود، بل تحولت إلى مشكلة عالمية متعددة الأوجه، تتجاوز الحدود الجغرافية وتطال الأفراد والمؤسسات والدول على حد سواء و.إن فهم طبيعة الجريمة السبرانية يتطلب منا بناء إطار مفاهيمي شامل يوضح أبعادها المختلفة. فليست الجريمة السبرانية مجرد فعل غير قانوني يتم في الفضاء الرقمي، بل هي ظاهرة تتشابك فيها الجوانب التقنية والقانونية والاجتماعية والاقتصادية ومن هنا، سنتطرق في هذا الفصل مفهوم الجريمة السبيرانية (المبحث الأول) وأثار الجريمة السبيرانية على الدول في (المبحث الثاني).

المبحث الأول : مفهوم الجريمة السبيرانية

لقد تطورت الأساليب ارتكاب الجرائم عن ما هو معروف سابقا فلم تعد الإعتداءات تسهدف النفس والمال فقط بل تعدتها إلى المعلومات والبيانات الخاصة لمتعاملي البيئة الرقمية أصبح بإمكان المجرمين ارتكاب أبشع الجرائم في هدوء تام . وعليه نتطرق في (الفرع الاول) استكشاف مفهوم الجريمة السبرانية بشكل معمق، بدءًا من محاولة معرفة نشاة ومراحل تطورها (الفرع الثاني) وضع تعريف شامل يجمع بين جوانبها اللغوية والقانونية والفقهية. وسننتقل بعد ذلك إلى تفصيل اركانها، إن إدراك هذه الجوانب الأساسية لمفهوم الجريمة السبرانية هو الخطوة الأولى نحو بناء استراتيجيات وقائية وتشريعات رادعة لمكافحتها في عالمنا الرقمي المعاصر.

المطلب الأول: النشأة ومراحل التطور الجريمة السبيرانية

إن ظاهرة الجريمة السبيرانية التي قد تبدو حديثة نسبيًا، لم تظهر بين عشية وضحاها، بل هي نتاج تطور مستمر للفضاء الرقمي نفسه. لفهم حجم وخطورة الجريمة السبرانية في صورتها الحالية، من الضروري أن نتتبع مسار نشأتها ومراحل تطورها عبر الزمن.إن تاريخ الجريمة السبرانية يتشابك بشكل وثيق مع تاريخ تطور الإنترنت وتكنولوجيا المعلومات. فمع كل تقدم في البنية التحتية الرقمية وظهور تقنيات جديدة، ظهرت في المقابل أساليب جديدة للاستغلال الإجرامي. من الأيام الأولى لاختراق الأنظمة البسيطة وصولاً إلى الهجمات المعقدة واسعة النطاق التي نشهدها اليوم، مرت الجريمة السبرانية بتحولات جذرية في طبيعتها، أهدافها، والأدوات المستخدمة فيها.وسنحاول شرحها فيما يلي:

الفرع الأول: مرحلة الخمسينيات من القرن الماضي

تعد بداية صناعة الحواسيب وانطلاق ثورة تكنولوجيا المعلومات الإلكترونية مستقلة عن وسائل الاتصال التي وقعت بالأربعينيات القرن الماضي وعليه يعد تاريخ ظهور الجرائم الإلكترونية حديثا نسبيا، حيث ارتبأ ظهورها التاريخي مع ظهور الكمبيوتر وانتشار استعماله والذي كان عام 1954 في الولايات المتحدة الأمريكية، حيث بدأ طرح أول جهاز كمبيوتر للشراء وبدأ الاستخدام التجاري للحواسيب في الخمسينيات ومنذ ذلك الوقت بدأت ظاهرة جرائم الحاسوب في الظهور، ولكن كانت بدايتها تقتصر على إساءة استخدام الحاسوب على البعد الأخلاقي، حيث تم تسجيل أول جريمة إلكترونية في الولايات المتحدة الأمريكية عام ،1957 وبعدها صدرت عدة تقارير تبين نسب ورصد حالات إساءة استخدام الحاسوب وصنفت هذه الجريمة إلى جرائم العبث والتخريب وسرقة المعلومات أو الاحتلال والاستخدام غير المصرح به، وفي هذا الوقت كان هناك عدم التمييز بين الجرائم الا تستهدف مادية الحاسوب أو التي تستهدف معطيات الحاسوب بسبب أن الأنشطة الإجرامية المتعلقة بالحاسوب تصاغ

وفق مدلول أخلاقي أكثر منه قانوني، أما من حيث التكييف القانوني للجريمة الإلكترونية كانت تتعامل معها بذات الدلالة التي تتعامل معها مع الجرائم التقليدية....[1].

الفرع الثاني: مرحلة الستينات والسبعينات والثمانينات في القرن الماضي

تمتد من شيوع استخدام الحاسب الآلي من الستينات إلى 1970 اقتضت معالجة على المقالات تمثلت في التلاعب بالبيانات المخزنة وتدميرها....[2].

حيث طفح على السطوح مفهوم جديد للجرائم الكمبيوتر والانترنت بمثلث في اقتحام الأنظمة ونشر الفيروسات...[3]

الفرع الرابع: مرحلة التسعينات من القرن الماضي والقرن الحالي:

شهدت هذه المرحلة أنواعا فريدة من جرائم الكمبيوتر التي ظهرت بظهور الانترنت منها الدخول غير مصرح به إلى نظام الكمبيوتر والعبث بمحتوياته وتدميرها والهجوم على المواقع معلوماتية وتدميرها وشملت جرائم الكمبيوتر التجسس الصناعي والأمني واستلاء على بطاقة الائتمان البنكية واستخدامها بطريقة غير مشروعة وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم عبر وسائل الكترونية....[4]

أما في الألفية الجديدة فإنها شهدت تزايدا في حجم الجرائم الإلكترونية ومن خلال ما سبق فانه يتبين أن الجرائم الإلكترونية جذور تاريخية ترجع في ذلك إلى الأربعينيات والخمسينيات من القرن الماض ولكنها لم تكن معروفة كما هي عليه الآن، حيث بدأت الآن الدول تتسابق في وضع التشريعيات التي تعمل على الوقاية والمكافحة من هذه الجرائم الالكترونية.

وبنتيجة هذا التطور في عالم المعلوماتية نشأت ونمت أنواع جديدة من الجرائم التي ما كانت لتبصر النور لولا ظهور الكمبيوتر حيث شهدت التسعينيات والقرن الحالي أنواعا فريدة من جرائم الكمبيوتر وترافق ذلك مع ظهور الإنترنت وبدأت أنشطة الهاكرز باختراق مواقع المعلومات ونظمه عبر الإنترنت"، والدخول دون تصريح أو تخويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيها أو تدميرها التي يتيحها الإنترنت بشكل كبير، وكذلك تعطيل الأنظمة والبرمجيات الخبيثة أو التدمير المادي لها أو استغلالها دون تصريح أو الهجوم عبر الإنترنت على مواقع

[1]- عفاف بعون، نسيمة أولاد سالم، (**الجريمة الالكترونية، قراءة سوسيوتاريخية في النشأة وآثار**)، مجلة القبس للدراسات النفسية والاجتماعية ، جامعة قاصدي مرباح الجزائر، المجلد 05، العدد 20، تاريخ النشر 2023/12/22، ص 72. 73

[2]- (**الجريمة السبيرانية**) wiki.htts://ar.wikipedia.org، موسوعة حرة وكبيديا، اطلع عليه يوم: 2025/04/17، ساعة 12:30.

[3] - المرجع نفسه.

[4]- عفاف بعون، نسيمة ولاد سالم، مرجع سابق، ص 73.

المعلوماتية لتعطيل عملها، وشملت جرائم الكمبيوتر أنشطة التجسس الصناعي والأمن والاستيلاء على البيانات ذات القيمة الاقتصادية أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستيلاء على الأموال، وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم على الرسائل الالكترونية أو استغلال مواقع انترنت لترويج محتوى غير قانوني...[1]

المطلب الثاني: مفهوم الجريمة السيبرانية:

الجريمة السيبرانية بشكل عام ،أنها أي فعل إجرامي يتم باستخدام الحاسوب أو الشبكة المعلوماتية كأداة رئيسية، أو يكون الفضاء السيبراني مسرحًا لهدف ارتكاب الجريمة. تتخذ هذه الجرائم أشكالاً متعددة وتتطور باستمرار مع التقدم التقني، مما يجعلها تحديًا مستمرًا لأنظمة العدالة والأمن حول العالم. فهم طبيعة هذه الجرائم وأبعادها أصبح ضرورة ملحة لمواجهة مخاطرها المتزايدة.

الفرع الأول تعريف الجريمة السيبرانية

إن فهم طبيعة هذه الجريمة يتطلب تعريفًا واضحًا وشاملاً، يميزها عن الجرائم التقليدية ويبرز خصائصها الفريدة. هذا الفرع سيتناول التعريف الدقيق للجريمة السيبرانية من مختلف الجوانب، موضحًا أركانها وعناصرها الأساسية، ، بهدف بناء أساس متين لفهم أبعادها وتحديات مكافحتها.

أولا: تعريف اللغوي للجريمة السيبرانية:

عند البحث في قواميس اللغة العربية التقليدية عن مصطلح "الجريمة السيبرانية"، غالبًا ما لا تجد تعريفًا مباشرًا لها، وذلك لأن هذا المصطلح حديث النشأة، ويرتبط بتطور التقنيات الرقمية والإنترنت. لذلك، يتطلب فهمه لغويًا تحليل كلمتيه "الجريمة" و"السيبرانية" بشكل منفصل.

تعريف الجريمة لغة:كلمة **"الجريمة "**في اللغة العربية تأتي من الفعل "جَرَمَ"، ويدور معناها

الذنب والإثم: يقول ابن منظور في "لسان العرب": "جَرَمَ يَجْرِمُ جَرْماً وجَرِيمةً وجُرْماً: أَذْنَبَ" أي ارتكب ذنبًا أو خطيئة. ...[2]

أما تعريف الجريمة في القانون يعرف هذا النوع من الجرائم بأنها "كل عمل مخالف لأحكام قانون العقوبات والأخير يتضمنه طبيعة العمل ومقدار العقوبة المنصوص عليها" .

وهناك تعريف آخر: " كل عمل غير مشروع الصادر عن إرادة آثمة يحدث لها عقوبة أو تدبير وقائي " أي بأنها الفعل أو الترك المعاقب عليه جنائيا.

[1]- عفاف بعون، نسيمة ولاد سالم، مرجع سابق، ص 74.
[2]- ابن منظور محمد بن مكرم بن علي أبو الفضل جمال الدين جمال الدين الأنصاري الرويفعي الإفريقي، لسان العرب، المجلد الثاني، طبعة صادر، دار صادر، بيروت، ص 90

فالجريمة هي فعل أو الترك الذي نص عليه القانون بعقوبة مقدرة له.

حيث يقصد كلمة "السيبرانية" في اللغة العربية هي تعريب لكلمة "Cyber" الإنجليزية، والتي تُشتق من"Cybernetics" (التحكم الآلي)، وتُشير "السيبرانية" في سياقها الحديث إلى كل ما يرتبط بالإنترنت، الشبكات الحاسوبية، والفضاء الافتراضي.

تعريف السيبرانية: هي دراسة متعددة التخصصات للأنظمة المنظمة ذاتيًا والمتحكمة ذاتيًا .ينصب تركيزها على كيفية معالجة الأنظمة للمعلومات، وكيفية استجابتها للتغيرات في بيئتها، وكيفية تنظيم نفسها للحفاظ على حالة مستقرة أو لتحقيق هدف معين.

ثانيا: تعريف الفقهي اللجريمة السبيرانية

لم يتفق الفقه الجنائي على تسمية موحدة لهذا النوع من الجرائم إذ يطلق البعض عليها الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية وآخرون يطلقون عليها جرائم إساءة استخدام تكنولوجيا المعلومات واتصال ويسميها البعض جرائم الكمبيوتر و الإنترنت....[1]

ولذلك لم يتفق الفقهاء والباحثون على تعريف موحد للجرائم السبيرانية فمنهم من ينظر إلى موضوع الجريمة ومنهم من ينظر إلى الوسيلة المستعملة لارتكابها، يرى هذا الاتجاه أنها كل سلوك إيجابي أو سلبي يقع باستخدام تقنية المعلومات على مصلحة مشروعة بالاعتداء في الحين ينظر آخرون إلى الوسيلة ارتكاب الجريمة ويرون أنها كل فعل إجرامي يستخدم الكمبيوتر...[2]

ثالثا: تعريف القانوني للجريمة السبيرانية

على المستوى الدولي، لم يتم التوصل إلى تعريف عالمي متفق عليه للجريمة السيبرانية بسبب التطور المستمر للتقنيات والظروف المتغيرة .بشكل عام، يُعتبر أي عمل إجرامي يُرتكب باستخدام تكنولوجيا المعلومات والاتصالات لتهديد الشبكات، الأنظمة، البيانات، أو المواقع الإلكترونية، أو وسيلة ارتكابها.

اتفاقية بودابست بشأن الجريمة السيبرانية وهي اتفاقية أعدها مجلس أوروبا عام 2001، هي الصك الدولي الأكثر شمولية في مجال مكافحة الجريمة السيبرانية والأكثر اعتمادًا على مستوى العالم (حتى من دول ليست أعضاء في المجلس، على الرغم من أنها لا تقدم تعريفًا موجزًا وموحدًا للجريمة السيبرانية

[1]- بيدي آمال، **(جهود الأمم المتحدة في مكافحة الجرائم السيبرانية)**، مجلة البحوث في الحقوق والعلوم السياسية ، جامعة الجلفة، المجلد 08، العدد 01، تاريخ النشر 2022/06/03، ص 311.

[2]- مهدي رضا، **(الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري)**، مجلة إيليز للبحوث والدراسات ، جامعة محمد بوضياف المسيلة، المجلد 06، العدد 02 ، تاريخ النشر :2021/12/15 ، ص 113.

في مادة تعريفية صريحة، إلا أنها تُعرّف الجريمة السيبرانية من **خلال** الأفعال التي تُجرمها وتُلزم الدول الأطراف بتجريمها في قوانينها الوطنية.

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطني وبروتوكولاتها، على الرغم من أن هذه الاتفاقية ليست مخصصة حصريًا للجريمة السيبرانية، إلا أنها توفر إطارًا قانونيًا لمكافحة الجريمة المنظمة التي تتجاوز الحدود الوطنية، والتي يمكن أن تشمل الجرائم السيبرانية عندما ترتكبها جماعات إجرامية منظمة. لا تُعرّف الجريمة السيبرانية بشكل مباشر، بل تركز على تجريم الأفعال التي تُرتكب من قبل جماعة إجرامية منظمة وتكون ذات طابع عابر للحدود

إن التعريف القانوني للجريمة السيبرانية على المستوى الدولي يتشكل بشكل أساسي من خلال تجريم أفعال محددة في الاتفاقيات الدولية، بدلاً من وجود تعريف واحد شامل في مادة تعريفية. اتفاقية بودابست هي النموذج الأبرز في هذا الصدد، مع وجود جهود مستمرة لتطوير إطار أوسع تحت مظلة الأمم المتحدة.

وبالرجوع إلى التشريع الجزائري لم يستقر على استخدام مصطلح واحد للدلالة على هذه الجرائم حيث سماها بموجب القانون 04-15 المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الآلية للمعطيات. ...[1]

قانون09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وعرفها بأنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظم الاتصالات الالكترونية....[2]

والمشرع الجزائري اعتمد على عدة معايير للجريمة الالكترونية:

- يتمثل في وسيلة الجريمة يقصد به نظام الاتصالات الالكترونية
- يقصد به موضوع الجريمة ويقصد به المساس بأنظمة المعالجة الآلية للمعطيات.
- القانون الواجب التطبيق أو الركن الشرعي المنصوص عليه في قانون...[3]

[1] - المادة 394 مكرر قانون رقم 15/04 مؤرخ في 27 رمضان 1425 الموافق لـ 10 نوفمبر 2004 يعدل ويتمم الأمررقم 66-156 المؤرخ في 18 صفر 1386 الموافق لـ 8يونيو 1960 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، ص 08.

[2]- المادة (2) من قانون 09-04 **(المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات والإعلام واتصال ومكافحتها)** ، المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009، الصادرفي الجريدة الرسمية الجزائرية، العدد 47، تاريخ صدور الجريدة الرسمية 25 شعبان 1430الموافق لـ 16 غشت 2009، ص 5.

[3]- مهدي رضا، مرجع السابق، ص 113.

الفرع الثاني: خصائص الجرائم السيبيرانية

تجاوز الجريمة السيبرانية مفهوم الجريمة التقليدية في أبعادها بحيث تتسم بسمات خاصة تجعلها أكثر انتشارًا، تعقيدًا، وصعوبة في الكشف والملاحقة وفهم هذه الخصائص يُعد حجر الزاوية في بناء استراتيجيات فعالة لمكافحتها.

أولا: من حيث وسيلة التنفيذ

تتميز هذه الجرائم ترتكب بواسطة الأجهزة الإلكترونية الحاسوب أو الموبيل أو شبكة الانترنت لأنها من الجرائم المستحدثة التي تحمل في طياتها العديد من الاجابيات والسلبيات وتعتبر هذه الادوات هي ءادات ومحل لارتكاب الجريمة... [1]

كما أنها جرائم عن بعد يمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه.

وعليه فإنه يطلق عليها جرائم ناعمة وهي لا تمارس بالعنف ولا تحتاج إلى أي مجهود عضلي أو استخدام آلة أو وسيلة خطيرة لارتكابها لأنها تعتمد على مجهود ذهني وفني وتقني بالحاسوب وشبكة الانترنت ولاتعتبر عنيفة مثل الجرائم التقليدية...[2]

ثانيا: من حيث قابلية الاثبات والسرعة

مما يميز هذا النوع من الجرائم أنها صعبة الإثبات وتكمن صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة ومن الصعوبة حصرها في مكان معين حيث أنها لا تترك أثرا واضحا للعيان، أو تشاهد بالعين المجردة فما هي إلا أرقام تدور في السجلات والمواقع الالكترونية، كما أن الجرائم لم تكتشف هي أكثر بكثير من تلك التي كشف عنها وتعود الصعوبة لعدة أسباب: إنها جريمة لا تترك أثرا بعد ارتكابها، صعوبة الاحتفاظ الفني بآثارها ،إن وجدت تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها تعتمد على الخداع في ارتكابها، والتضبيب في التعريف على مرتكبيها تعتمد على مستوى من الذكاء المرتفع في ارتكابها...[3]

وتتميزبسهولة إتلاف وتدمير الدليل المادي يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك ... [4]

---

[1]- واجعوط سعاد،**(مكافحة الجريمة السيبرانية على المستوي الوطني)**، دفاتر البحوث العلمية، معهد الحقوق والعلوم السياسية المركز الجامعي تيبازة، المجلد 12، العدد 02، تاريخ النشر 04/03/ 2024، ص 420.

[2]- المرجع نفسه، ص420.

[3]- روان بنت عطية الله الصحفي، **(الجرائم السيبرانية)**، المجلة الإلكترونية الشاملة متعددة التخصصات، المملكة العربية السعودية، جدة، العدد 24، 2020/05، ص 11.

[4]- جميل عبد الباقي الصغير، **(القانون الجزائي والتكنولوجيا الحديثة)**، دار النهضة العربية، القاهرة، مصر 2024، ص65

كذلك هي جرائم سريعة التنفيذ فسرعة ارتكاب الجريمة قد تكون من خلال جزء من الثانية وقد لا تتطلب الإعداد قبل التنفيذ...[1]

ثالثا: من حيث النطاق الجغرافي

وتتصف من حيث نطاقها الجغرافي انها عابرة الحدود فهي لا تعرف الحدود الجغرافية للدول لارتباط العالم بالشبكة واحدة وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق المحاكمة، ولذلك تبعا لتعقيد ا لاجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية والتنازع فيما بينها على أي قانون واجب التطبيق...[2]

كذلك صعوبة تحديد مكان وقوع الجريمة تعقيد التتبع نظرًا لأن الجريمة تتم عبر شبكات عالمية متعددة، قد يكون من الصعب تحديد "المكان" الدقيق الذي وقعت فيه الجريمة، أو من أين انطلقت، أو أين انتهت آثارها...[3]

رابعا: من حيث الظهور والاخفاء

هي عبارة عن جرائم خفية فليس من السهولة اكتشفاها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم، ولربما أيضا لمهاراته الفنية والعلمية المتقدمة لقدرته على اخفاء أو خوف الضحية من الابلاغ عن الجريمة تجنبا للإساءة إلى السمعة...[4]

وهي جرائم مستحدثة لأن التقدم العلمي والتكنولوجي في ظل العولمة تجاوز قدرات الدولة الرقابية وإمكانيتها بل وأضعف قدرتها على تطبيق القوانين بالشكل الذي أصبح يهدد أمنها وسلامتها لهذا تعد الجريمة الإلكترونية جريمة مستحدثة تفرز إشكاليات عديدة وتحديات كبرى على الدول من أجل تصدي لها... [5]

الفرع الثالث: أنواع الجرائم السيبيرانية

ولو نظرنا إلى الجرائم السيبيرانية نجدها تتنوع بتنوع الممارسات التي تهدد الأمن السيبيراني وبتنوع أهدافها والجهات التي تعتمدها ويمكن إيراد بعضها على الشكل التالي:

---

[1]- قطاف سليمان، بوقرون عبد الحليم، **(مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية)**، مجلة البحوث القانونية والاقتصادية ، جامعة عمر ثليجي الأغواط، المجلد 05، العدد 02، تاريخ النضر 2022/05/03، ص 71.

[2]- روان بنت عطية الله الصحفي، مرجع سابق، ص 11.

[3]-. سعد فهد سعد ادبيس المطيري، **(مفهوم الجرائم الإلكترونية وسماتها)** المجلة القانونية، جامعة القاهرة، مجلد 16، العدد 5، تاريخ النشر غير موجود، ص 1268.

[4]- قطاف سليمان، مرجع سابق، ص 71.

[5]- فريد ناشف، **(آليات التعاون الدولي في مكافحة الجرائم الإلكترونية)**، مجلة البحوث في الحقوق السياسية جامعة تيارت، جامعة البليدة 02، مجلد 8، العدد 1، تاريخ النشر 06/03/ 2022، ص 435.

أولا: جرائم التعرض لسرية الاتصالات

بحيث تطال البريد الالكتروني والدردشة ونقل الملفات ودخول إلى الأنظمة للاطلاع على المعلومات دون إذن ويشابه هذا التنصت على المخابرات الهاتفية والاطلاع على البريد الشخصي ودخول المنازل لتفتيشها ما يتطلب عادة وبحسب القواعد القانونية إذنا مسبقا من قبل السلطات المختصة في البلاد التي تقوم على احترام القاعدة القانونية، وتعتبر هذه الأعمال في غير تلك الحالة سواء قام بها الأفراد أو قامت بها السلطات العامة جرائم اعتداء على الحريات والحقوق الشخص...[1].

ثانيا: جرائم الأضرار بالبيانات

يعتبر الأشد في الخطورة وتأثيرا وأكثرها حدوثا وتحقيقا للخسائر للأفراد والمؤسسات ويشمل كل أنشطة تعديل أو محو أو سرقة أو اتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية على الحواسب الآلية المتصلة أو غير متصلة بشبكات المعلومات او مجرد الدخول بطريقة الغير مشروعة عليها ابسط تلك الأنشطة هو الدخول للأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها. ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوي القباعات البيضاء الذين يقومون بالدخول بالطريقة غير مشروعة على انظمة الحاسب او الشبكات المعلوماتية او مواقع الانترنيت مستغلين بعض الثغرات في تلك نظم المخترقين بذلك كل سياسات وإجراءات أمن المعلومات التي يقوم بها مديري تلك الانظمة والشباكات...[2]

ثالثا: جرائم الاعتداء على الأفراد والتي تتخذ الصور التالية :

أ. جرائم التشهير وتشويه السمعة: مع انتشار الشائعات والاخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الإنترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الاشخاص بنشر الشائعات عنهم، وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور الغير لائقة أو معلومات غير الصحيحة...[3]

ب. جرائم الاعتداء على الحياة الخاصة: يكون بالإفشاء العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعة إصابته بمرض مخزي ، أو عجز عن سداد ديونه أو نشر صورة البنه تشويه

[1]- قطاف سليمان، مرجع سابق ، ص 70

[2]- عفاف بعون، نسيمة أولاد سالم، مرجع سابق، ص 86.

[3]- عمار حشان، **(الجريمة المعلوماتية في التشريع الجزائري)** رسالة ماستر، تخصص إدارة التحقيقات الاقتصادية والمالية ، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير قسم علوم التسيير، جامعة قاصدي مرباح ورقلة، 02 جويلية 2019، ص 6.

سمعة الشخص في نظر الجمهور، والتشهير به أي الاستيلاء على بعض العناصر الشخصية كالاسم الصورة والبيانات الشخصية المتصلة بالحياة الخاصة...[1]

رابعا: جرائم صناعة ونشر الفيروسات.

جرائم صناعة ونشر الفيروسات: الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنه مصمم بحيث يمكنه التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن يجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل وأما عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، وقد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، و تعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشار، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي "فون نيومان" على صعيد الحاسب الآلي دون الانترنت ، ومن أشهرها فيروس رسائل الحب، فيروس الدودة الحمراء، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في أقل من 9 ساعات عام 2001...[2]

المطلب الثالث: أركان الجريمة السبيرانية

فهم طبيعة الجريمة السيبرانية وكيفية التعامل معها قانونيًا، من الضروري تحليل أركان الجريمة السيبرانية التي تُشكل الأساس القانوني لتجريم هذه الأفعال ومعاقبة مرتكبيها، وتُحدد متى يمكن اعتبار الفعل إجراميًا في الفضاء الرقمي بحيث لا تختلف أركان الجريمة السبيرانية على أركان الجريمة عموما فلا بد من توافرالركن الشرعي و الركن المادي والمعنوي.

الفرع الأول: الركن الشرعي للجريمة السبيرانية

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص و الالتزام بمضامينه .

يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي، إلا إذا

[1]- روان بنت عطية الله الصحفي، مرجع سابق، ص17.
[2]- المرجع نفسه، ص7-8.

نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم . إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين وهما مطابقة الفعل لنص التجريم وألا يخضع الفعل المرتكب لسبب من أسباب الإباحة .

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب إجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة....[1]

وتستمد الجرائم السيبيرانية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة السيبيرانية فقد بذلت هيئة الامم المتحدة جهودا كبيرات إضافة إلي جهود المجلس الاوروبي لإقناع الدول بوضع تشريعات لتصدي ومواجهة ومكافحة جرائم الإلكترونية وتعزيز التعاون الدولي....[2]

الركن الشرعي للجريمة السيبيرانية يعني وجود نص قانوني يُجرم الفعل ويُحدد العقوبة عليه اتفاقية بودابست تُوفر هذا الأساس التجريمي لعدة أنواع من الجرائم السيبرانية تحديد الأفعال المجرمة (الجزء الأساسي للركن الشرعي). تخصص الاتفاقية الفصل الثاني (المواد من 2 إلى 10) لتحديد الجرائم الجنائية التي يجب على الدول الأطراف تجريمها في تشريعاتها الداخلية. هذه المواد هي اللبنة الأساسية للركن الشرعي

مثال: المادة 2 الدخول غير المشروع ، تنص على ضرورة قيام الدول بتجريم الدخول المتعمد إلى نظام معلوماتي دون حق.

ورد في الاتفاقية العربية في فصلها الثاني "التجريم" عددًا من الجرائم التي تُلزم الدول الأطراف بتجريمها في تشريعاتها الوطنية، هذه المواد هي المصدر المباشر للركن الشرعي في القانون الجنائي السيبراني العربي.

مثال : المادة 3 الدخول غير المشروع تُجرِّم الدخول عمدًا إلى موقع أو نظام معلوماتي أو جزء منه، أو تجاوز حدود هذا الدخول، دون تفويض صحيح.

أما الركن الشرعي في التشريع الجزائري يتمثل في:

انطلاقا من مبدأ الشرعية وفقا للأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على ًلا جريمة ولا عقوبة او تدابيرأمن بغير قانون ً جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية

[1]- بلعليات إبراهيم ، (**أركان الجريمة وطرق اثباتها في قانون العقوبات**) الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص94-95.

[2]- حشيخة عبد الهادي، **(التعاون الدولي في مجال مكافحة الجرائم الالكترونية)**، مذكرة نيل شهادة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، تاريخ 2020/2019،ص 19.

ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات"من الفصل الثالث المعنون " الجنايات والجنح ضد الاموال من باب الثاني المتعلق بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات المعدل والمتمم. ...[1]

في الحين جاء القانون 09-04 السابق الذكر متضمنا القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع ترتيبات تقنية لمرتبة الاتصالات الإلكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية...[2]

ولجوء المشرع إلى التقنين أو النص على مثل الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جوا ز لجوء القاضي الجنائي إلى قياس الفعل لم يرد نص على تجريمه على فعل ورد نص بتجريمه، فيقرر القاضي الجنائي للأول عقوبة الثانية بسبب التشابه بين الفعلين..[3]

الفرع الثاني: الركن المادي للجريمة السيبيرانية

ويعرف أن النشاط المادي الذي يصدر عن الجاني متخذا مظهرا خارجيا يتدخل من أجله القانون بتقرير العقاب وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثالث عناصر وهي السلوك الإجرامي, النتيجة الإجرامية, العلاقة السببية بين الفعل والنتيجة.

أولا: السلوك الإجرامي

وصوره متعددة كالسلوك الإجرامي الإيجابي وذلك بمخالفته نصا ينهي عن الإتيان بهذا الفعل كسرقة بيت أو جهاز معين سواء كان في التحرك الإيجابي بحركة واحدة كالقتل بالرصاص أو بحركات متعددة كالشجارة التي تنتهي بالوفاة...[4]

وقد يكون سلبيا بمخالفة نص بأمر بإتيان فعل معين كامتناع ممرضة عن إعطاء جرعة الدواء لمريضها العاجز مما يؤدي إلى وفاته وقد يكون السلوك الإجرامي بصورة بسيط كما في جريمة القذف وقد تكون بصورة معقدة كما في جريمة الارهاب أو السطو المسلح فالقانون الجنائي لا يعول كثيرا على

[1]- القانون رقم 04-15 ينص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات"من الفصل الثالث المعنون " الجنايات والجنح ضد الاموال من باب الثاني المتعلق بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات المعدل والمتمم.

[2]- المادة 03 من قانون 09-04 السابق الذكر

[3]- حمزة خضري، عشاس حمزة، **(خصوصية الجريمة المعلوماتية في التشريع الجزائري)** مجلة الدراسات القانونية والسياسية ، جامعة محمد بوضياف المسيلة، المجلد 06، العدد 02، تاريخ النشر 2020، ص173

[4]- روان بنت عطية الله الصحفي، مرجع سابق، ص22.

الوسيلة التي ارتكبت بها الجريمة أو وقع فيها السلوك الإجرامي ولا يعتد الزمان أو مكان وقوع الجريمة إلا عند تقديره للظروف المشددة أو المخففة بمستوى القتل أن يكون بمسدس أو بالسكين أو حتى عن طريق الريموت كنترول أو بواسطة أجهزة الحاسوب...[1]

أما في الجريمة السيبرانية فهي من الجرائم ذات السلوك المجرد، وذلك لعدة أسباب جوهرية تميزها عن الجرائم التقليدية من خلال الطبيعة غير المادية للفعل الإجرامي ، غالبًا ما لا ينطوي السلوك الإجرامي على تفاعل مادي مباشر بين الجاني والضحية، أو بين الجاني ومكان الجريمة بالمعنى التقليدي. فالأفعال مثل اختراق نظام حاسوبي، نشر برمجيات خبيثة، أو سرقة بيانات تتم في الفضاء الافتراضي (السيبراني) ولا تترك آثارًا مادية ملموسة بنفس طريقة الجرائم التي تحدث في العالم المادي.

السلوك المجرد للجريمة السيبرانية يتجلى أيضًا في غياب الحدود الجغرافية.يمكن للجاني أن يرتكب جريمته من أي مكان في العالم ويستهدف ضحية في مكان آخر، مما يجعل تحديد الاختصاص القضائي وتطبيق القوانين أمرًا معقدًا ويؤكد على الطبيعة غير الملموسة للعمل الإجرامي.

الطبيعة المجردة للجريمة السيبرانية تتيح للجناة إمكانيات أكبر للتخفي وإخفاء هويتهم، من خلال استخدام أدوات وتقنيات تضمن إخفاء آثارهم الرقمية. هذا يجعل عملية تعقبهم وتحديد هويتهم تحديًا كبيرًا، مقارنة بالجرائم التقليدية التي غالبًا ما تترك آثارًا مادية أو شهود عيان.

الأدوات المستخدمة في الجرائم السيبرانية هي أيضًا مجردة، حيث تعتمد على البرمجيات، الشبكات، والمعلومات الرقمية بدلاً من الأدوات المادية. هذا يعزز من فكرة أن السلوك الإجرامي نفسه يتم في نطاق غير ملموس.

على الرغم من أن الجرائم السيبرانية يمكن أن تؤدي إلى خسائر مالية ضخمة أو أضرار مادية غير مباشرة، إلا أن السلوك الإجرامي نفسه يستهدف غالبًا البيانات والمعلومات والأنظمة الرقمية، وهي كيانات غير مادية بطبيعتها.

باختصار، يمكن القول إن مصطلح "السلوك المجرد" يصف بدقة الطريقة التي تُرتكب بها الجرائم السيبرانية، حيث لا تعتمد على التفاعل المادي المباشر، وتتخطى الحواجز الجغرافية، وتستخدم أدوات غير مادية

إن اتفاقية بودابست توضح لنا ذلك:

[1]- روان بنت عطية الله الصحفي، مرجع سابق، ص22.

- الدخول غير القانوني المتعمد: وقد استخدمت الاتفاقية مصطلح في حين أن غالبية إن لم يكن جميع التشريعات الوطنية تستخدم تعبير الدخول غير المصرح به وذلك بالدخول المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق أو إذن سواء أكان بنية انتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر أو لأية نية غير مشروعة (المادة2)

- الاعتراض غير القانوني المتعمد ودون حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أي من نظام كمبيوتر وكذلك اعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أي نظام كمبيوتر تحمل مثل هذه المعطيات (المادة 3).

- التدخل المتعمد أو الإرادي في المعطيات بالتدمير أو الحذف أو التشويه والإفساد أو تبديلها أو تغيرها أو تعديلها أو تعطيلها أو كبتيا أو إخمادها، "وقد ذهبت لجنة الخبراء إلى أن تعديل البيانات يشمل خلطها (الغش) أما تعطيل أو اخماد أو كبت البيانات فيتعلق بإجراءات منع وصولها إلى العنوان المرسلة إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموضع الفيزيائي المطلوب أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها، وذهب بعض الخبراء إلى وجوب اشتراط حصول الضرر جراء التدخل في البيانات كعنصر من عناصر التجريم إلا أن النص لم يشر لهذا العنصر فجرم كل تدخل في المعطيات على أن يكون مقصودا المادة (4)

- التدخل المتعمد في الأنظمة: وهنا نقوم ببث وارسال(المادة 5)ذات الأفعال المشار إليها في المادة(4) وذلك المتعمقة بالدخول في المعطيات بغية تعطيل بإدخال أو تعدي أو حذف أو إخفاء بيانات أداء وعمل الأنظمة بالتدمير والحذف الكمبيوتر على نحو يظهر بيانات غير والتعديل والتعطيل

- إساءة استخدام الأجهزة: تنص ديباجة اتفاقية بودابست نيتها عمى السياسة الجنائية التي تهدف إلى حماية المجتمع من الجرائم الإلكترونية "، وتعتز- على وجه التحديد "ردع الإجراءات الموجهة ضد السرية والنزاهة، وتوافر أنظمة الكمبيوتر والشبكات وبيانات الكمبيوتر بالإضافة إلى إساءة استخدام هذا النظام والشبكات كالبيانات من خلال النص على تجريم مثل هذا السلوك، سبق وسميت هذه الجريمة في المسودات الأولى للاتفاقية السابقة (الأدوات الغير قانونية) وان كان بعض يرى أن هذا العنوان أكثر دقة، وتحتوي هذه الجريمة على نوعين من الأفعال الأولى المنصوص عليها في الفقرة أ من المادة (6) وتشمل الإنتاج المتعمد أو بيع أو شراء أو استخدام أو استيراد أو توزيع أو غير ذلك من أدوات ووسائل توفير الأجهزة بما فيها برامج الكمبيوتر بهدف ارتكاب أية فعل إجرامي من الافعال المنصوص عليها في المواد (2-5) المشار إليها سابقا وكذلك كلمات السر ورموز الدخول أو أية برامج مشابهة بحيث تتيح اختراق نظام الكمبيوتر أك الدخول إليه أو إلى أي جزء منه بنية ارتكاب ي فعل من الأفعال المنصوص عليها في المواد 2-5 ،كما تشمل هذه الجريمة وفق الفقرة 2 من المادة 6 الحيازة والتملك ت لأي عنصر أو أداء مما ورد ذكره في الفقرة 1 أعلاه بنية ارتكاب أي من الأفعالث المشار إليها في المواد 2-5 من الاتفاقية.

- التزوير المتعمد باستخدام جهاز الكمبيوتر وذلك بإدخال أو تعديل أو الحذف وإخفاء بيانات الكمبيوتر عمى نحو يظهر بيانات غير أصلية لتكون مقبولة قانونا وكأنها بيانات أصلية كبغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة ويحق لدولة أن تشترك‌ى نية أو قصد الغش لقيام المسؤولية الجنائية (المادة7)

- الاحتيال المتعمد باستخدام الكمبيوتر بدون حق و على نحو يسبب خسارة الغير لممتلكات و بيانات الكمبيوتر أو من خلال التدخل بعمليات نظام الكمبيوتر أو برامج و بنية الحصول على منفعة اقتصادية لنفسه أو لغيره (المادة 8)

- الجرائم المرتبطة بدعارة الأطفال: وهنا يلاحظ اولا أن هناك جرائم كثيرة في المحتوى إلا أن الاتفاقية نصت عليها صراحة إلا أن مشرعي الاتفاقية اقتصروا في جرائم المحتوى على هذه الجريمة فقط فقضت في المادة التاسعة منها بوجوب اتخاذ الدولة المنظمة للاتفاقية التدابير التشريعية للتجريم قيام اية شخص وبشكل قصدي عرض أو توزيع أو نقل أو غير ذلك من الأفعال التي من شانها توفير أو تتيح توفير المواد الإباحية المتعلقة بالأطفال من خلال نظام الكمبيوتر وتجريم إنتاج مواد دعارة الأطفال بغرض توزيع عبر نظام الكمبيوتر ولا شك أن تفسير الجريمة يؤدي إلى أن عرض المواد الإباحية يتضمن كذلك إعطاء معلومات حول وسائل العرض و الاتصال هذه وكذلك ربط المواقع بمداخل إلى مواقع إباحية تعرض هذه المواد، أما فيما أما فيما يتعلق بالجدل حول مفهوم المواد الإباحية المتعلقة بالأطفال كما تشمله فمثلما هو الحال في المفاوضات الدولية حينما تختلف الثقافات وتتنوع وتصل لحد عدم الاتفاق يتم ترك ذلك للنظم الوطنية حسب قواعد النظام كالآداب العامة لكن تم الاتفاق أنها تشمل كل مادة جنسية تتعلق بالاتصال الجنسي بالأطفال وفي ضوء الخلاف حول المحتوى ونطاقه، جرى الاتفاق على معايير الحد الأدنى التي نص عليها في الفقرتين الثانية والثالثة من ذات المادة، فقضت الفقرة الثانية من المادة (9) على أن مواد دعارة تشمل أية مراد تظهر بشكل مرئي قيام القاصر بتصرفات جنسية أو ظهور أي شخص باتصال أو تصرف جنسي مع قاصر وكذلك الصور الواقعية التي تمثل أو تظهر قاصرا يتدخل بتصرف جنسي، أما الفقرة الثالثة فقد قررت أن المقصود بالقاصر يحدد تبعا للقانون الداخلي لمدلول الأعضاء على أن يتضمن في جميع الاحوال الاطفال الأشخاص دون سن 18 وإتاحة ا الفرصة لكل دولة لتحديد السن على أن يكون حده الأدنى وفقا لما تقدم (المادة 9) ...[1]

[1]- الاتفاقية المتعلقة بالجريمة الالكترونية بوداست، اعتمدها مجلس أوربا سنة 2001، دخلت حيز التنفيذ سنة 2004

ثانيا: النتيجة

بناء على ما تم طرحه نرى أن الجريمة السبيرانية تعتبر من الجرائم ذات سلوك المجرد, حيث لا تتطلب نتيجة محددة يتم تحقيقها بل يحدث بمجرد وقوع السلوك ذاته على سبيل المثال يمكن اعتبار الابلاغ عن الجريمة السبيرانية كفعل إجرامي بمفرده دون حاجة إلى انتظار النتيجة...[1]

ثالثا: العلاقة السببية

يراد بالعلاقة السببية الصلة التي تربط بين الفعل (السلوك الإجرامي) والنتيجة الإجرامية، إذ يثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وللسببية هذه أهميتها فهي التي تربط بين عنصرين الركن المادي فتقيم بذلك وحدته وكيانه, فإذا انتقلت هذه العلاقة كانت مسؤولية مرتكب الفعل تقتصر على الشروع إذا كانت الجريمة عمدية وتوافرت العناصر هذا الشروع وإذا كانت غير عمدية فلا يسأل مرتكب الفعل...[2]

وعليه يمكن القول أن الركن المادي للجريمة السيبيرانية على صورتين أساسيتين تتمثل الأولى في الاعتداء على نظم المعالجة الآلية وتحتوي على نوعين إما الدخول والبقاء الغير مشروع في النظام المعالجة الآلية يشمل هذا النوع ثلاثة أفعال: فعل الدخول والبقاء والعرقلة، أو في نظام المعالجة التعطيل والاعتداء العمدي في نظام المعالجة الآلية والمعطيات وتندرج تحت هذا النوع ثلاثة أفعال وهي الدخول والمحو والتعديل.

وثانية تتمثل في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي...[3]

أما الركن المادي في التشريع الجزائري يتمثل في:

يعتبر الركن المادي للجريمة السبيرانية هو المظهر الخارجي لها وكيانها المادي الظاهر وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، فالقاعدة أنه " لا جريمة دون ركن مادي" أو ًلا جريمة فعلً....[4]

إلا أن الركن المادي للجريمة السبيرانية يختلف نوعا ما عن الجرائم التقليدية كون انه يقوم على صور في الفعل الاعتداء والمتمثلة في

---

[1]- نورهان محمد الربيعي، **(الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة))** مجلة الفرابي للعلوم الانسانية، جامعة عجمان، الإمارات العربية المتحدة، المجلد 03، العدد 01، تاريخ النشر2024، ص 78.

[2]- المرجع نفسه، ص 78.

[3]- حشيخة عبد الهادي، مرجع سابق، ص 23.

[4]- عبد الرحمان خلفي، **(محاضرات في القانون الجنائي العام)**، دار الهدى للنشر والطباعة وتوزيع، الجزائر، ص 101.

أ- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك، ونصت المادة 394 مكرر في قانون العقوبات على أن الدخول والدخول والبقاء غير مشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك يشكل فعلا إجراميا، وحسب المادة المذكورة فلهذا الفعل صورتين وهما كالتالي:

1. الصورة البسيطة:

يتمثل النشاط الإجرامي في هذه الصورة في أفعال التالية: فعل الدخول يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا الأشخاص معنيين أو يسمح بالدخول لكن مقابل نفقات والبقاء، معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، أو يتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطيع معلومات حين يسمح له برؤية فقط...[1].

2. الصورة المشددة:

نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير مشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام أشغال المنظومة.

أما في الاتفاقيات الدولية كاتفاقية بودابست لا تصنف بشكل صريح الجرائم إلى "بسيطة" و"مشددة" في نصوص المواد التي تُعرف الجرائم. بدلاً من ذلك، تُحدد أنواعًا معينة من السلوك الإجرامي التي يجب على الدول الأطراف تجريمها. ومع ذلك، يمكن استنتاج ظروف التشديد من خلال الطبيعة العامة للجريمة والقصد المتطلب لها.

الجرائم ضد سرية وسلامة وتوفر بيانات وأنظمة الحاسوب وتتخذ السورة البسيطة وتتمثل في الصورة البسيطة (السلوك الإجرامي الأساسي):

الوصول غير المشروع ، أي الدخول المتعمد وغير المصرح به إلى نظام حاسوبي بأكمله أو جزء منه، قد تكون العقوبة أقل إذا لم ينتج عن الدخول أي ضرر كبير أو إذا كان القصد مجرد الاختراق للفضول حسب ما نصت عليه المادة الثانية منها أما المادة الثالثة فصت على الحذف المتعمد أو الإتلاف أو التغيير أو الحجب لبيانات الحاسوب، التدخل في البيانات في الحين نصت المادة الرابعة على التدخل في النظام إعاقة متعمدة للتشغيل السليم لنظام حاسوبي عن طريق إدخال أو نقل بيانات، أو إتلاف أو تغيير أو حذف بيانات حاسوب.

[1]- حمزة خضري، عشاش حمزة، مرجع سابق، ، ص 174.

أما الصورة المشددة (ظروف التشديد المستنتجة) فتكون إذا أدى الوصول أو التدخل إلى ضرر جسيم مالي أو تشغيلي أو تعطيل واسع النطاق لأنظمة حيوية (مثل مستشفيات، شبكات كهرباء، بنوك

إذا كان الهدف هو الوصول إلى معلومات سرية للغاية أمن قومي، أسرار تجارية

إذا تم الفعل ضمن مجموعة إجرامية منظمة أو كان له طابع دولي... ...[1].

ب- إدخال المعلومات بطريق الغش:يقصد بفعل الإدخال حسب المادة 394 مكرر01 من قانون العقوبات إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، ومثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير...[2].

أما في اتفاقية بودابست تتمثل في الجرائم المتعلقة بالحاسوب في الصورة البسيطة: (السلوك الإجرامي الأساسي) المادة السابعة تزوير الحاسوب إدخال أو تغيير أو حذف أو حجب بيانات حاسوبية ينتج عنه بيانات غير حقيقية أو تزوير بيانات بغرض الاحتيال ،و الثامنة التي نصت على الاحتيال المرتبط بالحاسوب إحداث فقدان في الممتلكات لشخص آخر عن طريق التلاعب ببيانات الحاسوب أو النظام الحاسوبي.

أما الصورة المشددة: (ظروف التشديد المستنتجة) فتكون في حالات إذا كان الاحتيال أو التزوير يهدف إلى مبالغ مالية ضخمة وإذا استهدف مؤسسات مالية كبرى أو عددًا كبيرًا من الضحايا و إذا تم استخدام تقنيات متقدمة ومعقدة لتجنب الكشف ...[3]

وعليه يمكن القول لا تُقدم الاتفاقيات الدولية تصنيفًا مباشرًا للسلوك الإجرامي السيبراني إلى "بسيط" و"مشدد" في صيغتها النصية، بل تُحدد الأفعال التي يجب تجريمها. ومع ذلك، فإن الطبيعة والخطورة والنتائج المترتبة على هذه الأفعال، بالإضافة إلى القصد الجنائي وطبيعة التنظيم الإجرامي، هي العوامل التي تُستخدم في التشريعات الوطنية لتقرير ما إذا كان السلوك يندرج تحت الصورة البسيطة أو المشددة للجريمة السيبرانية، وتُعد الاتفاقيات الدولية مثل بودابست واتفاقية الأمم المتحدة لعام 2024 بمثابة إطار عمل للدول لوضع هذه التشريعات.

[1]- الاتفاقية المتعلقة بالجريمة الالكترونية بوداست، اعتمدها مجلس أوربا سنة 2001، دخلت حيز التنفيذ سنة 2004.
[2]- حمزة خضري، عشاش حمزة، مرجع سابق، ص 174.
[3]- اتفاقية بودابست، مرجع سابق.

الفرع الثالث: الركن المعنوي للجريمة السبيرانية

وهو ما يعرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها وبالتالي يتكون هذا الركن من عنصرين هما العلم والارادة... [1]

فالركن المادي والركن المعنوي يرتبطان ببعض ارتباطا قويا وذلك أن الركن المعنوي انعكاسا لما في نفسية المجرم من يقصد الجريمة وتوجه إرادته نحو تحقيق ذلك الركن المادي للجريمة ولا يتحقق إلا بوجود هذين العنصرين:

أولا: العلم

الذي يشمل عدة عناصروهما العلم بالوقائع والعلم بالموضوع الجريمة والعلم بحقيقة الفعل وخطورته وأنه يلحق ضررا بالحق المعتدي عليه.

ثانيا: الإرادة

القوة النفسية والنشاط النفسي يوجه لتحقيق هدف معين بوسيلة معينة، فهي ظاهرة نفسية يصدر عن وعي وادراك يقوم على عنصرين: إرادة الفعل وإرادة النتيجة.

يختلف الركن المعنوي في الجرائم السبيرانية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام 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 فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي. ...[2]

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص أخر من ممتلكاته على نحو غير مشروع . ...[3]

[1]- محمود أحمد القرعان (**الجرائم الالكترونية**)، دار وائل للنشر والتوزيع، عمان، 2017، ص 35.
[2]- عمار حشمان، مرجع سابق، ص15.
[3]- أحمد خليفة الملط (**الجرائم المعلوماتية**) دار الفكر الجامعي، الطبعة 2، 2005، ص112-113

ومن أمثلة لتأكيد عمدية هذه الجرائم (المادة 2) من إتفاقية بودابست الدخول غير القانوني المتعمد يشمل الدخول غير المصرح به إلى أي نظام حاسوبي أو جزء منه بقصد انتهاك الأمن، أو الحصول على بيانات، أو لأي غرض غير مشروع.

و(المادة11) تجريم المساعدة والتحريض :تلتزم كل دولة طرف باتخاذ التدابير التشريعية وغيرها اللازمة لتجريم المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 10 من الاتفاقية، وذلك إذا ارتكبت عمداً وبنية ارتكاب جريمة من هذا القبيل.

أما الركن المعنوي في التشريع الجزائري يتمثل في

تتخذ أغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بإذن القانون بجرمه....[1].

ونفس الأمر ينطبق على الجريمة السبيرانية التي يقوم ركنها المعنوي على توافر الإرادة الجرمية لدى الفاعل، وهذا هو ما يظهر من خلال استعمال المشرع الجزائري لعبارة " الغش"، و" العمد" و"الإعداد لجريمة " من مواد 394 مكرر و 2 وفي الأخير 394 مكرر 5 من قانون العقوبات، وهذا إن دل فإنما يدل على أن الجريمة المعلوماتية جريمة عمدية بامتياز ولا يفترض فيها عنصر الخطأ.

ومن مثال ذلك في اتفاقية بودابست(مادة 4) التدخل في المعطيات" التدخل المتعمد أو الإرادي في المعطيات بالتدمير أو الحذف و(مادة 5) التدخل في الأنظمة التدخل المتعمد في الأنظمة بغية تعطيل أداء وعمل الأنظمة وغيرها من المواد.

المبحث الثاني: آثار الجريمة السبيرانية

لا تقتصر الجريمة السيبرانية على مجرد أفعال إجرامية تُرتكب في الفضاء الرقمي، بل تمتد آثارها لتُحدث تداعيات عميقة ومتباينة على مختلف المستويات: على حقوق الإنسان على الحياة الاجتماعية، وحتى الأمنية والسياسية للدول، وكذلك التاثير على الشركات الاقتصادية من خلال تغلغل التكنولوجيا في كل جانب من جوانب حياتنا، وعليه سنعالج اثار الجريمة السبيرانية على حقوق الانسان (المطلب الأول) تأثيرها على الدول (المطلب الثاني) بالإضافة إلى بحث آثارها على الجانب الاقتصادي (المطلب الثالث).

المطلب الأول: آثار الجريمة السبيرانية على حقوق الإنسان

[1]- عبد الرحمان خلفي، مرجع سابق، ص 101.

لم تعد الجريمة السيبرانية مجرد انتهاكات تقنية أو خسائر مادية فحسب، بل امتد تأثيرها ليطال صميم حقوق الإنسان، مهددةً بذلك الحريات الأساسية والأمن الشخصي للأفراد في جميع أنحاء العالم.بحيث تتخذ أشكالًا متعددة، من سرقة الهوية والبيانات الشخصية إلى التجسس الرقمي، والابتزاز الإلكتروني، ونشر خطاب الكراهية، والتلاعب بالمعلومات، هذه الأفعال، وإن كانت تحدث في العالم الافتراضي، إلا أن لها عواقب وخيمة وملموسة على حياة الأفراد وحقوقهم الأساسية. فحق الخصوصية، وحرية التعبير، والحق في عدم التمييز، بل وحتى الحق في الحياة والأمن الشخصي، كلها حقوق تتعرض للتهديد المباشر وغير المباشر جراء هذه الأنشطة الإجرامية.

الفرع الأول: جرائم مواقع التواصل الاجتماعي وتهديداتها لكرامة الإنسان

ساهمت استخدامات مواقع التواصل الاجتماعي بمختلف أنواعها، في الزيادة من انتهاكات هذه حقوق وهذا كان نتيجة للتوظيف السيء لها، واستغلالها في نشر الحروب والفتن، مما ألبس الضبابية على مفهوم حقوق الإنسان وحال دون تحقيقها وحمايتها، فحسب بعض التحليلات خلصت إلى أن "التطبيقات المستندة إلى الإنترنت والتي يقوم المستخدمون من خلالها بنمذجة علاقتهم مع أشخاص آخرين، على سبيل المثال الفيسبوك، ويخلص إلى أن هذه التطبيقات هي هدف محتمل للجرائم الإلكترونية ".وفي هذا المجال تتعدد أنواع هذه الاعتداءات، لكن سوف يتم التركيز على البعض منها...[1]

بحيث هناك جهود للأمم المتحدة في صياغة اتفاقية جديدة للجرائم الإلكترونية، وهي تعمل حاليًا على صياغة اتفاقية عالمية شاملة لمكافحة الجرائم الإلكترونية. هذه الجهود تأخذ في الاعتبار التطورات الحديثة في الفضاء الرقمي، بما في ذلك مواقع التواصل الاجتماعي، وتسعى إلى تحقيق توازن بين مكافحة الجريمة وحماية حقوق الإنسان، لا سيما الخصوصية وحرية التعبير.

الفرع الثاني: التعدي على حقوق الخصوصية

تعد عملية الاختراق التي تتعرض لها حسابات الأشخاص، وبياناتهم الخاصة، من أهم مظاهر الجريمة السيبرانية التي تمس بحقوق الانسان، بحيث يلجا فيها المجرم الالكتروني إلى الدخول غير القانوني لهذه الحسابات، وبطرق احترافية، يجمع فيها بين المهارة العالية في استخدام الكومبيوتر، وفهم عميق لأسرار الشبكة العنكبوتية، بهدف انتهاك السرية، وهذا النوع من الجرائم يدخل في نطاق التصيد الاحتيالي الذي أصبح يعرف انتشارا واسعا بين الدو ل..[2]

[1]- قدوس خديجة، جامعة وهران 2 محمد بن أحمد الجزائري، عمتون كمال، جامعة ظاهري محمد بشار، **(انتهاكات حقوق الإنسان في ظل انتشار الجريمة الالكترونية)**، مجلة التدوين، مجلد 12، العدد 02، تاريخ النشر 2020/12/30، ص 136

[2]- المرجع نفسه، ص136.

وبينت اتفاقية بودابست بشأن الجرائم الإلكترونية (2001) الحق في الخصوصية والأمن الرقمي، وهي أمور مرتبطة بكرامة الإنسان. على سبيل المثال، تجريم الدخول غير المشروع واعتراض البيانات يهدف إلى حماية سرية وسلامة البيانات، وبالتالي خصوصية الأفراد.تعتبر هذه الاتفاقية، التي صاغها مجلس أوروبا، أهم صك دولي لمكافحة الجرائم الإلكترونية. ورغم أنها لا تركز بشكل مباشر على حقوق الإنسان، إلا أنها تجرم أفعالاً مثل الدخول غير المشروع إلى أنظمة الحاسوب، واعتراض البيانات غير المشروع، وتدمير البيانات، والتزوير والاحتيال المتعلق بالحاسوب.

الفرع الثالث: انتهاكات حقوق الطفل

أصبح من السهل جدا الوصول إلى المواد الإباحية والصور الفاحشة نتيجة الاستخدام السيء لمواقع التواصل الاجتماعي والانترنت، فالجناة يستغل عن طريقها الأطفال والقصر في تحقيق مآربهم ومحاولة الاعتداء عليهم جنسيا وأذيتهم جسديا ونفسيا...[1].

وسبيلهم في هذا القيام بإنتاج مواد إباحية ثم يتم مشاركتها وبيعها على الانترنت، تكون بدايتها بإقامة علاقة صداقة سواء بالرسائل النصية أو التواصل الصوتي مع اتباع أسلوب الإطراء وتقديم الهدايا ، وهذا بهدف الاستمالة لكن بمجرد حصول المعتدي على المواد الجنسية، فإنه يهدده بإساءة استغلالهم مالم يتمثل الطفل له /لها.

إلى جانب الابتزاز الجنسي، يستغل الجناة هذه المواقع في عملية الاختطاف، وفي سياق هذا الحديث نجد أن الجرائم الإلكترونية المنتهكة لحقوق الانسان ، تعددت مظاهرها ، وتتنوع أساليبها ، فهي لا تتوقف إلى حد الاختراق ، والابتزاز والاختطاف ، بل تتجاوزه إلى الاتجار بالبشر واستغلال الاطفال في الأعمال الدنيئة.

دور التشريعات والقوانين الدولية والإقليمية في مواجهة التهديدات الرقمية (قراءة في التعليق العام رقم 52 على حقوق الطفل فيما يتعلق بالبيئة الرقمية):

أكد المنشور الأممي المنشور حديثا ان الطفل يتمتع بحقوقه في العالم الرقمي على الرغم من ان الاتفاقية حقوق الطفل لم تنص على ذلك صراحة وخلال المشاورات التي أجريت مع الأطفال حول العالم أعرب الأطفال عن وجهة نظر مفادها أن البيئة الرقمية يجب أن تدعم وتعزز وتحمي فرص مشاركتهم بصورة آمنة ومنصفة "نود من الحكومة وشركات التكنولوجيا ومن المعلمين مساعدتنا على إدارة

[1]- قدوس خديجة، عمتون كمال، مرجع سابق، ص 137.

المعلومات غير الجديرة بالثقة المنشورة على الانترنت" "أود أن أستوضح ما يحدث حقا جمع؟ وكيف تجمع؟" لبياناتي الخاصة...ولماذا ت "أنا... قلق إزاء تقاسم بياناتي ".[1]

وقد شرحت اللجنة الأممية في هذا التعليق العام كيف ينبغي للدول الأطراف أن تنفذ الاتفاقية فيما يتعلق بالبيئة الرقمية، وقدمت إرشادات بشأن التدابير التشريعية والسياساتية لضمان الامتثال الكامل لالتزاماتها بموجب الاتفاقية والبروتوكولات الملحقة بها في ضوء الفرص المتاحة والمخاطر والتحديات التي تواجهها في تعزيز جميع حقوق الطفل في البيئة الرقمية واحترامها وحمايتها وإعمالها.

وقدم التعليق أربعة مبادئ بمثابة دليل لتحديد التدابير اللازمة لضمان إعمال حقوق الطفل فيما يتعلق بالبيئة الرقمية...[2]:

الفرع الرابع: تقييد الحقوق الرقمية وتضييق نطاق التعبير

بسبب التوظيف السلبي لمواقع النت تحول هذا المحتوى إلى شكل من أشكال التحريض الإلكتروني، أو فيما يعرف بجريمة الترويج لخطاب الكراهية ويكون عن طريق نشر العداوة بين الدول والطوائف والأشخاص والسكان من خلال إرسال رسائل وهمية تحمل في طياتها كل أنواع الشتم وتمييز العنصري والإشاعات بهدف تفعيل كل آليات الحرب وهذا الأمر يتسبب في أعمال العنف تعسفية ضدهم، عن طريق الإهانة أو التحقير بطريقة خبيثة أو التشويه سمعة أجزاء من السكان بطريقة يمكن التعكير صفو السلم العام، ويستخدم الجناة الاختلافات العرقية، والدينية، كأداة أساسية في تشجيع هذا النوع من الخطابات، مثلما يجري اليوم في بعض الدول العربية التي وقعت ضحية هذا الفعل الإجرامي...[3].

على هذا النحو يتعارض خطاب الكراهية مع حرية التعبير، من حيث أن الاول يسعى للتفرقة والهدم وينتهك الحقوق الاساسية للإنسان ، في الحين تهدف حرية التعبير إلى مساعدة كل فرد على تحقيق الذات اكتشاف الحقيقة وتقوية الذات، وإقامة التوازن مقبول بين الاستقرار والتغيرات في المجتمع.

كما يسمح للجميع بخلق معتقداته الخاصة ونقلها للأخرين بحرية، وفي هذا السياق حدد مقرر الامم المتحدة الخاص بحماية حق التعبير أربعة أشكال من التعبير يجب أن يحظرها القانون الدولي**:** استغلال الاطفال في المواد الإباحية التحريض المباشر والعام لارتكاب إبادة جماعية الترويج للكراهة القومية أو العنصرية أو الدينية التي تشكل تحريضا على التمييز العداء أو العنف والتحريض ، وحسب المنظمة

[1] - التعليق العام رقم 25 لعام 2021 الصادر عن اللجنة المعنية بحقوق الطفل التابع للأمم المتحدة، والذي يُعنى بحقوق الطفل في البيئة الرقمية.

[2]- كريمة بوفلاقة **(سلامة الطفل في البيئة الرقمية الدولية، أية مخاطر وأية حلول؟ -دراسة تحليلية ألهم النصوص التشريعية الدولية في مجال حماية الطفل من المحتويات الرقمية غير اللائقة)** مجلة التشريع الإعلامي، جامعة الجزائر3، المجلد 01، العدد 04، تاريخ النشر 2023، ص 8.

[3]- قدوس خديجة، مرجع سابق، ص 138.

الاوروبية لحماية حقوق الانسان إن هذه الحرية بما فيها على الانترنت تختفي فيها حالات انتهاك حقوق الانسان عند استخدامها لغرض تعبير الحقوق والحريات...[1].

لكن الحاصل أنه رغم هذه المجهودات الدولية في سعيها لفرض القيود على حرية التعبير، إلا أن الأمر الواقع انه من الصعب تقييد الحريات على مساحة الانترنت، فهي منطقة متاحة اكثر من الإعلام التلفزيوني والصحافة بشتى انواعها بسبب احترافية الجناة في هذا المجال، وربما يظهر فشل هذا المسعى في انتشار جريمة الارهاب الالكتروني في العالم بدرجة رهيبة.

المطلب الثاني: آثار الجريمة السبيرانية على الدول

تعتمد الجريمة السبيرانية بالأساس على وسائل اتصال متطورة وأدوات تقنية حديثة في خلق أزمات مختلفة في الدول من الناحية الاجتماعية والسياسية والاقتصادية والأمنية وهذا ما سنتطرق إليه في هذا المطلب بيان الآثار الاجتماعية (الفرع الأول) وآثار الجريمة السبيرانية على الأمن السياسي والأمني (الفرع الثاني).

الفرع الأول: الآثار الاجتماعية

ما يمكن إدراكه أن الجريمة السبيراينة عموما لها تأثيراتها على الأفراد والأسرة والمجتمع خاصة في مجال القيم والعادات والسلوك ومن الآثار التي تترتب على سلوك جرائم الانترنت والحاسوب بصفة عامة.

قد تؤدي التحديات المعاصرة، مثل تفشي ظاهرة ارتياد المواقع الجنسية وانتشار الأخبار الكاذبة والإشاعات والتشهير ببعض الأفراد، إلى تدهور عميق في النسيج الاجتماعي والأخلاقي، تتسبب هذه الظواهر في انهيار الحياة الأسرية واضطراب نظام الأسرة، مما يقود إلى اضطراب العلاقات الاجتماعية وانهيار المجتمع تدريجياً، على المستوى الفردي، تتجلى هذه المشكلات في الإحباط والاكتئاب النفسي، واضطراب النوم والقلق والتوتر الدائم، والعزلة الاجتماعية ورفض الاختلاط بالآخرين .كما يلاحظ انحراف جنسي لدى الشباب والشابات واللجوء إلى الجنس السلبي، وتزايد معدل الجريمة الجنسية، لا سيما مع الإحجام عن الإبلاغ خشية افتضاح الأمر. بالإضافة إلى ذلك، تشهد المجتمعات تدميراً للأخلاق ونشراً للرذائل، وظهور حالات الاختطاف والاغتيالات حتى بعد دفع المبالغ المالية، وتفاقم إدمان الشباب على الألعاب الإلكترونية.

[1]- المرجع نفسه، ص 139.

الفرع الثاني: الآثار السياسية و الأمنية

يبرز هذا من خلال التجسس على الشخصيات السياسية أو تهديدهم بالقتل أو اختراق مؤسسات عمومية وحيوية للدولة وفي هذا السياق وقعت عدة حوادث تبين تعرض بعض المراكز العسكرية لجرائم قرصنة معلوماتية بهدف الوصول والحصول على معلومات مخزنة في ذاكرة الحسابات الآلية المستعملة فيها...[1]

أولا: التأثيرات الأمنية: تسعى التنظيمات الإرهابية إلى تحقيقها من خلال منظومة الإرهاب الإلكتروني ما يلي:

أ- إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها مما هدد أمن الدولة...[2]

ب- الاختراق الإلكتروني إلى الأنظمة الأمنية في دولة ما وفك الشفرات السرية بتشغيل منصات إطلاق الصواريخ الاستراتيجية والأسلحة الفتاكة وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها...[3]

ثانيا: التأثيرات السياسية:

وتأخذ صورة تهديد شخصيات سياسية بارزة في المجتمع بالقتل و القيام بتفجير المنشآت الوطنية أو بنشر الفيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية و اختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية أو تهديدهم لحملهم على إثبات الأفعال مع معينة يخططون لاختراقها...[4]

الفرع الثالث: الآثار الاقتصادية

تعدّ الجريمة السيبرانية إحدى أخطر التهديدات التي تواجه الاقتصادات العالمية في العصر الرقمي الحالي. فمع التوسع الهائل في استخدام التكنولوجيا والاعتماد المتزايد على الرقمنة في كافة القطاعات،

---

[1] - صباح كزيز،(**اثار الجريمة الإلكترونية على الأمن واستقرار الدول قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا**) مجلة الناقد للدراسات السياسية، جامعة محمد خيضر بسكرة، العدد 03، أكتوبر 2018، ص127.

[2] عجاني سهيلة، راهم أميرة، **(الهجومات السيبرانية وأثرها على تهديد السلم والأمن الدوليين)**، مذكرة ماستر في القانون، تخصص قانون عام، جامعة 08 ماي قالمة، 2024/2023، ص 31.

[3]- عجاني سهيلة، راهم أميرة، مرجع سابق، ص 31.

[4] - المرجع نفسه، ص31.

أصبحت البيانات والمعلومات تُشكل عصب الحياة التجارية والمالية، لم تعد تداعيات الهجمات السيبرانية مقتصرة على خسارة البيانات فحسب، بل امتدت لتُلحق أضرارًا اقتصادية فادحة ومتعددة الأوجه، تتراوح بين الخسائر المالية المباشرة، وتكاليف استعادة الأنظمة، وصولًا إلى فقدان الثقة وتشويه السمعة الذي يؤثر سلبًا على النمو الاقتصادي والاستقرار المالي على المستويين الكلي والجزئي. يهدف هذا المطلب إلى تسليط الضوء على أبرز هذه الآثار الاقتصادية المدمرة التي تُخلّفها الجريمة السيبرانية.

أولا: الآثار الاقتصادية الناجمة عن جرائم الاختراق وقرصنة البيانات.

تُعدّ جرائم الاختراق وقرصنة البيانات من أخطر التهديدات التي تواجه الاقتصادات العالمية في العصر الرقمي الحالي. فمع تزايد الاعتماد على التكنولوجيا وشبكات الإنترنت في كافة جوانب الحياة التجارية والمالية، أصبحت البيانات تُشكل أصولاً لا تُقدر بثمن بالنسبة للمؤسسات والشركات. إنّ أي اختراق لهذه البيانات أو قرصنتها لا يقتصر تأثيره على مجرد خسارة معلومات، بل يمتد ليشمل أضرارًا اقتصادية جسيمة ومتعددة الأوجه.

1: الآثار الجرائم الإلكترونية المالية.

يقصد بها استخدام شبكة الانترنت بهدف الحصول على المال كالدخول إلى شبكات البنوك والتحويل غير المشروع للأموال من حساباتها او التلاعب في الحسابات المودعة لدى البنوك بتحويلها من حساب إلى آخر او الحصول على الرقم السري الذي يمكن للمجرم للدخول إلى هذه الحسابات والتلاعب بها، ومن صورها كذلك السرقة الاموال باستخدام البطاقات البنكية المسروقة والقيام بتصنيع البطاقات المزورة بعد الحصول على اسماء وارقام البطاقات الاصلية ويمكنهم الحصول على هذه المعلومات خلال شبكة الانترنت ممن قاموا بالشراء عن طريقتها او من خلال الفنادق ومحطات البنزين والمحلات الكبرى.... [1].

تعتبر البنوك الهدف المفضل لمجرمي الإنترنت المحترفين، تفرض تكلفة باهضة على الموارد المالية للمؤسسات المالية والمصرفية جاء في أحد تقارير أن البنوك ينفق ثلاثة أضعاف على الأمن السيبراني مقارنة بالأمن الغير مالي...[2].

2: الآثار الاقتصادية الناجمة عن الفيروسات

[1]- صباح كزيز، مرجع سابق، ص131

[2]- بن جدو بن علية، دراد عياش، **(الآثار الاقتصادية للجرائم الالكترونية)** مجلة الابحاث الاقتصادية المعاصرة ، جامعة بومرداس، المجلد 05، العدد 01، تاريخ النشر: 2022/02/31، ص 569.

فيروسات الفدية هي أسرع الجرائم الإلكترونية انتشارا يشمل ضحايا برامج الفدية الشركات الكبرى والمؤسسات الصغيرة والمتوسطة والأفراد والمستهلكين في الحين أن التكلفة التي يهملها الفرد منخفضة...[1].

ثانيا: الخسائر الناجمة عن هده الجرائم

تعدّ الفيروسات الإلكترونية والبرمجيات الخبيثة أدوات رئيسية بيد مجرمي الإنترنت لشن هجمات تستهدف بشكل مباشر تحقيق مكاسب مالية غير مشروعة .لم يعد الأمر يقتصر على مجرد إتلاف البيانات أو تعطيل الأنظمة، بل تطور ليصبح وسيلة فعّالة لسرقة الأموال، والابتزاز، والتسبب في أضرار اقتصادية واسعة النطاق. إن التغلغل العميق للتكنولوجيا في حياتنا اليومية والأعمال التجارية يجعل هذه الفيروسات قادرة على إحداث خسائر مالية فادحة لا تقتصر على الشركات الكبرى، بل تمتد لتطال المؤسسات الصغيرة والمتوسطة، وحتى الأفراد. يهدف هذا الفرع إلى تسليط الضوء على الأوجه المتعددة لهذه الخسائر المالية المباشرة وغير المباشرة التي تُلحقها الفيروسات الإلكترونية، موضحةً تأثيرها المدمر على الأداء الاقتصادي والاستقرار المالي.

1 : الخسائر المالية

تؤثر الجرائم السبيرانية على الشركات الكبرى ماليًا. ويمكن لاختراقات البيانات، وهجمات برامج الفدية، والاحتيال المالي، وغيرها من الجرائم السبيرانية أن تُلحق أضرارًا مالية جسيمة بالشركات. وتُظهر الدراسات أن الشركات تنفق ملايين الدولارات في المتوسط على اختراقات البيانات.

من المعروف أن كل شركة تحتوي على بيانات المستخدمين، ومن الضروري تأمين على اختراق هذه البيانات، عند كشف هذه المعلومات الحساسة، توجه الشركات عقوبات وغرامات نتيجةً للمسؤوليات القانونية. تؤدي عوامل مثل التحقيقات والمعالجة وتعويض العملاء إلى إفراغ خزائن هذه الشركات.

لا تقتصر الخسائر المالية على اختراق البيانات فحسب، بل تنجم أيضًا عن عوامل أخرى، فيما يلي بعض منها:

أ- **هجمات برامج الفدية:** يستهدف مجرمو الإنترنت الشركات، ويشفّرون بياناتها المهمة، ويطلبون فدية مقابل تحريرها. تقع المؤسسات ضحيةً لهذه الهجمات، وتتكبّد خسائر مالية نتيجة دفع الفدية واستعادة الأنظمة، مما يؤدي إلى خسارة في الإيرادات.

[1]- المرجع نفسه، ص 570.

ب- الاحتيال المالي: تُعد عمليات التصيد الاحتيالي وسرقة الهوية من أكثر الهجمات شيوعًا، مما يُسبب خسائر مالية فادحة للشركات. يستهدف مجرمو الإنترنت الشركات المرتبطة بالبنوك، ويستخدمون بيانات اعتماد مسروقة أو يحصلون على وصول غير مصرح به إليها لتنفيذ أنشطة احتيالية.

ولتخفيف هذه الخسائر المالية، تستثمر الشركات في تدابير قوية للأمن السيبراني مثل التشفير، واكتشاف التطفل، وتدريب الموظفين .... [1]

2 : الضرر الذي يلحق بالسمعة

لا يُبالي العالم الحديث بسمعة الشركات. ومع ذلك، يُمكن أن تُؤثر أنشطة الجرائم الإلكترونية تأثيرًا بالغًا على صورة الشركة وتُضعف ثقة العملاء. وهذا بدوره يُؤدي إلى إنقاذ سوق العمل وتراجع إجمالي مبيعات الشركة، فيما يلي بعض العوامل:

أ- تشويه سمعة الشركة: تؤدي الهجمات التي تستهدف بيانات العملاء إلى تشويه سمعة الشركات، مما يؤدي إلى فقدان ثقة العملاء، والتعرض لإجراءات قانونية محتملة. وينتهي الأمر بتعرض الشركة للخطر وفقدان الثقة، مما يُلحق الضرر بسمعته.

ب- اهتزاز ثقة الجمهور بالشركة :تنتشر أخبار الهجمات الإلكترونية بسرعة، مما يؤثر على ثقة الجمهور بالشركة، التعرض لمثل هذه الهجمات يُعطي انطباعًا سلبيًا ويؤثر سلبًا على سمعة الشركة. الدعاية السلبية والكاذبة قد تُثني العملاء والشركاء والمستثمرين عن التعامل معها.

ولإعادة بناء السمعة الإيجابية والحفاظ عليها، ينبغي للشركات إعطاء الأولوية للأمن السيبراني، والتواصل الفوري مع العملاء المتضررين في حالة حدوث خرق، والاستثمار في استراتيجيات العلاقات العامة الاستباقية.

3: الاضطراب التشغيلي

تُعطّل الهجمات السيبرانية عمليات الشركات، مما يُؤدي إلى انخفاض الإنتاجية. وهذا يُلحق الضرر بالنظام البيئي الداخلي للشركة، ويُعطّل الأنظمة الحيوية، مما يُعرّضها لاختراقات البيانات، مما يُقوّض ثقة العملاء. فيما يلي الأشكال الشائعة لتعطيل العمليات الناجم عن الجرائم الإلكترونية:

أ- هجمات البرامج الضارة**:** تواجه الأنظمة توقفًا تشغيليًا عند تعرضها لأنشطة البرامج الضارة التي تصيب أنظمة الكمبيوتر مما يؤدي إلى تعطل النظام وفقدان البيانات.

[1]- **(تأثير الجرائم الإلكترونية على الاعمال) sprintzeal.com** نشر في 31يوليو2023 تاريخ الاطلاع 19ماي 2025على الساعة 10.4

ب- هجمات حجب الخدمة الموزعة**:** تُسيطر على شبكات الشركات، مما يجعلها غير قابلة للوصول من قِبل العملاء، وقد يؤدي ذلك إلى الإضرار بعلاقات العملاء.

ج- اختراقات النظام: يُعدّ الوصول غير المصرح به إلى الأنظمة الحيوية هدفًا رئيسيًا، مما يُعطّل عمليات الأعمال ويُعرّض المعلومات الحساسة للخطر. ويؤدي ذلك إلى بذل جهود مكثفة لاستعادة الوصول والبيانات الحساسة.

ينبغي للشركات وضع ضمانات قوية للأمن السيبراني، وتحديث برامجها بشكل متكرر، وإنشاء ... . من أجل تقليل الاضطراب التشغيلي... [1]

4: العواقب القانونية والتنظيمية

للجرائم السيبرانية آثار قانونية وتنظيمية على الشركات، وقد تؤدي إلى عقوبات وإجراءات قانونية صارمة، من الاعتبارات الرئيسية الالتزام بقوانين حماية البيانات وتطبيق تدابير أمنية فعّالة لحماية المعلومات الحساسة، لا تدع التهديدات الإلكترونية تُعرّض أعمالك للخطر، اجعل الأمن السيبراني أولوية قصوى واحمِ مستقبلك.

أ- قوانين حماية البيانات: يجب على المؤسسات الامتثال لقوانين ولوائح حماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR)، قد يؤدي عدم الامتثال إلى عقوبات صارمة وغرامات باهظة.

ب- المسؤولية والإجراءات القانونية: قد تخضع الشركة لإجراءات قانونية، مثل دعاوى قضائية جماعية، واستفسارات تنظيمية، وعقوبات تفرضها السلطات الحكومية، عندما تفشل في حماية بيانات عملائها بشكل فعال..

لتعامل مع جميع العواقب القانونية والمحتملة، يجب على الشركات أن تظل على اطلاع بالقوانين ذات الصلة، وتنفيذ تدابير الخصوصية والأمان، والعمل فقط مع المتخصصين القانونيين في مجال الأمن السيبراني.. .... [2]

5: سرقة الملكية الفكرية

لسرقة الملكية الفكرية القيّمة، كالأسرار التجارية وبراءات الاختراع والمعلومات الخاصة، غالبًا ما يستهدف مجرمو الإنترنت الشركات، ولسرقة الملكية الفكرية آثارٌ جسيمة:

[1]- **sprintzeal.com** ، مرجع سابق.

[2]- المرجع نفسه. **sprintzeal.com** ، مرجع سابق.

أ- فقدان الميزة التنافسية**:** يمكن أن تؤدي الملكية الفكرية المسروقة إلى منح المنافسين ميزة غير عادلة، مما يؤدي إلى فقدان حصة السوق، وانخفاض الربحية، وتقليص الابتكار.

ب- الإضرار بالسمعة: يمكن لسرقة الملكية الفكرية أن تضر بسمعة الشركة، حيث قد يشكك أصحاب المصلحة في قدرتها على حماية الأصول القيمة.

لحماية الملكية الفكرية، ينبغي للشركات تطبيق ضوابط وصول قوية، ومراقبة الشبكات بحثًا عن الوصول غير المصرح به، وتثقيف الموظفين حول أهمية حماية المعلومات الملكية.

خلاصة الفصل:

مما سبق فإن الجريمة السبيراينية جريمة مستحدثة تستهدف للاعتداء على المعطيات بدلالتها التقنية الواسعة أو الاستعانة بها لارتكاب جرائم تحاكي الجرائم التقليدية في العالم الافتراضي، وفي هذا الفصل تم تناول تعريف الجريمة السبيرانية وذلك حسب الاتجاهات القانونية، ثم بعد ذلك تم تحديد خصائصها، بالإضافة إلى انواعها وأركانها، ثم تم التعريج بعد ذلك إلى استيضاح موقف التشريع الجزائري من الجريمة السبيرانية من خلال النصوص القانونية الموضوعة لمواجهة هذه الجريمة، وآثارها على حقوق الانسان والدول والشركات، ولقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ بين الدول للتعاون فيما بينها لمواجهتها.

الفصل الثاني:

آليات مواجهة المجتمع الدولي للجريمة السيبرانية

الفصل الثاني: آليات مواجهة المجتمع الدولي للجريمة السيبرانية.

يعتبر التعاون الدولي آلية ضرورية لمكافحة الجرائم السبيرانية، نظرا لما تنطوي عليه هذه الجريمة المستحدثة من مميزات وخصائص يصعب معها على الدولة المنفردة مكافحتها أو الحد منها، ومن آثارها، وبمقتضى هذه الضرورة أدرك المجتمع الدولي خطورة هذه الظاهرة، بحيث اصبحت الدول توحد جهودها وسياساتها من أجل الكشف عن مرتكبي هذه الجريمة الخطيرة، وتوقيع الجزاء المناسب عليهم ،مما دفعهم إلى البحث عن آليات وسبل فعالة لمواجهة هذا التحدي المتزايد. يتناول هذا الفصل الآليات المختلفة التي يتبناها المجتمع الدولي لمكافحة الجريمة السبيرانية، بدءًا من صور التعاون الدولي في مواجهة الجرائم السبيرانية (المبحث الأول) كما سيسلط الضوء على أبرز التحديات التي تواجه هذا التعاون الدولي، وكيف يمكن التغلب عليها (المبحث الثاني).

المبحث الأول: صور التعاون الدولي في مواجهة الجريمة السيبرانية.

يبرز التعاون الدولي كركيزة أساسية وضرورة حتمية لمواجهة الجرائم السبيرانية المتزايد، فبدون تضافر الجهود التعاون بين الدول، ستظل الإجراءات الوطنية غير كافية لردع هذه الجرائم وملاحقة مرتكبيها بفاعلية، من خلال هذا المبحث نسلط الضوء على أبرز صور التعاون الدولي في مجال مكافحة الجريمة السيبرانية، بدءًا من التعاون القانوني (المطلب الأول) مرورا بالتعاون القضائي في (المطلب الثاني)كما سيتناول التعاون الأمني (المطلب الثالث)،

المطلب الأول: التعاون القانوني لمواجهة الجريمة السبيرانية.

تظهر أهمية الجهود الدولية والإقليمية في مواجهة الجريمة الإلكترونية من خلال العمل على مكافحة هذه الجريمة، والتي رسخت في مساعي عقد وإبرام اتفاقيات دولية ثنائية ومتعددة الأطراف، والذي برز بدوره كعنصر فعال في مكافحة الظاهرة خصوصا المحافظة على الثقة المتبادلة بين الدول في تقديم المساعدات الفنية والتقنية والقضائية، الأمر الذي جعلها تضع توصيات وتبرم اتفاقيات تدرج في التشريعات الداخلية وتعالج كل ما هو مستحدث في مجال التقدم العلمي...[1]

الفرع الأول: الجهود الدولية في مكافحة الجريمة السيبرانية

إن هناك العديد من الهيئات والمنظمات الدولية التي لها دور ملحوظ في إبرام الاتفاقيات لمواجهة الجرائم السيبرانية.

أولا: جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية

اتخذ المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دورا رئيسيا في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية الدولية، وفعلا تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة في عام 1950 على هذه التوصية التي بموجبها تم إنشاء اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين التي يقع على عاتقها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام، وإيجاد البرامج، ووضع الخطط، ورسم السياسات لتدابير دولية في مجال منع الجريمة ومعاملة المجرمين...[2]

وبعد انعقاد مؤتمر الأمم المتحدة لمنع المجرمين في كيوتو باليابان عام 1970 ثم استبدال اللجنة الاستشارية بالجنة منع الجريمة ومكافحتها بناء على توصية للمجلس الاقتصادي والاجتماعي عام 1971 حيث تهدف مؤتمرات الأمم المتحدة المعنية بمنع الجريمة ومعاملة المجرمين التي تعقد كل خمس

[1]- فريد ناشف، مرجع سابق، ص 442.
[2]- سليمان قطاف، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ظل الاتفاقات الدولية)**، مرجع سابق، ص 73.

سنوات إلى تعزيز تبادل المعرفة والخبرات بين الأخصائيين من مختلف الدول وإلى تدعيم التعاون الدولي والإقليمي في مكافحة الجريمة...[1]

وهي بذلك تشكل محفلا رئيسيا للتعاون الدولي والذي يعنينا في هذه الدراسة هي الجهود الأممية من خلال مؤتمراتها الخاصة لمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية وجرائم الحاسب الآلي، وهنا نشير إلى أن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده في مدينة ميلانو بإيطاليا عام 1985 انبثقت عنه مجموعة من القواعد التوجيهية والتي اكتملت صياغتها في المؤتمر الثامن الذي أجاز هذه المبادئ والذي عُقد في هافانا بكوبا عام 1990، والذي أقر المعاهدات النموذجية لتسليم المجرمين وتبادل المساعدات في المسائل الجنائية، ونقل الإشراف على المجرمين المحكوم عليهم بأحكام مشروطة، أو المفرج عنهم إفراجا مشروطا...[2]

أما في مجال الجرائم المتعلقة بالحاسوب، فلقد أشار القرار في هذا المؤتمر إلى أن هناك إجراءات يستوجب على الدول اتخاذها والتي من بينها، تحديث القوانين وأغراضها الجنائية من أجل تطبيق أفضل القوانين الجنائية الراهنة وعلى نحو ملائم، وإدخال تعديلات إن تطلب الأمر ذلك، ومصادرة العائد والأصول من الأنشطة غير المشروعة واتخاذ تدابير الأمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الانسان، والتأكيد على رفع الوعي لدى الجماهير والقضاة والأجهزة المعنية في هذا المجال بأهمية مكافحة هذا النوع من الجرائم ومحاكمة مرتكبيها، وذلك بتدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة، والتعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب، و حماية مصالح وحقوق ضحايا جرائم الحاسوب.

المؤتمر التاسع للأمم المتحدة حول منع الجريمة ومعاملة المجرمين "الجريمة": عقد هذا المؤتمر فى الفترة من 29 فريل إلى 8 ماي 1995 بالقاهرة وقد تضمن جدول أعمال المؤتمر الموضوعات الآتية:

- التعاون الدولي والمساعدة التقنية لتعزيز سيادة القانون .
- التدابير اللازمة لمنع الجريمة الاقتصادية الوطنية وعبر الدولية والجريمة المنظمة الوطنية .
- انظمة العدالة الجنائية والشرطة
- استراتيجيات منع الجريمة...[3]

[1]- سليمان قطاف، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ظل الاتفاقات الدولية)**، مرجع سابق، ص 74.
[2]- المرجع نفسه، ص74.
[3] محمود محمد صفاء الدين على شرشر، **(الجهود الدولية والتشريعية لمكافحة جرائم الانترنت)** مجلة البحوث القانونية والاقتصادية، جامعة المنوفية، مصر، المجلد 54، العدد 3، أكتوبر 2021، ص 534.

ربما تكون أفضل استراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال الاتفاقات الدولية التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة، نظرًا للانتشار العالمي للإنترنت، ويمكن أن تنشأ الجريمة الإلكترونية نفسها في أي مكان في العالم وتستهدف أي دولة بها مستخدمو الإنترنت تتمثل المشكلة المتكررة في مزيج من الاختصاصات القضائية التي تتجاوزها الجرائم الإلكترونية، وتتم معظم الجهود في مكافحة الجرائم السيبرانية من خلال تدابير أمنية تقنية مثل مكافحة الفيروسات وتصفية البريد العشوائي والتشفير هذا يمنع الهجمات الإلكترونية من النجاح حيث تكون هذه الإجراءات الأمنية كافية، لكنها لا تمنع مجرمي الإنترنت من العثور على أهداف مناسبة في مكان آخر، ويحتمل أن يكون أفضل وسيلة يتم القضاء على هجمات مجرمي الإنترنت تمامًا عن طريق حبس الجاني.[1]

المؤتمر الثاني عشر للأمم المتحدة حول منع الجريمة والعدالة والجنائية المنعقد في سلفادور البرازيلية في الفترة الممتدة 12 و 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات في مجال مكافحة الجريمة، لاسيما أن منظمة الأمم المتحدة تعد الإطار الأمثل لمكافحة الإجرام السيبراني، وقد وضعت مجموعة من القواعد الموضوعية والإجرائية لمواجهة هذا النوع من الجرائم...[2]

وتأكيدًا منها في هذا المؤتمر جاء البند 41 من تقريره يحث الدول على بناء قدرات سلطاتها الوطنية من أجل التعامل مع الجرائم الإلكترونية، بما في ذلك المنع والكشف والتحقيق وملاحقة هذه الجريمة بكافة أشكالها وتعزيز الأمن في شبكات الكمبيوتر.

كما دعت لجنة منع الجريمة والعدالة الجنائية في البند 42 من تقرير هذا المؤتمر، النظر والدراسة الشاملة لمشكلة الجرائم الإلكترونية وردود فعل الدول الأعضاء عليها، وطلب من المجتمع الدولي والقطاع الخاص بتبادل المعلومات بشأن التشريعات الوطنية والمساعدة التقنية والتعاون الدولي بهدف دراسة الخيارات الوطنية، والاستجابات القانونية الدولية أو غيرها من الاستجابات للجرائم الالكترونية...[3]

المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة بقطر في الفترة الممتدة بين 12 و19 أفريل 2015، ومن أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة السيبرانية والمتمثلة في وجوب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة السيبرانية ومنعها، حيث أن هذا النوع من الجرائم يتطلب من الدول أن تنمي قدرتها في جانب تدابير المنع

[1] سليمان قطاف، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ظل الاتفاقات الدولية)**، مرجع سابق، ص 75.
[2] مراد مشوش، **(الجهود الدولية لمكافحة الإجرام السيبراني)**، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 12، العدد 2، تاريخ القبول2019/11/24 ، ص 707.
[3] - بيدي أمال، مرجع سابق، ص 309.

والتحري المضادة، بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية والتحقيق فيها، وعمليات الاستدلال الجنائي الرقمية، وكيفية التعامل مع الأدلة الإلكترونية، وإمكانية استحداث أطر متعددة الأطراف، حيث أوصى اجتماع أفريقيا الإقليمي التحضيري للمؤتمر الثالث عشر بأن تنظر الدول في وضع اتفاقية بشأن الجريمة السيبرانية ضمن سياق المؤتمر، ووالواضح أن الكثير من أجهزة إنفاذ القانون تواجه صعوبات في إمكانية الوصول إلى البيانات الموجودة خارج نطاق إقليمها أثناء التحري عن الجرائم السيبرانية، وفي المقابل لابد من أن تكون ضمانات حقوق الإنسان وسيادة القانون وصون الحرمة الشخصية كافية لضمان أن يكون ذلك الوصول إلى البيانات من أجهزة إنفاذ القانون مجددا وقابلا للتنبؤ ومتناسبا وخاضعا للرقابة التأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة السيبرانية.

كما قامت الجمعية الدولية بعقد المؤتمر الخامس عشر لقانون العقوبات في ريو دي جانيرو البرازيلية عام 1994م، ولقد أقر العديد من التوصيات بشأن جرائم الكمبيوتر منها:

في الشق الموضوعي: لقد أوصى المؤتمر بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي:

- الاحتيال أو الغش المرتبط بالكمبيوتر: ويشمل الإدخال والإتلاف ومحو لمعطيات الكمبيوتر أو برامجه، أو القيام بأفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص، وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
- تزوير الكمبيوتر أو التزوير المعلوماتي: ويشمل إدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد - فيها لو ارتكبت بغير هذه الطرق - من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.
- الإضرار بالبيانات والبرامج (الاتلاف): وتشمل النحو والإتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.
- تخريب وإتلاف الكمبيوتر: وتشمل الإدخال أو المحو أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات).
- الدخول غير المصرح به: وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق الاعتراض غير المصرح به، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام الكمبيوتر أو عدة نظم أو شبكة اتصالات...[1]

[1] بيدي أمال، مرجع سابق، ص 307 – 308.

في الشق الإجرائي: أصدر المؤتمر في هذا الشق الكثير من الإجراءات من أهمها ما يلي:

- يتطلب التنقيب بالنسبة لجرائم الحاسب الآلي وضع تحت تصرف سلطات التحقيق والتحري ما يكفي لتحقيق حماية حقوق الإنسان وحرمة الحياة الخاصة له.

- لتجنب تعسف السلطات الرسمية، فإن القيود التي ترد على حقوق الإنسان لا يمكن أن تكون مقبولة إلا إذا كانت بسند قانوني واضح ودقيق ومتماشية مع المعايير الدولية لحقوق الانسان.

- على ضوء هذه المبادئ العامة يجب أن يحدد بوضوح ما يلي ،السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء وتفتيش شبكات الحاسب، يجب تحديدها وضرورة وضع القواعد المتعلقة بالإثبات ومصادقة الأدلة...[1]

- واجبات التعاون الفعال من جانب المجني عليهم، والشهود، وغيرهم من مستخدمي تكنولوجيا المعلومات، وذلك حتى تكون الأخيرة مناحة ويمكن استخدامها للأغراض القضائية .السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب ذاته، مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

- نظرا لتعدد وتنوع البيانات المدرجة في معظم معالجة البيانات، يجب عند بدء التحريات أن يوضع في الاعتبار - بالإضافة إلى القيم المالية التقليدية كل القيم المرتبطة ببيئة تكنولوجيا المعلومات، مثل: التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء تكامل البيانات كما كانت من قبل.

- القواعد القائمة في مجال قبول ومصداقية الأدلة، يمكن أن تثير مشاكل عند تطبيقها، نظرا لتقييم تسجيلات الحاسبات في الإجراءات القضائية، لذا ينبغي إدخال بعض التغييرات التشريعية في حالة الضرورة.

قرار الجمعية العامة للأمم المتحدة 121/45 هو قرار أصدرته الجمعية العامة للأمم المتحدة في عام 1990 .يتعلق القرار بموضوع منع الجريمة والعدالة الجنائية، ويتناول بشكل خاص حماية حقوق الإنسان في سياق استخدام تكنولوجيا المعلومات ...[2]

قرار الجمعية العامة للأمم المتحدة 693/55 لعام 2000، والذي يتعلق بـ "مكافحة الجريمة المنظمة عبر الوطنية"، هو قرار أصدرته الجمعية العامة للأمم المتحدة في 22 يناير 2001. هذا القرار يحدد إجراءات مكافحة الجريمة المنظمة عبر الوطنية، ويحث الدول الأعضاء على تبني تدابير لمنع الجرائم المنظمة عبر الوطنية، يتضمن القرار إبقاء مسألة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية

[1] محمد طارق عبد الرؤوف الحن، **(جريمة الاحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية)**، منشورات الحلبي الحقوقية، ط1 ، 2010، ص 188.

[2]- قرار الجمعية العامة للأمم المتحدة 121/45 الصادر في عام 1990.

على جدول أعمال دورة الجمعية العامة السادسة والخمسين ضمن البند المعنون "منع الجريمة والعدالة الجنائية ."[1]

القرار 239/57 في 20 كانون الاول/ديسمبر 2002 بشأن» إنشاء ثقافة عالمية للأمن السيبراني «قرارات الجمعية العامة 239/57 في 31 كانون الثاني/يناير 2003 و199/58 في 30 كانون الثاني/يناير 2004 بشأن «إنشاء ثقافة السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.[2]

ثانيا: الاتفاقية الدولية لمواجهة الجريمة السيبرانية 2024

اعتمدت الجمعية العامة للأمم المتحدة اليوم اتفاقيةً جديدةً ملزمةً قانونًا تهدُف إلى منع ومكافحة الجريمة السيبرانية، لتتوج بذلك عملية تفاوض استمرت خمس سنوات في 24ديسمبر 2024.

وتهدف اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية إلى زيادة فعالية جهود منع ومكافحة الجرائم السيبرانية، بما في ذلك من خلال تعزيز التعاون الدولي وتوفير الدعم الفني وبناء القدرات، خاصة إلى الدول النامية.

وقال فيليمون يانغ، رئيس الجمعية العامة للأمم المتحدة: "نعيش جميعًا في عالم رقمي، ولدى تكنولوجيا المعلومات والاتصالات قدرة كبيرة على دعم التنمية في المجتمعات، إلا أنها تحمل أيضاً تهديدًا متزايدًا من الجرائم السيبرانية. من خلال اعتماد هذه المعاهدة، اتفقت الدول الأعضاء على الأدوات والآليات اللازمة لتعزيز التعاون الدولي ومنع ومكافحة الجرائم السيبرانية وحماية الأشخاص وحقوقهم في المجال الرقمي."

إن اعتماد هذه الاتفاقية التاريخية يُمثل انتصارًا كبيرًا للتعددية، إذ تُعد أول صك قانوني دولي للأمم المتحدة بشأن قضايا الجريمة منذ أكثر من 20 عامًا. إنها خطوة بالغة الأهمية نحو تعزيز جهودنا لمكافحة الجرائم، بما في ذلك الاعتداء الجنسي على الأطفال عبر الإنترنت، والاحتيال الإلكتروني المعقد، وغسل الأموال،" صرّحت غادة والي، المدير التنفيذي لمكتب الأمم المتحدة المعني بالمخدرات والجريمة.

وأضافت والي: "في العصر الرقمي اليوم، أصبحت الجريمة الإلكترونية أكثر انتشارًا وضررًا، حيث تستغل الفئات الأكثر ضعفًا وتستنزف تريليونات الدولارات من اقتصاداتنا سنويًا. مكتب الأمم المتحدة المعني بالمخدرات والجريمة على أتم الاستعداد لدعم الدول الأعضاء في التوقيع على الاتفاقية الجديدة،

[1]- قرار الجمعية العامة للأمم المتحدة 693/55 لعام 2000.
[2]- قرار الجمعية العامة للأمم المتحدة 239/57 في 20 كانون الأول/ديسمبر2002.

والتصديق عليها، وتنفيذها من خلال توفير الأدوات والمساعدة التقنية، وبناء القدرات التي تحتاجها الدول لحماية اقتصاداتها وضمان فضاء رقمي آمنٍ وخالٍ من الجرائم السيبرانية

اعتمدت الجمعية العامة القرار دون تصويت. وتفاوضت الدول الأعضاء في الأمم المتحدة، بمشاركة المجتمع المدني، والمؤسسات الأكاديمية، والقطاع الخاص، على نص الاتفاقية على مدار خمس سنوات، حيث اكتملت صياغة مسودتها النهائية في 9 أغسطس2024.[1]

ثالثا: جهود الهيآت الدولية الأخرى في مجال مكافحة الجريمة السيبرانية

1. **منظمة التعاون الاقتصادي والتنمية (OECD):**

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجريمة السيبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة والقواعد الإرشادية التي تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من الأفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به. الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو تخريب ما يحتويه من بيانات وبرامج، والإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله...[2].

وفي عام 1992 وضعت المنظمة توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة تتمثل في حدود ،التجميع يتعين فرض قيود على تجميع البيانات.، ونوعية هذه البيانات حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله، بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة ومحددة سلفا. ،محدود الاستخدام اي يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك، الوقاية الأمنية **اي** ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات. المشاركة الفردية حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها و المسائلة والمحاسبة التي تقتضي محاسبة الأشخاص والجهات المرخص لهم

[1] - https://www.unodc.org/romena/ar/press/2024/August/press-release -united-nations -member-states- finalize-a-new-cybercrime-convention.html اطلع عله يوم: 17-06-2025، الساعة 11.55.

[2]- مراد مشوش، مرجع سابق، ص 709.

الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة...[1]

2. الاتحاد الدولي للاتصالات(ITU) :

اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم (45) الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلوماتي ومكافحة الرسائل الإقتحامية، وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين العام 2006، وقد تم تبني مجموعة من التوصيات في مجال الأمن المعلوماتي والرسائل الإقتحامية، كما أطلق الأمين العام للاتحاد في أيار 2007، جدول أعمال الأمن المعلوماتي العالمي لوضع إطار لمواجهة التحديات المتزايدة لأمن الإنترنت، ولإيجاد حلول لتعزيز الثقة والأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشأ فريق من الخبراء رفيع المستوى (HLEG) ضم أكثر من مائة خبير قدموا التقارير والتوصيات في حزيران 2008 حيث نشرت الاستراتيجية العالمية في 12/11/2008 وقد اشتملت الاستراتيجية على المجالات التالية: التدابير القانونية والتدابير التقنية والإجرائية والهياكل التنظيمية وبناء القدرات والتعاون الدولي...[2]

الفرع الثاني: الجهود الإقليمية في مكافحة الجريمة السيبرانية

الاتفاقيات والمعاهدات الدولية هي واحدة من أهمها أشكال التعاون الدولي بشكل عام، وفي مجال المكافحة الجرائم الناتجة عن الجرائم الإلكترونية على وجه الخصوص بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال المكافحة الجرائم الإلكترونية، ومعاهدة بودابست لمكافحة جرائم الإنترنت واتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية وتوصيات المجلس الأوروبي بشأن المشاكل الجنائية الإجراءات المتعلقة بتكنولوجيا المعلومات ونوضحها في التالية:

أولا: على المستوى الأوروبي

تعد الجريمة السيبرانية تهديدًا متزايدًا لا تعترف بالحدود، مما يستدعي استجابة إقليمية موحدة وفعالة في أوروبا، شهدت السنوات الأخيرة تكثيفًا للجهود المشتركة لمواجهة هذا التحدي المتنامي ومن هذه الجهود نذكر.

1- اتفاقية بودابست لمكافحة جرائم السيبرانية 2001:

تعتبر اتفاقية بودبست بشأن الجرائم الإلكترونية مراجعة جماعية استجابة لجرائم الإلكترونية من قبل دول الأعضاء في البلدان من أوروبا وبعض الدول الغير أعضاء، وهي أول معاهدة ملزمة متعددة

[1]- مراد مشوش، مرجع سابق، ص 710.
[2]- سليمان قطاف، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ظل الاتفاقيات الدولية)**، مرجع سابق، ص 77.

الجنسيات لفهم معالجة الجريمة السيبرانية بحذافيرها"، وكاف لها تأثير عميق بشأن التشريعات الدولية لمكافحة جرائم الإنترنت، وكان لها دورا مهما على المستوى الدولي في مكافحة الجرائم السيبرانية بدأ مجلس أوروبا يعمل في جرائم الكمبيوتر منذ السبعينيات وفي عام 1989 قدم مجلس أوروبا مبادئ توجيهية للهيئات التشريعية الوطنية في توصيات والجنة الأوروبية للجريمة اعتمد تقرير مشاكلئ في الجريمة ذات الصلة بالحاسوب لتطوير القانون الجنائي الموضوعي الضروري ضد الجرائم السيبرانية وتوصية أخرى تتناول قوانين الإجراءات الجنائية المتعلقة بتقنية المعلومات في عام1995،واستنادا إلي هذه التوصيات يكون بين عامي1997 و2001 قد تم تطوير اتفاقية بشأن الجرائم الإنترنيت وتم الافتتاح والتفاوض من قبلئ "لجنة الخبراء حول الجريمة" في الفضاء السيبراني(PC- CY(التي عينتهم اللجنة لجنة الوزراء وفي اكتوبر1999 اجتمع وزراء العدل ووزراء الداخلية الدول الثمانية الكبار في موسكو وطلبوا من ممثليهم وضع خيارات وحلول عملية تسمح بكشف الاتصالات الإلكترونية الدولية في إطار تحقيقات الجنائية والمتابعة تلك الاتصالات...[1]

ثم تبعتها عدة لقاءات الى ان تم عقد في العاصمة المجرية بودابست في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الإنترنت، ومواكبة للتطور فقد أبرم المجلس الأوروبي اتفاقية بود است في 2001/11/8 ووضعت للمصادقة في 2001/11/23 والتي تضمنت التعريف بأهدافها، ووضعت قائمة للجرائم التي يجب على الدول المصادقة عليها، وتعد الأولى في مجال مكافحة جرائم الإنترنت، وشملت العديد من جرائم الانترنت منها الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال، وتعمد الاتفاقية إلى تنسيق القوانين الجديدة في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر، وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة...[2]

كما تُعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الانترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول من جويلية لعام 2004 على مستوى الدول أعضاء مجلس الاتحاد الأوروبي، وكما سبق الإشارة، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس أوروبا مثل كندا، واليابان، وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية، كما أن هذه الاتفاقية بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الإنترنت جاءت نتيجة محاولات عديدة منذ ثمانينات القرن العشرين حتى ظهرت بشكلها النهائي في 23/11/2001م في بودابست وقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي المشاركة في إعداد هذه الاتفاقية وفي كندا واليابان وجنوب أفريقيا

[1]- سليمان قطاف، بوقرين عبد الحليم (**الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**)، مرجع سابق، ص337

[2]- قطاف سليمان، بوقرين عبد الحليم،**(مواجهة الجرائم السيبرانية في ظل الاتفاقيات الدولية)**، مرجع سابق، ص 79.

والولايات المتحدة الأمريكية، وقد تضمنت هذه الاتفاقية الأقسام تتمثل في تحديد المصطلحات، والخطوات الواجب اتخاذها في إطار التشريع الوطني، والتعاون الدولي، والشروط النهائية حول الانضمام إلى الاتفاقية.

كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء وذلك على النحو التالي:..[1]

- الجرائم المتعلقة بأمن الشبكات، الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه.الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتمال المعلوماتي... الخ. جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال، جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستنساخ المصنفات المشمولة بالحماية، المسؤولية الجنائية للأشخاص المعنوية، وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك، وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات التي يلزم اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية كما أشرنا أعلاه، وألزمت الدول الأعضاء بمراعاة حقوق الإنسان وحرياته الأساسية التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية على حد سواء والالتزام بعدم انتهاكها، مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية، عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الإنترنت.

كما تضمنت الاتفاقية جانبا آخر من التعاون انصب هذه المرة حول تدريب أعوان الأمن لإكسابهم خبرات عملية كما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم السيبرانية، وتعد الولايات المتحدة الأمريكية من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات، وهي تساعد على تدريب أجهزة الشرطة و قضاة الدول الأخرى بتمكينها من تعزيز قدراتها على ضبط مشاكل هذه الجرائم، قبل أن تفلت منها زمام الأمور، فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة والتدريب لتطوير أجهزة الادعاء العام في الدول الأخرى، ويعمل إلى جانبه البرنامج الدولي للمساعدة و التدريب (ICITAP) لتوفير المساعدات لأجهزة الشرطة بالدول النامية...[2]

القواعد الموضوعية للجرائم السيبرانية في الاتفاقية وزعت الاتفاقية الجرائم التي ترتكب بواسطة الانترنت، على أربع مجموعات كبرى، تضم الأولى: الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات، مثلث النفاذ غير الشرعي، كالاعتراض غير الشرعي، وتشويه البيانات، وسلامة النظام، وتضم المجموعة الثانية جرائم التزوير والاحتيال، بينما تندرج في الثالثة، الجرائم المتصلة

[1]- قطاف سليمان، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ظل الاتفاقيات الدولية)**، مرجع سابق، ص 80.
[2]- المرجع نفسه، ص 81.

بالمحتوى، مثل انتاج، وتوزيع، كحيازة مواد إباحية يستخدم فييا الاطفالئ، وفي المجموعة الرابعة، جرائم الاعتداء عن الملكية الفكرية، والحقوق المجاورة، ونصت في توصيتها رقم 15/ 87 علي تنظيم ومراقبة استخدام البيانات الشخصية في المجال الشرطي، وفي التوصية رقم 04/90 على حماية البيانات الشخصية المنزلة في المجال الإلكتروني المعلوماتي، ونصت في مادتها الثانية على أن الاعتراض الغير قانوني للبيانات الشخصية والمتداولة بين الحواسيب يعد جريمة معلوماتية، كما لم تستثني الاتفاقية في الباب الخامس بتحديد المسؤوليات الجزائية للشخص المعنوي أسوة بالشخص الطبيعي عن الجرائم المعلوماتية و العقوبات المقررة لهما، واستنادا إلى المواد (2-13) فإن الاتفاقية تلزم الدول الأعضاء فيها باتخاذ الإجراءات كالتدابير التشريعية الملائمة لتجريم تسع جرائم في ميدان الجرائم المعلوماتية وهي...[1]:

2- توصيات المجلس الأوروبي

أدى التطور السريع في مجال الحاسبات وتقنية الإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية، مما عجل إلى إصدار المجلس الأوروبي التوصية رقم: 95/13 بتاريخ: 11/09/1995، بخصوص مشاكل الإجراءات الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات، وعقوبات وطنية لتتناسب مع التنمية في هذا المجال، ومن بين أهم الأمور المذكورة في التوصية الأوروبية:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

- أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها.

- أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات بشرط أن يكون هذا الإجراء ضروريا...[2]

- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

---

[1] - سليمان قطاف، بوقرين عبد الحليم (**الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**)مرجع سابق، ص341

[2] هند نجيب، **(التعاون القضائي الدولي في مجال الجرائم الدولية)**، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، المجلد 59، العدد 2، يونيو 2016، ص 3016.

- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات، ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة.

- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء كانت برامج أم قواعد أم بيانات تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.

- يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها...[1]

- يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة، ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

- قد تتطلب إجراءات التحقيق من الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة ويفترض التدخل السريع وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.

- يجب أن تكون هناك إجراءات سريعة ومناسبة، ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع أدلة معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط الفوري.[2]

ثانيا: على المستوى العربي

تمثل الجريمة السيبرانية تحديًا متناميًا لا يقتصر تأثيره على حدود جغرافية، مما يستدعي استجابة إقليمية موحدة وفعالة، في المنطقة العربية، تزايد الاهتمام بمواجهة هذا الخطر المتزايد، ما دفع الدول إلى تكثيف جهودها المشتركة ومن هذه الجهود نذكر.

أ. اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية:

صدر عن جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم تقنية الفضاء السيبراني، سعت الدول العربية لتقنين وتجريم الأعمال غير المشروعة المرتكبة من خلال استخدام الفضاء السيبراني

[1]- هند نجيب، مرجع سابق، ص 3016.
[2]- قطاف سليمان، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية)** مرجع سابق، ص 79.

بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010/12/21 لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

ودعا مجلس الدول العربية إلى المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس باتخاذه من إجراءات المواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الجرائم الإلكترونية لمنع الإرهابيين من استخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكترونية.

كما دعا مجلس الدول العربية إلى التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود... [1]

بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية وعلى المستوى الإقليمي وخاصة اتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية، والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعرف الحدود الجغرافية.

ب. المكتب الاقليمي العربي للاتحاد والاتصالات

عقد محضر الاجتماع الأول في الجزائر يومي 25 و26 فيفري 2013 تم تشكيل فريق العمل حول حماية الأطفال على الإنترنت في المنطقة العربية ويهدف إلى تنسيق الجهود وتوحيد الرؤية في المنطقة العربية من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل على الإنترنت في المنطقة العربية وتم الاتفاق على ان تكون مهمة الفريق كالتالي تحديد الأفعال التي تشكيل خطرا على الأطفال في الفضاء السيبراني ووضع المبادئ التوجيهية للإطار القانوني الإقليمي لحماية الأطفال في الفضاء السيبراني في إطار التعاون والتنسيق الإقليمي في المنطقة العربية وتقديم توصيات عامة حول الاسترشاد بالمبادئ التوجيهية على المستوى الوطني لكل دولة عند صياغة قوانينها الخاصة .والقوانين النموذجية اعتمدت جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العدل العرب ما سمي بالقوانين العربية الإسترشادية الخاصة بمكافحة الجرائم الالكترونية ومنها ... [2]

[1]- قطاف سليمان، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية)**، مرجع سابق، ص81.
- [2]فاروق خلف، **(الآليات القانونية لمكافحة الجريمة المعلوماتية)**، مجلة الحقوق والحريات، جامعة محمد خليل بسكرة، جامعة حمة لخضر – الوادي ، العدد 02، 2015، ص14.

1. القانون العربي الاسترشادي لإثبات بالتقنيات الحديثة: اعتمده مجلس وزراء العدل العرب بالقرار رقم (771/د24) بتاريخ 2008/11/27 يحتوي على سبعة فصول، و(24)مادة ونجد الفصل الخامس من المادة (23) إلى (32) وما يليه يحتوي على الجرائم والعقوبات الخاصة بالجرائم الإلكترونية .

2. قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها: اعتمده مجلس وزراء العدل العرب في دورته (19) بالقرار رقم (495/د19) بتاريخ 08/10/2003 واعتمده مجلس وزراء الداخلية العرب في دورته (21) بالقرار رقم (417 -د2004/21)ويحتوي على (27) مادة تخص العقوبات للجرائم الإلكترونية .

3. القانون العربي الاسترشادي لحماية حق الملكية الفكرية: اعتمده مجلس وزراء العدل العرب بقرار رقم (940/د28) سنة 2012 والذي يحوي في الجزء الأول على حماية حق المؤلف والحقوق المجاورة، ويتكون من (10) فصول ونجد الفصل الرابع في المادة (19) الذي يوضح المصنفات المشمولة بالحماية منها "برامج الحاسوب مهما كانت لغتها بما فيها الأعمال التحضيرية" أما المادة (20) تتمتع بالحماية المقررة في هذا القانون المصنفات المشتقة التالية قواعد البيانات، سواء أكانت مقروءة أم غير مقروءة من الحاسب وفي الفصل التاسع نجد الإجراءات التحفظية والاجراءات في المادة (74) وما يليها .... [1]

ج. مجلس وزار العدل العرب:

بموجب القرار رقم (229) سنة 1996(26) وباستعراض الباب التاسع الخاص ضد الأشخاص نجد القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية وذلك في المواد (461.464) حيث أشارت المواد (461-463) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها والمادة (464) نصت على عقاب من يقوم بفعل الدخول الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظيفته المعتادة وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات... [2]

المطلب الثاني: التعاون القضائي لمواجهة الجريمة السيبرانية

فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالحاسب الآلي غالباً ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الشبكة الدولية للمعلومات أو الشركات المقدمة لتلك الخدمات، مع توصيل أجهزة الحاسب الآلي بالشبكة الدولية للمعلومات، وحتى ينجح

[1]- فاروق خلف، **(الآليات القانونية لمكافحة الجريمة المعلوماتية)**، مرجع سابق، ص15.
[2]- المرجع نفسه، ص15.

المحققون في ذلك عليهم أن يتتبعوا أثر قنوات الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة، ولتحديد مصدر الجريمة غالباً ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبيّن متى أُجريت تلك التوصيلات ومن أين ومن الذي أجراها وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه، وعندما يكون مقدم الخدمات خارج نطاق الولاية القضائية للمحقق - وهو ما يحدث غالباً - فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولاية قضائية أخرى بمعنى الحاجة إلى ما يسمى التعاون القضائي...[1]

وقد تعرضت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة إلى ضرورة تفعيل المساعدة القضائية المتبادلة بين الدول في مرحلة التحقيق أو المحاكمة المتعلقة بالجرائم المنصوص عليها في هذه الاتفاقية، حيث نصت المادة 18 على أن تقدم الدول الأطراف بعضها لبعض أكبر قدر ممكن من المساعدات القانونية المتبادلة في التحقيقات، الملاحظات، والإجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية...[2]

وترتبط ايضا بما تقدمه دول لبعضها البعض ما من إجراءات من شأنها تسهل مهمة المحاكمة في دول أخرى بصدد جريمة من الجرائم.

وتعتبر الاتفاقية الدولية منبع الالتزامات بين الدول، على أن يظل ما ليس ملزما ممكنا، وفقا لما ينص عليه في القانون الداخلي في كل من الدولتين، وقد أدرجه المشرع الجزائري ونص عليه في القانون 09/04 في المادة (16) معتبرا أنَّه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم الإلكترونية، يمكن للسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكل إلكتروني...[3]

أما عن صور المساعدة القضائية الدولية فتتمثل في: تبادل المعلومات (الفرع الأول)، نقل الإجراءات (الفرع الثاني)، باللإضافة إلى الإنابة القضائية (الفرع الثالث).

[1] هند نجيب، مرجع سابق، ص 123.
[2] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: اعتمدت الجمعية العامة للأمم المتحدة هذه الاتفاقية في 15 نوفمبر 2000، ودخلت حيّز التنفيذ في 29 سبتمبر 2003.
[3] المادة 16 من قانون رقم 09/04، مرجع سابق.

الفرع الأول: تبادل المعلومات

وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها السلطة القضائية الأجنبية وهي بصدد النظر في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، وقد يشمل تبادل السوابق القضائية للجناة...[1]

وفي إطار الجرائم الإلكترونية، أقرت الاتفاقية الأوروبية حول الجريمة الافتراضية تبادل المعلومات في المادة (23) منها، بنصها صراحة على وجوب توفر التعاون الدولي بين الدول الأطراف وتعميقه وتقليل العوائق بما يوفر أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الأطراف...[2]

كما نصت المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي على هذا التبادل بنصها "تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المتعلقة بالتنظيم القضائي...[3]

كما حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة الإلكترونية ومعاملة المجرمين المنعقد في هافانا 1990 في قراره المتعلق بالجرائم ذات الصلة بالحاسوب، حث الدول الأعضاء لتكثيف جهودها لمكافحة الجريمة الإلكترونية باتخاذ العديد من الإجراءات منها: مضاعفة الأنشطة التي تبذلها الدول على الصعيد الدولي من أجل مكافحة الجرائم الإلكترونية بما في ذلك دخول الدول أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل المرتبطة بالجرائم الإلكترونية، وتطابق تشريعات الدول الأعضاء مع أشكال جديدة للجرائم...[4]

ولقد نص عليها المشرع الجزائري في المادة 17 من القانون رقم 09/04 مؤكداً على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الإلزامية لتبادل المعلومات، وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل...[5]

---

[1] هند نجيب، مرجع سابق، ص 124.

[2] اتفاقية بودابست هي أول معاهدة ملزمة تهدف إلى معالجة الجرائم المرتكبة عبر الإنترنت (الفضاء السيبراني)، وُضعت تحت إشراف مجلس أوروبا، وتم توقيعها في مدينة بودابست – المجر بتاريخ 23 نوفمبر 2001، ودخلت حيّز التنفيذ في 1 يوليو 2004.

[3] المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي، وافق عليها وزراء العدل العرب بموجب القرار 01 المؤرخ في 1983/04/06، ووقعت الاتفاقية ودخلت حيز النفاذ 1985/10/30.

[4] هادي زيادة، مرجع سابق، ص44.

[5] المادة 17 من القانون رقم: 09/04.مرجع سابق.

الفرع الثاني: نقل الإجراءات

يقصد بنقل الإجراءات أن تقوم الدولة بإجراءات الجنائية تجريها فوق أراضيها بمعرفة سلطاتها القضائية بناء على طلب دولة أخرى بشأن جريمة وقعت فوق أراضي الدولة الأخيرة، وتُسمى الدولة قائمة بالإجراءات "الدولة المطلوب إليها" بينما الدولة التي تطلب اتخاذ الإجراءات بـ"الدولة الطالبة" ويتم ذلك وفق شروط معينة من أهمها التجريم المزدوج، ويقصد به أن يكون الفعل المنسوب إلى الشخص يُشكِّل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان حيث تؤدي دورا هاما في الوصول إلى الحقيقة...[1]

معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية: اعتمدت الجمعية العامة للأمم المتحدة هذه المعاهدة بموجب القرار 118/45 بتاريخ 14 كانون الأول/ديسمبر 1990. تهدف هذه المعاهدة إلى تسهيل التعاون بين الدول في المسائل الجنائية، بما في ذلك نقل الإجراءات القضائية.

المادة (11) من معاهدة الامم المتحدة أثر نقل الإجراءات بالنسبة للدولة المطالبة، تخضع الإجراءات المنقولة بناء على اتفاق لقانون الدولة المطالبة. وعلى هذه الدولة، عند توجيهها الاتهام بموجب قانونها إلى الشخص المشتبه فيه، أن تجرى التعديل اللازم فيما يتعلق بعناصر معينة من التوصيف القانوني للجرم، وإذا كان اختصاص هذه الدولة مبنيا على الحكم الوارد في الفقرة 2 من المادة (1) من هذه المعاهدة، يجب ألا تكون العقوبة التي يحكم بها في هذه الدولة أشد من العقوبة المنصوص عليها في قانون الدولة الطالبة، يكون لأي إجراء يتخذ في الدولة الطالبة، وفقا لقوانينها، بصدد الإجراءات أو المتطلبات الإجرائية نفس الشرعية في الدولة المطالبة كما لو كان ذلك الإجراء قد اتخذ في هذه الدولة أو من قبل سلطاتها، ما دام ذلك متفقا مع أحكام قانونها،على الدولة المطالبة إبلاغ الدولة الطالبة بالقرار الذي اتخذ نتيجة للإجراءات، ولهذا الغرض، تحال إلى الدولة الطالبة نسخة من أي قرار نهائي يتخذ، عندما يطلب منها ذلك.

المادة (22) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية هي النص القانوني الرئيسي الذي يتناول نقل الإجراءات بشكل مباشر ضمن هذه الاتفاقية، وهي تشجع الدول على دراسة وإمكانية نقل الإجراءات الجنائية عندما يكون ذلك في مصلحة العدالة ويلبي المعايير المحددة، مما يعزز التعاون القضائي الفعال في مكافحة الجريمة المنظمة عبر الوطنية.

وقد نصت المادة بصراحة على ما يلي:

[1] هند نجيب، مرجع سابق،، ص 126.

تتخذ الدول الأطراف، دراسة، وفقا لقانونها الداخلي، إمكانية نقل الإجراءات الجنائية المتصلة بجريمة مشمولة بهذه الاتفاقية إلى دولة طرف أخرى عندما يعتبر هذا النقل في مصلحة العدالة، ولا سيما عندما تكون دولتان أو أكثر متورطتين في الجريمة، أو عندما تكون الأدلة موجودة في أراضي الدولة الأخرى، أو عندما يكون المتهم موجودا في أراضي الدولة الأخرى، أو عندما يكون نقل الإجراءات مناسبا لتحقيق أهداف هذه الاتفاقية..."[1].

الفرع الثالث: الإنابة القضائية

تعبر الإنابة القضائية عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية للدولة الأخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن، وتهدف الإنابة القضائية إلى تذليل العقبات التي تعترض سير الإجراءات الجنائية في ظل ما تشهده الظواهر الإجرامية من تطور...[2]

من شأن الإنابة القضائية تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، فإجراءات التفتيش الضبط والمعاينة، وتماشياً مع سرعة الجريمة الإلكترونية وتجنباً لطول إجراءات طلب الإنابة القضائية فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في اختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق...[3]

تضمنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات نصوصًا متعلقة بالمساعدة المتبادلة بين الدول الأعضاء لمكافحة الجرائم المعلوماتية بحيث حثت الاتفاقية الدول الأطراف علي التعاون فيما بينها وتقديم المساعدة المتبادلة لغايات التحقيق وجمع الأدلة في الجرائم المعلوماتية وأن يكون الطلب خطي وحثت الاتفاقية الدول الأطراف تبادل المعلومات فيما بينهم التي حصلت عليها الدولة أثناء التحقيقات بالإضافة إلى اتخاذ إجراءات المساعدة المتبادلة وقد تضمنت الاتفاقية في المادة 35 حق الدولة الأخرى رفض طلب المساعدة إذا كانت متعلقة بجرائم سياسية أو جرائم متعلقة بالأمن أو النظام أو المصالح الأساسية...[4]

كما تضمنت المادة (27) من اتفاقية بودابست على الإجراءات المتعلقة بالمساعدة القضائية في حالة عدم وجود اتفاقية دولية واجبة التطبيق بشأن الطلبات المتعلقة بالمساعدة المتبادلة، وتضمنت أن يتم

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، مرجع سابق.
[2] - فريد ناشف مرجع سابق،، ص 141.
[3] - المرجع نفسه، ص 142.
[4] - المادة 35 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

رفض طلب المساعدة إذا كان الطلب متعلقا بجريمة سياسية، أو أن الطلب يمس سيادة الدول أو الأمن أو النظام العام...[1]

الفرع الرابع: التعاون الدولي لتسليم المجرمين لمواجهة الجرائم السيبرانية

التعاون الدولي لتسليم المجرمين يعرف على أنه الإجراءات القانونية التي تتخذ بغية قيام الدولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى لتنفيذ حكم صادر من محاكمها أو لمحاكمته، وذلك تطبيقا لاتفاقية دولية أو لمبدأ المعاملة بالمثل أو للمجاملة الدولية ويعد التسليم قاعدة مستقر عليها في القانون الدولي، حيث استقر مجمع القانون الدولي في أكسفورد عام 1880م على مبدأ التسليم كقاعدة دولية، إلا أن بعض الدول لا تأخذ به إلا بموجب اتفاقيات دولية خاصة بالتسليم، والمثال على ذلك الحكم الصادر عن محكمة التمييز الأردنية والذي تضمن رفض تسليم المتهم بالسرقة والتزوير إلى دولة قطر نظراً لعدم وجود اتفاقية بين دولة قطر والأردن في هذا الخصوص .ويعتبر تسليم المجرمين صورة من صور التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، والتعاون في هذا المجال يتطلب تعاون تشريعي وقضائي وتنفيذي، وقد حرصت أغلب دول المجتمع الدولي على عقد اتفاقيات دولية وسن تشريعات في مجال تسليم المجرمين، وهناك شروط للتسليم من أهمها التجريم المزدوج علاوة على شروط تتعلق بالأشخاص المطلوب تسليمهم، وشروط تتعلق بالجريمة المطلوب التسليم فيها ...[2]

ومن التبريرات نظام تسليم المجرمين أنه حق تمارسه الدولة وفقا لما يمثله الإجراء من أهمية بتحقيق مصالحها مع الدول الأخرى، ويقوم التسليم على أساس العلاقات الدبلوماسية الدولية أيا كانت طبيعة الجرائم المطلوب فيها التسليم. لا يوجد أي نظام دولي أو وطني يلزم أية دولة القيام بعملية التسليم يكون فيه مساس بمقتضيات السيادة الممارسة على الإقليم، فنظام التسليم ليس فيه مساس بسيادة الدولة . كما يعتبر التسليم نظاما يحقق مبدأ الإقليمية للدولة طالبة التسليم في شقيه الموضوعي والإجرائي، وهو المبرر الأساسي للتسليم والذي يمكن من معاقبة المجرمين وضمان إفلاتهم من العقاب لمجرد وجودهم فوق إقليم دولة أخرى. كما يعتبر من أهم صور التعاون الدولي في مجال محاربة الجريمة الدولية...[3] .

القانون الواجب التطبيق على التسليم تخضع عملية تسليم المجرمين الى الاتفاقية الثنائية بين الدولة طالبة التسليم والدولة المطلوب إليها التسليم في مجال التعاون القضائي أما في حالة عدم وجود اتفاقية بين الدولتين، يمكن اللجوء الى تطبيق الاتفاقيات المتعددة والتي تجد أساسها القانوني في المادة (16)

[1] - خالد ظاهر عبدالله جابر السهيل المطيري **(مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية)** مجلة البحوث القانونية والاقتصادية، المجلد 31، العدد 2، 2019، ص51.

[2] مريم عبد اللطيف مسلماني، **(مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية)** مجلة القانون والمجتمع، جامعة أدرار، جامعة قطر، المجلد 10، تاريخ النشر 2022، ص39-40

[3] بن حاج الطاهر محمد، شكيرين الديلمي، **(سبل الحماية الدولية من الجريمة الالكترونية)** مجلة الناقد للدراسات السياسية جامعة محمد خيضر بسكرة، جامعة خميس مليانة الجزائر، المجلد 6، العدد01، تاريخ النشر2022/04/18، ص 716.

فقرة 4 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة .و تشير الاتفاقيات الدولية إلى أن مسألة التسليم يخضع لإجراءات القانون الداخلي لكل دولة. ...[1]

أولا: الاتفاقية العربية لمكافحة جرائم التقنية المعلومات كأساس لتسليم المجرمين

قبل إقرار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ورغبة في توثيق التعاون الأمني في مجال تسليم المجرمين الفارين من العدالة وافق مجلس جامعة الدول العربية على اتفاقية تسليم المجرمين (بصفة عامة(بموجب القرار رقم 431 بتاريخ 1952/9/24، من دور انعقاده العادي (السادس عشر) وبعد ذلك أقرت الجامعة العربية كما سبق أن أوضحنا اتفاقية دعت للتعاون الدولي بين الدول الأطراف لتسليم المجرمين وقد أشارت الاتفاقية في المادة 31 إلي جواز الاعتداد بالاتفاقية كأساس قانوني بين الدول الأطراف لتسليم المجرمين وحددت شروط التسليم وهي أن تكون من الجرائم المشار إليها في الفصل الثاني التي لا تقل مدة العقوبة السالبة للحرية فيها في الدولة عن سنة وخضوع التسليم للشروط المنصوص عليها في الدولة مقدمة طلب التسليم مع تقرير حق الدول الأطراف في رفض هذا الطلب مع التعهد بتوجيهه الاتهام للجناة. ..[2]

ثانيا: اتفاقية بودابست لمكافحة الجرائم السيبرانية

تعد اتفاقية بودابست كأساس لتسليم الجناة مرتكبي الجرائم المعلوماتية، فقد نصت الاتفاقية على تسليم المجرمين في حالة إذ ما كانت الجرائم المنصوص عليها في الاتفاقية معاقب عليها في الدولتين أ و الدول الأطراف المعنيين وألا تقل العقوبة المقيدة للحرية عن سنة أو عقوبة أشد، ونصت على تطبيق العقوبة الأقل في حالة وجود اتفاقية ثنائية بين الدولتين . وقد أقرت للدول التي لا تجعل تسليم المجرمين مشروط على اتفاقية تسليم أن تعد اتفاقية بودابست كأساس لتسليم المجرمين بالنسبة لهم، واعتبرت الاتفاقية الجرائم المنصوص عليها من المادة (13-2)من الجرائم التي يجوز فيها التسليم. ...[3]

المطلب الثالث: التعاون الأمني لمواجهة الجريمة السيبرانية.

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، بحيث لا تستطيع بجهودها المنفردة القضاء على الجريمة السيبرانية لوحدها، وهذا بسبب الانتشار الواسع والسريع لها، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي لمواجهتها بأقصى سرعة ممكنة ومتابعة المجرمين الفارين من العدالة، وفي سبيل مكافحة الجريمة السيبرانية فقد شهدت العديد من صور التعاون

[1] فريد ناشف، مرجع سابق، ص 141.
[2] - خالد ظاهر عبدالله جابر السهيل المطيري، مرجع سابق، ص 49
[3] - المرجع نفسه، ص 50.

الأمني، خصوصا منها تلك التي كانت في غطار المنظمة الدولية للشرطة الجنائية (الفرع الأول) وفي إطار منظمة الويب الدولية (الفرع الثاني).

الفرع الأول: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)

الإنتربول هو شبكة عالمية تنسق الجهود الشرطية وتوفر الأدوات والخدمات لمساعدة الدول على العمل معًا لمكافحة الجريمة العابرة للحدود، وذلك بهدف بناء عالم أكثر أمانًا. وتهدف المنظمة إلى التأكيد وتشجيع التعاون بين أجهزة الشرطة في دول الأطراف وعلى نحو فعال في مكافحة الجريمة، وبمقتضى ميثاق المنظمة ونظامها الداخلي، تتمتع هذه الأخيرة بجملة من الاختصاصات تخولها القيام بنشاطات متعددة.

أولاً: تجميع وتبادل المعلومات والبيانات المتعلقة بالجريمة والمجرم، حيث تتسلم المنظمة هذه البيانات والمعلومات وتتبادلها مع المكاتب المركزية للشرطة الجنائية مع دول الأعضاء، وتقوم المنظمة بتجميع هذه البيانات وتنظيمها لديها، وهذه الوثائق مهمة في مكافحة الجريمة على المستوى الدولي...[1]

ثانياً: تنسيق الجهود بين الدول الأعضاء خاصة في مسألة هروب المجرمين، حيث تتولى التنسيق مع الدولة العضو من خلال المكاتب المركزية الوطنية التابعة للمنظمة، وذلك بتعيين مكان تواجد المجرم والإسراع في اتخاذ إجراءات القبض عليه وتسليم المجرمين.

فإذا ما أريد القبض على المجرم الهارب تخبر السلطة أو الجهاز المعني سواء رجال القضاء أو الشرطة أو المصالح الأخرى المكلفة بالمسائل الأمنية العامة المكتب المركزي للشرطة المحلية، فيدقق في الطلب ثم يوجهه إلى الأمانة العامة للإنتربول طالبا إذاعة دولية لقرار التوقيف الذي استلمته، فإذا ما قررت الأمانة العامة إذاعة الطلب بعدما تصلها المذكرة التي تتضمن كافة البيانات والمعلومات الخاصة بالشخص المطلوب ضبطه وتسليمه إليها، وبعدها تقوم بدراسة هذه المعلومات والتأكد من كون الجريمة المنسوبة للمجرم الهارب تدخل في جرائم القانون العام، كي تخرج من الجرائم الأخرى التي يمنع على الإنتربول التدخل فيها...[2]

بعدها تقوم الأمانة العامة بإرسال الطلب، سواء بواسطة النشرة أو بواسطة الإذاعات، فتلتقطه الإذاعات المنتشرة في المكاتب المركزية الوطنية، ويعمل كل من جهته على البحث على المجرم والقبض عليه، ويخبر المكتب المركزي الرئيسي بذلك.

[1]- أسامة غربي، **(المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة)** جامعة المدية، ص 162.
[2]- المرجع نفسه، ص 162.

وفي بعض الحالات المستعجلة وتفادياً لضياع الوقت فإن منظمة الإنتربول أجازت للمكاتب الوطنية إجراء اتصالات مباشرة فيما بينها وهذا بإرسال إنابة قضائية...[1]

ونذكر أن إجراءات القبض وتسليم المجرمين يجب أن تكون ضمن احترام القوانين والنظم الداخلية للدول، والالتزام بروح اتفاقيات حقوق الإنسان.

أما في مجال الجرائم المعلوماتية فقد أنشأت المنظمة الدولية للشرطة الجنائية الإنتربول خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات لمواجهة هذا النوع من الجرائم من خلال إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف واستخدام وسائل حديثة في تلك المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف من خلال استخدام برنامج التحليل والمقارنات لتلك الصور، وتزويد شرطة دول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها...[2]

أما على المستوى الأوروبي، أنشأ المجلس الأوروبي عام 1991 في لوكسمبورغ الشرطة الأوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول الأطراف لملاحقة الجناة في الجرائم العابرة للحدود، ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت...[3]

أما على المستوى العربي، فقد أنشأ المكتب العربي للشرطة الجنائية من قبل وزراء الداخلية والعدل العرب في سنة 2010 بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء...[4]

الفرع الثاني: شرطة الويب الدولية

أنشئت هذه المنظمة الأمنية في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا، والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة.

ويضم فريق العمل بهذه المنظمة المتخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية، وضباط الشرطة، ومتطوعين فنيين من 61 دولة حول العالم، ونظراً لاتساع نشاط هذه المنظمة وما تقوم

[1]- أسامة غربي، مرجع سابق، ص 163.
[2] - فريد ناشف، مرجع سابق، ص 432.
[3]- المرجع نفسه ، ص 439.
[4]- سليمان أحمد الفضل،(**المواجهة التشريعية والأمنية لجرائم الناشئة عن استخدام شبكة المعلومات الدولية**)، دار البعثة العربية، القاهرة، 2007، ص 414.

به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء، فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم، وفي إطار مسألة الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الإنترنت، فهناك من يرى أنه من الضروري وضع ضوابط وقواعد بحيث لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان من ناحية، وأن لا تستخدم الإنترنت لأغراض إجرامية أو نشر مواد إباحية تسيئ إلى المجتمع من ناحية أخرى...[1]

المبحث الثاني: التحديات وآفاق التعاون الدولي في مكافحة الجريمة السيبرانية

إذا كان التعاون الدولي هو اللبنة الأولى والركيزة الأساسية لمواجهة الجرائم السيبرانية، إلا أنه يقف في وجه هذا التعاون تحديات تسعى الدول للتغلب عليها، وعلى هذا الأساس سنتناول في هذا البحث ثلاثة مطالب، المطلب الأول التحديات القانونية، المطلب الثاني التحديات التقنية، المطلب الثالث سبل تعزيز هذا التعاون.

المطلب الأول: التحديات القانونية التي تواجه التعاون الدولي في مكافحة الجريمة السيبرانية

إن فهم هذه التحديات القانونية وتحليلها بعمق يُعدّ الخطوة الأولى نحو بناء استراتيجيات تعاون دولي أكثر فعالية. فبدون معالجة هذه العقبات التشريعية والإجرائية، ستظل الجهود المبذولة لمكافحة الجريمة السيبرانية مجزأة وغير كافية لردع مرتكبيها وحماية المجتمع الدولي من تهديداتهم المتزايدة.

الفرع الأول: القصور التشريعي للدول والتعارض بين مصالحها

إن اختلاف الأنظمة القانونية للدول يعد عقبة كبيرة تعترض سبيل التعارض الدولي بين تلك الدول في مجال مكافحات الجرائم السيبرانية مما يترتب على ذلك الاختلاف من مشكلات تطبيق القانون وما يثيره هذا الاختلاف من مشكلات في الواقع العملي، كما أن قصور غالبية النظم التشريعية للدول عن وضع مفهوم محدد للجرائم السيبرانية، وكذلك قصورها في وضع نظام قانوني خاص لتلك الجرائم يجعل سبل التعاون الدولي أمرا صعبا...[2]

وبنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم السيبرانية، يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، أو بمعنى آخر عدم وجود نظام قانوني لدى الدول خاص بمكافحة الجرائم السيبرانية، فما يكون مباحاً في أحد الأنظمة قد يكون مجرماً في نظام آخر، ويمكن إرجاع ذلك لعدة

[1] - فريد ناشف، مرجع سابق، ص 439.

[2] عادل عبد العالي إبراهيم خراشي،(**إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**)، مجلة كلية الشريعة والقانون، جامعة الأزهر، المجلد 16، العدد 1، ص 234.

أسباب وعوامل كاختلاف البيئات، والعادات والتقاليد، والديانات، والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر....[1]

الفرع الثاني: اختلاف النظم القانونية والإجراءات الجنائية

بسبب تنوع النظم القانونية الإجرائية واختلافها، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما، قد تكون عديمة الفائدة في دول أخرى، أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية والتسليم المراقب والعمليات المستترة وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، فقد تكون الطريقة ذاتها غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى ستشعر بخيبة أمل لعدم مقدرة سلطات القانون في الدولة الأخرى على استخدام ما يعتبره أداة فعالة، فضلا عن أن السلطات القضائية لدى الدولة الثانية ربما لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق تراها غير مشروعة حتى وإن كان هذا دليل تم الحصول عليه في اختصاص قضائي وشكل مشروع...[2]

وبالنظر إلى الاختلافات التي توجد بين التشريعات المختلفة فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود، يجب إعادة النظر في أطر التعاون القضائي من أجل صياغة شكل جديد له، فمنذ سنة 1993 أدرك المجلس الأوروبي المشكلات التي يمكن أن تثيرها الشبكة المعلوماتية الجديدة في مجال الإجراءات الجنائية...[3]

الفرع الثالث: تنازع الاختصاص القضائي الدولي

يقصد بتنازع الاختصاص القضائي بين الدول تقديم دعوى عن ذات الجريمة أو عدة جرائم مرتبطة إلى جهتين أو أكثر من جهات حكم أو تحقيق، وتمسك كل جهة باختصاصها بالنظر أو التحقيق في الدعوى وهو ما يعرف بتنازع الاختصاص الإيجابي، أو رفض كل دولة النظر في الدعوى على أساس عدم اختصاصها وهو ما يسمى بتنازع الاختصاص السلبي...[4]

الفرع الرابع: التجريم المزدوج

يعتبر نظام تسليم المجرمين من الأنظمة التي تساهم بصورة إيجابية وفعالة في تحقيق الاستقرار العالمي ودفاع الدول المتضامنة بجد الجريمة في سبيل تحقيق مصالحها المشتركة إلا أن التجريم

[1] عادل عبد العالي إبراهيم خراشي، مرجع سابق، ص 234.

[2] - جمال محمد حلفان محمد النقبي، سلطان محمد سالم عوض هيسان العصبي،(**التعاون الوطني والدولي في الجرائم الإلكترونية، مشكلات وحلول)** مجلة المعهد العالي للدراسات النوعية، مصر، المجلد 03،عدد 16، يوليو 2023، ص 5500.

[3] - المرجع نفسه، ص 5500.

[4] - عزيزة لرقط، (**التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكاليات وآليات التنفيذ)**) مجلة التواصل في الاقتصاد وإدارة القانون، جامعة باجي مختارعنابة، المجلد 25، العدد 04، تاريخ القبول27 ديسمبر 2019، ص 05.

المزدوج الذي يفرض في تسليم المجرمين بعد عناية كبيرة أمام التعاون الدولي في مجال التسليم المجرمين بالنسبة للجريمة الإلكترونية نفسها أو الجرائم الأخرى، ومن بين عقبات التعاون الدولي عدم وجود اتفاق حول الوصف الإجرامي الذي تنعت به الجريمة السيبرانية.

المطلب الثاني: التحديات التقنية التي تواجه التعاون الدولي لمكافحة الجريمة السبيرانية

إن فهم هذه التحديات التقنية وتحليلها بعمق يُعدّ ضروريًا لتطوير استراتيجيات تعاون دولي قادرة على مواكبة التهديدات المتزايدة للجريمة السيبرانية. فدون معالجة هذه الفجوات التكنولوجية، ستظل القدرة على كشف وملاحقة المجرمين السيبرانيين محدودة، مما يقوض الأمن الرقمي العالمي، ومن هذه التحديات خصوصا تلك المتعلقة بصعوبة تحديد هوية المجرمين (الفرع الأول)، صعوبة جمع الألة الرقمية (الفرع الثاني) بالإضافة إلى عدم وجود قنوات الاتصال (الفرع الثالث) الصعوبات المتعلقة بالتعاون الدولي في مجال التدريب (الفرع الرابع).

الفرع الأول: صعوبة تحديد هوية المجرمين

في سياق التحقيقات لمكافحة الجرائم السيبرانية نشهد تحديات كبيرة في محاولة تحديد مواقع الأجهزة المستعملة في الأنشطة الإجرامية، يستند نظام البصمات الإلكترونية على تتبع الحركة العكسية للمسارات عبر الإنترنت وتحديد العنوان الرقمي كوسيلة رئيسية لتحديد موقع الحاسوب، في هذا السياق نتعامل أولاً مع تحديات عمل بروتوكول انترنت TCP/IP حيث تتسارع التعقيدات في حالات الصيد الإلكتروني واستخدام الهويات المزيفة مما يجعل من الصعب تحديد هوية الجاني...[1]

وفي المؤتمر الدولي لجرائم الحواسيب الذي أقيم في أوسو بين 29 و 30 مايو 2000 أثيرت مسألة حيوية تتعلق بالتحقيق في الجرائم الإلكترونية، تم التركيز على التحديات التي تواجه هياكل الإنترنت وهي تحديد هوية الجناة، رغم وجود وسائل معالجة لتحديد مكان الأجهزة مثل غانوين (IP) التي تستخدم كوسيلة رئيسية لارتكاب هذه الجرائم، وفي هذا السياق أشار بعض المشاركين في المؤتمر إلى أن قضية عدم الكشف عن هوية الفاعلين وراء رسائل غير شرعية هي قضية نسبية، هم يبرزون عدم إمكانية تجهيل شامل في شبكة المعلومات، حيث يترك الجناة أثرا يمكن للمحققين استخدامها، يتوقف الأمر إلى حد كبير على ذكاء رجال الضبطية القضائية في تحليل الأدلة ورصد الشكوك، وفي حالة استخدام الجريمة حاسوبا شخصيا يمكن للمحقق استجواب صاحب الحاسوب المشتبه به حول تفاصيل استخدامه ومدة استخدامه ومقارنته بتفاصيل الجريمة...[2]

[1] بوفرحات نور الدين، عمري عبد القادر، (**تحديات كشف الهوية الإلكترونية للجناة بين أساليب التمويه والحواجز القانونية**) مجلة الحقوق والحريات، جامعة يحي فارس، المدية، المجلد 12، العدد 1، 2004، ص 264.
[2] المرجع نفسه، ص 267.

الفرع الثاني: صعوبة جمع الأدلة الرقمية

تسعى الدول للحد من الجريمة السيبرانية من خلال فرض سياسات دولية وعقوبات كبيرة على مرتكبيها، وتفعيل أحدث التقنيات والوسائل للكشف عن هوية الفاعلين، وكذلك نشر التوعية في المجتمعات حول الجرائم السيبرانية وخطرها، وتعريف الأفراد بكيفية الحفاظ على معلوماتهم وخصوصياتهم، وتوجيه التشريعات والقوانين وتحديثها بما يتماشى مع التطورات لفرض قوانين جديدة فيما يستجد من هذه الجرائم...[1]

ولا شك أن للقاضي في القوانين الوضعية سلطة تقدير الأدلة واستنباط القرائن وما تحمل من دلالات شرط أن يكون الدليل مرتبطا بالواقعة، وثابتا بيقين، ومنسجما مع التسلسل المنطقي للأحداث، وينسحب هذا القول على الدليل الجنائي الرقمي كونه أحد أقسام الأدلة المادية العلمية، بل أكثر منها حجية في الإثبات لأنها جاءت وفق قواعد علمية وحسابية لا تقبل الشك أو التأويل.

أما عن حجية الدليل الرقمي الناشئ عن التفتيش كما هو معلوم بأن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط أشياء مادية تتعلق بالجريمة، وتفيد في كشف حقيقتها، إلا أن ذلك لا يتوافق مع الطبيعة غير المادية للدليل الجنائي الرقمي.

إلا إن هناك خلافاً فقهياً حول موضوع تفتيش أجهزة الحاسوب، حيث إن القواعد العامة تفترض وجود شيء مادي ليقع عليه التفتيش، وهناك جانب من الفقه لا يعتبر الحاسوب شيئاً مادياً، وهناك جانب آخر إلى اعتبار أن التفتيش ينطبق على الحاسوب.[2]

من الطبيعي أن البحث في الأدلة الجنائية الرقمية يتطلب تسليط الضوء على الإطار القانوني لها، وبيان نظرة المشرع عنه، وتعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن القضاء الإلكتروني، وقد أدركت العديد من الدول الأخطار المتسارعة لتقنية المعلومات على الحق في الخصوصية، الأمر الذي دفع البعض منها إلى حماية هذا الحق في الدساتير الخاصة بها، ومن أبرز المجموعات والمنظمات الدولية التي عمدت في موضوع جرائم شبكة الإنترنت مجموعة الدول الثماني (G8) والأمم المتحدة ومنظماتها، والاتحاد الدولي للاتصالات، ومجلس أوربا...[3]

[1] عدنان إبراهيم الحجار، فايز أخضر بشير،(**الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل**)، مجلة الاستقلال للأبحاث، المجلد 06، العدد 01، تشرين الأول 2021، ص 137.
[2] عدنان إبراهيم الحجار، فايز أخضر بشير، مرجع سابق، ص 138.
[3] المرجع نفسه، ص 138.

الفرع الثالث: عدم وجود قنوات الاتصال

من أهم الأهداف المرجوة من التعاون الدولي الحصول على معلومات وبيانات متعلقة بالجريمة والمجرم السبيراني، ولتحقيق هذا الهدف كان لزاماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أخرى، خاصة الأجنبية منها، لتسهيل عملية جمع الأدلة والمعلومات المهمة المطلوبة بخصوص الجرم المرتكب، ولكن غياب مثل هذا النظام يعني عدم قدرة على جمع الأدلة الإلكترونية والمعلومات التي ستساعد على مكافحة الجريمة الإلكترونية...[1]

الفرع الرابع: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب

إن تدريب الجهات المختصة بالبحث والتحري ورجال العدالة هو شيء في غاية الأهمية، ففي كثير من الأحيان تكون بداية المكافحة من هذه النقطة، وإذا لم تكن البداية صحيحة فأكيد لن تكون النتيجة المتوصل إليها مرضية، فعملية التحري في الجريمة الإلكترونية وضبط المجرم الإلكتروني، والتحصل على الأدلة الإلكترونية، ووضع الملف كاملا أمام العدالة، وقبوله من طرفها، هي سلسلة مترابطة إن فقدت حلقة منها فلن تستطيع إكمال دائرة مكافحة الجريمة الإلكترونية...[2]

ولكن موضوع التدريب في هذا المجال تعتريه عدة صعوبات، منها على سبيل المثال النظرة السلبية لبعض القيادات الإدارية والمدربين أنفسهم، الذين يرون أن هذه العملية التدريبية ما هي إلا مضيعة للوقت والمال، كما أن الفوارق الفردية التي نجدها بين المدربين سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال، تعد عائقا آخر أمام هذه العملية، لذا يجب إعطاء هذه العملية مكانتها في المجال العلمي، ويجب اختيار المدربين بناء على كفاءاتهم التعليمية وطموحاتهم المهنية، دون المغالاة في الميزانية المالية المخصصة لهذه العملية...[3]

المطلب الثالث: سبل القضاء على التحديات التي تواجه الجهود الدولية في مكافحة الجرائم السيبرانية

إن الجهود المبذولة ما تزال تصطدم بجملة من التحديات وتتراوح بين غياب إطار قانوني موحد، مرورًا بتعقيدات التعاون القضائي عبر الحدود وغيرها من التحديات، من هنا تبرز الحاجة إلى تحليل هذه التحديات واقتراح سبل فعالة لتجاوزها، بما يضمن بناء منظومة دولية متماسكة وقادرة على مواجهة الجرائم السيبرانية بمختلف صورها لذا سنتناول السبل المتعلقة بالمساعدات القضائية الدولية في (الفرع الأول) وتوحيد النظم القانونية والإجرائية (الفرع الثاني) وحل صعوبة عدم وجود قنوات اتصال (الفرع

[1] محمد أحمد سليمان عيسى،(**التعاون الدولي لمواجهة الجريمة الإلكترونية**) المجلة الأكاديمية للبحث القانوني جامعة عبد الرحمان ميرة، بجاية، المجلد، 14، العدد، 02، تاريخ النشر 2016/11/27، ص 60.
[2] شنتير خضرة، (**الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)**)، أطروحة دكتوراه تخصص قانون جنائي، جامعة أدرار، 2021/01/25، ص 2017.
[3] المرجع نفسه، ص 2020.

الثالث) وحل صعوبة الخاص في مجال التدريب (الفرع الرابع) وحل صعوبة التزاحم في طلبات التسليم (الفرع الخامس).

الفرع الأول: السبل المتعلقة بالمساعدات القضائية الدولية

أصبح من الضروري استعراض السبل الكفيلة بتجاوز هذه التحديات، من خلال تعزيز الاتفاقيات الثنائية ومتعددة الأطراف، واعتماد أدوات تكنولوجية تضمن سرعة وفعالية تبادل الأدلة والمعلومات، بما يسهم في بناء بيئة دولية أكثر تنسيقًا وعدالة في مواجهة الجرائم السيبرانية.

أولا: تبادل المعلومات: وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم.

ثانيا: البطء في نقل الإجراءات: ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة...[1]

وذلك بالتواصل المباشر بين السلطات القضائية في الدولتين وهو يعد أحد الأساليب المهمة للتغلب على البطء في الإجراءات، حيث بمقتضى هذه الوسيلة يتم الاتصال مباشرة بين السلطة القضائية الطالبة والسلطة القضائية المطلوب إليها، ويعد هذا الطريق أكثر اختصارا وبالتالي أكثر سرعة ومرونة، وهو بالتالي يتلاءم مع أحوال الضرورة والاستعجال التي تتطلب سرعة اتخاذ إجراء من إجراءات التحقيق، خشية من استحالة اتخاذ الإجراء بفوات الوقت، ولهذا فقد نصت غالبية التشريعات الوطنية والاتفاقيات الدولية المعنية بتنظيم الإنابة القضائية الخارجية على جواز اتباع هذا الطريق في أحوال الاستعجال . وهذا بالفعل ما اوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي انعقد في بانكوك في الفترة من 18 – 4/25 2005م، حيث أكدت على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما وبغية ضمان تنفيذ الطلبات في الوقت المناسب، حيث أن مرور إجراءات التعاون القضائي بالطريق الدبلوماسي يجعلها تتسم بالبطء وكثرة الشكليات، وهو ما يتعارض مع طبيعة الجرائم المعلوماتية التي تتميز بسرعة عبور وتبادل المعلومات من خلال شبكتها، لذلك فإن مكافحة الجرائم المتعلقة بالإنترنت تقتضي ردود سريعة، خشية التلاعب في البيانات التي قد تشكل دلي" ضد المتهم. وبالنسبة للرد على طلبات التماس المساعدة فإنه من الضروري استجابة الفورية و السريعة على هذه الطلبات لأجل ذلك تنص المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية

[1] قطاف سليمان، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية)** مرجع سابق، ص 83.

والسريعة على طلبات التماس المساعدة، حيث أكدت على ذلك المادة 36/02 من اتفاقية بودابست، حيث نصت على ما يلي:" يمكن لكل طرف في حالة الاستعجال أن يقدم طلب المساعدة المتبادلة أو الاتصالات عن طريق وسائل سريعة لاتصال، كالفاكس أو البريد الإلكتروني، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق بما في ذلك التشفير لو كان ضروريا- مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا بواسطة الدولة الموجهة إليها الطلب، ويجب على الدولة المقدم إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال...[1]

الفرع الثاني: توحيد النظم القانونية والإجرائية

يتم حل هذا التحدي بتوحيد النظم القانونية، والتخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية، وذلك من خلال تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.

بالنسبة للتحدي الخاص بتنوع واختلاف النظم القانونية الإجرائية نجد أن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقبة والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة.

التي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى النطاق المكاني لذلك الطرف الأخر، والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الكشف عن البيانات المشار إليها، كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابكة وأن يضبط أو يحصل بطريقة مماثلة وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات أيضا، نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة...[2]

[1] سليمان أبو نمر يوسف بوكشريدة **(مكافحة الجريمة المعلوماتية في إطار القانون الدولي)** مذكرة ماستر، جامعة محمد خيضر بسكرة، السنة الجامعية: 2020 – 2021 ، ص 68.

[2] - اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعروفة أيضًا بـ اتفاقية باليرمو، هي إحدى الأدوات القانونية الدولية الرئيسية التي اعتمدتها الجمعية العامة للأمم المتحدة في 15 نوفمبر 2000، وبدأ العمل بها في 29 سبتمبر 2003

ونلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة **بشبكة** الإنترنت.

يمكن التغلب على هذا التحدي من خلال التزام الدول بتجريم الأفعال الواردة في الاتفاقيات المبرمة فيما بينها ،فإن ذلك يوفر الأساس الكافي لتحقيق شرط ازدواج التجريم، حيث أكدت على ذلك اتفاقية الأمم المتحدة لمكافحة الفساد في نص المادة 2/23،حيث نصت على الآتي:" "في مسائل التعاون الدولي كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفي، بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة، أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تلتمس بشأنه المساعدة بعد يعتبر فعال إجراميا في قوانين كلا الطرفين ."...[1]

ويمكن أيضا التغلب على هذا التحدي من خلال التخفيف من التطبيق الصارم لهذا الشرط وذلك إما برد الأفعال والتي تتطلب أن تجريم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا أو بمجرد السماح بالتسليم ألي سلوك تم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة، وهذا بالفعل ما ركزت عليه الاتجاهات والتطورات التشريعية الخاصة بنظام تسليم المجرمين ...[2]

الفرع الثالث: حل صعوبة عدم وجود قنوات اتصال.

للحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها، ومن الأمثلة على هذه الصكوك الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة...[3]

الفرع الرابع: حل صعوبة الخاص في مجال التدريب

يمكن التغلب على هذه الصعوبة من خلال عدة أمور، وهي كالآتي إجراء المزيد من الحملات التوعوية للتنبيه بمخاطر جرائم المعلومات والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها التنسيق بين الأجهزة المعينة بتدريب رجال تنفيذ القانون وإيجاد برامج تدريبية مشتركة

[1] - اتفاقية الأمم المتحدة لمكافحة الفساد، والمعروفة اختصارًا بـ UNCAC، هي أول صك دولي شامل مُلزم قانونًا لمكافحة الفساد بجميع أشكاله. اعتمدتها الجمعية العامة للأمم المتحدة في 31 أكتوبر 2003، ودخلت حيّز التنفيذ في 14 ديسمبر 2005.

[2] - سليمان أبو نمر يوسف بوكشريدة، مرجع سابق، ص69

[3] - قطاف سليمان، بوقرين عبد الحليم، **(مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية)** مرجع سابق، ص 84.

تناسب جميع الفئات والقيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب 35وجهات النظر بشأنه...[1]

الفرع الخامس: حل صعوبة التزاحم في طلبات التسليم

لم يستقر الفقه الدولي على تحديد وترتيب التسليم في حالة تزاحم طلبات التسليم، حيث توجد الاختلافات الكثيرة ترتيب في هذه الأولويات، بل إن هذا اختلاف موجود أيضا على نطاق الدولة الواحدة في كل اتفاقية على حدة، وهذا كله يرجع بصفة أساسية إلى مصالح وأولويات الدول ومصالحها مع أطراف المتعاقدة .حيث اعتمدت اتفاقية العربية الخاصة بالتسليم على معيار جسامة الفعل الإجرامي، ويظهر ذلك في المادة 13 منها، حيث تقضي بأنه "إذا قدمت إلى الدولة المطلوب إليها عدة طلبات من مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية التسليم للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أرضها، ثم للدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة، فتكون الأولوية التي طلبت التسليم قبل غيرها ."ولكن يزداد هذا الصعوبة تعقيدا في حالة الشخص متعدد الجنسيات، حيث تتعدد أسباب تعدد الجنسية فمنها ما يتحقق وقت الميلاد، ومنها ما يتحقق في تاريخ لاحق على الميلاد، ومنها ذلك التعدد المعاصر للميلاد، وهو أكثر الحالات شيوعا والشك أن مشكلة التنازع بين الجنسيات تختلف حسب المبدأ الذي تتبناه الدولة المطلوب إليها، سواء كان مبدأ تسليم الرعايا أو حظر تسليمهم، ولم تعالج التشريعات هذا الأمر، وتركته لمبدأ العاملة بالمثل وقواعد المجاملات الدولية وفي حالة ما إذا كان الشخص المطلوب يتمتع بجنسية الدولة الطالبة إلى جانب دولة أخرى فإن هذه الدولة بالتأكيد ستتمسك بالقواعد العامة التي تطبقها في هذا الخصوص، فقد ترفض تسليمه للدولة الثانية حتى ولو كان يحمل جنسيتها، وقد توافق على التسليم في ضوء الضوابط والمعايير التي تحددها، انطلاقا من حقوقه كمواطن .وتزيد المشكلة أكثر إذا لم يكن الشخص المطلوب يحمل جنسية الدولة المطلوب إليها، وبالتالي يخضع الأمر هنا كله إلى العلاقات الدبلوماسية، لأنه لا يمكن وضع معيار محدد يفصل بين الدول التي يحمل جنسيتها شخص واحد، ويكون القرار في النهاية بيد الدولة المطلوب إليها، وهي التي ستملك ترجيح دولة على أخرى لإعادة الشخص المطلوب إليها، لكن من الممكن أن يخضع التسليم هنا لمبدأ المعاملة بالمثل ليفصل في التنازع بين الدول، بالإضافة إلى قواعد المجاملات الدولية التي تحدد طبيعة العالقة بين الدول الأطر اف في التسليم ولكن هناك عدة حالات يجوز فيها للدولة المطلوب إليها التسليم أن ترفض ذلك الطلب وتمتنع عن التسليم، وهذه الحالات كالآتي_إذا توافرت أسباب جدية للتخوف من أن طلب التسليم قد قدم بغرض معاقبة الشخص المطلوب تسليمه لأسباب متعلقة بجنسيته، أو ديانته، أو أصله العرقي، أو توجهاته وآرائه السياسية، أو انتمائه لجماعة أو طائفة معينة .إذا كانت هناك أسباب موضوعية تدعو لاعتقاد بأن

[1]- سليمان أبو نمر يوسف بوكشريدة، مرجع سابق، ص65

الشخص المراد تسليمه سيتعرض للتعذيب، أو المعاملة أو العقوبة القاسية أو الإنسانية، أو الإحاطة بالكرامة أو المخالفة المبادئ وحقوق الإنسان، وهو عمل لا يليق بالدولة المطلوب إليها التسليم أن تساهم في تنفيذه عدم وجود اتفاقية تسليم مع الطرف طالب التسليم، أو أن المعاهدة المبرمة ال تشمل مثل هذا الطلب، وهذه الحالة نصت عليها اتفاقية بودابست في المادة 3/24...[1]

[1] سليمان أبو نمر يوسف بوكشريدة، مرجع سابق، ص71

خلاصة الفصل

على الرغم من اعتبار التعاون الدولي حجر الأساس في مكافحة الجرائم السيبرانية، الا أنه تواجه العديد من التحديات على الصعيد الدولي والوطني .حيث تتمثل التحديات الدولية في العديد من العراقيل التي تنتج سواء عن تعارض مصالح أشخاص القانون الدولي،، أو التي تنتج عن تنازع الاختصاص القضائي الدولي نتيجة صعوبة اثبات هذه الجرائم و صعوبة إجراءات المتابعة القضائية، وأما التحديات الوطنية تتمثل في العراقيل التي تنتج عن عدم ملائمة غالب التشريعات الوطنية لطبيعة الخاصة بهذه الجرائم، وكذلك نتيجة صعوبة التحقيق فيها .يمكن التغلب على كل هذه التحديات من خلال ابرام اتفاقيات دولية تزيل التعار ض بين أشخاص القانون الدولي من خلال انشاء قانون نموذجي موحد لمكافحة الجرائم السبيرانية.

الخاتمة

الخاتمة

دراسة الجريمة السبيرانية تساهم في التعرف على هذا النوع الجديد من الجرائم الذي يشكل خطورة على الأفراد والدول بحيث بدأت في الظهور والانتشار مع التطور التكنولوجي، لذلك أصبح التعاون الدولي في مكافحة هذه الصورة من الجرائم أحد المتطلبات العصر خاصة إذا كان هذا التعاون من أجل الحفاظ على أمن الأفراد والدول وممتلكاتهم ، وهناك معوقات غالبا ما تجعل هذا التعاون أمرا صعب التحقيق وفي نهاية دراستنا لموضوع التعاون الدولي في مواجهة الجريمة السبيرانية وأصبحت أحد التهديدات التي تواجه الدول (سياسيا واقتصاديا) وتهدد بشكل خاص حقوق الانسان وحرياته الاساسية ،والذي يكون وفقا للآليات متعددة منها القانونية والقضائية والامنية والتي سعت الدول لتكريسها إلا أنه مع ذلك تجدر الإشارة أن هذه الجهود تواجه العديد من التحديات والمعوقات التي حالت دون أن يحققه التعاون الدولي في هذا المجال محدود النتائج منها تلك المتعلقة بطبيعة الجريمة السبيرانية.

1. الجريمة السبيرانية من الجرائم ذات الطبيعة الخاصة لارتباطها بشكل خاص بالتطور الكبير في التكنولوجي المعلومات والاتصال لذلك نجد أن مرتكبو هذه الجريمة يتمتعون بكفاءة مميزة في هذا المجال تمكنهم من ارتكاب جرائمهم وتسترهم عليها وحتى طمس ادلة اثباتها.
2. تختلف دوافع ارتكاب الجرائم السبيرانية من شخص إلى اخر هناك دوافع نفسية واجتماعية ومالية وقد تكون دوافع بغرض الانتقام.
3. الجرائم السبيرانية كغيرها من الجرائم التقليدية تتميز بالخطورة لكونها تلحق اثار في الانسان والمؤسسات وقد تشكل خطر حتى على أمن واستقرار الدول.
4. تعتمد الجرائم السبيرانية على وسائل متطورة للكشف عنها واجراءات خاصة (امنية وقضائية وفنية).
5. إن سعي الدول والمنظمات الدولية لإجاد بيئة دولية ملائمة للتعايش بما يكفل حقوق الجميع دفعهم للإقرار بحتمية التعاون الدولي في مجال مكافحة الجريمة السبيرانية كأحد المهددات باتت تهدد النظام القانوني الدولي.
6. إن خصوصية الجريمة السبيرانية ومحدودية إمكانيات بعض الدول في مجال تكنولوجيا المعلومات والاتصال يحد من العوامل التي شكلت عائقا أمام تحقيق نتائج إجابيه في مجال المكافحة الدولية لها غلى عدم وعي لأفراد من جهة وعدم التزامهم بالتوجيهات من جهة اخرى

وبناء على النتائج المتوصل اليها من خلال دراستنا نقدم الاقتراحات التالية :

1. ضرورة تنمية الجهود الدولية لمواجهة جرائم السبيرانية من خلال سن مجموعة من التشريعات الوطنية زيادة على ما هو عليه وتكثيف من الاتفاقيات الدولية والإقليمية (الجماعية والثنائية) .

2. دعوة الدول المتقدمة في مجال المعلوماتي إلى تقديم المساعدات إلى البلدان الأقل نموا لتمكينها من مكافحة هذه النوعية من الجرائم ومن خلال توفير المزيد من برامج التدريب والمساعدات الفنية.

3. الاهتمام بعقد دورات التدريبية التي تعتني بفحص سبل مواجهة الجرائم المعلوماتية وعقد مؤتمرات دولية وبصفة دورية على المستويين الوطني والدولي.

4. بما أن المجرم الإلكتروني يعتمد بالدرجة الأولى على الوسائل التقنية الحديثة ولأن الإجراءات التقليدية غير كفيلة بمواجهة هذه الجرائم فينبغي على المشرع وضع إجراءات حديثة تعتمد على ذات الوسائل المستخدمة في الجريمة للكشف عنها وتتبع مرتكبيها.

5. تفعيل المراقبة الدولية والإقليمية عبر شبكة الإنترنت بحيث يتم تتبع الملفات المدخلة والمخرجة وتعقب الاختراقات غير مشروعة للأنظمة وتخريبها وملاحقة مرتكبيها.

6. نشر الوعي بين المواطنين و خاصة الشباب بمخاطر التعامل مع المواقع الالكترونية خصوصا السيئة والمشبوهة لما تحمله من خطورة على حقوقهم وحرياتهم قد تصل لحد ارتكاب بعض الصور من الجرائم. وتوعيتهم في عدم الدخول إلى المواقع المتنافية مع القيم الاخلاقية والدينية ونشر بعض وترويج صور تلك التجاوزات بهدف التحسيس .

قائمة
المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

1- الاتفاقيات:

1) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: اعتمدت الجمعية العامة للأمم المتحدة هذه الاتفاقية في 15 نوفمبر 2000، ودخلت حيّز التنفيذ في 29 سبتمبر 2003.
2) الاتفاقية المتعلقة بالجريمة الالكترونية بوداست، اعتمدها مجلس أوربا سنة 2001، دخلت حيز التنفيذ سنة 2004.
3) اتفاقية الأمم المتحدة لمكافحة الفساد، والمعروفة اختصارًا بـ UNCAC، هي أول صك دولي شامل مُلزم قانونًا لمكافحة الفساد بجميع أشكاله. اعتمدتها الجمعية العامة للأمم المتحدة في 31 أكتوبر 2003، ودخلت حيّز التنفيذ في 14 ديسمبر 2005.
1) اتفاقية الرياض العربية للتعاون القضائي، وافق عليها وزراء العدل العرب بموجب القرار 01 المؤرخ في 1983/04/06، ووقعت الاتفاقية ودخلت حيز النفاذ 1985/10/30.
2) اتفاقية بودابست ، وتم توقيعها في مدينة بودابست – المجر بتاريخ 23 نوفمبر 2001، ودخلت حيّز التنفيذ في 1 يوليو 2004.

2- القرارات الدولية:

1) قرار الجمعية العامة للأمم المتحدة 121/45 الصادر في عام 1990.
2) قرار الجمعية العامة للأمم المتحدة 693/55 لعام 2000.
3) قرار الجمعية العامة للأمم المتحدة 239/57 في 20 كانون الأول/ديسمبر2002.
4) التعليق العام رقم 25 لعام 2021 الصادر عن اللجنة المعنية بحقوق الطفل التابع للأمم المتحدة، والذي يُعنى بحقوق الطفل في البيئة الرقمية.

3- النصوص القانونية الوطنية:

1) القانون رقم 15/04 مؤرخ في 27 رمضان 1425 الموافق لـ 10 نوفمبر 2004 يعدل ويتمم الأمررقم 66-156 المؤرخ في 18 صفر 1386 الموافق لـ 8يونيو 1960 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71.
2) القانون 09-04 (المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات والإعلام واتصال ومكافحتها) ، المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009، الصادرفي الجريدة الرسمية الجزائرية، العدد 47، تاريخ صدور الجريدة الرسمية 25 شعبان 1430الموافق لـ 16 غشت 2009.

ثانيا- المراجع

1. الكتب:

1) احمد خليفة الملط (الجرائم المعلوماتية) دار الفكر الجامعي الطبعة 2، تاريخ النشر 2005 .
2) بلعليات ابراهيم ،اركان الجريمة وطرق اثباتها في قانون العقوبات، دار الخلد ونية الجزائر الطبعة الاولى ، 2007
3) سليمان أحمد الفضل، المواجهة التشريعية والأمنية لجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار البعثة العربية، القاهرة، 2007.
4) محمد طارق عبد الرؤوف الحن، جريمة الاحتيال عبر الإنترنتّ، الأحكام الموضوعية والأحكام الإجرائية، ط1، منشورات الحلبي الحقوقية، تاريخ الاصدار 26يوليو 2010.
5) محمود أحمد القرعان الجرائم الالكترونية، دار وائل للنشر والتوزيع، تاريخ النشر2017
6) جميل عبد الباقي الصغير، القانون الجزائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر 2024.

2. أطروحات الدكتوراه:

1) شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة) ، أطروحة دكتوراه تخصص قانون جنائي، جامعة أدرار، 2021/01/25.

3. مذكرات الماستر:

1) عمار حشان، (الجريمة المعلوماتية في التشريع الجزائري) رسالة ماستر، تخصص ادارة التحقيقات الاقتصادية والمالية ، كلية، العلوم الاقتصادية والعلوم التجارية وعلوم التسيير قسم علوم التسيير، جامعة قاصدي مرباح ورقلة،تاريخ نشر 02جويلية 2019.
2) حشيخة عبد الهادي ،(التعاون الدولي في مجال مكافحة الجرائم الالكترونية) ،مذكرة نيل شهادة ماستر ، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة ،تاريخ 2020/2019.
3) سليمان أبو نمر يوسف بوكشريدة (مكافحة الجريمة المعلوماتية في إطار القانون الدولي)مذكرة ماستر، جامعة محمد خيضر بسكرة ،لسنة الجامعية: 2020 – 2021.
4) هادي زيادة، آليات التعاون الدولي في مكافحة الجريمة السيبرانية، مذكرة ماستر في القانون الجنائي، تخصص قانون جنائي وعلوم جنائية ، جامعة عبد بن باديس مستغانم، نوقشت يوم2023/06/14.
5) عجاني سهيلة، راهم أميرة، (الهجومات السيبرانية وأثرها على تهديد السلم والامن الدوليين)، مذكرة ماستر في القانون، تخصص قانون عام، جامعة 08ماي قالمة، 2024/2023.

4-المقالات:

1) عادل عبد العالي إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، **مجلة** كلية الشريعة والقانون المجلد 16، العدد 1، كلية الشريعة والقانون جامعة الأزهر،2014 .

2) فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، ، جامعة حمة لخضر – الوادي ، العدد 02، 2015.

3) محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجريمة الإلكترونية جامعة عبد الرحمان ميرة، بجاية ، المجلة الأكاديمية للبحث القانوني، المجلد، 14، العدد، 02، ، تاريخ النشر 2016.

4) هند نجيب، التعاون القضائي الدولي في مجال الجرائم الدولية، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، المجلد 59، العدد 2، تاريخ النشر2019.

5) صباح كزيز، اثار الجريمة الإلكترونية على الامن واستقرار الدول قرصنة الموقع الالكتروني لوكالة الانباء القطرية نموذجا، مجلة الناقد للدراسات السياسية، جامعة محمد خيضر بسكرة الجزائر ، العدد 3، 2018.

6) مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبرانية، مجلة الواحات للبحوث والدراسات جامعة غرداية، ، المجلد 12، العدد 2، تاريخ القبول2019 .

7) خالد ظاهر عبدالله جابر السهيل المطيري ،مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية لمجلد 31، العدد 2، 2019.

8) عزيزة لرقط، التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكاليات وآليات التنفيذ) ، مجلة التواصل في الاقتصاد وإدارة القانون، ، جامعة باجي مختار عنابة، المجلد 25، العدد 04، تاريخ القبول 2019.

9) حمزة خضري، عشاس حمزة، خصوصية أركان الجريمة المعلوماتية في تشريع الجزائري ، مجلة الدراسات القانونية والسياسية ، جامعة محمد بوضياف المسيلة، مجلد6 العدد2، تاريخ النشر 2020.

10) قدوس خديجة، جامعة وهران 2 محمد بن أحمد الجزائري، عمتون كمال، ، انتهاكات حقوق الإنسان في ظل انتشار الجريمة الالكترونية، مجلة التدوين، جامعة ظاهري محمد بشار، مجلد 12.العدد 02، تاريخ النشر 2020

11)محمود محمد صفاء الدين على شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت مجلة البحوث القانونية والاقتصادية ، جامعة المنوفية، ، لمجلد 54 العدد3، 2021.

12) مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري (الجزائر)، مجلة إيليز للبحوث والدراسات ، جامعة محمد بوضياف المسيلة، المجلد 6، العدد 02 ، تاريخ النشر: 2021.

13) عدنان إبراهيم الحجار، فايز أخضر بشير، الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل، مجلة الاستقلال للأبحاث/ المجلد 06، العدد 01، 2021.

14) بيدي آمال، جهود الأمم المتحدة في مكافحة الجرائم السبيرانية مجلة البحوث في الحقوق والعلوم السياسية ، جامعة الجلفة، المجلد 08 العدد01، تاريخ النشر2022.

15) قطاف سليمان، مواجهة الجرائم السبيرانية في ضوء الاتفاقيات الدولية ، مجلة البحوث القانونية والاقتصادية آفلو، جامعة عمار ثليجي الأغواط، المجلد 5 العدد02 ، تاريخ النشر 2022.

16) مريم عبد اللطيف مسلماني ، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الالكترونية، مجلة القانون والمجتمع ، جامعة قطر، المجلد10، تاريخ النشر سنة 2022.

17) ابن جدو بن علية، دراد عياش، الآثار الاقتصادية للجرائم الالكترونية ، مجلة الابحاث الاقتصادية المعاصرة ، جامعة بومرداس، المجلد 05 العدد 01، تاريخ النشر: 2022

18) بن حاج الطاهر محمد، شكيرين الديلمي، سبل الحماية الدولية من الجريمة الالكترونية، المجلة الناقد للدراسات السياسية ، جامعة خميس مليانة المجلد 6 العدد01، تاريخ النشر2022.

19) فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية ، مجلة البحوث في الحقوق السياسية ، جامعة البليدة 02، مجلد 8 العدد 1، تاريخ النشر 2022 .

20) سليمان قطاف، بوقرين عبد الحليم ،الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، لمجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 06، العدد 01، تاريخ النشر2023 .

21) عفاف بعون، نسيمة أولاد سالم ،الجريمة الالكترونية، قراءة سيبوتاريخية في النشأة وآثار ، مجلة القيس لدراسات النفسية والاجتماعية ، جامعة قاصدي مرباح، المجلد 05 العدد 20، تاريخ النشر 2023 .

22) كريمة بوفلاقة ، سلامة الطفل في البيئة الرقمية الدولية، أية مخاطر وأية حلول؟ -دراسة تحليلية ألهم النصوص التشريعية الدولية في مجال حماية الطفل من المحتويات الرقمية غير اللائقة، مجلة التشريع الإعلامي، جامعة الجزائر3، المجلد 01، العدد 04، تاريخ النشر 2023

23) جمال محمد حلفان محمد النقبي، سلطان محمد سالم عوض هيسان العصبي،التعاون الوطني والدولي في الجرائم الإلكترونية، مشكلات وحلول، مجلة المعهد العالي للدراسات النوعية، مجلد 03، عدد 16، يوليو 2023 .

24) واجعوط سعاد، مكافحة الجريمة السبيرانية على المستوي الوطني، دفاتر البحوث العلمية، المركز الجامعي تيبازة، المجلد 12، العدد 02، تاريخ النشر: 2024.

25) نورهان محمد الربيعي، الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة)،مجلة الفرابي للعلوم الإنسانية جامعة عجمان، العدد 01، المجلد 03، تاريخ النشر: 2024.

26)سعد فهد سعد ادبيس المطيري مفهوم الجرائم الإلكترونية وسماتها ، المجلة القانونية، جامعة القاهرة، مجلد 16، العدد 5.

27) بوفرحات نور الدين، عمري عبد القادر، تحديات كشف الهوية الإلكترونية للجناة بين أساليب التمويه والحواجز القانونية، مجلة الحقوق والحريات، المجلد 12، العدد 1، جامعة يحي فارس، المدية، 2024 .

5- المحاضرات

1) عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دار الهدى للنشر والطباعة وتوزيع،

2) أسامة غربي، المنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مكافحة الجريمة المنظمة، جامعة المدية.

6- مواقع الانترنت

1) https://www.unodc.org/romena/ar/press/2024/August/press-release_-united-nations_-member-states-finalize-a-new-cybercrime-convention.html اطلع عله يوم: 17-06-2025، الساعة 11.55.

2) (الجريمة السبيرانية) wiki.htts://ar.wikipedia.org، موسوعة حرة وكبيديا، اطلع عليه يوم: 2025/04/17، ساعة 12:30.

3) تاثير الجرائم الإلكترونية علي الاعمال)sprintzeal.com نشر في 31يوليو2023 تاريخ الاطلاع 19ماي 2025على الساعة 10.4

الفهرس

الفهرس:

الرقم	الموضوع	الصفحة
01	**الإهداء**	-
02	**شكر وتقدير**	-
03	مقدمة	1 - 2
04	**الفصل الأول : الإطار المفاهيمي للجريمة السبيرانية**	03
05	المبحث الأول: مفهوم الجريمة السبيرانية	04
06	المطلب الأول: النشاة ومراحل تطور الجريمة السبيرانية	04
07	الفرع الأول: مرحلة الخمسينيات من القرن الماضي	04
08	الفرع الثاني: مرحلة الستينات والسبعينات والثمانينات في القرن الماضي	05
09	الفرع الثالث: مرحلة التسعينات	05
10	المطلب الثاني: مفهوم الجريمة السبيرانية	06
11	الفرع الأول: **:** تعريف الجريمة السبيرانية	06
12	الفرع الثاني: خصائص الجرائم السبيرانية	09
13	الفرع الثالث: أنواع الجرائم السبيرانية	10
14	المطلب الثالث: أركان الجريمة السبيرانية	12
15	الفرع الاول**:** الركن الشرعي للجريمة السبيرانية	12

16	الفرع الثاني: الركن المادي للجريمة السبيرانية	14
17	الفرع الثالث: الركن المعنوي للجريمة السبيرانية	21
18	المبحث الثاني: آثار الجريمة السبيرانية	22
19	المطلب الأول :آثار الجريمة السبيرانية على حقوق الإنسان	22
20	الفرع الأول: **:** جرائم مواقع التواصل الاجتماعي وتهديداتها لكرامة الإنسان	23
21	الفرع الثاني: التعدي على حقوق الخصوصية	23
22	الفرع الثالث: انتهاكات حقوق الطفل	24
23	الفرع الرابع: تقييد الحقوق الرقمية وتطبيق نطاق التعبير	25
24	المطلب الثاني: آثار الجريمة السبيرانية على الدول	26
25	الفرع الأول: الآثار الاجتماعية	26
26	الفرع الثاني: **:** الاثار السياسية والأمنية	27
27	الفرع الثالث : آثار الاقتصادية	27
28	خلاصة الفصل	33
29	**الفصل الثاني: آليات مواجهة المجتمع الدولي للجريمة السيبرانية**	34
30	المبحث الأول: صور التعاون الدولي في مواجهة الجريمة السيبرانية	35
31	المطلب الأول: التعاون القانوني في مواجهة الجريمة السيبرانية	35
32	الفرع الأول: الجهود الدولية في مكافحة الجريمة السيبرانية	35
33	الفرع الثاني: الجهود الإقليمية في مكافحة الجريمة السيبرانية	42
34	المطلب الثاني: التعاون القضائي لمواجهة الجريمة السيبرانية	48

35	الفرع الأول: تبادل المعلومات	50
36	الفرع الثاني: نقل الإجراءات	51
37	الفرع الثالث: الإنابة القضائية	52
38	الفرع الرابع: التعاون الدولي لتسليم المجرمين لمواجهة الجرائم السبيرانية	53
39	المطلب الثالث: التعاون الأمني لمواجهة الجريمة السيبرانية	54
40	الفرع الأول: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)	55
41	الفرع الثاني: شرطة الويب الدولية	56
42	المبحث الثاني: التحديات وآفاق التعاون الدولي في مكافحة الجريمة السيبرانية	57
43	المطلب الأول: التحديات القانونية	57
44	الفرع الأول: القصور التشريعي للدول والتعارض بين مصالحها	57
45	الفرع الثاني: اختلاف النظم القانونية والإجراءات الجنائية	58
46	الفرع الثالث: تنازع الاختصاص القضائي الدولي	58
47	الفرع الرابع: التجريم المزدوج	58
48	المطلب الثاني: التحديات التقنية التي تواجه التعاون الدولي لمكافحة الجريمة السيبرانية	59
49	الفرع الأول: صعوبة تحديد هوية المجرمين	59
50	الفرع الثاني: صعوبة جمع الأدلة الرقمية	60
51	الفرع الثالث: عدم وجود قنوات الاتصال	61
52	الفرع الرابع: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب	61
53	**المطلب الثالث: سبل القضاء على التحديات التي تواجه الجهود الدولية في مكافحة الجرائم السيبرانية**	61

54	الفرع الاول : السبل المتعلقة بالمساعدات القضائية الدولية	62
55	الفرع الثاني: توحيد النظم القانونية والإجرائية	63
56	الفرع الثالث: حل صعوبة عدم وجود قنوات اتصال	64
57	الفرع الرابع: حل صعوبة الخاص في مجال التدريب	64
58	الفرع الخامس: حل صعوبة التزاحم في طلبات التسليم	65
59	**خلاصة الفصل**	67
60	**الخاتمة**	68
61	**قائمة المصادر والمراجع**	70
62	**فهرس الموضوعات**	75