وزارة التعليم العالي والبحث العلمي

جامعة مولود معمري –تيزي وزو

كلية الحقوق والعلوم السياسية

الإطار القانوني الدولي و الأوروبي للعنف السيبيراني

مذكرة تخرج لنيل شهادة الماستر في الحقوق

تخصص:القانون الدولي العام

إعداد الطالب **إشراف**

– لزوم علال – د. مومو نادية

أعضاء لجنة المناقشة

الأستاذ: دخلافي صفيان، أستاذ التعليم العالي، جامعة مولود معمري، تيزي وزو.....رئيسا.

الأستاذة: مومو نادية، أستاذ محاضرة (أ)، جامعة مولود معمري، تيزي وزو..مشرفة ومقررة.

الأستاذة: دراني ليندة، أستاذة محاضرة (أ)، جامعة مولود معمري، تيزي وزو.....مقررة.

السنة الجامعية 2025/2024

إهداء

أهدي هذا العمل المتواضع إلى عائلتي الكبيرة ، الوالدين الكريمين ، إخوتي وأخواتي .

إلى عائلتي الصغيرة ، زوجتي وولدي انس وريان .

إلى زملائي في الدراسة .

إلى كل شخص ساعدني من بعيد أو من قريب في انجاز هذه المذكرة .

أهدي هذا العمل

علال

شكر
وعرفان

أتقدم بجزيل الشكر والعرفان والتقدير للأستاذة المشرفة

الأستاذةمومو نادية

التي قبلت الإشراف على هذا العمل ، والتي كانت لي نعم الموجه والمشرف طيلة فترة انجاز هذه المذكرة ، والتي لم تبخل علي بنصائحها وتوجيهاتها المثمرة.

كماأشكر الأساتذة الكرام اللذين سيتفضلون بمناقشة هذه المذكرة .

مقدمة

مقدمة:

يشهد العالم اليوم تطورا تكنولوجيا متسارعًا بفضل الثورة المعلوماتية التي أعقبت الثورة الصناعية،مما دفع الإنسان إلىالاعتماد المتزايد على التقنيات الحديثة واستعمالها في مختلف مجالات العمل والحياة ، ونتيجة لهذا التحول، أصبح العالم عبارة عن قرية صغيرة تتواصل بين مجتمعاتها دون قيود جغرافية أو زمنية، مما أدى إلى تحقيق نقلة حضارية نوعية مست كل القطاعات ووفر خدمات جليلة للأمم والشعوب.

إلا أن هذا الجانب الايجابي للتطور التكنولوجي المعلوماتي أفرز معه بعض الانعكاسات السلبية التي نتجت عن إساءةإستخدام الأنظمة المعلوماتية، وإستغلالها بطريقة غير شرعية بغرض الإضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط وصور مستحدثة من أعمال العنف تحت تسمية أعمال العنف السيبيراني.

وعليه أدى التطور التكنولوجي الهائل وخاصة في مجال الإتصالاتإلى تطور أعمال العنف التقليدية بوجه عام وظهور أنماط جديدة على المستوى الدولي والإقليمي لاسيما الأوروبي منه، فزادت معاناة العالم من أعمال العنف، وفي ظل ثورة المعلومات والمعرفة الإلكترونية، وتطور وسائل الإتصال التقني والرقمي الحديث استفاد الأشخاص المرتكبون للعنف من مكاسب هذه الثورة والمعرفة التقنية لتحقيق أهدافهم، حيث استغل هؤلاء الأشخاص شبكة الانترنت بمختلف مكوناتها في تمويل نشاطاتهم تحت غطاء ما يعرف بالعنف السيبيراني، أين أصبح الفضاء السيبيراني مسرحًا لمختلف صور العنف هدفها الإهانة، التشهير، والإحتقار والتعليقات التي تسعى إلى الشتم ونشر صور وفيديوهات جارحة ومخلة بالحياء بهدف التهديد والابتزاز.

وهذا كله أثار الجدل بشأن كيفية تحقيق التوازن بين ضمان الاستخدام الحر لشبكة الانترنت، وفي الوقت ذاته تجنب المخاطر الناتجة عن سوء إستخدامها أو بالأحرى كيفية

تنظيم التعامل مع هذه التقنية الجديدة، بحيث يمكن الاستفادة المثلى منها مع الحد من الظواهر السلبية المصاحبة له.

وقد ظهرت ظاهرة العنف السيبيراني في الستينيات إلى غاية سنة 1970، وهذا مع بداية شيوع استخدام الحاسوب، أين إقتضت معالجة المقالات، وتمثلت في التلاعب بالبيانات المخزنة وتدميرها، أما المرحلة الثانية فتمثلت في الثمانيات، أين ظهر مفهوم جديد للعنف السيبراني وجرائم الكمبيوتر والانترنت، تمثلت في اقتحام الأنظمة ونشر الفيروسات، أما المرحلة الثالثة فقد شهدت سنوات التسعينات تناميا هائلا في الجرائم السيبرانية، نظرًا لإنتشار الإنترنت في هذه الفترة، مما سهل ظهور سلوكيات غير مشروعة عبر الفضاء الرقمي أو السيبراني، ومن أجل ذلك سعت بعض الدول والمنظمات الدولية والإقليمية لإيجاد آليات قانونية وطرف من أجل مكافحة ومجابهة ظاهرة العنف السيبراني.

لقد كانت بداية استخدام شبكة الانترنت في مجالات بحثية وعسكرية بحتة، ثم تطورت إلى مجالات عديدة منها التجارية والثقافية والتواصلية وحتى الترفيهية، ولم يكن يعلم أحد من واضعي هذه الشبكة أنها سوف تستخدم في يوم ومن الأيام في ابتكار العديد من الأفعال غير المشروعة والجرائم، حيث أن المجرمين قاموا بنقل أعمالهم الغير مشروعة والإجرامية إلى هذا الفضاء الافتراضي، نظرا لما يقدمه من تسهيلات كعدم خضوعه إلى أي سلطة وتعديه للحدود الجغرافية للدول، وتميزه باللامادية وسهولة إخفاء الهوية والأفعال، أدى هذا الوضع بالمجتمع الدولي والدول على حد سواء إلى محاولة مواجهة هذا النوع المستحدث من الأفعال غير المشروعة، وذلك في بادئ الأمر عن طريق وضعها في نطاق النصوص القانونية القائمة،غيرأن هذه الوضعية لم تدم طويلاً نظرًا للسرعة في التطور الذي تعرفه هذه الجريمة، الأمر الذي أدىإلى ضرورة استحداث نصوص قانونية دولية وإقليمية منها الأوروبية خاصة بها، في إطار هذا التباين بين الرؤى بين الدول .

تتجلى أهمية هذا الموضوع في ارتباطه بحقوق الإنسان في البيئة الرقمية، كما أنه يمس بشكل مباشر بسيادة الدول وأمنها المعلوماتي ويطرح تحديات قانونية تتعلق بالاختصاص والتجريم، ومن هذا المنطلق جاء اختيار هذا الموضوع كونه يجمع بين الجوانب القانونية والتقنية ويستجيب لمتطلبات الساعة، في ظل تزايد الهجمات السيبيرانية ذات الطابع العنيف.

وبناءا على ذلك، تطرح الإشكالية المحورية التالية :

إلى أي مدى تعتبر الآليات الدولية والأوروبية المعتمدة حاليا فعالة في مواجهة العنف السيبراني؟

ومن أجل معالجة هذه الإشكالية، تم إعتماد المنهج الوصفي والتحليلي بالدرجة الأولى، من خلال معالجة الإطار النظري والمفاهيمي المتعلق بالعنف السيبراني من خلال الوقوف عند مختلف المفاهيم المختلفة المرتبطة بهذه الظاهرة، مع التطرق إلى الأسس العامة التي يقوم عليها التنظيم الدولي في هذا المجال، لاسيما تلك المستمدة من الاتفاقيات والمعايير الدولية ذات الصلة (الفصل الأول)، ثم يستكمل التحليل بإستعراض التجربة الأوروبية من حيث المنظومة القانونية المعتمدة لمكافحة أشكال العنف في الفضاء الرقمي، ومدى تكامله مع المنظومة القانونية الدولية، مع محاولة تقييم مدى فعاليتها في الحد من هذه الظاهرة وتوفير الحماية القانونية للأطراف المتضررة (الفصل الثاني).

الفصل الأول :

الإطار المفاهيمي للعنف السيبيراني

مع تطور العصر الرقمي وإنتشار تكنولوجيا المعلومات، شهد مفهوم العنف تحولا من الطابع التقليدي، الذي يتمثل في إلحاق الأذى المادي والمعنوي بالأفراد، إلى أشكال جديدة أكثر تعقيدا، أبرزها العنف السيبراني، ورغم تشابهه مع العنف التقليدي في طبيعته وأهدافه ، إلا أنه يختلف عنه من حيث الوسائل المستخدمة، إذ يعتمد على التقنيات الرقمية والوسائط الإلكترونية، فضلا عن صعوبة تحديد هوية الجاني أو موقعه الجغرافي، وقد إرتبط العنف السيبراني إرتباطا وثيقا بمفهوم الأمن السيبراني، الذي يسعى إلى حماية الأفراد والبيانات من التهديدات الرقمية، وبناءا على ذلك ، أصبح من الضروري دراسة الإطار المفاهيمي لهذه الظاهرة، حيث سيتم التطرق إلى مفهوم العنف السيبراني (المبحث الأول)، ثم تحليل ماهية الأمن السيبراني وذلك لفهم العلاقة بينهما وتحديد السبل الكفيلة للتصدي لهذه الظاهرة المتنامية (المبحث الثاني).

المبحث الأول: مفهوم العنف السيبراني

يعتبر العنف السيبراني أو الرقمي صورة من صور الجريمة الإلكترونية، إذ يعد المجرم فيه غير معروف لا في هويته الشخصية أو المكان الذي يمارس في إجرامه، وقد نتج عن الإستخدام الواسع لشبكة الانترنت وتنوع مستخدميها وأساليب التعاطي والإستعمال، ويرتبط العنف السيبراني بصفة عامة بالفضاء السيبراني الذي يقصد به ذلك المكان الذي أوجدته تكنولوجيا المعلومات والإتصالات وفي مقدمتها الأنترنت، ويرتبط الفضاء السيبراني ارتباطا وثيقا بالعالم المادي، عبر البنى التحتية لمختلف الإتصالات والأنظمة المعلوماتية وعبر العديد من الخدمات التي لم يكن بالإمكان الحصول عليه من دونه ،ولذلك يتعين علينا تحديد تعريف للعنف السيبراني (المطلب الأول)، مع تبيان خصائصه(المطلب الثاني).

المطلب الأول : تعريف العنف السيبراني

إتفق الفقهاء والعلماء على أن العنف يتخذ أشكالا متعددة، حيث ينقسم إلى عنف مادي ، مثل الضرب والإيذاء الجسدي، وعنف معنوي، كالإهانة والسب والتشهير، غير أن العنف السيبراني يختلف عن هذه الأشكال التقليدية، إذ يرتبط بإستخدام الوسائل الرقمية والتكنولوجية، مما يجعله يأخذ أبعادا جديدة تتجاوز المفاهيم التقليدية للعنف.

وفي هذا السياق، يمكن التمييز بين مفهومين أساسيين للعنف السيبراني، حيث يتجلى في بعده الضيق كعنف موجه ضد الأفراد (الفرع الأول) ، بينما يتسع نطاقه ليشمل الهجمات السيبرانية التي تستهدف الدول والبنى التحتية الحيوية (الفرع الثاني).

الفرع الأول : التعريف الضيق للعنف السيبراني

لكي نستطيع الوصول لجوهر البحث والمتمثل في العنف السيبراني، لابد لنا من تحديد المفاهيم ذات الصلة، وذلك حتى نتمكن من إدراجها ضمن سياق أفكار هذا البحث، لذا يستلزم أن نقف أمام مصطلح العنف السيبراني، والذي بدوره يتكون من مصطلحين العنف والسيبرانية، ومن ثم يجب تحديد مفهوم هذين المصطلحين من الناحية اللغوية والإصطلاحية.

أولا : العنف لغة

ورد مصطلح العنف في معجم لسان العرب على أنه الخرق بالأمر وقلة الرفق به،أي أنه ضد الرفق، ويقال "عنف به" بضم النون، وعليه "يعنف عنفا " "عانفه وأعنفه" بفتح النون وتشديدها وهو عنيف[1]، وقد حدد قاموس أكسفورد العنف أنه فعل إرادي متعمد بقصد إلحاق الضرر أو التلف أو تخريب الأشياء والممتلكات أو المنشات الخاصة أو العامة أهلية أو حكومية عن طري إستخدام القوة.[2]

ثانيا :العنف إصطلاحا

للعنف العديد من التعريفات الإصطلاحية نذكر منها :

يعرف العنف إصطلاحا على أنه مجموعة من السلوكيات التي تهدف إلحاق الأذى بالنفس، أو بالأخرين، ويأتي بشكلين إما بدني مثل الضرب، التشاجر، إتلاف الأشياء، والعنف اللفظي مثل التهديد، و يؤدي هذا العنف بطريقة مباشرة أو غير مباشرة إلحاق الأذى.[3]

(1) –أبو الفضل ابن منظور، لسان العرب، مجلد 9 ، دار صادر للطباعة والنشر، لبنان، 1956 ، ص257.

(2)– نبيل رمزي ،علم إجتماع المعرفة ، دراسة مقارنة الوعي والإيديولوجية، دار الفكر العربي، الإسكندرية ، 1991 ، ص74.

(3)– العربي بوعمامة، رقاد حليمة ،العنف في الفضاء السيبراني، منشورات ألفا للوثائق والنشر والتوزيع، الجزائر، 2023 ، ص05 .

وما يلاحظ على هذا التعريف أنهيشمل السلوكيات التي تهدف إلى إلحاق الأذى،وأنه كل سلوك يهدف إلى إلحاق الأذى بالأشخاص، كما يعرف انه ذلك السلوك الذي يلجأ إليه الأفراد أو بعضهم إتجاه آخرين بقصد إلحاق الأذى والضرر بهم ، سواء كان ماديا أو معنويا، كما أنه لغة العضلات، وهو تصرف ناتج عن غياب لغة الحوار الحضاري بين الطرفين، ويكون الهدف منه ممارسة العنف والإكراه والإرغام والإذلال والسيطرة.[1]

ومن بين التعريفات الأخرى للعنف، يمكن القول أنه هو إستخدام القوة المادية والمعنوية بغرض إرهابالأشخاص، لتحقيق مصالح مشروعة وغير مشروعة.[2]

1- الفضاء السيبراني

الفضاء السيبراني هو مجال إفتراضي من صنع الإنسان يقوم على إستخدام الحواسيب وشبكات الأنترنت وكم هائل من البيانات والمعلومات والأجهزة، بالإضافة إلى الأجهزة الرقمية، وقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام بأنه "فضاء للتواصل يتشكل من خلال الترابط العالمي بين معدات المعالجة الآلية للبيانات الرقمية"، ويركز هذا التعريف بشكل أساسي على البعد التقني، إلا أنه يغفل الجانب البشري، الذي يعد عنصرا جوهريا في تكوين الفضاء السيبراني.[3]

يمكن أيضا الاستناد إلى تعريف الاتحاد الدولي للإتصالات، الذي يصف الفضاء السيبراني بأنه"مجال يجمع بين الجوانب المادية وغير المادية، ويتشكل من عدة عناصر مترابطة، تشمل أجهزة الحاسوب، والشبكات، والبرمجيات، وحوسبة البيانات، والمحتوى

(1)–العربي بوعمامة، رقاد حليمة ، المرجع السابق، ص05.

(2)– العربي بوعمامة، رقاد حليمة ، المرجع نفسه ، ص 16.

(3)–إسماعيل زروقة، "الفضاء السيبيراني والتحول في مفاهيم القوة والصراع"، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 10، العدد1 ،الجزائر، 2019 ، ص 1020 .

الرقمي، بالإضافة إلى معطيات النقل والتحكم ، فضلا عن المستخدمين الذين يتفاعلون مع هذه العناصر ويوجهون إستخدامها.[1]

وعليه يمكننا القول،أن الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين أو مستعملين.

ثالثا : التعريف الفقهي للعنف السيبراني

لايوجد تعريف موحد أو متفق عليه عالميا للعنف السيبراني أو مايعرف باللغة الأجنبيةCyberviolence،والذي يشمل أيضا المضايقة الإلكترونية، ويعود هذا لغموض وتنوع التقنيات الحديثة وتعدد الأساليب المستخدمة في ممارسته، مما يجعل تحديده بدقة أمرا معقدا.[2]

وفي هذا السياق، وردت عدة تعريفات للعنف السيبراني نجد من بينها، أنه يمثل سلوكا عدائيا يمارس داخل الفضاء الإلكتروني، ويأخذ شكل التعدي اللفظي على الآخرين مثل السب، والشتم، والقذف، وهي ممارسات من شأنها المساس بكرامة الأفراد أو الجماعات، وإلحاق الأذى بهم نفسيا و إجتماعيا، وبالتالي ينظر إلى العنف الرقمي عل أنه أي تعبير لفظي سلبي يوجه عبر الوسائل الإلكترونية ويترك أثرا سلبيا على المتلقين.

إضافة إلى ذلك، يتمثل العنف السيبيراني في أشكال أخرى، مثل إنتهاك الخصوصية من خلال مواقع الأنترنت، أو نشر تسجيلات صوتية وصور إلتقطت بإستخدام كاميرات الهواتف

(1)-عادل عبد الصادق ، الفضاء الالكتروني في ضوء القانون الدولي ، سلسلة أوراق ، العدد 23 ، مكتبة الإسكندرية ، مصر، 2016 ، ص17 .

(02)-Kim Barker and Ola Juras,online Violence against women as an obstacle to Gender Equality a Crtical view from Europe,European Equality law Review,2020, .52p

المحولة، وكذا إستخدام مواقع الصحف الإلكترونية، ومنصات التواصل الإجتماعي للتشهير بالأشخاص والتعدي على سمعتهم، وبذلك يعتبر أي سلوك إلكتروني يستهدف الأفراد بكل مباشر أو غير مباشر ويؤدي إلى إنتهاك خصوصيتهم أو حرياتهم الشخصية، يعد شكلا من أشكال العنف السيبراني.[1]

ومن خلال هذه التعريفات، يمكن إستخلاص مجموعة من الخصائص التي تميز العنف السيبيراني ومنها :

-أنه يرتكب بإستخدام الوسائل التكنولوجية الحديثة .

-أنه يمارس عبر مختلف وسائل الإتصال، ولاسيما وسائل التواصل الإجتماعي.

-أن أضراره غالبا ما تكون نفسية وإجتماعية أكثر من كونها مادية.

-أنه يستهدف إختراق خصوصية الأفراد وإنتهاك حرياتهم الشخصية.

-أنه قد يتطور ليأخذ شكلا من أشكال التهديد والإبتزاز، خاصة إذا كان الغرض منه الحصول على أموال أو تحقيق مكاسب غير مشروعة.

وبناءا على ماسبق، يتضح أن العنف الممارس عبر الفضاء السيبيراني لا يقتصر فقط على الأذى النفسي والإجتماعي، بل يشمل تهديدا خطيرا للحريات الفردية، وقد أفرزت هذه الظاهرة العديد من المصطلحات المرتبطة بها مثل:العنف الرمزي، الإستغلال المعلوماتي، الفجوة الرقمية، تزييف العقول بعد الإمبريالية الرقمية، القمع الإيديولوجي،وإختلال الفضاء المعلوماتي.

وفي هذا الإطار، قدمت الأمم المتحدة تعريفا للعنف عبر الأنترنت، حيث وصفته بأنه " أي عمل عنيف يرتكب ضد الأفراد بمساعدة تكنولوجيا المعلومات والإتصالات، مثل "الهواتف الذكية، الأنترنت، منصات التواصل الإجتماعي، أو البريد الإلكتروني، مما يسهم

(1)-العربيي بوعمامة، رقاد حليمة، المرجع السابق ، ص17 .

في تفاقمه وإنتشاره، وبالتالي فإن العنف السيبراني يعد إنتهاكا صارخا لحقوق الإنسان، حيث يمس بحرية التعبير ويتعدى على الحقوق الأساسية التي تكفلها المواثيق والإتفاقيات الدولية.[1]

-مواقع التواصل الاجتماعي

يعتبر مصطلح مواقع التواصل الإجتماعي من المصطلحات المثيرة للجدل نظرا لتداخل الآراء والإتجاهات في دراسته، وقد عرف الباحثان ولونلي والسون" أن مواقع التواصل الإجتماعي بأنها صنف من المواقع تقدم خدمات تقوم على تكنولوجيا الويب،تتيح للأفراد التواصل في إيطار بناء متاح للعموم أو شبه متاح للعموم "، وقد عرفها الأستاذ زاهي رضا أنها "منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به ، ومن ثم ربطه به عن طريق نظام جماعي إلكتروني مع أعضاء آخرين لديهم الإهتمامات والهوايات نفسها.[2]

إذا فإن شبكات التواصل الاجتماعي هي عبارة عن مواقع على شبكة الانترنت، توفر لمستخدميها فرصة الحوار وتبادل الآراء و الأفكار من خلال الملفات الشخصية وغرف الدردشة والصور، وتتمثل هذه المواقع في الفايسبوك، التويتر،الأنستغرام، موقع الفيديو يوتيوب ، لنكدان، وغيرها من المواقع.

الفرع الثاني : التعريف الواسع للعنف السيبراني

لقد شهد مفهوم العنف السيبيراني تطورا ملحوظا فلم يعد يقتصر على الأفراد فحسب، بل إمتد ليشمل الدول والكيانات،مما أدى إلى ظهور ما يعرف اليوم بالهجمات السيبرانية أو

(1)-العربي بوعمامة، رقاد حليمة، المرجع نفسه ، ص 18 .

(2)-زاهي رضا، "إستخدام مواقع التواصل الاجتماعي في العالم العربي"، مجلة التربية ، جامعة عمان،العدد 15، 2003، عمان، ص 23 .

الإرهاب السيبيراني، ويقصد بهذا المفهوم الهجوم المنظم وغير العشوائي، والذي يكون بدوافع سياسية ويستهدف أنظمة المعلومات والبرمجيات والبيانات ، مما يشكل تهديدا مباشرا للبنى التحتية الحيوية ، وغالبا ما يكون لهذه الهجمات تأثيرا مدمرا ، إذ تقتصر على التهديد بالعنف، أو يؤدي إلى إحداث أضرارا فعلية على أرض الواقع.[1]

وفي هذا السياق، تعد الهجمات السبيرانية شكلا جديدا من التهديدات الأمنية التي تستهدف الدول، حيث إرتبط ظهورها بتطور إستخدام الفضاء السيبراني، الذي يمثل بيئة افتراضية تترابط فيها أجهزة الكومبيوتر عبر شبكات معقدة، ومع تزايد الاعتماد على هذه التقنيات، باتت العديد من القطاعات الحيوية معرضة لهذه الهجمات، بما في ذلك الشركات الخاصة، والإدارات العامة، أنظمه النقل الجوي، الطرق، والسكك الحديدية، محطات توليد الطاقة والمياه، فضلا عن الأسلحة الحديثة مثل الطائرات بدون طيار والصواريخ النووية، ويؤدي هذا الواقع إلى تعرض الدول لمخاطر جديدة ومتعددة الأوجه، ناتجة عن إستغلال الفضاء السيبراني كأداة هجومية فعالة.[2]

وبالنظر إلى طبيعة هذه التهديدات، يمكن وصف الهجمات المنسوبة بأنها عمليات تنفذها جهات حكومية أو جهات تدعمها الدول، وتستهدف شبكات الكومبيوتر الخاصة بدولة أخرى بهدف إلحاق أضرارا مادية أو غير مادية، تختلف في درجة خطورتها وفقا للأهداف المنشودة، ومن أبرز خصائص هذه الهجمات أنها تتميز بطابعها السري والتخفي، الأمر الذي يجعلها تتحدى المفاهيم التقليدية المتعلقة بالحدود الجغرافية، والقوة العسكرية، والتدخل

(1)–نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة والتوزيع ،الأردن، 2008 ، ص140 .

(2) – سفيان دخلافي، العدوان في القانون الدولي والهجمات السيبيرانية بين الدول، مجلة العلوم القانونية والسياسية جامعة تيزي وزو ، المجلد 14 ، العدد 2، ، الجزائر،2023 ، ص85 .

في شؤون الدول، فلم يعد من الضروري اللجوء إلى القوة العسكرية التقليدية ولإحداث أضرارا جسيمة في دولة ما[1].

ونتيجة لذلك، أصبح الفضاء السيبيراني ساحة جديدة للصراعات بين الدول، حيث أضحى يمثل بيئة خصبة للإشتباكات غير التقليدية، ولم يعد الأمن الوطني لأي دولة، مهما بلغت قوتها، في مأمن من تهديدات هذا الفضاء، مما يستدعي إستراتيجيات حديثة لمواجهة هذه المخاطر المتزايدة.

المطلب الثاني : خصائص العنف السيبراني

يتميز العنف السيبراني أو الرقمي بمجموعة من الخصائص التي تميزه عن العنف التقليدي، مما يمنحه طابعا فريدا من حيث التأثير والإنتشار، وفي هذا السياق، سنتناول الخصائص العامة لهذه الظاهرة (الفرع الأول)، بينما سنبحث في السمات والخصائص التي تميز مرتكبي العنف السيبراني، بهدف فهم سلوكهم، وآليات تنفيذهم لهذه الأفعال(الفرع الثاني).

الفرع الأول : الخصائص العامة للعنف السيبيراني

يتسم العنف السيبراني بعدد من الخصائص التي تميزه عن العنف التقليدي، ويمكن تلخيص هذه الخصائص في مايلي:

1- شدة وسرعة التنفيذ

يعتبر العنف السيبيراني أكثر قسوة من نظيره التقليدي، ويرجع ذلك إلى طبيعة الفضاء الإلكتروني الذي يتيح للمعتدي إخفاء هويته، مما يقلل من إحساسه بمسؤوليته الأخلاقية

(3)-دخلافي سفيان ، المرجع نفسه، ص88 .

إتجاه الضحية، حيث انه لايرى تأثير أفعاله بشكل مباشر، كما أن تحديد حجم الضرر الناجم عنه يكون أكثر صعوبة، نظرا لسرعة إنتشاره.[1]

إذ يكفي مثال "فيروس علة الحب " الذي اجتاح العالم في غضون ساعتين ليصل في الليلة الأولى من إطلاقه إلى عشرات الآلاف من المستخدمين، هو ما وصفته قناة ABC TVبأنه"موجة إنتشار للجريمة بسرعة فائقة "، هذه الطبيعة المتسارعة للعنف السيبراني تفرض تحديات أمنية كبيرة، وتؤكد وجود فروق جوهرية بينه وبين العنف التقليدي، مما يجعل النصوص القانونية التقليدية غير كافية لمكافحته.[2]

2- إخفاء الهوية وصعوبة التتبع

يوفر الفضاء السيبيراني للمعتدين قدرة غير مسبوقة على إخفاء هوياتهم أو تمويهها، على عكس العالم الواقعي، حيث يمكن التعرف على الأشخاص من خلال ملامحهم أو صفاتهم الجسدية ، في المقابل يمكن للجاني في الفضاء الرقمي أن ينتحل شخصية مختلفة تماما، كرجل يظهر بهيئة إمرأة، أو طفل يتظاهر انه بالغ، أو حتى أجنبي يدعي انه مواطن محلي، هذه القدرة على التمويه تجعل من الصعب تعقب الجناة، خاصة مع إمكانية محو الأدلة الرقمية بسرعة فائقة، مما يزيد من تعقيد عملية إثبات الجريمة وملاحقة مرتكبيها.[3]

3 –الطابع العابر للحدود

يتميز العنف السيبيراني بأنه عالمي بطبيعته، غير مقيد بحدود جغرافية أو زمنية إذ يمكن إرتكاب الأفعال العدائية في أي وقت ومن أي مكان دون الحاجة إلى التواجد الفعلي في موقع الجريمة.[4]

---

(1)-Willard ,Nancy,Meducator's guide to Cyber bulling and Cyberthereats, Center for Safe and responsible Use of the internet,2007 , page 7-8

(2)-عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، شبكة الانترنت وشبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية: دراسة قانونية مقارنة، دارالثقافة للنشر والتوزيع ، الأردن، 2011 ، ص185

(2)-عادل عزام سقف الحيط ، المرجع السابق، ص 185 .

(4)-المكاوي محمد محمود، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت) ، المكتبة العصرية للنشر والتوزيع .، المنصورة ، مصر ، 2015 ، ص 34 .

ويظهر ذلك جليا، في القضية المشهورة المتعلقة "بفيروس الإيدز"، التي سلطت الضوء على البعد الدولي للعنف السيبراني، حيث تميزت هذه القضية بأمرين أساسيين هما :

-أنها شهدت لأول مرة تسليم متهم في جريمة معلوماتية .

-أنها كانت أول محاكمة لشخص متهم بإنشاء فيروس إلكتروني .

نظرا لهذه الطبيعة العابرة للحدود، أصبح التعاون الدولي أمرا ضروريا لمكافحة العنف السيبراني، وذلك من خلال إبرام المعاهدات والاتفاقيات الدولية لتعزيز التنسيق بين الدول[1]، ورغم ما يطرحه ذلك من تحديات قانونية وإدارية، أبرزها تحديد الولاية القضائية والقانون الواجب التطبيق خصوصا في الحالات التي يقع فيها السلوك الإجرامي في قارة ، بينما تمتد تأثيراته إلى قارة أخرى .

4 -التطور المستمر

يتطور العنف السيبراني بإستمرار مع تقدم التكنولوجيا، حيث تزداد أساليبه تعقيدا وخطورة مع مرور الوقت، كما أنتأثيره غالبا ما يكون طويل الأمد، خاصة في حالات السب والقذف والتشهير والقذف والتشهير، حيث تظل آثار هذه الجرائم إلى أن يتم التدخل التقني لإزالتها، وهذا التطور المستمر يجعل مكافحته أكثر تعقيدا، ويتطلب آليات قانونية وتقنية متجددة لمواجهته.[2]

5-سهولة الارتكاب وصعوبة الإثبات

يرتكب الجناة العنف السيبراني بإستخدام تقنيات متطورة ووسائل معقدة، غالبا في بضع ثواني معدودة، مما يجعل من الصعب تتبعهم أو ضبطهم، كما يسهل محو الأدلة الرقمية أو

(1)-سليمان أبو نمر، يوسف بوكشريدة ، مكافحة الجريمة المعلوماتية في اطار القانون الدولي، مذكرة ماستر، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، 2020 ، ص 8.

(2)-الرشيدي محمود كامل، العنف في جرائم الأنترنت أهم القضايا، الحماية والتأمين، الدار اللبنانية، القاهرة ، 2011 ، ص 38 .

التلاعب بها، وهو ما يزيد من تعقيد من تعقيد عملية الإثبات أمام القضاء[1]، وتكمن صعوبة إثباته إلى أن متابعته وإكتشافه عن طريق الصدفة، ومن الصعوبة حصره في مكان معين، حيث أنها لا يترك آثارا واضحة للعيان أو يشاهد بالعين المجردة، وإن وجدت تحتاج لخبرة فنية يصعب على المحقق التقليدي معها، خصوصا في الدول التي لا تزال قوانينها غير مهيأة للإعتراف بالأدلة الرقمية، وعلى عكس الجرائم التقليدية التي تترك آثارا مادية واضحة يمكن الإستدلال بها، فإن العنف السيبراني يعتمد على بيانات إلكترونية مجردة، تتطلب خبرات تقنية متخصصة لإكتشافها.[2]

6- سهولة التنفيذ مقارنة بالجرائم التقليدية

لا يتطلب العنف السيبيراني أي مجهود بدني، مما يجعله أكثر سهولة في التنفيذ مقارنة بالجرائم التقليدية، إذ يكفي أن يمتلك الجاني بمهارات تقنية متقدمة، ليتمكن من إختراق الأنظمة أو نشر الفيروسات أو تنفيذ هجمات الكترونية ذات تأثير واسع.

كما أن الدوافع وراء هذه الجرائم تختلف، فقد يكون بعضها ماليا نتيجة البطالة أو الحاجة إلى كسب غير مشروع ، وقد تكون إيديولوجية أو سياسية أو حتى بهدف التجسس وإنتهاك الخصوصية. [3]

7-خطورة التأثير على الأفراد والدول

تتسم الجرائم السيبرانية بخطورتها العالية، حيث يمكن أن تؤثر بشكل مباشر على حياة الأفراد وخصوصيتهم، كما قد تستهدف المؤسسات الاقتصادية والأمن القومي للدول، فقد يؤدي إختراق الأنظمة المصرفية إلى خسائر مالية ضخمة، بينما قد يشكل الهجوم على

(3)- الرشيدي محمود كمال، المرجع السابق، ص 40.

(2)- قطاف سليمان، بوقرين عبد الحليم، "مواجهة الجرائم السيبيرانية في ضوء الإتفاقيات الدولية" ، مجلة البحوث القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، جامعة ثليجي عمار الأغواط ، العدد 4 ،الجزائر، 2022، ص 70.

(3)- روان بنت عطية الله، "الجرائم السيبيرانية"، المجلة الإلكترونية الشاملة متعددة الإختصاصات، العدد 24، المملكة العربية السعودية، 2020 ،ص 20 .

البنية التحتية للدولة تهديدا لأمنها وإستقرارها، وبالتالي، فإن العنف السيبراني يمثل تحديا عالميا يتطلب إستراتيجيات شاملة لمواجهته والحد من تداعياته.[1]

الفرع الثاني : صفات مرتكبي أفعال العنف السيبراني

لا يوجد إتفاق عام حول السمات والخصائص التي تميز مرتكبي العنف السيبراني ،إذ لا يمكن حصرهم ضمن فئة محددة أو وضع قالب ثابت يحدد ملامحهم، ومع ذلك، توصلت الدراسات المتخصصة إلى وجود بعض الصفات المشتركة بين الأفراد الذين تم التحقيق معهم وإدانتهم في مثل هذه الجرائم، فقد أشارت عدة أبحاث من بينها دراسة جون (2008) ودراسة بيكر (2009)، بالإضافة إلى بعض الدراسات العربية، إلاأن الفئة العمرية الغالبة لمرتكبي العنف السيبراني تتراوح بين 14 و38 عاما ، وهذا يعكس أن معظم هؤلاء ينتمون إلى فئة الشباب[2].

وعليه، فإن مرتكبي العنف السيبراني يتميزون بسمات تميزهم عن مرتكبي الجرائم التقليدية ، وتتمثل أبرز هذه الخصائص فيما يلي :

أولا : شخص يتسم بالمهارة والذكاء

يتميز الشخص مرتكب العنف السيبراني غالبا بالذكاء، حيث يستخدم قدرته العقلية ولا يلجا إلى استخدام العنف بل يحقق هدفه الإجرامي بهدوء، فالعنف السيبراني هو فعل الأذكياء بالمقارنة مع أفعال الإجرام التقليدي الذي يميل إلى العنف.[3]

(1)– صغير يوسف ، "جرائم الانترنت جرائم حقيقية في عالم إفتراضي"، مجلة المعارف،المجلد 11، العدد 2، جامعة البويرة ،الجزائر، 2022 ، ص230.

(2)–منصور بن صالح الجهني، "الجرائم المعلوماتية أنواعها وصفات مرتكبيها"، مداخلة ملقاة في المؤتمر الدولي الرابع للعلوم الإجتماعية ، كلية العلوم الاجتماعية ، جامعة الكويت، الكويت ، 2010 ، ص05.

(3)–صغير يوسف ، المرجع السابق ، ص 222 .

ثانيا :العود في إرتكاب فعل العنف

يتسم مرتكب العنف السيبراني بتكرار أفعاله،حيث يستغل مهاراته التقنية فهو تشغيل الحواسيب وإدارة البيانات والمعلومات والتحكم في أنظمة الشبكات للوصول غير المصرح به مرارا وتكرار، فهدفه لا يقتصر فقط على تنفيذ عملية الإختراق، وإنما ينبع من إحساسه بقدرته الفائقة على التسلل والإختراق، مما يدفعه إلى تكرار هذا السلوك لإثبات مهاراته وتعزيز شعوره بالتحكم والتفوق التقني.[1]

ثالثا : شخص له دوافع

تعد دوافع إرتكاب العنف السيبيراني من قبل الأفراد معقدة وصعبة الفهم ، حيث غالبا ما يكون الإحباط عاملا رئيسيا وراء ضعف التزامهم بأمن المعلومات، ويؤكد خبراء علم النفس وعلم الإجرام بأنه وضع تصنيف ثابت لهذه الدوافع يعد أمرا بالغ الصعوبة، نظرا لتعقيدها وتغيرها المستمر، ومع ظلك تشير الدراسات إلى أن الدوافع الشائعة وراء هذه الأفعال تشمل الرغبة في الإنتقام من صاحب العمل،أو تحدي الأنظمة والرغبة في التفوق أو حتى التعاون والتواطؤ مع جهات أخرى.[2]

المطلب الثالث : أنواع العنف السيبيراني

مع إنتقال مظاهر العنف التقليدي إلى الفضاء الرقمي، برزت أشكال جديدة من السلوك العدواني، اتسمت بقدر أكبر من التعقيد والتأثير المباشر على الضحايا، وقد تنوعت هذه الأشكال وفقًا لوسائل التنفيذ وأهداف المعتدين، مما أدى إلى بروز أنواع مختلفة من العنف السيبراني، ومن بين هذه الأنواع، نجد التنمر الإلكتروني، الذي يقوم على توجيه الإهانات،

(1)– علاء الرواشدة ، أسماء ربحي ، الجريمة في ظل العولمة ، دراسة تحليلية للبنية وسياسات المواجهة ، مجلة الحقيقة للعلوم الاجتماعية والانسانية ، جامعة ادرار، مجلد 18 ، عدد 2 ،الجزائر، 2019 ، ص 223 .

(2)–كوثر مازوني، الجريمة المعلوماتية، أعمال ندوة وطنية ،دارالخلدونية، الجزائر،2019، ص136.

والتحقير، والتشهير العلني ضد الأفراد عبر الوسائط الرقمية (الفرع الأول)، كما تندرج ضمن هذا الإطار الهجمات السيبرانية الخطيرة، التي تستهدف المعلومات الشخصية أو الحسابات الرقمية للضحية(الفرع الثاني)، بالإضافة إلى ذلك، تظهر الجرائم الجنسية الإلكترونية كأحد أخطر أشكال العنف السيبراني وما يترتب عنها من أضرار نفسية واجتماعية جسيمة (الفرع الثاني).

الفرع الأول : التنمر الإلكتروني

يهدف هذا الفرع إلى تعميق الفهم القانوني والإجتماعي لظاهرة التنمر الإلكتروني، وذلك من خلال تسليط الضوء على أبعاده المفاهيمية وتحليل خصائصه المميزة مقارنةً بباقي صور العنف السيبراني، سنبدأ بتحديد تعريف واضح ودقيق لهذا السلوك (أولًا)، ثم ننتقل إلى إستعراض أبرز أنواعه وصوره (ثانيًا)، وسنُرفق هذا العرض بتحليل واقعي مدعوم بأمثلة تطبيقية، تُظهر مدى خطورة هذه الممارسات على الضحايا.

أولا :تعريفه

تزامن ظهور التنمر الإلكتروني مع التطور السريع في وسائل الإتصال الرقمي وإنتشار الشبكات الإلكترونية والإفتراضية، التي حوّلت الفضاء السيبراني من مجرد شبكة لنقل المعلومات والأرقام إلى بيئة ديناميكية للتفاعل والعلاقات الإجتماعية، هذا التحول ساهم في تقليص الرقابة الأسرية والمجتمعية تدريجيًا، مما أتاح للأفراد هامشًا واسعًا من الخصوصية والحرية في إستخدام هذه الوسائط، وفي هذا السياق، برز التنمر الإلكتروني كأحد أبرز التحديات النفسية والسلوكية في البيئة الرقمية.[1]

(1)–العربي بوعمامة، رقاد حليمة، المرجع السابق، ص30.

ويُعرف هذا النوع من السلوك بأنه "مضايقات أو تحرشات تتم عن بُعد، بإستخدام وسائل الإتصال الحديثة، من قبل شخص يُطلق عليه المتنمر، بهدف خلق مناخ نفسي للضحية يتسم بالخوف والقلق والإضطراب"، ويستند المتنمر في تصرفه إلى إستغلال قوة أو سلطة رمزية يمتلكها، ليمارس سلوكًا عدوانيًا متكررًا تجاه شخص أقل قوة، مستخدمًا منصات مثل فيسبوك، وتويتر، وتطبيقات الألعاب الإلكترونية، وغيرها.[1]

وتعتبر فئة الأطفال من الفئات الأكثر هشاشة وعرضة للتنمر الإلكتروني، وذلك لعدة أسباب مترابطة، أولًا، يتميز الأطفال بقابلية عالية للخداع، نظرًا لصغر سنهم وقلة خبرتهم في التفاعل مع الآخرين، مما يجعلهم عاجزين في كثير من الأحيان عن التمييز بين السلوك العادي والسلوك المؤذي، ثانيًا، تعاني فئة واسعة من الأطفال من عزلة إجتماعية نسبية، إلى جانب ضعف الوعي بسبل مواجهة هذه الظاهرة، وهو ما يزيد من قابليتهم للتأثر بها، ثالثًا، يؤدي ضعف تقدير الذات وغياب المهارات الاتصالية الأساسية إلى الحدّ من قدرتهم على فهم ذواتهم والتفاعل الآمن مع المحيط الخارجي خارج نطاق الأسرة.[2]

ومع التحولات التي عرفتها الأسرة المعاصرة، أصبح الطفل يمتلك بسهولة وسائل الإتصال الحديثة ويستخدم شبكات التواصل الإجتماعي دون رقابة مباشرة، ما يعرّضه لمخاطر متعددة في بيئة إفتراضية مفتوحة، في هذا السياق، يُستغل حضور الطفل الرقمي لتوجيه سلوكيات تنمرية تعتمد على تقنيات حديثة وأدوات متنوعة، تشمل الكلمات المسيئة، الصور المهينة، أو نشر معلومات خاصة، مما يرسّخ الأذى النفسي ويُعمّق من آثار العنف السيبراني عليه.[3]

(1)–عباس سعيدة ، التنمر الإلكتروني ، ماهيته وأسبابه وآليات حماية أبنائنا منه ، مجلة الربئة ،جامعة باتنة 01 ،العدد1 الجزائر،2020 ، ص13 .

(2)–حسين محمود هتيمي ، العلاقات العامة وشبكات التواصل الإجتماعي ، دار أسامة للنشر، الأردن،2015 ، ص50 .

(3)–عباس سعيدة ، المرجع نفسه، ص14.

ويتم التنمر الإلكتروني حسب الباحث "سميث وآخرون "، بعدة أساليب تكنولوجية وهي : المكالمات الهاتفية، التي تحمل ألفاظ السب والشتم والقذف والتهديد، والرسائل النصية والصور ومقاطع الفيديو، والبريد الإلكتروني، أين يرسل المتنمر رسائل إلكترونية للضحية بمجرد فتحها من طرف الأخير يستولي المتنمر على البريد الإلكتروني، وكذا غرف الدردشة عبر الويب، أين يقوم المتنمر الإتصال عبر غرف الدردشة ليكون على إتصال مباشر مع ضحيته، وذلك بحسابات مزيفة ووهمية، يستطيع من خلالها قرصنة الحساب ونشر الصور في مواقع إباحية.[1]

ثانيا :أنواع التنمر الإلكتروني

يتخذ التنمر الإلكتروني عدة أشكال وأنواع ، ويمكن ذكرها كما يلي :

1 -الهجاء الإلكتروني

ويكون في التنابز بالألقاب والتجاوزات اللفظية التي يتراشقها مستخدمو منصات التواصل في المنشورات وقسم التعليقات، ولا يخرج هذا الهجاء من نوعه عن تمجيد العنصرية والتحدث بإسم الكراهية والتقليل من الآخر ودحض مشاعره، ناهيك عن ألفاظ التحرش المؤذية الضاربة بالأخلاق والمجتمع عرض الحائط والتي يطلقها البعض على صور الآخرين ومشاركاتهم في مثل هذه المواقع.[2]

2- تنمر صناع المحتوى

لا شيء أكثر وطأة على نفسية المستهدف من أن يستهزأ به أو يتنمر عليه شخص ذو شهرة إلكترونية مهيب كمؤثر ما أو صانع محتوى يبلغ عدد متابعيه ما يماثل عدد سكان مدينة بأكملها، ويعدّ هذا النوع أسهل أنواع التنمر في نشر العنصرية والكراهية وما يتبعهما

(1)-نهلا عبد القادر المومني، المرجع نفسه ، ص 153.

(2)-علي حسن الطوالبة، الجرائم الإلكترونية، جامعة العلوم التطبيقية ،سلسلة الكتب القانونية،البحرين ،2008 ، ص236

من الأذى النفسي والوصمة الإجتماعية التدميرية والتي قد يتسبب بهما المؤثر إن لم يكن مسؤولًا ومدركًا لعمق أثر أقواله وأفعاله.[1]

3-التنمر الجماعي(النبذ الإلكتروني)

وهو غالبًا ما يكون نتيجة للنوع الذي يسبقه، حيث يُنبَذُ المستهدف إجتماعيًا في العالم الإلكتروني الموازي للعالم الواقعي بعد حملات إلكترونية نالت من سمعته ونجحت في تحقيره ونبذه من مجتمعه، أوعندما يتعمد مجتمع أو مجموعة ما ترك المستهدف خارج نطاق دائرتهم، كطرده من أنشطة الأنترنت أو مواقع اللعب وغيرها.[2]

4-التجسس

ويكون هذا الفعل المشين أسهل إرتكابًا في العالم الرقمي منه على أرض الواقع، وذلك عبر برامج وتطبيقات رقمية تم تصميمها خصّيصًا للتلصص على خصوصيات الآخرين وهتكها ومن ثم القيام بإبتزازهم أو التشهير بهم وإضرار حياتهم العائلية والعملية والإجتماعية بأكملها.

5-الملاحقة الإلكترونية

يتمثل هذا النوع من التنمر في الرسائل المزعزعة التي يتلقاها المستهدف باستمرار من المتنمر بهدف تهديده ومضايقته أو تخويفه وهو ما يجعل المستهدف خائفًا على سلامته ويعيش في هلع وقلق دائمين.[3]

ثالثا: أمثلة عن التنمر الإلكتروني

يصعبٌ غالبًا تحديد واكتشاف التنمر الإلكتروني، وذلك بسبب خفائه وتستّره خلف قناع المزاح وألوان السخرية الطريفة، لكن لابدّ من أن نكون أكثر وعيًا وتيقّظًا لنتمكّن من التعرّف على هذا النوع من التنمّر في مراحله الأولى.

(1)-العربي بوعمامة ، رقاد حليمة ، المرجع السابق، ص 20.

(2)-علي حسن الطوالبة، المرجع السابق ، ص236 .

(3)-علي حسن الطوالبة، المرجع نفسه ،ص238 .

وفيما يلي بعض من أمثلة التنمّر الإلكتروني الأكثر شيوعًا:

1. ترك تعليقات مؤذية أو ساخرة على الأنترنت ونشر إشاعات في مختلف المنصات لإحراج الشخص المستهدف وتحقيره والتقليل من شأنه.
2. التهديد والوعيد بالإيذاء أو حتى مجرد كتابة كلمات غير مسؤولة ومؤذية كهذه:" فلتقتل نفسك، ألقي بنفسك من حافة جرف، اذهب ومُت".
3. القيام بنشر أو تصميم مقاطع فيديو أو صور أو ردات فعل تؤذي المستهدف وتربط به النكتة للأبد.
4. تزييف الهوية الحقيقة لصاحب حساب موقع التواصل، وذلك بهدف التجسس واستقصاء معلومات المستهدف الخاصة أو تشويه سمعته بتزييفها ونشرها كإشاعات تضرّ به.
5. نشر تعليقات وصور كارهة، أو نكات عنصرية تمسّ الصفات الشخصية، وذلك كالتهكّم على أعلام ترمز لجنسيات مختلفة أو أديان أو بلدان أو أعراق.[1]
6. خلق صفحة معينة كمدونة أو ما شابه وتسخيرها لإيذاء أحدهم، وتتبع زلّاتهم أو تسليط الضوء على عيوبهم الظاهرة منها والخفية، حقيقة كانت أو مزيفة.[2]
7. إسقاط الوثائق أو ما يعرف بالـ (doxing)، ويكون ذلك عن طريق نشر جزء من معلومات شخصية كصورة الهوية الشخصية، أوعنوان المنزل، أو رقم الهاتف، أو الضمان الإجتماعي، أو البطاقة المصرفية، أو روابط الحسابات الشخصية على مواقع التواصل الإجتماعي وما شابه؛ وذلك بدافع الإنتقام والإيذاء حيث تُخترق خصوصية المستهدف وتستباح للعامة.[3]

(1)–مريم ناريمان نومار، إستخدام مواقع الشبكات الإجتماعية وأثره على العلاقات الإجتماعية، مذكرة ماجستير ،كلية علوم الإتصال والإعلام ، جامعة باتنة ، 2012 ، ص12 .

(2)–حسين محمود هتيمي ، المرجع السابق ، ص56 .

(3)–عباس سعيدة ، المرجع السابق ، ص 14.

الفرع الثاني :الهجمات الإلكترونية ذات الطابع العنيف

تعتبر الهجمات الإليكترونية أحد أخطر أشكال العنف في الفضاء الرقمي، لما لها من آثار مباشرة على الأفراد والمؤسسات على حدّ سواء، سنسعى من خلال هذا الفرع إلى تقديم تعريف دقيق لهذا النوع من الهجمات، مع تحليل أهم أشكالها وأنماطها الأكثر شيوعًا، بهدف توضيح الكيفية التي تُرتكب بها هذه الأفعال، والوسائل التقنية التي تُستعمل فيها، وإنعكاساتها القانونية و الإجتماعية.

أولا : تعريفها

لقد أصبح الفضاء السيبراني عنصرا في النظام الدولي المعاصر نظرا لما يحمله من أدوات تكنولوجية متطورة ، حيث كشف عن محاور جديدة للصراع الدولي وأضاف مستويات كثيرة من التعقيد للعمليات العسكرية ، وبات أكثر تأثيرا في الحسابات الإستراتيجية للدول.

وأغلب التعاريف التي وردت بشان الهجمات السيبرانية تشترك في مصطلح واحد متقارب، وهو استهداف مواقع إلكترونية من خلال وسائل إتصال إلكترونية أخرى.[1]

وإن كان المختصون في القانون الدولي العام يقرون بأن المصطلح يكتنفه الغموض واللبس،بسبب عدم الإتفاق على تعريف محدد له،فمنهم من تبنى مصطلح الفضاء السيبيراني بالإستناد إلى المحيط الذي تجري فيه الإعتداءات السيبرانية، ومنهم من تبنى مصطلح الحرب السيبرانية إستنادا إلى إيديولوجية أمنية أوعسكرية ضد العدو المفترض، بينما فضل البعض الأخر مصطلح الهجمات السيبرانية لأن مصطلح الحرب هو مصطلح غير محدد في وقتنا الراهن على مستوى التنظيم القانونية الدولي، فبذلك فمصطلح الهجمات السيبيرانية

(1)–أحمد عيسى الفتلاوي، "الهجمات السيبيرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق المحلي للعلوم القانونية والسياسية ، كلية القانون، جامعة بابل ،العدد 4 ،العراق، 2016، ص 613 .

أكثر دقة ودلالة ومعنى، لأنه يتماشى مع مقتضيات القانون الدولي المعاصر، فهي تعرف أنها "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية لتعطيلها أو تدميرها أو الإضرار بها.[1]

وقد عرفت القيادة الإستراتيجية الأمريكية الهجمات الإلكترونية بأنها "تطويع عمليات نظام الكومبيوتر بهدف منع الخصوم من الإستخدام الفعال لها، فضلا عن التسلل إلىأنظمة المعلومات وشبكات الإتصال، بهدف جمع وحيازة وتحليل البيانات التي تحتويها "، وهذا التعريف يتماشى مع ما جاءت به إتفاقية بودابست لسنة 2001 المتعلقة بالجريمة السيبرانية التي جرمت إعاقة أو عرقلة الإستخدام الشرعي لنظام المعلومات عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات الكومبيوتر.[2]

وقد تطرقت إتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية الصادرة بتاريخ ديسمبر 2024، إلى تجريم إتلاف بيانات إلكترونية أو حذفها أوإفسادها أو تزويرها أو إخفائها عمدا بدون وجه حق، وان كل دولة طرف ملزمة باتخاذ تدابير تشريعية من أجل تجريم قانونها الداخلي كل إعاقة خطيرة لعمل نظام تكنولوجيا معلومات واتصالات عن طريق إدخال بيانات الكرتونية أو إرسالها أو إتلافها أو إفسادها أو تحويرها أو إخفائها.[3]

ثانيا : صور الهجمات الإلكترونية

تتعدد صور وأشكال الهجمات السيبرانية ذات الطابع العنيف التي يتم فيها إستخدام الأسلحة الإلكترونية كالتجسس وتسريب المعلومات و إختطافها، والتسلل إلى أنظمه البيانات

(1)– حمد عيسى الفتلاوي ، المرجع السابق ، ص 614 .

(2)–المادة 05 من إتفاقية بودابست لسنة 2001 .

(3)–حسين بن أحمد الشهري، "الإرهاب الالكتروني،حرب الشبكات "، المجلة العربية الدولية للمعلوماتية، السعودية، 2015 ، ص 35.

الحكومية، ويمكن تصنيف الهجمات السيبرانية في سياق هذا البحث إلى صنفين هما : الحرب السيبرانية و الإرهاب السيبراني.[1]

1-الحرب السيبرانية

لم يُجمع الباحثون والمتخصصون في المجال الأكاديمي على تعريف موحّد لمفهوم "الحرب السيبرانية"، نظرًا لتعدد زوايا النظر إلى هذا المصطلح وتعقيد طبيعته، ومع ذلك، حاول بعض المفكرين تقديم تعريفات تقريبية له. من بين هؤلاء، نجد "ريتشارد كلارك" و"روبرت كناكي"، اللذين عرفا الحرب السيبرانية بأنها: "أعمال تنفذها دولة بهدف اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى لإحداث أضرار جسيمة أو تعطيلها".[2]

من جهة أخرى، يرى عدد من خبراء حلف الناتو أن الحرب السيبرانية تشمل "جميع العمليات السيبرانية، سواء كانت دفاعية أو هجومية، والتي قد تُفضي إلى إصابات بشرية، أو وفيات، أو أضرار مادية أو تلف"، ورغم أهمية هذا الطرح، إلا أنه يُؤخذ عليه إغفاله للجانب النفسي والعنصر البشري، ما يجعله قاصرًا عن الإحاطة الكاملة بأشكال الصراع السيبراني. كما لا يمكّن هذا التعريف من التمييز بدقة بين الحرب السيبرانية وحرب المعلومات، أو بين هذه الأخيرة وأشكال الجريمة السيبرانية والإرهاب السيبراني.[3]

إنطلاقًا مما سبق، يمكن إعتبار الحرب السيبرانية شكلًا من أشكال الإعتداء الذي تقوده دولة ضد أخرى بهدف الإضرار بمقدراتها التقنية والمعلوماتية، وتتمثل هذه الإعتداءات أساسًا

(1)-حسين بن احمد الشهري ، المرجع السابق، ص 44 .

(2)-محمد عبد الله ابوبكر سلامة ، موسوعة الجرائم المعلوماتية وجرائم الكومبيوتر والأنترنت ، منشأة المعارف،الإسكندرية ، 2006 ، ص 95.

(3)- جبور منى الأشقر ،" الأمن السيبيراني" هاجس العصر" ، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية، المجلد 1، لبنان ،2018 ،ص230 .

في تهديد أنظمة الإتصالات أو تدميرها، و إستهداف قواعد البيانات الحيوية، بما في ذلك أنظمة المراقبة الجوية، وأنابيب نقل الغاز والبترول، والمفاعلات النووية. [1]

وتتميّز الحرب السيبرانية بخصائص تجعلها أكثر تعقيدًا مقارنة بالحروب التقليدية، إذ تتسم بقصر مدتها، وسعة نطاقها في الفضاء الإلكتروني، فضلًا عن طبيعتها غير الملموسة، ما يمنحها في ذات الوقت طابعًا مدمرًا شبيهًا بالمعارك العسكرية، ومن أبرز الأمثلة التي جسدت هذا النوع من الحروب، الهجوم السيبراني الذي إستهدف دولة إستونيا في أفريل 2007، حيث تعرضت لهجمات إلكترونية متكررة عطلت شبكات الاتصال الرسمية في البلاد، بما في ذلك المواقع التابعة لرئيس الوزراء ورئيس البرلمان والوزارات المختلفة، وقد جاءت هذه الهجمات في سياق خلاف سياسي حاد مع روسيا، ما أثار جدلًا واسعًا حول مفهوم السيادة والعدوان في الفضاء الرقمي.[2]

كما عرفت جورجيا، خلال نزاعها المسلح مع روسيا سنة 2008، سلسلة من الهجمات السيبرانية التي تزامنت مع العمليات العسكرية، فقد تم تعطيل أنظمة الاتصال الإلكترونية التابعة للقوات الجورجية قبل انطلاق الهجوم العسكري بيوم واحد، مما ساهم في إضعاف قدراتها الدفاعية، لاسيما في مجال الدفاع الجوي ، وتشكل هذه الهجمات نموذجًا واضحًا لتكامل العمل السيبراني مع العمل العسكري في إطار إستراتيجية هجومية منسقة، وفي سياق آخر، شهد العالم سنة 2010 تطورًا نوعيًا في إستخدام الأسلحة السيبرانية، حيث قامت الولايات المتحدة الأمريكية، وفق ما أكدته عدة تقارير، بإستخدام فيروس"ستاكسنت " (Stuxnet)لاستهداف المنشآت النووية الإيرانية، ويُعد هذا الفيروس أول سلاح إلكتروني

(1)–حسين بن احمد الشهري ، المرجع السابق ، ص 50.

(2)–رغدة البهي، الردع السيبيراني، المفهوم والإشكالات والمتطلبات ، مجلة العلوم السياسية والقانون ، المركز الديمقراطي العربي للدراسات الإستراتيجية والإقتصادية العدد01 ، ألمانيا، 2007 ، ص54 .

معروف يُستخدم بين الدول[1]، إذ تمكن من إلحاق أضرار كبيرة بأجهزة الطرد المركزي الخاصة بتخصيب اليورانيوم، مما فتح الباب واسعًا أمام إستخدام البرمجيات الخبيثة كأداة في الصراعات الجيوسياسية المعاصرة.[2]

2- الإرهاب السيبراني

يرجع إستخدام مصطلح "الإرهاب السيبراني" إلى ثمانينيات القرن الماضي، حيث يُنسب إلى الباحث باري كولين (Barry Collin)، الذي قدّم تعريفًا قريبًا لمفهوم "الإرهاب الإلكتروني"، معتبرًا إياه "هجومًا إلكترونيًا يستهدف تهديد الحكومات أو الإعتداء عليها، بغرض تحقيق أهداف سياسية أو دينية أو أيديولوجية، شريطة أن يكون لهذا الهجوم طابع تدميري وتخريبي يُضاهي في تأثيره الأعمال الإرهابية التقليدية"،وفي السياق ذاته، عرّف جيمس لويس (James Lewis)الإرهاب السيبراني بأنه "استخدام أدوات وتقنيات شبكات الحاسوب لتدميرأو تعطيلالبنىالتحتية الوطنية الحيوية، كقطاعات الطاقة والنقل والخدمات الحكومية، أو لإرهاب السكان أو حكومة معيّنة، مع الإعتماد في هذه الهجمات على عنصر الترويع والغموض في تحديد مصدرها.[3]

وقد إزدادت المخاوف الدولية من الإرهاب السيبراني بشكل ملحوظ عقب هجمات الحادي عشر من سبتمبر 2001، حيث دفعت هذه الأحداث إلى فتح نقاشات موسعة حول إمكانية إستغلال التنظيمات الإرهابية لتكنولوجيا المعلومات و الإتصالات في تنفيذ مخططاتها ، وعلى الرغم من أن الهجمات لم تكن سيبرانية بطبيعتها، إلا أن التقارير كشفت إستخدام

(1)–رغدة البهي، المرجع السابق ، ص 56.

(2)–العلي ناصر، "الجهود الدولية في مكافحة الإرهاب الإلكتروني"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية ، جامعة باتنة ، العدد 08 ، 2021 ،ص 32 .

(3)–العلي ناصر ، المرجع نفسه ، ص 40 .

الجناة للإنترنت في التخطيط والتنظيم، مما أبرز أهمية الفضاء السيبراني كوسيلة للتحضير للهجمات الإرهابية.[1]

وتجسدت هذه المخاوف من خلال عدة أمثلة عملية، من أبرزها ما وقع في إيطاليا سنة 1998، حيث شنّت جماعة "الأولوية الحمراء" هجمات إلكترونية إستهدفت عدّة وزارات ومؤسسات حكومية ومالية، وقامت بتخريب مراكز المعلومات التابعة لها، كما شهدت ولاية كاليفورنيا الأمريكية سنة 2001 إختراقًا خطيرًا لشبكة الكهرباء من قبل متسللين، في محاولة لتعطيل بنيتها التحتية.

وفي تطوّر خطير لنمط الإرهاب السيبراني، تمكنت تنظيمات مثل داعش والقاعدة من إستخدام الإنترنت وشبكات التواصل الإجتماعي المغلقة في التنسيق لعدة هجمات إرهابية في أوروبا، لاسيما في فرنسا وبلجيكا، وقد إعتمد الإرهابيون على وسائل رقمية يصعب تتبعها، بما في ذلك أجهزة ألعاب الفيديو المتصلة بالأنترنت، التي مكّنتهم من تبادل المعلومات وتحديد الأهداف دون كشف أنشطتهم، وقد أفضت هذه العمليات، خصوصًا هجوم باريس في نوفمبر 2015، إلى مقتل نحو 200 شخص، وفشلت أجهزة الإستخبارات الأوروبية في اكتشاف المخطط قبل وقوعه، وإن كانت قد تمكنت لاحقًا من تحديد هوية المنفذين من خلال تتبع هواتفهم المحمولة.[2]

الفرع الثالث : الجرائم الجنسية الإلكترونية

لقد ساهم إنتشار الأنترنت ومواقع التواصل الإجتماعي في إحداث تحول جذري في مفاهيم الاتصال وتبادل المعلومات، مما أدى إلى تحقيق مفهوم "القرية الكونية" الذي طالما تنبأ به العلماء، ورغم ما وفره الفضاء السيبراني من مزايا إيجابية هامة في مجالات متعددة، إلا أنه

(1)–العلي ناصر، المرجع نفسه ، ص43.

(2)–هشام بشير، "مستقبل الإرهاب الإلكتروني، تحديات وأساليب المواجهة"، مداخلة بندوة المركز الدولي للدراسات المستقبلية والاستراتيجية ، 2112 ، على الرابط/http://www.siyassa.org.eg :

أصبح أيضًا بيئة خصبة لانتشار المواد الإباحية والجرائم الجنسية، ما أدى إلى ما يُوصف اليوم بثورة جنسية غير مسبوقة تجاوزت كل الضوابط والحدود، وقد إعتُبرت هذه الجرائم من أكثر التهديدات خطورة على كيان الإنسان والمجتمعات، خاصة في ظل ما أشار إليه الصحفي جيمس رستون في مجلة نيويورك تايمز بقوله: "إن خطر الطاقة الجنسية قد يكون في نهاية الأمر أكبر من خطر الطاقة الذرية".[1]

وفي هذا السياق، سنتناول في هذا الفرع أهم أشكال الجرائم الجنسية في الفضاء السيبراني، وعلى رأسها جريمة الإستغلال الجنسي للأطفال بإعتبارهم الفئة الأكثر هشاشة وعرضة للإستهداف، بالإضافة إلى جريمة التحرش الجنسي الإلكتروني التي إنتشرت بشكل لافت عبر الوسائط الرقمية الحديثة.

أولا : جريمة الإستغلال الجنسي الإلكتروني للأطفال

1- تعريفها

على خلاف الجرائم الجنسية التقليدية التي تستهدف الجسد بشكل مباشر كحالات الاغتصاب، فإن جرائم الاستغلال الجنسي عبر الإنترنت تركز على إستغلال جسد الطفل بصورة غير مباشرة، وذلك بهدف تحقيق مكاسب مادية أو غير مادية، مثل تصويره في أوضاع مخلة أو الترويج لمواد إباحية.[2]

وفي هذا الإطار، يُطرح مصطلح "الإستغلال الجنسي للأطفال عبر الإنترنت" كمفهوم إشكاليمن حيث التعريف والمجال،فقد تناولت اتفاقية بودابست المتعلقة بالجريمة المعلوماتية

(1)–يقرو خالدية، "الإستغلال الجنسي عبر شبكة الأنترنت"، مجلة القانون، المركزالجامعي غليزان ،كلية الحقوق، العدد03 ،الجزائر، 2012 ، ص 333 .

(2)–عادل عبد العال إبراهيم خراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها ، دار الجامعة الجديدة ، الإسكندرية ، 2015، ص 1152.

لسنة 2001 هذا النوع من الجرائم، وأكدت على ثلاث صور رئيسية لما يعرف ببورنوغرافيا الأطفال، الصورة الأولى تتضمن إعتداءات جنسية حقيقية وموثقة على الأطفال.[1]

-الصورة الثانية، تشمل صورًا مركبة، كاستبدال وجه شخص راشد بوجه طفل باستخدام أدوات رقمية.

-أما الصورة الثالثة، فتتعلق بصور يظهر فيها بالغون تم إختيارهم بمواصفات جسدية توحي بأنهم أطفال، وذلك لإثارة ميول شاذة لدى بعض المنحرفين جنسياً.

لقد ساهمت سهولة الوصول إلى الأنترنت وتنوع المنصات الرقمية ومواقع التواصل الإجتماعي في تزايد هذه الظاهرة بشكل ملحوظ، إذ توفر هذه الوسائط بيئات تبدو آمنة، لكنها في الواقع تتيح للمجرمين إستهداف الأطفال بسهولة.[2]

ويُعرف النظام الأساسي للمحكمة الجنائية الدولية الإستغلال الجنسي للأطفال، بإعتباره صورة من صور الإتجار بالبشر، بأنه "كل فعل جنسي تجاري يتم بالقوة أو الإحتيال أو الإكراه، أو بأية وسيلة أخرى تقع على من هم دون الثامنة عشرة من العمر".

وتجدر الإشارة إلى أن تصوير الأطفال في أوضاع إباحية أصبح يُمثّل تجارة قائمة بذاتها، حيث يُلتقط للأطفال صورٌ ذات طابع جنسي، تُدمج لاحقاً في أفلام أو تُنشر على مواقع إلكترونية مشبوهة ، وغالباً ما يُجبر الطفل على القيام بذلك إما بالترغيب المالي أو بالإكراه أو تحت التهديد، وفي بعض الحالات يكون تحت تأثير المخدرات، مما يزيد من فداحة الجريمة.[3]

---

(1)-عادل عبد العالي ابراهيم ، المرجع السابق ، ص1159

(2)-علي حسن الطوالبة، المرجع السابق، ص295 .

(3)-تشير التقارير الصادرة عن الشرطة الدولية انتربول ، أن هذا الشكل من أشكال الإستغلال الجنسي للأطفال يقدر رقم مبيعاته السنوي في ألمانيا وحدها بأكثر من 65مليون مارك ألماني ، حيث تعتبر ألمانيا المصدر الرئيسي لهذا النوع من الإستغلال الجنسي التجاري للأطفال ، أنظر ذلك على الموقع التالي : www.interpol.int.

ويمكن القول إن الاستغلال الجنسي للأطفال عبر الإنترنت هو نوع من الجرائم الجنسية السيبرانية التي تُرتكب من خلال الوسائط الرقمية الحديثة، ويتخذ هذا النوع من الجرائم عدة أشكال، منها:

-الإستغلال الجنسي عبر الدردشات والمحادثات الإلكترونية.

-الإبتزاز الجنسي، والذي يتم عبر إستدراج الطفل لإرسال صور أو مقاطع فيديو غير لائقة، ثم يُهدَّد بنشرها إذا لم يستجب للمجرم.

-التواصل من خلال ألعاب الإنترنت، حيث يستغل المجرمون هذه البيئات التفاعلية لبناء علاقات مع الأطفال والتأثير عليهم تدريجياً وصولاً إلى الإستغلال.

إن هذا النوع من الجرائم يُعد من التحديات الكبرى التي تواجه التشريعات الجنائية في العصرالرقمي، ويتطلب تعاونا دوليا فعالاً لتتبع الجناة وحماية الأطفال في البيئة الافتراضية[1]

ثانيا : التحرش الجنسي عبر الوسائط الرقمية

ينظر إلى التحرش الإلكتروني بإعتباره إمتدادًا للجرائم التقليدية في بُعدها الرقمي، حيث تتجلى خطورته في كونه يستهدف على وجه الخصوص النساء والفتيات، ما يجعله ظاهرة مقلقة تمس أمن الأفراد وكرامتهم في الفضاء السيبراني، وتنتشر بشكل ملحوظ في معظم المجتمعات، بغضّ النظر عن مستواها الثقافي أو التكنولوجي.

وبناء على ما سبق، سنقوم في هذا الفرع بدراسة ظاهرة التحرش الجنسي الإلكتروني من خلال التطرق إلى تعريفها، وتحليل أنماطها وصورها المتعددة.[2]

(1)-علي حسن الطوالبة ، المرجع نفسه ، ص296 .

(2)-علي حسن الطوالبة ، المرجع نفسه ، ص298 .

1-تعريف جريمة التحرش الجنسي عبر الوسائط الرقمية

تعتبر جريمة التحرش الجنسي من الظواهر الإجتماعية المعقدة التي تشكّل تحديًا حقيقيًا للمجتمعات والدول في مختلف أنحاء العالم، نظراً لما تخلّفه من مساس مباشر بكرامة الأفراد وسمعتهم، وما تسبّبه من آثار نفسية واجتماعية سلبية، لاسيما لدى النساء، ومن الملاحظ أن سلوك التحرش لا يتخذ نمطاً واحداً، بل يتنوّع من حيث الوسائل والأساليب، ويتطوّر بتطوّر الوسائط التقنية المستخدمة.[1]

ومع التطور الهائل في تكنولوجيا الإتصال، وتوفّر الوسائط الرقمية وسهولة إستخدامها من قبل الجميع، ظهرت أنماط جديدة من هذه الجريمة في الفضاء الإلكتروني، الأمر الذي يستدعي الوقوف عند تعريف جريمة التحرش الجنسي عبر الوسائط الرقمية، وتحليل أشكالها وصورها المختلفة[2]

ومع التطور الهائل في تكنولوجيا الإتصال، وتوفّر الوسائط الرقمية وسهولة إستخدامها من قبل الجميع، ظهرت أنماط جديدة من هذه الجريمة في الفضاء الإلكتروني، الأمر الذي يستدعي الوقوف عند تعريف جريمة التحرش الجنسي عبر الوسائط الرقمية، وتحليل أشكالها وصورها المختلفة[3]

ويُعد التحرش الجنسي عبر الوسائط الرقمية أحد أبرز أشكال العنف السيبراني، حيث عرفه علماء الاجتماع بأنه سلوك إرادي ناتج عن دوافع نفسية وبيولوجية مكبوتة، يسعى من خلالها الفرد إلى التنفيس عن رغبات جنسية بطرق مشينة تخدش الحياء وتتنافى مع القيم الإنسانية السليمة.

---

(1)-العربي بوعمامة ، رقاد حليمة ،المرجع السابق، ص66 .

(2)-علي حسن الطوالبة ، المرجع السابق ، صفحة نفسها .

(3)- وردة دلال، "السياسة التشريعية المتبعة في تجريم التحرش الجنسيالتشريع الجزائري والتشريع السعودي نموذجا"، مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، المجلد 4، العدد 7، الجزائر،2017 ، ص 100

وفي الإطار القانوني الدولي، نجد أن تعريف الأمم المتحدة للتحرش الجنسي يركّز على طبيعته الإكراهية وغير المرغوب فيها، إذ تصفه بأنه: "أي تلميح جنسي غير مرحب به، أو طلب جنسي، أو سلوك لفظي أو جسدي، أو إيماءة ذات طابع جنسي، وأي سلوك آخر ذي طابع جنسي واضح، قد يُسبب الإساءة أو الإذلال للطرف الآخر، أو يمسّ بكرامته، أو يُستَخدم كشرط للعمل، أو يُفضي إلى خلق بيئة عدوانية وغير آمنة.[1]

وعلى الرغم من تعدد التعاريف، إلا أنها تتفق جميعاً على أن التحرش الجنسي هو شكل من أشكال العنف الموجّه أساساً نحو النساء، من خلال سلوكيات تحمل دلالات جنسية صريحة أو ضمنية، إذ تُعد المرأة الفئة الأكثر عرضة لهذه الإعتداءات غير الأخلاقية.

وتجدر الإشارة إلى أن التحرش قد يحدث بين شخصين من جنسين مختلفين أو من الجنس ذاته، وقد يكون حادثاً عرضياً أو متكرراً، يصدر من شخص في موقع نفوذ أو سلطة أو من أي شخص آخر، داخل بيئة العمل أو خارجه.[2]

أما فيما يخص التحرش الجنسي الإلكتروني، فقد عرّفه المختصون في علم الإجتماع على أنه إستخدام الوسائل الإلكترونية ووسائل التواصل الرقمي في توجيه رسائل تتضمن مواد مزعجة أو ذات طبيعة جنسية، سواء من خلال تلميحات للتقرب بهدف جنسي، أو ألفاظ نابية، أو صور ومقاطع فيديو ذات محتوى جنسي، أو عبر التهديد والإبتزاز بإستخدام صور الضحية أو نشرها دون علمها أو موافقتها، مستغلين في ذلك الطبيعة المفتوحة و الإنتشار السريع لمحتويات الشبكات الرقمية.[3]

(1)–أنظر موقع الأمم المتحدة www.uun.org .

(2)–وردة دلال ، المرجع السابق ، ص102 .

(3)–العربي بوعمامة ،رقاد حليمة ، المرجع السابق، ص 180 .

ويتم هذا النوع من التحرش من خلال عدد من الوسائط، أبرزها :غرف الدردشة، المنتديات الإلكترونية، مواقع التواصل الإجتماعي، الرسائل الفورية، البريد الإلكتروني، الإعلانات المنبثقة، الصور الرمزية، والروابط التلقائية،وقد أدخلت العديد من القواميس مصطلحات جديدة للتعبير عن هذه الظاهرة، مثل :التحرش الإلكتروني، التحرش الافتراضي، التحرش الرقمي، التحرش عن بُعد، والتحرش السايبيري، ورغم تنوع هذه المصطلحات، فإنها تصف جميعاً سلوكاً غير لائق ذي طابع جنسي، يعتدي على خصوصية المرأة، ويشوّه إحساسها بالأمان، ويؤثر سلباً في توازنها النفسي وحالتها المزاجية.[1]

2- أنواع التحرش الجنسي الالكتروني

يتخذ التحرش الجنسي الإلكتروني أشكالاً متعددة، تتنوع بحسب الوسيلة المستخدمة وطبيعة السلوك المنطوي عليه، ويمكن تصنيفه إلى ثلاث صور رئيسية، تمثل أكثر الأشكال شيوعًا لهذه الظاهرة:

أ-التحرش اللفظي

يتجسّد هذا النوع من التحرش من خلال استخدام العبارات والكلمات ذات الطابع الجنسي الصريح أو المبطّن، والتي غالباً ما تُرسل عبر الرسائل النصية أو المكالمات الصوتية. كما يشمل هذا الشكل من التحرش التعليقات ذات الإيحاءات الجنسية، والنكات الفاضحة، وطلبات ممارسة "الجنس الإلكتروني"، وهو ما يمسّ بكرامة الضحية ويؤثر سلباً على توازنها النفسي والشعور بالأمان في الفضاء الرقمي.[2]

ب-التحرش البصري

ويُقصد به إرسال صور أو مقاطع فيديو تحمل محتوى جنسياً صريحاً، سواء للضحية أو من قبل المتحرش نفسه، حيث يظهر الأخير في أوضاع مخلة بالآداب، كما يتضمّن هذا النوع من التحرش الطلب من الضحية الكشف عن أجزاء من جسدها أثناء محادثة مرئية أو

(1) -العربي بوعمامة، رقاد حليمة ، المرجع السابق، ص176 .

(2)- العربي بوعمامة، رقاد حليمة، المرجع نفسه ، ص176 .

غيرها، ما يُعد انتهاكاً صارخاً للخصوصية والآداب العامة، ويُعرّض المتحرش للمساءلة القانونية.[1]

ج-التحرش بالإكراه أو التهديد (البلطجة الرقمية)

يُعد هذا الشكل من أخطر صور التحرش الإلكتروني، إذ يتم من خلاله إستخدام وسائل العنف السيبراني القائمة على الإكراه والإبتزاز، ففي كثير من الحالات، يعمد المتحرش إلى إختراق الجهاز الإلكتروني الخاص بالضحية، وسرقة صورها أو بياناتها الشخصية، ليستخدمها لاحقاً في تهديدها أو إجبارها على تلبية طلباته، سواء عبر اللقاء الواقعي أو التفاعل الرقمي، ويتخذ هذا النوع من التحرش مظاهر متعددة، مثل: الملاحقة الإلكترونية، التجسس، التهديد بنشر الصور الخاصة، التشهير، التتبع عبر التعليقات المسيئة، أو حتى إنتحال الهوية بإستخدام البريد الإلكتروني أوالحسابات المزيفة على مواقع التواصل الإجتماعي.[2]

المبحث الثاني : دور الأمن السيبراني في الحد من العنف السيبراني

رغم الفوائد الكبيرة التي وفّرتها تكنولوجيا المعلومات ووسائل الإتصال الرقمي، إلا أن إساءة إستخدامها لأغراض إجرامية جعلت منها مصدرًا لتهديد الأفراد والدول، خاصة مع تنامي ظواهر الإختراق والقرصنة والتجسس، وقد أدّى ذلك إلى بروز مفهوم "الأمن السيبراني" كوسيلة لحماية الفضاء الرقمي من هذه التهديدات، لاسيما في ظل إرتباطه المباشر بالعنف السيبراني المتزايد، والذي بات يشكل خطرًا حقيقياً على الأمن الفردي والجماعي، بناءً عليه،

(1)- نهلا عبد القادر المومني ، المرجع السابق ، ص 201

(2)-إيهاب الحضري،"الفضاء البديل الممارسات السياسية والإجتماعية للشباب العربي على شبكة الأنترنت"، مركز الحضارة العربية، الجيزة، 2010 ،ص 30 .

سيتم تناول الموضوع من خلال: مفهوم الأمن السيبراني(المطلب الأول)، وبيان علاقته بمكافحة العنف السيبراني(المطلب الثاني).

المطلب الأول :مفهوم الأمن السيبراني

نظرًا لما يشمله الفضاء السيبراني من عمليات متواصلة للدخول إلى مواقع متعددة تُعنى بتخزين وتداول المعلومات والبيانات، فإن ذلك يفرض حتمًا ضرورة وضع قواعد وآليات دقيقة لترسيخ مبادئ الأمن وضمان حماية هذه المواقع وأنظمتها المعلوماتية من التهديدات المحتملة، وفي هذا السياق، يبرز تساؤل أساسي يطرحه كل من يتعامل أو ينشط داخل هذا الفضاء، ويتعلق بمفهوم "الأمن السيبراني" من حيث تعريف مصطلح الأمن السيبراني(الفرع الأول)، أنواعه(الفرع الثاني)، وأبعاده المختلفة(الفرع الثالث).

الفرع الأول : تعريف الأمن السيبيراني

لقد تعددت التعاريف المتعلقة بمفهوم "الأمن السيبراني"، الأمر الذي يفرض ضرورة الرجوع إلى أكبر عدد ممكن من هذه التعاريف بغرض الإحاطة الشاملة بالمفهوم، غير أنه، وقبل التطرق إلى هذه التعاريف، من المهم التمهيد لذلك من خلال الوقوف عند بعض المفاهيم المرتبطة به، والتي تساعد على فهم الأمن السيبراني من زوايا متعددة:

أولا: تعريفه من الناحية اللغوية

ترجع كلمة "سيبرانية" إلى المصطلح "سيبر" الذي يعني كل ما هو آلي أو مرتبط بثقافة الحواسيب، وتكنولوجيا المعلومات، أو الواقع الإفتراضي، وتشير هذه الكلمة إلى الفضاء الإلكتروني الذي يُعد إمتدادًا لأنشطة الإنسان في البيئة الرقمية[1]، ويُذكر أن أصل الكلمة

(1)–إيهاب الحضري، المرجع نفسه ، ص31.

يعود إلى المصطلح اليوناني sybernetes، والذي ورد في أدبيات الخيال العلمي للدلالة على "ربان السفينة" أو "قائد النظام[1]

إستُخدم هذا المصطلح لأول مرة بالمعنى التقني الحديث من طرف عالم الرياضيات الأمريكي نوربرت وينر (Norbert Wiener) سنة 1948، حيث وظّفه ضمن نظرية "التغذية الراجعة (Feedback) "لوصف عملية ضبط مخرجات الأنظمة للتحكم في مدخلاتها وضمان إستقرار أدائها.[2]

ثانيا: من الناحية الإصطلاحية

بالإنتقال إلى مفهوم الأمن السيبراني، نجد أن هذا الأخير يحظى بعدد كبير من التعاريف، أبرزها ما يلي: فقد عرّفه "ريتشارد كيمرر (Richard Kemmerr) "بأنه "مجموعة من الوسائل الدفاعية التي تهدف إلى كشف وإحباط المحاولات التي ينفذها القراصنة"، من جهته، يرى "إدوارد أمورسو (Edward Amoroso) "أن الأمن السيبراني يتمثل في الوسائل التي تحد من خطر الهجوم على البرمجيات، وأجهزة الحاسوب، والشبكات، وتشمل هذه الوسائل أدوات مواجهة القراصنة، وبرامج كشف الفيروسات وإيقافها، إضافة إلى توفير الاتصالات المشفرة[3]

وعليه، يمكن القول إن الأمن السيبراني يُعدّ فنًا وتقنية تهدف إلى ضمان استمرارية مجتمع المعلومات، وتأمين الفضاء الإلكتروني وما يحتويه من بيانات ومعلومات وأصول رقمية

(1)–شريفة كلاع، الأمن السيبيراني وأشكال التهديد ، تحديات عالمية، ألفا للوثائق للنشر والتوزيع ، الجزائر، 2023 ص50.

(2)–طماطمي سالم ،الصحافة الإلكترونية و الأمن السيبراني دراسة حالة الجزائر، مذكرة ماستر، كلية العلوم الإنسانية والإجتماعية ،جامعة أدوار، السنة الجامعية 2021–2022 ، ص 15.

(3)– إدريس عطية ،"مكانة اللأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية المدرسة العليا العسكرية للإعلام والاتصال،المجلد 1، العدد 1،الجزائر، 2019،ص 110 .

وبُنى تحتية، كما يندرج ضمن هذا المفهوم حماية الشبكات المعلوماتية والمحتوى الرقمي من أي إختراق أو تخريب متعمَّد[1]

ويتجلى جوهر الأمن السيبراني في حماية الأنظمة الإلكترونية والشبكات والتطبيقات والبرمجيات من مختلف الهجمات الرقمية التي قد يتعرض لها المستخدمون، وتقوم عملية الحماية على ثلاث وظائف أساسية، وهي:إكتشاف الهجوم، التحقيق في أسبابه، ثم اتخاذ الإجراءات المناسبة لمعالجته.

ويهدف الأمن السيبراني في نهاية المطاف إلى المحافظة على سرية المعلومات الإلكترونية، ومنع الفيروسات من اختراقها، وضمان وصولها إلى الجهات المختصة والمستخدمين المصرح لهم، في الوقت المناسب، دون تسربها إلى جهات خبيثة أو إجرامية. وتتأكد هذه الأهمية خاصة في ظل الثورة الرقمية التي اجتاحت مجالات الاتصال والمعاملات الإلكترونية، وجعلت من الأمن السيبراني أحد أبرز الهواجس الإستراتيجية للقوى الدولية الكبرى مثل الولايات المتحدة الأمريكية، والصين، وروسيا، حيث تدور حاليًا حرب إلكترونية بين هذه الدول تستهدف إختراق المعلومات والتأثير على أسواق المال والاقتصاد العالمي.[2]

بناءً على ما سبق، يتضح أن الأمن السيبراني يُمثل مزيجًا من التقنيات والعمليات والممارسات التي تهدف إلى حماية التطبيقات، والشبكات، وأجهزة الحاسوب، والبيانات من الهجمات الخبيثة، ويشمل هذا الأمن بُعدين رئيسيين:

الأول: بُعد مادي يتعلق بحماية الأجهزة والأنظمة.

(1)–طماطمي سالم ، المرجع السابق ، ص17 .

(2)–علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في إستراتيجيات الإشتباك الرقمي، دار أمجد للنشر والتوزيع،عمان، 2020 ، ص 54

الثاني:بُعد غير مادي يختص بحماية البيانات والمعلومات من السرقة والتلاعب والوصول غير المشروع،مع التأكيدعلى التحكم في آليات الوصول الصحيح.

ويُمارس هذا الحماية في بيئة الفضاء السيبراني، سواء من طرف الدول أو الفاعلين السيبرانيين غير الحكوميين، الذين باتوا يُشكلون تهديدًا مستمرًا لأمن المجتمعات الرقمية.[1]

الفرع الثاني : أنواع الأمن السيبراني

يهدف الأمن السيبراني إلى حماية أجهزة الحاسوب، والشبكات، والأنظمة المرتبطة بها، من جميع أشكال التهديدات والهجمات السيبرانية، سواء كانت داخلية أو خارجية، ويُعدّ هذا النوع من الأمن ضرورة حتمية في ظل الاعتماد المتزايد على الوسائط الرقمية والتقنيات الحديثة، ويتفرّع الأمن السيبراني إلى عدة أنواع رئيسية، من أبرزها:

1-أمن التطبيقات(Application Security)

يُعنى هذا النوع من الأمن بالحماية التقنية للبرمجيات والتطبيقات الإلكترونية من التهديدات والإختراقات المحتملة، ويبدأ تأمين التطبيق منذ مرحلة تصميمه، بحيث يتم تطويره بطريقة تضمن عدم تمكّن المهاجم من الوصول إلى البيانات الحساسة أو التلاعب بها، ويُعدّ أمن التطبيقات من الركائز الأساسية لضمان سلامة النظام الرقمي بأكمله.[2]

2-الأمن السحابيCloud Security)

يرتكز الأمن السحابي على حماية المعلومات والبيانات الشخصية المخزنة عبر الإنترنت فيما يُعرف بالسحابة الإلكترونية، والتي تمثل بيئة تخزين رقمية تعتمدها كبرى الشركات والمنصات مثل Google Driveو .Microsoft OneDriveويهدف هذا النوع إلى منع

(1)-شريفة كلاع ،"الأمن السيبراني وتحديات الجوسسة والإختراقات الإلكترونية للدول عبر الفضاء السيبراني" ، مجلة الحقوق والعلوم الإنسانية ، جامعة الجزائر03 ، المجلد 15 ، العدد 1 ،الجزائر، 2022 ، ص 300 .

(2)- شريفة كلاع ، المرجع نفسه، ص 312 .

أي محاولة غير مشروعة للوصول إلى هذه البيانات أو التلاعب بها، من خلال تقنيات تشفير وتحكم متقدمة[1]

3-الأمن التشغيلي(Operational Security)

يهتم الأمن التشغيلي بحماية البيانات الإلكترونية من خلال مراجعة السياسات والإجراءات التشغيلية التي تحكم عملية الوصول إلى البيانات وتخزينها ومشاركتها، ويشمل ذلك تحديد صلاحيات المستخدمين، ومواقع تخزين البيانات، والزمن المناسب لمشاركتها، مما يساهم في تقليل فرص حدوث اختراقات أمنية داخلية أو سوء استخدام للمعلومات[2]

4-أمن الشبكات(Network Security)

يهدف أمن الشبكة إلى حماية بنية شبكة الحاسوب من التهديدات السيبرانية التي قد تستهدفها سواء من داخل الشبكة أو من خارجها، ويتمّ ذلك عبر إستخدام مجموعة من البروتوكولات والتقنيات الحديثة مثل أنظمة كشف التسلل (IDS) وجدران الحماية (Firewalls)، لضمان مراقبة حركة البيانات ومنع التهديدات قبل وقوعها.

5-التعافي من الكوارث واستمرارية الأعمال Disaster Recovery and Business Continuity):

يرتكز هذا النوع من الأمن على وضع خطط إستجابة فعالة لحوادث الإختراق التي قد تؤدي إلى فقدان البيانات أو تعطل الأنظمة، وتهدف هذه الخطط إلى إستعادة وظائف المؤسسة بأسرع وقت ممكن بعد الحادث، من أجل ضمان استمرارية العمليات الأساسية والحفاظ على الكفاءة التشغيلية للمؤسسة.[3]

(1)-جبور منى الأشقر، المرجع نفسه، ص220 .

(2)- جبور منى الأشقر ، المرجع نفسه، ص 221 .

(3)- طماطمي سالم ، المرجع السابق، ص 34.

6-تثقيف المستخدم النهائي(End-User Education)

يُعدّ وعي المستخدمين عنصراً محورياً في تحقيق الأمن السيبراني، ويتمثل ذلك في تقديم دورات توعوية وتدريبية حول كيفية التعامل الآمن مع الأجهزة الإلكترونية، وتجنب فتح الروابط المشبوهة أو تحميل ملفات ضارة قد تؤدي إلى إدخال الفيروسات إلى النظام دون قصد. فالمستخدم غير المدرب قد يشكل الحلقة الأضعف في منظومة الأمن الرقمي.[1]

7-الأمن السيبراني وأمن المعلومات

يُعرف أمن المعلومات على أنه مجموعة من الإجراءات والتدابير التي تهدف إلى حماية المعلومات من المخاطر التي تهددها، وذلك عبر ثلاثة عناصر أساسية تشمل:سرية المعلومات(Confidentiality) ،التي تضمن الخصوصية وعدم إفشاء البيانات؛ سلامة البيانات(Integrity) التي تعني الحفاظ على تكامل المعلومات وحمايتها من التلاعب أو التغيير غير المصرح به؛ وتوافر المعلوماتAvailability) ، التي تضمن إمكانية الوصول إلى البيانات واستخدامها عند الحاجة، يُرمز إلى هذه العناصر الثلاثة بالاختصار "CIA" (Confidentiality, Integrity, Availability)[2]

يتم تحقيق هذه الأهداف من خلال مجموعة من الوسائل والإجراءات التي تهدف إلى حماية المعلومات من المخاطر، سواء كانت تهديدات داخلية أو خارجية، في الوضع المثالي، يجب دائمًا الحفاظ على سرية وسلامة المعلومات لضمان أكبر قدر من الأمان لها.

من هذا المنطلق، يهدف أمن المعلومات إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي إلى البيانات أو التلاعب بها أثناء تخزينها أو معالجتها أو نقلها، كما يُعتمد

(1)-سلمى موضوع ،تاريخ الأمن السيبراني ، متاح على الموقع.comwww.mawdoo

(2)-شريفة كلاع ، المرجع السابق ، ص310.

الأمن السيبراني على أمن المعلومات بكل الوسائل الضرورية لإكتشاف التهديدات وتوثيقها وصدها، كما يحدث في أنظمة الأمان المستخدمة في المؤسسات المالية والبنوك.[1]

الفرع الثالث : أبعاد الأمن السيبراني

يمتلك الأمن السيبراني إمتدادات وأبعادًا إستراتيجية بالغة الأهمية، حيث يمكن لأي خلل في إحدى هذه الأبعاد أن يؤدي إلى نتائج وخيمة، في فضاء يتسم بالسرعة في التخطيط planningوالتنفيذ، يصبح من الضروري وجود قوة رادعة وأسلحة سيبرانية متطورة تكون قادرة على مواجهة الهجمات الإلكترونية، من بين الأبعاد التي يتأثر بها الأمن السيبراني، نجد:البعد العسكري، والبعد الإقتصادي، والبعد الإجتماعي، والبعد القانوني، والبعد السياسي.

أولا: البعـد العسـكري

تتمثل الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، مما يسهل تبادل المعلومات وتدفقها بسرعة، هذا التبادل الفعال يساهم في اتخاذ القرارات العسكرية بشكل سريع، وبالتالي تحقيق الأهداف عن بُعد.[2]

ومن المهم أن نلاحظ أنه في حالة عدم إستغلال هذه التقنية أو تأمينها بشكل جيد ضد أي إختراقات خارجية، فإن ذلك قد يؤدي إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، مما قد يتسبب في تدمير قواعد البيانات وتعطيل الأنظمة العسكرية.[3]

(1)–فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، دار الجامعة الجديدة، الإسكندرية ،2016 ، ص 320.

(2)– علي زياد علي ، المرجع السابق ، ص54 .

(3)– طماطمي سالم ، المرجع السابق، ص25 .

ثانيا: البعد الإقتصادي

لقد أدى استخدام الكمبيوتر وشبكة الأنترنت في تطوير الصناعات وتحريك الاقتصاد، بالإضافة إلى معالجة كافة المعاملات الاقتصادية والمالية، إلى زيادة أهمية توفير الأمن السيبراني لضمان حماية هذه المعلومات. [1]

ثالثــا: البعد الإجتماعي

تعد الشبكة الدولية للمعلومات مجالًا مفتوحًا لجميع الأفراد، حيث يمكن لجميع المتعاملين السيبرانيين الإستفادة من البنية التحتية والخدمات المتاحة لهم دون تحمل المخاطر الأمنية، وفي هذا السياق، يجب التأكيد على ضرورة التحسيس بأخلاقيات الأمن السيبراني.[2]

رابعــا: البعد السياسـي

أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي، وأصبح بإمكانه الإطلاع على خلفيات القرارات السياسية من خلال الكم الهائل من المعلومات التي يسهل الوصول إليها عبر الإنترنت، هنا نشير إلى التسريبات للوثائق الحساسة التي تثير مشكلات كبيرة، وأيضًا دور شبكات التواصل الإجتماعي في تنظيم الدعايات السياسية والانتخابية[3]، وكذلك في تنظيم التظاهرات الإفتراضية وإفتعال الإحتجاجات الإلكترونية، وغيرها، كما أصبح الفضاء السيبراني ملاذًا للتجنيد من قبل التنظيمات الإرهابية والعديد من الأيديولوجيات والدعايات الدينية.[4]

(1)–جبور منى الأشقر، المرجع السابق، ص223 .

(2)–طماطمي سالم المرجع السابق، ص26 .

(3)–بـارة سميرة ، "الأمن السيبراني في الجزائر" ، المجلة الجزائرية للأمن الإنساني ، جامعة قاصدي مرباح ورقلة ،العدد 4، الجزائر، 2017 ، ص 160

(4)–منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية" ،مجلة كلية التربية ، جامعة المنصورة ،العدد 111 ،المملكة العربية السعودية، 2022 ، ص109 .

خامسا: البعد القـانوني

تتعدد أساليب ممارسة العنف السيبراني في استخدام تقنيات المعلومات، مثل إنشاء المدونات، والتجمعات على الإنترنت، وكذلك الحق في حماية ملكية البرمجيات والإبلاغ عن المخالفات والجرائم الإلكترونية، وقد أدى هذا إلى ظهور ترسانة قانونية تتناسب مع التغيرات الحاصلة بهدف مواجهة ظاهرة العنف السيبراني.[1]

المطلب الثاني:علاقة الأمن السيبراني بمكافحة العنف السيبراني

يرتبط أمن المعلومات ارتباطًا وثيقًا بالأمن القومي في العديد من الدول، إذ أن الاعتداء على البنى التحتية الحيوية مثل أنظمة الإتصالات والأنظمة الإلكترونية قد يؤثر بشكل كبير على دول معينة في منطقة جغرافية محددة، وهذا يؤثر بدوره على مصالح الدولة المعنية في الفضاء السيبراني، بالإضافة إلى تهديد خصوصية الأفراد ومعلوماتهم المتواجدة في الفضاء السيبراني، الذين يستخدمون الوسائط الرقمية بمختلف أنواعها، وقد ارتبط مفهوم الأمن السيبراني ارتباطًا وثيقًا بمكافحة العنف السيبراني، ويشمل ذلك إستراتيجيات تعزيز الأمن السيبراني (الفرع الأول)، وكذلك أدوات الدفاع السيبراني والتحديات المرتبطة به (الفرع الثاني).

الفرع الأول : إستراتيجيات تعزيز الأمن السيبراني

لحماية الأنظمة والبيانات الشخصية للأفراد من التهديدات الإلكترونية وأشكال العنف السيبراني المختلفة، يجب على المؤسسات والأفراد تبني استراتيجيات فعّالة تشمل:

(1)–منى عبد الله السمحان ، المرجع نفسه ، ص 111 .

1-التشفير لحماية البيانات :يُعد التشفير أداة مهمة لتحويل البيانات إلى نصوص مشفرة لا يمكن قراءتها إلا بعد فك تشفيرها، يمكن إستخدام التشفير لحماية البيانات أثناء تخزينها أو نقلها، خاصة عندما تكون هذه البيانات حساسة.[1]

2-إعداد جدران الحماية :(Firewalls) تعمل جدران الحماية على مراقبة حركة البيانات الواردة والصادرة، ومنع أي نشاط مشبوه، كما تساهم في حظر الوصول غير المصرح به إلى الأنظمة.[2]

3-التدريب والتوعية :يعد تدريب الموظفين على أساسيات الأمن السيبراني خطوة مهمة لرفع وعيهم وتقليل احتمالية الوقوع ضحية لهجمات مثل التصيد الإحتيالي، يشمل التدريب كيفية التعرف على رسائل البريد الإلكتروني المشبوهة، استخدام كلمات مرور قوية، وتجنب مشاركة المعلومات الحساسة.[3]

4-إعداد أنظمة الكشف عن التسلل :تهدف هذه الأنظمة إلى مراقبة الأنشطة غير الطبيعية في الشبكة وتنبيه المسؤولين عند اكتشاف أي نشاط مريب، هذه الأنظمة تساعد في التصدي للهجمات السيبرانية في مراحلها المبكرة.

5-إدارة الوصول :من المهم تقييد الوصول إلى البيانات الحساسة وفقًا لمبدأ "الحد الأدنى من الامتيازات"، حيث يُمنح كل موظف أو نظام الصلاحيات الضرورية فقط لأداء المهام الموكلة إليهم.

(1)-طماطمي سالم ، المرجع السابق ، ص 30 .

(2)-طواهير عبد الجليل ، "إستراتيجيات الأمن السيبيراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة إلى تجربة الإمارات العربية المتحدة" ، مجلة الرسالة للدراسات الإعلامية ، جامعة ورقلة، المجلد 7، العدد 1، 2023 ، ص 285.

(3)-طواهير عبد الجليل ،المرجع السابق ، ص 286 .

الفرع الثاني: أدوات الدفاع السيبراني وتحديات تطبيق الأمن السيبراني

يعتبر الدفاع السيبراني أحد الركائز الأساسية التي تعتمد عليها الدول والمؤسسات في مواجهة التهديدات المتزايدة في الفضاء الرقمي، ويقتضي التصدي الفعال لهذه التهديدات، إعتماد مجموعة من الأدوات التقنية والتنظيمية التي تشكل منظومة متكاملة للأمن السيبراني (أولا)، غير أن وجود هذا الأدوات وتطورها المستمر، لا تخلو من التحديات البنيوية العملية التي تعيق أحيانا تحقيق الأمن السيبراني (ثانيا).

أولا : أدوات الأمن السيبراني

أصبح الأمن السيبراني أمرًا بالغ الأهمية في عصرنا الحالي، حيث يجب على المؤسسات والأفراد الإستثمار في أدوات الأمن السيبراني لحماية بياناتهم ومعلوماتهم الحساسة من الهجمات والتهديدات السيبرانية، سنستعرض في هذا السياق بعض أدوات الأمن السيبراني وأهميتها في حماية العالم الرقمي، والتي تشمل:

1-الشبكات الاجتماعية الإلكترونية :تعد الشبكات الإجتماعية من أبرز وسائل الاتصال في العصر الرقمي، ومن الضروري إتخاذ تدابير أمان لحمايتها من الهجمات السيبرانية

2-البريد الإلكتروني :يعتبر البريد الإلكتروني من أكثر وسائل الإتصال إستخدامًا في الأعمال اليومية، لذا يجب تأمينه ضد المخاطر المحتملة مثل الهجمات الخبيثة والتصيد الإحتيالي.[1]

3-مواقع وسائل الإعلام :تمثل مواقع الإعلام مصدرًا رئيسيًا للمعلومات، وبالتالي فهي عرضة للهجمات، ما يستدعي إتخاذ تدابير أمان لحمايتها من أي تهديدات.

(1)-طواهير عبد الجليل ، المرجع نفسه ، ص287.

4-تقنيات الحماية الإلكترونية :تتنوع تقنيات الحماية الإلكترونية لتشمل جدران الحماية، أنظمة الكشف عن التسلل، وبرامج مكافحة الفيروسات، وكلها أدوات أساسية لضمان الأمان السيبراني.[1]

5-مواقع الحماية من الفيروسات :تعتبر المواقع المتخصصة في مكافحة الفيروسات أحد الأدوات الحيوية في حماية الأجهزة والأنظمة من البرامج الضارة.

6-إدخال نشاط أمن المعلومات إلى الشركات:يجب على الشركات تعزيز ممارسات أمن المعلومات داخل بيئات العمل، من خلال برامج تدريبية ونظم مراقبة متقدمة لضمان الحماية.[2]

7-تحفيز مواقع الإنترنت الاحتياطية وتجهيز البريد الإلكتروني: من الضروري إنشاء مواقع إحتياطية وتزويد البريد الإلكتروني بحلول أمنية متقدمة لضمان إستمرارية العمل في حال حدوث أي هجمات.

ثانيا : التحديات التي تواجهها الدول في تطبيق الأمن السيبراني

يعد الأمن السيبراني من أبرز التحديات التي تواجه العالم في عصر الإتصالات الحديثة، حيث تتزايد أهميته يومًا بعد يوم مع الإنتشار الواسع للتقنيات الرقمية وإستخدام الأنترنت في شتى المجالات الحياتية، وفي إطار هذا المقال، سنتناول بعض التحديات الأساسية التي يواجهها الأمن السيبراني في هذا العصر، وطرق التعامل معها.

1- الهجمات الإلكترونية

تُعد الهجمات الإلكترونية من أبرز التحديات التي تهدد الأمن السيبراني، حيث تتعرض العديد من المواقع الإلكترونية والشبكات لمختلف أنواع الهجمات، مثل الاختراقات

(1)-الدسوقي عطية ، المرجع السابق، ص 316 .

(2)- طواهير عبد الجليل، المرجع السابق ، ص 287 .

الإلكترونية، الفيروسات، وبرامج التجسس، التي تستخدم لسرقة المعلومات الحساسة أو تعطيل الخدمات الرقمية، ولحماية الأنظمة والشبكات من هذه الهجمات، يُنصح بتحديث برامج الحماية بشكل دوري والتأكد من وجود أنظمة حماية قوية ومتطورة.[1]

2-الهجمات الجماعية

تُعتبر الهجمات الجماعية من التحديات الخطيرة التي تهدد الأمن السيبراني، حيث يقوم مجموعة من المهاجمين بتنفيذ هجوم متزامن على هدف واحد عبر عدة قنوات، وتستخدم هذه الهجمات بشكل رئيسي في الإختراقات الموجهة نحو الشركات والمؤسسات الكبرى، مما يهدد أمن المعلومات والأنظمة الحيوي.[2]

3-الإحتيال الإلكتروني

يُعد الإحتيال الإلكتروني من التحديات البارزة في الأمن السيبراني، حيث يتعرض المستخدمون لرسائل إلكترونية مزيفة وصور مزورة للمصادقات الإلكترونية، وهي صورة من صور العنف السيبراني، تهدف هذه الرسائل والمصادقات إلى سرقة البيانات الشخصية والحساسة، ولتفادي هذه المخاطر، يجب على الأفراد الحذر من الرد على الرسائل المشبوهة والتأكد من مصدر المصادقات الإلكترونية المرسلة.[3]

4- التجسس الإلكتروني

يُعتبر التجسس الإلكتروني من التحديات الأساسية التي تهدد الأمن السيبراني في عصر الاتصالات الحديثة، حيث تستهدف هذه العمليات جمع المعلومات الحساسة والسرية بطرق غير قانونية، مثل الاختراقات الإلكترونية واستخدام برامج التجسس، لحماية الأنظمة

(1)- شريفة كلاع ،المرجع السابق، ص 240 .

(2)-فريدة طاجين،تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى،مذكرة ماستر،جامعة ورقلة، السنة الجامعية 2018-2019 ، ص11.

(3)- شريفة كلاع ، المرجع السابق، ص 246

والشبكات من هذه التهديدات، يجب التأكد من تحديث برامج الحماية وإستخدام أنظمة حماية قوية ومتطورة.[1]

5-الرقابة الإلكترونية

تُعد الرقابة الإلكترونية من التحديات الهامة التي تواجه الأمن السيبراني، حيث تُستخدم هذه الرقابة في المجالات السياسية، الاقتصادية، والاجتماعية. تشمل الرقابة الإلكترونية منع الوصول إلى بعض المواقع الإلكترونية، الحد من الحرية الإعلامية، والتحكم في المعلومات المتداولة عبر الأنترنت، للتعامل مع هذه التحديات، يجب إستخدام تقنيات التشفيروتخزين المعلومات الحساسة بشكل آمن، مع المحافظة على حرية الوصول إلى المعلومات وضمان حرية الإعلام.[2]

6-تحدي التعرض للهجمات المستمرة

تشكل الهجمات المستمرة، التي تتم على مدار الساعة وطوال الأسبوع، تهديدًا حقيقيًا للأمن السيبراني، وتشمل هذه الهجمات الإختراقات الإلكترونية، الفيروسات، وبرامج التجسس التي تهدف إلى سرقة المعلومات الحساسة أو تعطيل الخدمات الرقمية، للتعامل مع هذه التهديدات، يجب تحديث أنظمة الحماية بشكل دوري، واستخدام تقنيات التشفير والتحقق الثنائي، مع مراقبة النشاط الإلكتروني بشكل مستمر.[3]

7-تزايد إستخدام التقنيات الذكية

يُعتبر تزايد إستخدام التقنيات الذكية،مثل الروبوتات،الذكاء الاصطناعي،وإنترنت الأشياء، من التحديات الجديدة التي تهدد الأمن السيبراني،هذه التقنيات تُستخدم في مختلف جوانب

(2)-شريفة كلاع ، المرجع نفسه ، ص 247 .

(3)- Dan Craiyen et al., "Defining Cyber scurity", Technology Innovation Management Rview, Montreal, Canada, (October 2014), p.14

(3)- بن علية بن جدو، "تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية"، المجلة الجزائرية للأمن السيبراني،جامعة باتنة، المجلد 7، العدد 2 ،الجزائر، 2022 ، ص 302.

الحياة اليومية، مما يستدعي تأمينها وحمايتها من الإختراقات الإلكترونية،يجب أيضًا التحكم في البيانات والمعلومات التي يتم تبادلها عبر هذه التقنيات لضمان أمان المعلومات.[1]

8-التهديدات الدولية

تشكل التهديدات الدولية أحد أبرز التحديات التي تهدد الأمن السيبراني، حيث تتمثل هذه التهديدات في محاولات الدول أو الجماعات الإرهابية للإستيلاء على المعلومات الحساسة والتأثير على الأنظمة الحيوية والاقتصادية والسياسية للدول، لمواجهة هذه التهديدات، من الضروري تطوير إستراتيجيات دفاعية وهجومية للأمن السيبراني، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية.[2]

(1)-دحان حزام القرطبي،الأمن السيبراني وحماية امن المعلومات ، دار الفكر الجامعي، الإسكندرية ،2024، ص 200

(2)-بن علية بن جدو ، المرجع السابق ، ص305 .

الفصل الثاني :

العلاقة بين الآليات الدولية والأوروبية في مكافحة العنف السيبيراني

في ظل الإنتشار الواسع لوسائل الإتصال الرقمية وتزايد تبادل البيانات عبر شبكات الإنترنت، برزت ظاهرة العنف السيبراني كأحد أبرز التحديات العابرة للحدود، لاسيما مع تصاعد استخدام الفضاء الرقمي في تنفيذ أعمال عدائية ضد الأفراد والمؤسسات والدول، ويزداد الأمر تعقيدًا مع الطابع العالمي للإتصالات الرقمية التي تتخطى الحدود الجغرافية والسيادة الوطنية، في ظل غياب إطار قانوني موحد ينظم تداول البيانات والمعلومات بين مختلف الأطراف الفاعلة في البيئة السيبرانية.

إن الطبيعة العابرة للحدود للعنف السيبراني تفرز صعوبات قانونية وتحديات أمنية تعجز الدولة الواحدة عن مواجهتها بمفردها، مما يجعل التعاون الدولي الركيزة الأساسية للتصدي لهذا النوع من العنف، وقد أسفر هذا الواقع عن بروز عدة آليات قانونية دولية وإقليمية، من ضمنها الأوروبية، تهدف إلى إيجاد حلول جماعية لمكافحة العنف السيبراني.

وبغية دراسة العلاقة بين هذه الآليات وتحديد مجالات التقاطع والتكامل بينها، سيتم التطرق في هذا الفصل إلى الإطار القانوني الدولي لمكافحة العنف السيبراني (المبحث الأول)، ثم إلى الإطار القانوني الأوروبي ومدى تكامله مع الجهود الدولية في هذا المجال (المبحث الثاني).

المبحث الأول : الإطار القانوني الدولي لمكافحة العنف السيبراني

نظراً لما يشكله العنف السيبراني من تهديدات جسيمة على الأفراد والمجتمعات، فقد أصبح محل إهتمام متزايد على المستوى الدولي، في ظل قصور التشريعات الوطنية عن الإحاطة الكافية بجوانبه التقنية والقانونية المرتبطة به، ورغم حداثة هذا المفهوم، فقد بدأ المجتمع الدولي في تفعيل آليات قانونية ومؤسساتية لمواجهته، سواء عبر الاتفاقيات متعددة الأطراف أو من خلال مبادرات المنظمات الدولية ذات الصلة.

وفي هذا السياق، يهدف هذا المبحث إلى إستعراض الجهود القانونية الدولية في مجال مكافحة العنف السيبراني،مع التركيز على الإطار المعياري الذي أرسته الأمم المتحدة(المطلب الأول)، وكذلك مساهمة منظمات دولية أخرى في تطوير آليات التعاون الدولي وتبادل المعلومات وتعزيز الملاحقة القضائية(المطلب الثاني).

المطلب الأول: دور الأمم المتحدة في وضع معايير مكافحة العنف السيبراني

إضطلعت منظمة الأمم المتحدة بدور محوري في إرساء معايير قانونية تهدف إلى توحيد الجهود وتنسيق السياسات الجنائية بين الدول لمواجهة الجريمة العابرة للحدود، وعليه ورغم غياب اتفاقية متخصصة حصريًا في مجال مكافحة العنف السيبراني، فقد ساهمت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود لعام 2000، والاتفاقية الدولية لقمع تمويل الإرهاب لعام 1999، في وضع أسس قانونية يمكن الاستناد إليها في التصدي للجرائم الرقمية (الفرع الأول)، وبموازاة ذلك، بادرت الأمم المتحدة إلى إطلاق مفاوضات لصياغة إتفاقية دولية جديدة لمكافحة إستخدام تكنولوجيا المعلومات لأغراض إجرامية (الفرع الثاني)، كما أصدرت العديد من القرارات والتوصيات التي تهدف إلى تعزيز التعاون الدولي في مجال مكافحة العنف السيبراني (الفرع الثالث).

الفرع الأول : الإتفاقيات الدولية ذات الصلة بمكافحة الجريمة المنظمة والعابرة للحدود

تعتبر الجريمة المنظمة العابرة للحدود وجريمة الإرهاب الدولي ، إحدى الأسباب الهامة التي تهدد السلم والإستقرار العالميين، ومن أجل ذلك كان لزاما على هيئة الأمم المتحدة أن تكرس جهودها في مجال مكافحتهما ، وذلك من خلال تبني إطارا تشريعيا دوليا خاص بمواجهة الجريمة المنظمة العابرة للحدود (أولا) وجريمة الإرهاب الدولي (ثانيا) ، والتي لهما صلة مباشرة بظاهرة العنف السيبراني.

أولا: إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000

إعتمدت الجمعية العامة للأمم المتحدة هذه الاتفاقية في 15 نوفمبر 2000، وتعد اليوم مرجعية دولية في مجال مكافحة الجريمة المنظمة[1]، ورغم عدم تضمينها نصوصًا صريحة تتعلق بالعنف السيبراني، إلا أن تطبيقها يمكن أن يمتد إلى هذا النوع من الجرائم نظرا لإرتباطه المتزايد بالجريمة المنظمة.[2]

1 -الإرتباط الموضوعي والإجرائي بين الإتفاقية والعنف السيبراني

تشير الممارسات الحديثة إلى تزايد إستغلال الجماعات الإجرامية المنظمة للفضاء الرقمي في تنفيذ أنشطة غير مشروعة ، مثل: الإتجار بالبشر، نشر المواد الإباحية، غسل الأموال، والقرصنة، ومن ثم، فإن العنف السيبراني كثيرًا ما يُنفذ من قبل كيانات منظمة عابرة للحدود.[3]

تُعرف الاتفاقية الجريمة المنظمة العابرة للحدود في الحالات التالية:

(1)-نسرين عبد الحميد نبيه ، الجريمة المنظمة عبر الوطنية ، دار الفكرالجامعي، الإسكندرية ،2016 ، ص578.

(2)-علي حسن الطوالبة ،المرجع السابق، ص 236

(3)-عادل عزام سقف الحيط ، المرجع السابق، ص 355 .

-إرتكاب الجريمة في أكثر من دولة.

-إرتكابها في دولة واحدة مع وجود عنصر التخطيط أو الإشراف من دولة أخرى؛

أو أن يكون لها أثر ملموس في دولة ثالثة.[1]

وبالتالي، فإن هذه المعايير تنطبق على العديد من صور العنف السيبراني، مما يسمح بإدماجه ضمن نطاق الإتفاقية.

2-الولاية القضائية في ظل الإتفاقية

تنص المادة 15 من الاتفاقية على إمكانية توسيع نطاق الولاية القضائية لتشمل الجرائم المرتكبة خارج إقليم الدولة، في حال إرتكبت من قبل جماعة منظمة ذات نية إجرامية تستهدف إرتكاب أفعال إجرمية داخل إقليمها.

كما تلزم الإتفاقية الدول الأطراف بمعاملة الجريمة المرتكبة خارج إقليمها كما لو ارتُكبت داخله، متى توافرت الشروط القانونية لذلك، خاصة إذا تعلقت الأفعال الإجرامية بجماعة إجرامية منظمة، وتؤكد المادة 16 على ضرورة تبادل الأدلة والمعلومات بين الدول وتقديم المساعدة القانونية المتبادلة، بما في ذلك تسليم المجرمين.[2]

وعليه، يمكن إعتبارهذه الإتفاقية قاعدة قانونية مهمة تُمكِّن من بناء تعاون دولي فاعل لمواجهة التهديدات المرتبطة بالعنف السيبراني.[3]

ثانيا: الإتفاقية الدولية لقمع تمويل الإرهاب لسنة 1990

تم التوقيع على هذه الاتفاقية بتاريخ 9 ديسمبر 1999، وتُعد من أهم الآليات الدولية لمكافحة تمويل الإرهاب، وتنص الفقرة الأولى من المادة الثانية على أن "كل من يقدّم أموالًا،

(1)-نسرين عبد الحميد نبيه ، المرجع السابق، ص 60 .

(2)-عادل عبد العال إبراهيم خراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها ، دار الجامعة الجديدة ، الإسكندرية، 2015 ، ص 31 .

3-علي حسن الطوالبة ، المرجع السابق ، ص95 .

بأي وسيلة كانت، سواء بشكل مباشر أو غير مباشر، وبطريقة غير مشروعة، وبإرادة حرة، بقصد إستخدامها أو مع علمه بأنها ستُستخدم كليًا أو جزئيًا لارتكاب أفعال إرهابية، يكون مرتكبًا لجريمة تمويل الإرهاب."

وقد أشارت الإتفاقية ضمنيًا إلى الوسائل الحديثة في تنفيذ هذه الجريمة، مثل إستخدام الوسائط الإلكترونية، وتمويل الأنشطة الإرهابية عبر الإنترنت، أو من خلال بطاقات الإئتمان الإلكترونية، وغسيل الأموال، كما حددت المادة السابعة المبادئ العامة للإختصاص القضائي الذي يمكن للدول الأطراف الاستناد إليه في مقاضاة مرتكبي هذه الجريمة.[1]

وعلى الرغم من أن الإتفاقيات الدولية، مثل هذه الإتفاقية، لا تُشير صراحة إلى مصطلح "العنف السيبراني"، إلا أنها تشكّل أساسًا قانونيًا لمحاكمة مرتكبي الجرائم السيبرانية، وذلك بسبب طبيعة أفعالها وإرتباطها الوثيق بمكافحة الجريمة المنظمة.[2]

الفرع الثاني: الإتفاقية الدولية لمكافحة إستخدام تكنولوجيا المعلومات لأغراض إجرامية

إن الجريمة السيبيرانية تعد شكل من أشكال الجريمة عبر الوطنية، والتي تحدث في الفضاء الالكتروني الذي لا حدود له، ويمكن لمرتكبي العنف السيبراني وضحاياه التواجد في مناطق مختلفة، ويمكن أن تمتد آثار الجريمة عبر جميع أنحاء العالم، مما جعل بمنظمة الأمم المتحدة إلى تبني إتفاقية دولية خاصة بمكافحة ظاهرة الجريمة السيبرانية، التي كانت لها أسباب خاصة لإنشائها (أولا)، وقد تضمنت أحكاما موضوعية وإجرائية تنظم طريقة مكافحة العنف السيبيراني (ثانيا).

(1)–فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، دار الجامعة الحديدة ، الإسكندرية، 2016 ، ص350.
(2)–عادل عزام سقف الحيط ، المرجع السابق، ص 364 .

أولاً: مسار إعتماد الإتفاقية الدولية لمكافحة الجرائم السيبرانية

على مدار سنوات، تعددت الدعوات لإعتماد إتفاقية دولية تنظم الأنشطة السيبرانية، لا سيما في سياق الجرائم العابرة للحدود وتهديدات الأمن الرقمي، وقد كانت روسيا من أبرز الدول التي طالبت بوضع إطار قانوني دولي للتعامل مع هذا النوع من الجرائم.

وفي عام 2019، قدّمت روسيا، بدعم من الصين، مشروعًا إلى الجمعية العامة للأمم المتحدة لإنشاء إتفاقية دولية لمكافحة الجرائم الإلكترونية، وبناءً عليه، صدر القرار رقم 247/74 بتاريخ 27 ديسمبر 2019، والذي نصّ على تشكيل لجنة حكومية دولية مفتوحة العضوية، مقرّها نيويورك، تضم خبراء متخصصين من مختلف الدول والأقاليم، وقد باشرت اللجنة عملها في يناير 2022، وإنتهت من إعداد مشروع الإتفاقية في الدورة التاسعة والسبعين للجمعية العامة.[1]

وفي 24 ديسمبر 2024، إعتمدت الجمعية العامة قرارًا يتضمّن إقرار الإتفاقية الدولية لمكافحة الجرائم السيبرانية.[2]

وقد رحّب الأمين العام للأمم المتحدة، أنطونيو غوتيريش، بهذا القرار، معتبرًا إياه أول معاهدة جنائية دولية يتم التفاوض بشأنها منذ أكثر من عشرين عامًا، ومؤكدًا أنها تمثّل إنجازًا هامًا في التعاون الدولي لمكافحة الجرائم الإلكترونية وتبادل الأدلة الإلكترونية.[3]

ثانيا: الأحكام الموضوعية والإجرائية في الإتفاقية

تتكوّن الاتفاقية من ستة أقسام رئيسية تتضمن أحكامًا موضوعية وإجرائية على النحو الآتي:

(1)– ميتيهان دورماز ،"إتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية"، الأهداف والثغرات، مقال منشور في موقع www.smex.org

(2)–ميتيهان دورماز، المرجع نفسه ، ص 01 .

(3)– ميتيهان دورماز، المرجع نفسه ، ص03.

1-التجريم (الفصل الثاني)

نصّت الاتفاقية على تجريم 11 نوعًا من الجرائم السيبرانية، وهي:

-الدخول غير المشروع إلى الأنظمة (المادة 7)،

-الإعتراض غير المشروع للبيانات (المادة 8)،

- التدخل في البيانات (المادة 9)،

- التدخل في نظم المعلومات والاتصالات (المادة 10)،

- إساءة استخدام الأجهزة (المادة 11)،

- التزوير (المادة 12)،

- السرقة أو الاحتيال (المادة 13)،

- الإعتداء الجنسي على الأطفال واستغلالهم (المادة 14)،

- الإستدراج الجنسي للأطفال (المادة 15)،

- النشر غير الرضائي للصور الحميمة (المادة 16)،

- غسل العائدات الإجرامية (المادة 17) [1]

2-التدابير الإجرائية (الفصل الرابع)

يشمل هذا القسم الصلاحيات الإجرائية الممنوحة لجهات إنفاذ القانون، لا سيما في مجال جمع الأدلة الإلكترونية ضمن التحقيقات الجنائية، مع التأكيد على ضرورة حماية حقوق الإنسان والحريات العامة، كما يتضمّن أحكامًا خاصة بحماية الشهود ومساعدة الضحايا.

3-الإختصاص القضائي (الفصل الثالث)

تحدد المادة 22 معايير تحديد الإختصاص القضائي، وتشير الفقرة الخامسة إلى ضرورة التنسيق بين الدول المعنية في حال وجود تحقيقات متزامنة حول نفس الجريمة.

(1)- إتفاقية الأمم المتحدة لمكافحة الجريمة السيبيرانية ، مقال منشور في موقع الأمم المتحدة: مكتب الأمم المتحدة المعني بالمخدرات والجريمة .

4-التعاون الدولي (الفصل الخامس)

توفر الاتفاقية إطارًا قانونيًا لتبادل الأدلة الرقمية، وتقديم المساعدة القضائية المتبادلة، ونقل الإجراءات، وتسليم المطلوبين، كما تنص على إنشاء نقطة اتصال وطنية تعمل على مدار الساعة (7/24) لتسهيل التعاون في التحقيقات الجنائية، ولا يقتصر نطاق هذا التعاون على الجرائم المنصوص عليها فقط، بل يشمل أيضًا الجرائم الخطيرة التي يُعاقب عليها بأربع سنوات أو أكثر.

5-التدابير الوقائية (الفصل السادس)

يتناول هذا الفصل السياسات والإجراءات التي ينبغي للدول تبنيها للوقاية من الجرائم السيبرانية والحد من إنتشارها.

6-بناء القدرات والمساعدة التقنية (الفصل السابع)

يُعد هذا القسم من أهم مكونات الاتفاقية، حيث يؤكد على ضرورة تقديم الدعم الفني وبناء القدرات للدول، لا سيما النامية منها، لمواجهة التهديدات السيبرانية بشكل فعّال، ومن المتوقع أن يلعب مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) دورا محوريا في تنفيذ هذه المبادرات[1]

وقد أكد رئيس الجمعية العامة للأمم المتحدة، فيليمون يانغ، أن "العالم الرقمي يحمل إمكانيات كبيرة للتنمية، لكنه يشكل في الوقت ذاته تهديدًا متزايدًا نتيجة الجرائم السيبرانية." وأشار إلى أن إعتماد هذه الإتفاقية يمثل خطوة مهمة في سبيل تعزيز التعاون الدولي، ومنع الجرائم الإلكترونية، وحماية الأفراد وحقوقهم في البيئة الرقمية.

(1)- ميتيهان دورماز ، المرجع نفسه ، ص 04.

الفرع الثالث : قرارات وتوصيات الجمعية العامة والمجلس الإقتصادي والإجتماعي ذات الصلة بالعنف السيبراني

ساهمت منظمة الأمم المتحدة، إلى جانب عدد من المنظمات الدولية المعنية بتكنولوجيا المعلومات، في صياغة إستراتيجيات لمجابهة العنف السيبراني عبر إصدار اتفاقيات دولية وتوصيات وقرارات صادرة عن مؤتمرات دولية. نعرض فيما يلي أبرز هذه الجهود.[1]

أولا: المؤتمر الثامن للأمم المتحدة لمنع الجريمة ومعاملة المجرمين هافانا 1990.

أصدر هذا المؤتمر قرارًا خاصًا بالجرائم المرتبطة بالحاسوب، تضمن عددا من التوصيات الجوهرية لمواجهة العنف السيبراني، أبرزها:

-تحديث التشريعات والإجراءات الجنائية بما يسمح بسلطات تحقيق مناسبة وقبول الأدلة الإلكترونية أمام القضاء.[2]

-تبني آليات خاصة بالتحقيق وجمع الأدلة لمواكبة طبيعة الجرائم السيبرانية.

-مصادرة واسترجاع الأصول المتأتية من الجرائم الإلكترونية.

-حماية حقوق ومصالح ضحايا الجرائم السيبرانية.[3]

-التعاون مع المنظمات المعنية لوضع قواعد أخلاقية لاستخدام أجهزة الحاسوب وتحديد مسؤولية مزودي خدمات الأنترنت.

---

(1)-رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية، الطبعة1 ، دار النهضة العربية، القاهرة ، 2011 ، ص210 .

(2)-رامي متولي القاضي ، المرجع نفسه ، ص212 .

(3)-بيدي آمال، "جهود الأمم المتحدة في مكافحة الجريمة السيبرانية" ، مجلة البحوث في الحقوق والعلوم السياسية ، جامعة الجلفة ، مجلد 08 ،العدد 1 ، الجزائر، 2022، ص 305 .

ثانيا- المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ريو دي جانيرو 1994 ، جاءت أبرز توصيات هذا المؤتمر في شقين: الموضوعي والإجرائي

1- في الشق الموضوعي

أوصى المؤتمر بضرورة تجريم الأفعال التالية ضمن قائمة الحد الأدنى للعنف السيبراني:

-الإحتيال والغش المعلوماتي.

-التزوير المعلوماتي.

-الإضرار بالبيانات والبرامج.

-تخريب أو إتلاف نظم المعلومات.

-الدخول غير المشروع والاعتراض غير المرخص[1].

2-في الشق الإجرائي

-ضمان حماية حقوق الإنسان وحرمة الحياة الخاصة في بيئة تكنولوجيا المعلومات[2].

-ضرورة تقنين صلاحيات السلطات العامة بدقة في ما يتعلق بالتفتيش والضبط الرقمي.

-تحديد الجهات المخولة قانونًا بإجراء عمليات الضبط والتحقيق.

-تفعيل التعاون بين الضحايا والشهود وسلطات التحقيق.

-السماح بإستخدام الأدلة المستخرجة من داخل نظم الكمبيوتر أمام المحاكم وفق ضوابط قانونية دقيقة[3].

ثالثا: المؤتمر الثاني عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية سلفادور، البرازيل 2010

تضمن هذا المؤتمر دعوة الدول إلى:

---

(1)-بيدي آمال ، المرجع نفسه ، ص306 .

(2)-بيدي آمال ، المرجع نفسه ، ص307

(3)- على حسن الطوالبة ، المرجع السابق ، ص112 .

-بناء قدراتها الوطنية للتصدي للعنف السيبراني.

-تعزيز التعاون الدولي وتبادل المعلومات حول التشريعات والتجارب الوطنية.

-تشجيع التنسيق مع القطاع الخاص وتقديم الدعم التقني المتخصص[1]

رابعا : المؤتمر الثالث عشر للأمم المتحدة – الدوحة، قطر 2015

أوصى هذا المؤتمر بما يلي:

- تطوير أدوات وبرامج فعالة لمكافحة ومنع العنف السيبراني.

-تعزيز التعاون بين الهيئات الرسمية والفرق الأكاديمية في المجالات التقنية.

-إشراك القطاع الخاص كشريك أساسي في جهود المكافحة.

-دراسة إمكانية إعداد اتفاقية دولية حول الجريمة السيبرانية.

- إصدار دليل إرشادي حول العنف السيبراني يشمل تعريفه، أنواعه، وأبرز التحديات المرتبطة به، مع إمكانية تعديله دوريًا لمواكبة التطورات.[2]

خامسا: قرارات الجمعية العامة للأمم المتحدة

1-القرار رقم 146/73، المتعلق بالاتجار بالنساء والفتيات

من بين القرارات التي إعتمدتها الجمعية العامة للأمم المتحدة في سياق معالجة أشكال العنف السيبراني، يُمكن الإشارة على سبيل المثال إلى القرار رقم 146/73 الصادر بتاريخ 17 ديسمبر 2018 بشأن الاتجار بالنساء والفتيات، والذي تضمّن إشارة صريحة إلى تنامي ظاهرة العنف ضد النساء في الفضاء الرقمي. وقد عبّر القرار عن القلق البالغ إزاء الاستغلال الجنسي عبر الوسائل التكنولوجية الحديثة، ولا سيما تلك التي تستهدف النساء

(1)-يبدي أمال ، المرجع السابق، ص310.

(2)-مكتب الأمم المتحدة المعني بالمخدرات WW.UNODC.ORG، تاريخ الاطلاع 2025/05/02 ، ص27 .

والفتيات من خلال إنتاج وتوزيع محتوى مسيء وغير مشروع، مؤكدًا بذلك على ضرورة تعزيز التدابير الوقائية والحماية القانونية في هذا المجال.[1]

كما أكد القرار على خطورة الإعتداءات والإستغلالات الجنسية التي تطال الأطفال في الفضاء الرقمي، لما تشكله من إنتهاك صارخ لحقوقهم الأساسية، وفي مقدمتها الحق في الكرامة والسلامة الجسدية والنفسية، داعيًا إلى تعزيز التدابير القانونية والمؤسساتية الكفيلة بمنع هذه الأفعال ومكافحتها.

وقد جددت الدول الأعضاء، من خلال هذا القرار، إلتزامها الكامل بأحكام القانون الدولي، لا سيما القانون الدولي لحقوق الإنسان، مشددة على أهمية تبني نهج وقائي ومتكامل يضمن الحماية الفعالة للضحايا، عبر سن تشريعات مناسبة، وتطوير آليات للرصد والإبلاغ، ومساءلة مرتكبي هذه الإنتهاكات.

كما سلط القرار الضوء على العلاقة الوثيقة بين الاستغلال الجنسي عبر الوسائط الرقمية والإتجار بالبشر، لاسيما فيما يخص النساء والفتيات لأغراض الاستغلال الجنسي، داعيًا إلى تعزيز التنسيق والتعاون بين الدول، وتبادل الخبرات وأفضل الممارسات، ودعم الجهود الوطنية والدولية الرامية إلى مكافحة هذه الجرائم، بما يشمل إعادة تأهيل ودمج الضحايا، وملاحقة الجناة ومعاقبتهم وفقًا لمبادئ العدالة الجنائية

2-قرار مجلس حقوق الإنسان رقم 51/10 المتعلق بمكافحة التنمر السيبراني

يشكل هذا القرار الذي تم إعتماده في 6 أكتوبر 2022، خطوة متقدمة في اتجاه الإعتراف الدولي الرسمي بخطورة ظاهرة التحرش والتنمر الإلكتروني(Cyberbullying) ، ولاسيما ما

(3)-الجمعية العامة، القرار رقم 146/73، المتعلق بالاتجار بالنساء والفتيات، لتاريخ 12 ديسمبر 2018، وثيقة الأمم المتحدة رقم: A/RES/73/146 ، ص 05.

تُخلّفه من آثار سلبية على الأطفال والفئات الهشة في المجتمع، وقد استند هذا القرار إلى المبادئ الجوهرية للقانون الدولي لحقوق الإنسان، لاسيما ما يتعلق منها بحماية حقوق الطفل، وحرية التعبير، والحق في السلامة الجسدية والنفسية.[1]

يُعرّف القرار ظاهرة التحرش الإلكتروني بأنها كل سلوك عدائي أو مسيء يمارس بشكل متعمد عبر الإنترنت أو وسائط الاتصال الرقمية، ويهدف إلى إلحاق الضرر النفسي أو الاجتماعي بالضحية. وقد أشار القرار إلى أن هذه الظاهرة تخلّف آثارًا عميقة على المستوى النفسي والعاطفي، مثل القلق، وتدني احترام الذات، والشعور بالعزلة، وقد تصل في بعض الحالات إلى التفكير في الانتحار، لاسيما بين الأطفال والمراهقين.

وفي هذا السياق، دعا المجلس الدول الأعضاء إلى تبني نهج شامل وتكاملي لمواجهة هذه الظاهرة المتنامية، وذلك من خلال إتخاذ تدابير تشريعية مناسبة لحماية الأفراد، لا سيما الأطفال، من العنف السيبراني، وتطوير آليات فعالة للرصد والإبلاغ، وتقديم الدعم النفسي والإجتماعي للضحايا، كما شدد القرار على أهمية إدراج التثقيف الرقمي والأمان الإلكتروني في المناهج التعليمية، بغرض رفع الوعي وتمكين الأطفال والشباب من التعامل الآمن مع الفضاء الرقمي[2]

من جهة أخرى، حث القرار شركات التكنولوجيا والمنصات الرقمية على الإضطلاع بمسؤولياتها الأخلاقية والقانونية، عبر تبني سياسات واضحة للوقاية من التحرش الإلكتروني، وتوفير أدوات فعالة للإبلاغ عن الانتهاكات، وضمان الإستجابة السريعة لحماية الضحايا ومعاقبة الجناة.

([1])-الجمعية العامة، مجلس حقوق الإنسان،" مكافحة التنمر السبيراني"، قرار رقم 51/10، لتاريخ 6 أكتوبر 2022، وثيقة الجمعية العامة : A/HRC/RES/51/10

(1)-قرار مجلس حقوق الإنسان رقم 51/10 ،المرجع نفسه ص08.

كما أكد المجلس على أهمية تعزيز التعاون الدولي والتنسيق متعدد الأطراف، بما يشمل الدول، والهيئات الأممية، والمنظمات غير الحكومية، والقطاع الخاص، من أجل تبادل الخبرات وأفضل الممارسات، وتوحيد الجهود للحد من هذه الظاهرة العابرة للحدود. ودعا المجلس مفوضية الأمم المتحدة السامية لحقوق الإنسان إلى جمع وتحليل البيانات المتعلقة بآثار التحرش الإلكتروني، وإعداد تقارير دورية تقيّم مدى استجابة الدول، وتقديم توصيات علمية قائمة على الأدلة.

يمثل هذا القرار تحوّلاً نوعياً في التعاطي مع العنف الرقمي بوصفه قضية حقوق إنسان بامتياز، ويتطلب تضافر الجهود التشريعية والتربوية والتكنولوجية والاجتماعية لمواجهته ويعكس القرار التزام المجتمع الدولي بحماية الفضاء الرقمي من أن يتحول إلى بيئة خصبة لانتهاك الكرامة الإنسانية، خاصة في ظل الإنتشار الواسع لاستخدام الإنترنت بين الأطفال والشباب، كما يسلّط الضوء على ضرورة وضع إستراتيجيات وطنية متكاملة تراعي الخصوصيات الثقافية والإجتماعية، وتستند إلى المعايير الدولية في مجال حقوق الإنسان.

المطلب الثاني: دور الأجهزة الدولية الأخرى في تعزيز الحماية ضد العنف السيبراني

لم تعد الإتفاقيات الدولية الخاصة بمكافحة العنف السيبراني كافية بمفردها لمواجهة التحديات المتزايدة لهذا النوع من الجرائم، فقد أدرك المجتمع الدولي، بما في ذلك المنظمات الدولية الحكومية، ضرورة تبني مقاربة متعددة الأطراف تشمل تدابير وإجراءات عملية لتعزيز التعاون الدولي لمكافحة العنف السيبراني، وفي هذا السياق، كان للأجهزة الدولية، وفي مقدمتها المنظمات الدولية المتخصصة التي لها علاقة بالفضاء السيبراني (الفرع الأول)،بالإضافة إلى الدور المحوري لجهاز الشرطة الجنائية الدولية "الإنتربول" (الفرع الثاني).

الفرع الأول: دور المنظمات الدولية المتخصصة في مكافحة العنف السيبيراني

تعتبر منظمة التعاون الاقتصادي والتنمية والاتحاد الدولي للإتصالات التابعين لمنظمة الأمم المتحدة، من أهم المنظمات الدولية المتخصصة في مجال الفضاء الرقمي، والتي سنتطرق إلى مجهوداتها في مجال مواجهة ظاهرة العنف الرقمي.

أولا : منظمة التعاون الاقتصادي والتنمية(oecd)

تعد منظمة التعاون الاقتصادي والتنمية من أبرز المنظمات التي ساهمت في إرساء قواعد قانونية دولية لمكافحة الجرائم المرتبطة بإستخدام تكنولوجيا المعلومات، خاصة فيما يتعلق بحماية الخصوصية ومكافحة إساءة إستخدام النظم المعلوماتية، وسيتم في هذا المطلب إستعراض الأسس القانونية التي أرستها المنظمة منذ السبعينيات، وكذلك المبادئ التوجيهية التي تبنتها في مجال الأمن السيبراني.[1]

تأسست منظمة التعاون الإقتصادي والتنمية بهدف تعزيز النمو الاقتصادي والتنمية الاجتماعية المتناغمة ، وقد بدأت منذ عام 1978 بالإهتمام بالقضايا المرتبطة باستخدام الحاسوب، حيث أصدرت عدة أدلة وقواعد تتعلق بحماية البيانات ومكافحة الجرائم السيبرانية. من أهم هذه المبادرات:

- دليل حماية الخصوصية ونقل البيانات (1980): يعد من أوائل الوثائق القانونية الدولية في هذا المجال، وقد أوصت المنظمة الدول الأعضاء بالامتثال له[2]
- تقرير الجرائم المرتبطة بالحاسوب (1983): قدم تحليلاً للسياسات الجنائية المتبعة في الدول الأعضاء، وحدد الحد الأدنى من الأفعال الواجب تجريمها، ومنها:
- الدخول غير المصرح به إلى نظم الحواسيب.

(1)–يوسف حسن يوسف ، الجرائم الدولية للأنترنت، المركز القومي للإصدارات، القاهرة، 2011، ص 99 .

(2)–قطاف سليمان، بوقرين عبد الحليم، المرجع السابق ،ص69.

-إفشاء المعلومات الإلكترونية دون إذن.

-إتلاف أو تخريب البيانات المخزنة.

-تعطيل أو حجب الوصول إلى البرمجيات والمعلومات[1]

- تقرير الجرائم المرتبطة بالحاسوب (1983): قدم تحليلاً للسياسات الجنائية المتبعة في الدول الأعضاء، وحدد الحد الأدنى من الأفعال الواجب تجريمها، ومنها:

الدخول غير المصرح به إلى نظم الحواسيب.

-إفشاء المعلومات الإلكترونية دون إذن.

-إتلاف أو تخريب البيانات المخزنة.

-تعطيل أو حجب الوصول إلى البرمجيات والمعلومات.[2]

ثانيا : الإتحاد الدولي للاتصالات(ITU)

يمثل الإتحاد الدولي للاتصالات الهيئة الأممية المختصة في قطاع الإتصالات وتكنولوجيا المعلومات، وقد إضطلع بدور محوري في دعم الجهود العالمية لمكافحة الجرائم السيبرانية، من خلال تطوير المعايير التقنية وتعزيز قدرات الدول في هذا المجال، وسنتناول التعريف به، ثم بيان جهوده في مكافحة العنف السيبراني.[3]

1-ماهية الإتحاد

الإتحاد الدولي للإتصالات هو وكالة متخصصة تابعة للأمم المتحدة، يضم في عضويته 194 دولة، إضافة إلى أكثر من 1000 مؤسسة من القطاعين العام والخاص، من جامعات، ومنظمات إقليمية، وهيئات تقنية.

(1)-قطاف سليمان، بوقرين عبد الحليم، المرجع نفسه، ص70.

(2)-قطاف سليمان، بوقرين عبد الحليم ،المرجع نفسه ، ص72.

(3)- العبيدي عمر عباس خضير ،الإرهاب الالكتروني في نطاق القانون الدولي ، رسالة ماجيستر، كلية الحقوق ، جامعة تكريت ، العراق ، 2019 ،ص101

يعمل الإتحاد على تطوير وتنسيق المعايير التقنية والبنية التحتية الرقمية حول العالم، ويغطي نشاطه مجالات متعددة تشمل: الإتصالات السلكية واللاسلكية، شبكات النطاق العريض، تكنولوجيا المعلومات، الأقمار الصناعية، الملاحة الجوية، الأمن السيبراني، والتقنيات الناشئة.

يمتلك الإتحاد شبكة من 11 مكتبًا إقليميًا تغطي مختلف القارات، منها مكتب القاهرة للدولالعربية، وأديس أبابا لإفريقيا، وبانكوك لآسيا، وموسكو لأوروبا، وبرازيليا للأمريكيتين.[1]

2-دور الإتحاد في مكافحة العنف السيبراني

على الرغم من أن مكافحة العنف السيبراني لا تقع ضمن المهام الأساسية للإتحاد، إلا أن دوره يظل مهمًا في هذا الإطار، وذلك من خلال:

-تطوير المعايير التقنية المرتبطة بأمن المعلومات.[2]

-إصدار دليل إلكتروني مشترك بالتعاون مع الوكالة الأوروبية لأمن الشبكات والمعلومات، لوضع خارطة طريق متكاملة حول المعايير الأمنية في مجال تكنولوجيا المعلومات.

-تمكين الدول الأعضاء من الوصول إلى قواعد بيانات حديثة تساعد على مواكبة التحديات الأمنية الجديدة.

-بناء القدرات من خلال برامج تدريب ودعم فني للدول النامية.[3]

الفرع الثاني : منظمة الأنتربول

(1)-موقع الأمم المتحدة بجنيف، دورالإتحاد الدولي للإتصالات في مجابهة الإجرام السيبيرانيwww. ungeneva.org

(2)-فهد عبد الله العبيد العازمي، المرجع نفسه ، ص 662 .

(3)-فهد عبد الله العبيد العازمي ، المرجع نفسه ، ص 663 .

يشكل الأنتربول، أو "المنظمة الدولية للشرطة الجنائية"، أحد أبرز آليات التعاون الدولي في مواجهة الجرائم العابرة للحدود، وعلى وجه الخصوص الجرائم السيبرانية، وتكمن المهمة الأساسية لهذه المنظمة في تعزيز التنسيق بين أجهزة الشرطة التابعة للدول الأعضاء، من خلال تبادل المعلومات والبيانات ذات الصلة بالأنشطة الإجرامية، وسنتناول في هذا السياق عنصرين رئيسيين:ماهيةالأنتربول، وإستراتيجيته في مكافحة العنف السيبراني.

أولا : ماهية الأنتربول

يشكل الإنتربول، أو "المنظمة الدولية للشرطة الجنائية"، أحد أبرز آليات التعاون الدولي في مواجهة الجرائم العابرة للحدود، وعلى وجه الخصوص الجرائم السيبرانية، وتكمن المهمة الأساسية لهذه المنظمة في تعزيز التنسيق بين أجهزة الشرطة التابعة للدول الأعضاء، من خلال تبادل المعلومات والبيانات ذات الصلة بالأنشطة الإجرامية، وسنتناول في هذا السياق عنصرين رئيسيين: ماهية الأنتربول، وإستراتيجيته في مكافحة العنف السيبراني.[1]

وقد أولت المنظمة في السنوات الأخيرة إهتمامًا خاصًا بمكافحة الجريمة المنظمة والأنشطة ذات الصلة، كغسل الأموال، عبر إنشاء وحدة تحليل المعلومات الجنائية، التي تعنى بإستخلاص وتحليل البيانات المتعلقة بالمنظمات الإجرامية، وإتاحتها للدول الأعضاء.[2]

وإستنادا إلى المادة (08) من ميثاق المنظمة، فإن الإنتربول يهدف إلى:

-جمع المعلومات المتعلقة بالجرائم والمجرمين، من خلال البيانات التي ترد من المكاتب المركزية الوطنية عبر شبكة اتصالات حديثة وآمنة.

(1)-يوسف حسن يوسف ، المرجع السابق ، ص 110 .

(2)-عادل عبد العالي إبراهيم خراشي ، المرجع السابق، ص26 .

-التعاون في ضبط المطلوبين دوليًا، سواءً من صدرت بحقهم أحكام قضائية، أو أوامر بالضبط والإحضار، وذلك عبر إصدار نشرات دولية.

-دعم جهود الشرطة في ميدان التحقيقات الجنائية، لا سيما في ما يتعلق بالبصمات الوراثية (DNA) والأدلة الفنية.

-تعزيز التعاون الشرطي الدولي في نطاق القوانين الوطنية، وبما يتوافق مع مبادئ الإعلان العالمي لحقوق الإنسان.[1]

ثانيا: إستراتيجيات الأنتربول في مكافحة العنف السيبيراني

في إطار تصاعد التهديدات الإلكترونية، أنشأ الإنتربول سنة 2004 وحدة متخصصة لمكافحة الجريمة السيبرانية، كما تعاون مع مجموعة الدول الثماني(G8) لتطوير إستراتيجيات حديثة للتصدي لهذا النوع من الجرائم، من خلال:

-إستخدام أدوات تقنية متقدمة، مثل قاعدة البيانات المركزية للصور الإباحية للأطفال، والتي يتم تحليلها باستخدام برنامج Excalibur للتعرف الآلي على الأنماط.

-إعداد أدلة تدريبية وإرشادية لأجهزة الشرطة حول كيفية التحقيق في الجرائم السيبرانية وأساليب مكافحتها.[2]

-تصنيف التهديدات السيبرية حسب الأولوية، بالتنسيق مع الشركاء من القطاع الخاص في مجال الأمن السيبراني، لتوفير معلومات محدثة تسهم في إتخاذ قرارات إستباقية.[3]

كما أطلق الأنتربول منصتين إلكترونيتين لتسهيل التنسيق ومشاركة المعلومات:

1-منصة تبادل المعارف المتعلقة بالجريمة السيبرية

(1)-عادل عبد العال إبراهيم خراشي ، المرجع نفسه ، ص27 .

(2)-نبيلة هبةهروال،الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دارالفكر العربي،الإسكندرية،2008 ، ص105 .

(3)-موقع الأنتربول ، www.interpol.int

وهي مساحة تفاعلية لتبادل المعلومات العامة غير الشرطية، مفتوحة لأجهزة إنفاذ القانون، والمنظمات الدولية، والحكومات، وخبراء الأمن السيبراني، وتهدف هذه المنصة إلى تعزيز التعاون المعرفي الدولي، ومناقشة أحدث الاتجاهات والتقنيات في التحقيق في الجرائم السيبرانية.[1]

2- منصة التعاون لمكافحة الجريمة السيبرية – العمليات-

تُعد هذه المنصة أول مركز عمليات إلكتروني من نوعه، وهي مخصصة لتنسيق العمليات الميدانية على المستوى العالمي، وتتيح للجهات الأمنية تبادل المعلومات الإستخباراتية بشكل آمن، مما يسهم في تحسين الفعالية الميدانية، وتوجيه الموارد بشكل أكثر كفاءة.[2]

03-المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرانية

أنشأ الأنتربول مركزا متخصصا يضم خبراء من أجهزة إنفاذ القانون والقطاع الخاص، يهدف إلى تحليل البيانات السيبرية، واستخلاص معلومات إستخباراتية قابلة للتحول إلى إجراءات عملية، وقد أصدر هذا المركز، منذ عام 2017، أكثر من 800 تقرير موجَّه إلى قوات الشرطة في أكثر من 150 دولة، تناولت تهديدات سيبرية مثل البرمجيات الخبيثة، التصيّد الإحتيالي، إختراق المواقع الحكومية، وأساليب الإحتيال الإجتماعي.[3]

4-برامج التدريب والتطوير

ينظم الأنتربول برامج تدريبية دورية لضباط الشرطة وخبراء تنفيذ القانون، تركز على التحليل الجنائي، وجمع المعلومات، وتوظيف قواعد البيانات المتخصصة مثل تلك الخاصة

(1)-موقع الأنتربول ،المرجع نفسه، www.interpol.int

(2)- موقع الأنتربول ،المرجع نفسه، www.interpol.int

(3)- موقع الأنتربول ،المرجع نفسه، www.interpol.int

بالبصمات والصور ووثائق الهوية، بهدف دعم قدرات الدول الأعضاء في التعامل مع التهديدات السيبرانية المعاصرة.[1]

المبحث الثاني: التكامل بين الآليات الأوروبية مع الجهود الدولية لمكافحة العنف السيبراني

تُعدّ القارة الأوروبية من أكثر النماذج تطورًا على مستوى العالم في مجال مكافحة الجريمة المنظمة العابرة للحدود، وذلك نتيجةً لتراكم عوامل موضوعية ومؤسساتية متعددة. فقد نجحت أوروبا، من خلال إزدواجية البُنى المؤسسية المتمثلة في كلٍّ من مجلس أوروبا والاتحاد الأوروبي، في إرساء منظومة متكاملة لمواجهة العنف السيبراني، وهو ما منحها موقع الريادة في هذا المجال على المستوى الدولي.

وقد أفضى هذا التقدّم المؤسساتي والقانوني إلى جعل التجربة الأوروبية مرجعًا يُحتذى به ومحل إهتمام متزايد من قبل عدد كبير من دول العالم، الراغبة في الاستفادة من الآليات الأوروبية في مواجهة التحديات السيبرانية المتصاعدة، وفي هذا الإطار، بذلت الدول الأوروبية جهودًا ملحوظة عبر آليتين أساسيتين: أولًا، من خلال وضع أطر قانونية متقدمة لمكافحة العنف السيبراني(المطلب الأول)،وثانيًا،من خلال تطوير مؤسسات متخصصة(المطلب الثاني)، وعلى رأسها الوكالة الأوروبية للأمن السيبراني، كما اتجهت أوروبا إلى تعزيز شراكاتها الدولية من أجل توسيع نطاق التعاون في هذا المجال على المستوى العالمي(المطلب الثالث)

المطلب الأول :الإطار القانوني الأوروبي لمكافحة العنف السيبراني

(1)–فهد عبد الله العبيد العازمي ، المرجع السابق، ص256 .

يمثل كل من مجلس أوروبا والإتحاد الأوروبي الإطارين المؤسسيين الرئيسيين في القارة الأوروبية في مجال مكافحة العنف السيبراني، ورغم إشتراكهما في بعض الأهداف، فإن لكل منهما طبيعة قانونية مختلفة؛ فمجلس أوروبا هو منظمة دولية تأسست عام 1949، وتضم 47 دولة، ويهدف إلى تعزيز حقوق الإنسان والديمقراطية وسيادة القانون، أما الاتحاد الأوروبي، فهو تكتل سياسي وإقتصادي يضم عدداً من الدول الأوروبية ويهدف إلى تعميق التكامل بين أعضائه.

وقد إضطلعت المؤسستان، كل في نطاق صلاحياته، بوضع أدوات قانونية لمكافحة العنف السيبراني، من أبرزها: اتفاقية بودابست لعام 2001 بشأن الجريمة السيبرانية، والتي أقرها مجلس أوروبا (الفرع الأول)، إلى جانب التوصيات والتوجيهات الصادرة عن كل من مجلس أوروبا والإتحاد الأوروبي لتعزيز التشريعات الوطنية والتعاون الدولي في هذا المجال (الفرع الثاني).

الفرع الأول: إتفاقية بودابست لمكافحة الجرائم السيبرانية 2001

جاءت إتفاقية بودابست تتويجا للجهود التي بذلها الإتحاد والمجلس الأوروبيمن أجل صيغة قانونية لمكافحة العنف السيبيراني،وهي تعد حاليا الإطار المرجعي لمواجهة الجريمة السيبيرانية، وقد عرفت هذه الاتفاقية ظروف سابقة على نشأتها (أولا)، وقد تضمنت احتكام موضوعية وإجرائية خاصة بمكافحة العنف السيبراني (ثانيا).

أولاً: نشأة الإتفاقية

تُعد إتفاقية بودابست لعام 2001 أول معاهدة دولية ملزمة تتناول بشكل شامل مكافحة الجرائم المعلوماتية والجرائم المرتكبة عبر الأنترنت، أعدّ مجلس أوروبا هذه الإتفاقية وتم فتح

باب التوقيع عليها في 23 نوفمبر 2001 بالعاصمة المجرية بودابست، ودخلت حيز النفاذ في يوليو 2004.[1]

صادقت على الإتفاقية 30 دولة في بادئ الأمر، بينما إمتنعت بعض الدول مثل إيرلندا والدانمارك عن المصادقة، ومن اللافت أن دولاً غير أوروبية أيضاً إنضمت إليها، مثل الولايات المتحدة وكندا واليابان وجنوب إفريقيا، ما يعكس البُعد العالمي للإتفاقية وأهميتها في وضع معايير مشتركة لمكافحة الجريمة السيبرانية.[2]

لقد شكلت الإتفاقية أو لمحاولة لمعالجة مشكلة تزايد العنف السيبراني، وكان الهدف الرئيسي منها، هو وضع سياسة جزائية مشتركة لمكافحة الجرائم السيبرانية، عن طريق موائمة القوانين الوطنية لضمان توفير الحماية الكافية للمجتمع الأوروبي من هذا النوع من الجرائم[3]

كما تهدف الإتفاقية إلى مواءمة التشريعات الوطنية للدول الأطراف، ووضع سياسة جنائية موحدة لمكافحة الجرائم الإلكترونية، وتيسير التعاون الدولي في مجال التحقيقات والملاحقة القضائية.

ثانيا : مضمون الاتفاقية

وقد تضمنت الاتفاقية 48 مادة موزعة على أربعة أقسام كما يلي :[4]

-القسم الأول: تعريف المصطلحات والمفاهيم الأساسية.

-القسم الثاني: إلتزامات الدول بشأن تعديل تشريعاتها الوطنية لتجريم أنواع معينة من الأفعال الإلكترونية.

---

(1)- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجيستر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013 ، ص100 .

(2)-قطاف سليمان، بوقرين عبد الحليم، المرجع السابق ،ص 80

(3)-عادل عزام سقف الحيط ، المرجع السابق، ص365 .

(4)-عادل عزام سقف الحيط ، المرجع نفسه ، ص366 .

-القسم الثالث: التعاون الدولي، ويتضمن أحكاماً بشأن تسليم المجرمين والمساعدة القضائية المتبادلة.

-القسم الرابع: الأحكام الختامية المتعلقة بالتصديق و الإنضمام و الإنسحاب.

من بين الجرائم التي تلزم الاتفاقية الدول الأعضاء بتجريمها:

-الدخول غير المشروع إلى الأنظمة المعلوماتية (اختراق الحواسيب).

-الإعتراض غير المشروع للمراسلات والبيانات.

-التعديلات غير المصرح بها على البيانات أو تعطيل الأنظمة.

-الإحتيال المعلوماتي و إنتحال الهوية الإلكترونية.

-الجرائم ذات الطابع الأخلاقي، مثل إنتاج أو نشر أو حيازة صور إستغلال الأطفال جنسياً.

-إنتهاك حقوق الملكية الفكرية عبر نسخ أو توزيع المواد المحمية دون إذن.[1]

- ضرورة التعاون الدولي لجمع الأدلة الإلكترونية وملاحقة مرتكبي الجرائم السيبرانية.[2]

-المساعدة القضائية المتبادلة وتيسير سبل تبادل المعلومات والإستجابة العاجلة لطلبات المساعدة.[3]

-تعيين نقطة إتصال دائمة (7/24) لتيسير التعاون والتحقيقات العاجلة بين الدول الأطراف.[4]

-ضمانات قانونية لحماية خصوصية الأفراد وحقوقهم أثناء إنفاذ الإتفاقية.[5]

وتُعد هذه الاتفاقية اليوم حجر الأساس لأي سياسة جنائية أوروبية فعالة لمكافحة الجرائم السيبرانية ذات الطابع العابر للحدود.[6]

---

(1)- قطاف سليمان، بوقرين عبد الحليم، المرجع السابق، ص82 .

(2) Brown , Jack,jurisdiction to proscute Crimes , commited by use of the interne , 38 jurimetrics , 1998 , p 611

(3)-أسامة بن غانم العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، مجلة الحقوق، العدد 4، المملكة العربية السعودية، 2015 ، ص145 .

(4)-أسامة بن غانم العبيدي، المرجع السابق، ص146 .

(5):Brown , Jack, of.cit , p 613.

الفرع الثاني :التوصيات والتوجيهات الصادرة عن مجلس أوروبا والإتحاد الأوروبي

نظراً للطابع الديناميكي والمتطور للعنف السيبراني، لم تقتصر جهود مجلس أوروبا والإتحاد الأوروبي على الإتفاقيات الملزمة، بل شملت أيضاً إصدار توجيهات وتوصيات لتوجيه السياسات الوطنية للدول الأعضاء وتحديث التشريعات والإجراءات القضائية لمواكبة التحديات الجديدة.

أولا : توصيات مجلس أوروبا

أصدر مجلس أوروبا التوصية رقم R(95)13 بتاريخ 11 سبتمبر 1995، بشأن التعديلات الواجب إدخالها على الإجراءات الجزائية لمواكبة تكنولوجيا المعلومات، من أبرز ما تضمنته:

-تمكين سلطات التحقيق من تفتيش أجهزة الحاسوب وضبط البيانات الرقمية المخزنة أو الجارية.

-توسيع نطاق التفتيش ليشمل أنظمة مرتبطة بالشبكة محل التحقيق، متى كان ذلك ضرورياً.[1]

-السماح بالمراقبة الإلكترونية (التنصت أو تسجيل البيانات) وفق ضمانات قانونية صارمة.

-التعاون الإجباري من مزودي الخدمة مع سلطات التحقيق.[2]

-الإعتراف بالأدلة الرقمية في الإجراءات القضائية، ومعاملتها بنفس قواعد الأدلة التقليدية.

---

(6)-أحمد هلالي عبد اللاه احمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية ، دار النهضة العربية، القاهرة ، 2008 ، ص298 .

(1)-قطاف سليمان، وقرين عبد الحليم، المرجع السابق ، ص8.

(2)-أحمد هلالي عبد اللاه أحمد ، المرجع السابق ، ص300 .

-إنشاء وحدات مختصة بجرائم الحاسوب وتدريب القضاة والضباط في مجال التكنولوجيا.

-تنظيم التعاون الدولي من خلال اتفاقيات تتيح التدخل العاجل عندما تمتد آثار الجريمة خارج حدود الدولة.[1]

ثانيا : توجيهات الاتحاد الأوروبي (Directives)

أصدر الإتحاد الأوروبي عدة توجيهات تشريعية في هذا المجال، من بينها:

- التوجيه EU/40/2013 المتعلق بمكافحة الهجمات على نظم المعلومات.

- التوجيه 1148/2016 (NIS Directive) بشأن أمن الشبكات ونظم المعلومات، والذي ألزم الدول الأعضاء بوضع استراتيجيات وطنية وتعزيز التعاون السيبراني بين الهيئات[2]

- اللائحة العامة لحماية البيانات (GDPR) لسنة 2016، التي لها بعد مهم في الحد من العنف السيبراني المتعلق بالانتهاكات الخصوصية.[3]

الفرع الثالث : دور الوكالة الأوروبية للأمن السيبراني في مكافحة العنف السيبراني

يعمل الإتحاد الأوروبي على عدة جبهات لتعزيز المرونة السيبرانية، إذ تهدف إستراتيجية الأمن السيبراني للإتحاد الأوروبي إلى بناء القدرة على الصمود في وجه العنف والتهديدات السيبرانية، وضمان إستفادة المواطنين والشركات من تكنولوجيات رقمية موثوقة وآمنة، وفي هذا السياق، قام الاتحاد الأوروبي بإنشاء هيئة متخصصة في هذا المجال، وهي الوكالة الأوروبية للأمن السيبراني.

أولا : ماهية الوكالة الأوربية للأمن السيبراني

(1)-أسامة بن غانم العبيدي ، المرجع السابق، صفحة نفسها.

(2)- الزهراني شيخة حسين، "التعاون الدولي في مواجهة الهجمات الإلكترونية"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1، الإمارات العربية المتحدة، ،2020، ص55 .

(3)- الزهراني شيخة حسين ، المرجع نفسه ، ص60 .

تعرف هذه الهيئة باسم وكالة الإتحاد الأوروبي للأمن السيبراني، ويرمز لها إختصاراً بـ (ENISA)، وهي وكالة رسمية تابعة للإتحاد الأوروبي، تم تأسيسها بموجب اللائحة رقم 460/2004 الصادرة عن الإتحاد في سنة 2004، تحت إسم "الوكالة الأوروبية لأمن الشبكات والمعلومات"، وبدأت ممارسة مهامها فعلياً بتاريخ 1 سبتمبر 2005، ويقع مقرها الرئيسي في أثينا، عاصمة اليونان.[1]

تخضع الوكالة لإدارة مدير تنفيذي، يساعده فريق من الخبراء المتخصصين الذين يمثلون مختلف الأطراف المعنية في قطاع الأمن السيبراني، ومن بينهم ممثلون عن صناعة تكنولوجيا المعلومات والإتصال، ومنظمات حماية المستهلك، والخبراء الأكاديميين، كما تُشرف على الوكالة هيئتان رئيسيتان، هما: المجلس التنفيذي ومجلس الإدارة، ويتكون أعضاؤهما من ممثلين عن الدول الأعضاء في الإتحاد الأوروبي إلى جانب ممثلين عن المفوضية الأوروبية.[2]

علاوة على ذلك، تساند الوكالةَ مجموعة إستشارية تضم 33 عضواً معينين من مختلف دول أوروبا، والذين يقدمون خبراتهم من أجل تعزيز فعالية عمل الوكالة وتوسيع نطاق تأثيرها.

ثانيا : مهام الوكالة الأوروبية للأمن السيبيراني

تتمثل مهام الوكالة في مجال الأمن السيبيراني في مايلي :

أ- تعمل الوكالة بشكل وثيق مع الدول الأعضاء في الاتحاد الأوروبي ومع مختلف أصحاب المصلحة، من أجل تقديم الإستشارات الفنية وإقتراح الحلول العملية، إلى جانب تحسين القدرات الوطنية في مجال الأمن السيبراني.

(1)- سي عبد القادر حنان، "الأمن السيبيراني وأثره على دول العالم"، مجلة البصائر للدراسات القانونية والاقتصادية ، كلية الحقوق والعلوم السايسية بسوسة، المجلد 4، العدد 7 ، تونس، 2024 ، ص33 .

(2)-موقع الوكالة الأوروبية للأمن السيبيراني https://enisa.europa.eu

ب- تسهم الوكالة في تطوير آليات الاستجابة الفعالة للحوادث والأزمات السيبرانية، وخاصة في حال التهديدات عابرة للحدود ومنذ سنة 2019، تتولى أيضاً مسؤولية وضع مخطط إصدار شهادات الأمن السيبراني لتعزيز الثقة في المنتجات والخدمات الرقمية.

ثالثاً: تدعم الوكالة المفوضية الأوروبية والدول الأعضاء، وكذلك القطاع الخاص، في الإمتثال لمتطلبات أمن الشبكات والمعلومات، بما يشمل تشريعات الإتحاد الأوروبي الحالية والمستقبلية.(1)

وأخيراً، تسعى الوكالة إلى أن تكون مركزاً أوروبياً للخبرة، يُعتمد عليه في تقديم المشورة الفنية والإستراتيجية في كل ما يتعلق بأمن الشبكات والمعلومات.

كما تنظم الوكالة، منذ سنة 2019، تمارين دورية في الأمن السيبراني تشمل جميع الدول الأوروبية، وذلك بهدف تعزيز الجاهزية والتنسيق الإقليمي في مواجهة التهديدات السيبرانية المتزايدة.(2)

المطلب الثاني :التعاون الأوروبي الدولي في التصدي للعنف السيبراني

يعد مبدأ التعاون الدولي من المبادئ الجوهرية في القانون الدولي، لاسيما في مجال مكافحة الجريمة التي باتت أكثر تعقيدًا وتشعبًا في ظل التطورات التقنية المتسارعة، وقد تناول الفقه هذا التعاون، لاسيما في بعده الأمني، كأحد أشكال التعاون الدولي متعدد الأوجه، لما له من دور في ملاحقة المجرمين والتصدي للجرائم العابرة للحدود، ومنها العنف السيبراني، ويتجاوز هذا التعاون مجرد ملاحقة الجناة، ليشمل أيضًا إحترام حقوق المتهمين والضحايا، وضمان سيادة الدول، من خلال تبادل العون والمساعدة بين مختلف الأطراف الدولية لتحقيق مصلحة مشتركة في مكافحة الإجرام السيبرانيمن خلال تبادل العون

(1)-موقع الوكالة الأوروبية للامن السيبراني ،.https://enisa.europa.eu

(2)- سي عبد القادر حنان ، المرجع السابق، ص 34.

والمساعدة بين مختلف الأطراف الدولية لتحقيق مصلحة مشتركة في مكافحة الإجرام السيبراني، وفي هذا الإطار، يتجلى التعاون الأوروبي والدولي في مجال مكافحة العنف السيبراني من خلال محورين رئيسيين: أولًا، تبادل البيانات بين الإنتربول واليوروبول(الفرع الأول)، وثانيا ،آلية الإنابة القضائية الدولية (الفرع الثاني).

الفرع الأول :تبادل البيانات بين الأنتربول واليوروبول

يشكّل التعاون الأمني الدولي بين اليوروبول والإنتربول ركيزة أساسية في التصدي للعنف السيبراني، إذ يقوم على تبادل المعلومات وتعزيز التنسيق العملياتي وتقديم الدعم القانوني المتبادل لمواجهة التهديدات الإجرامية العابرة للحدود، وتسعى هذه الشراكة إلى تعزيز فعالية أجهزة إنفاذ القانون، وتيسير التحقيقات المشتركة، وضمان إستجابة منسّقة ومتكاملة لمختلف التحديات الأمنية، وإنطلاقًا من ذلك، سيتم أولًا التطرّق إلى مهام جهاز اليوروبول كجهاز شرطي أوروبي، ثم إلى إستراتيجياته التعاونية مع الأنتربول في مجال تبادل البيانات.

أولا : تأسيس و مهام اليوربول

تم إنشاء جهاز اليوروبول استنادًا إلى معاهدة ماستريخت لعام 1992، ويعد من أبرز الأجهزة الشرطية على المستوى الأوروبي، ويقع مقره في مدينة لاهاي بهولندا. وتتمثل مهمته الأساسية في معالجة المعلومات المتعلقة بالأنشطة الإجرامية داخل الإتحاد الأوروبي، وتقديم الدعم لسلطات التحقيق الجنائي من خلال تعزيز تبادل المعلومات والمساعدة القضائية في التحقيقات والملاحقات والإجراءات القانونية.[1]

(1)–فهد عبد الله العبيد العازمي ، المرجع السابق، ص 669 .

كما يُعنى اليوروبول بتجميع وتحليل البيانات المتعلقة بالجريمة المنظمة والعابرة للحدود، فضلًا عن تسهيل التعاون وتبادل المعلومات بين الدول الأعضاء، حيث تمتلك كل دولة عضو مكتب اتصال وطني يُعنى بتنسيق هذا التعاون على المستوى الوطني.[1]

ثانيا : التعاون بين اليوروبول والأنتربول في مجال تبادل البيانات

نصَّ الباب الرابع من إتفاقية ماستريخت على إنشاء نظام لقاعدة بيانات مركزية يُعنى بدعم التعاون الشرطي الدولي، خاصة في مجال مكافحة الجريمة العابرة للحدود والعنف السيبراني، وتكمن وظيفة هذا النظام في جمع وتبادل المعلومات ذات الصلة، مثل بيانات الأشخاص المطلوبين، والأدوات والأجهزة والمستندات محل البحث أو المصادرة، وقد تم ربط النظام المركزي للبيانات، الموجود في مدينة ستراسبورغ، بشكل مباشر مع الأنظمة الوطنية للدول الأطراف في الاتفاقية، مما يتيح تبادلًا فوريًا وفعالًا للمعلومات، وتجدر الإشارة إلى أن هذا التبادل يجب أن يتم وفقًا لضوابط قانونية صارمة تراعي إحترام الحقوق والحريات الأساسية للأفراد، بما يعكس التوازن بين الفعالية الأمنية وضمانات حقوق الإنسان.[2]

1-التعاون القانوني بين المنظمتين في مجال مكافحة العنف السيبراني

في إطار تعزيز التعاون الدولي في مكافحة الجريمة المنظمة والعنف السيبراني، تم توقيع إتفاقية تعاون بين منظمة الأنتربول والشرطة الأوروبية يوروبول سنة 2001 في **بروكسل،** وقد نصّت هذه الإتفاقية على أسس التعاون بين الطرفين، حيث تمثّل هدفها الرئيسي في

(1)-فهد عبد الله العبيد العازمي ، المرجع نفسه ، ص 670 .

(2)-محمد نذير بن عرفة، يوسف حوري ، اليوروبول كآلية لمكافحة الجريمة الإلكترونية ،مجلة الدراسات القانونية والسياسية ،جامعة الجزائر، المجلد 11 ،العدد 1 ،الجزائر، 2025 ، ص 40 .

إنشاء وتعزيز إطار دائم للتعاون من أجل مكافحة أشكال الجريمة الدولية المنظمة، بما في ذلك العنف السيبراني، في حدود إختصاص كل طرف ووفقًا لأحكامه القانونية والدستورية.
وقد تم تحديد وسائل هذا التعاون في تبادل المعلومات التشغيلية والإستراتيجية والتقنية، وتنسيق الأنشطة المختلفة، بما في ذلك وضع معايير وخطط عمل مشتركة، وتنفيذ برامج تدريب، وتشجيع البحث العلمي، وإعارة ضباط اتصال بين المؤسستين. ويُعد هذا التعاون من أهم أوجه الشراكة بين الأنتربول والإتحاد الأوروبي، نظرًا لكون المنظمتين تُعنيان بمكافحة الجريمة العابرة للحدود، كما تمتلك كل منهما وحدات متخصصة في مكافحة الجريمة الإلكترونية والعنف السيبراني.[1]

وفي سياق تعميق العلاقات المؤسسية بين الأنتربول والأتحاد الأوروبي، أصدرت الجمعية العامة للأنتربول قرارها رقم (05-GA-2019-88-RES)، الذي أكد على الأهداف الإستراتيجية للمنظمة، لاسيما في ما يتعلق بتحسين الوصول إلى منظومة الأنتربول وتعزيز التواصل مع المنظمات الإقليمية والدولية المختصة، من أجل سد الثغرات وتعزيز التكامل في العمل الشرطي الدولي، وقد أشار القرار إلى مجموعة من الإتفاقات، من بينها إتفاق التعاون مع اليوروبول (2001)،وإتفاق العمل مع وكالة فرونتكس(2009)، بالإضافة إلى إفتتاح مكتب دائم للممثل الخاص للأنتربول لدى الإتحاد الأوروبي في العام ذاته.

وإختُتم القرار بتفويض الأمانة العامة للإنتربول بالدخول في مفاوضات مع الاتحاد الأوروبي بغرض إبرام اتفاق تعاون موسّع، يُمكن أن يشمل مجالات متعددة، من بينها :تبادل المعلومات، ومنح الإتحاد الأوروبي (عن طريق اليوروبول) إمكانية الوصول إلى منظومة الأنتربول للمعلومات، والتعاون مع الهيئات التابعة للإتحاد داخل أراضيه وخارجها.[2]

(1)-فنور حاسين ، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة ، رسالة ماجستير، جامعة الجزائر، كلية الحقوق بن عنكون ، 2013 ، ص 113 .

(2)-فنور حاسين ، المرجع نفسه ، ص114 .

2- مؤتمرات اليوروبول والأنتربول لمكافحة الجريمة السيبرانية

أما من ناحية المؤتمرات، فقد عُقد مؤتمر مشترك بين اليوروبول والأنتربول حول مكافحة الجريمة السيبرانية سنة 2013، والذي أوصى في ختام أعماله بضرورة إستحداث حلول مبتكرة في مجال العمل الشرطي، للنهوض بجهود التحقيق في الجرائم السيبرانية، ومساعدة الدول على الإستفادة من الأدلة الرقمية.

وفي عام 2021، عُقد المؤتمر التاسع لمكافحة الجريمة السيبرانية بتنظيم مشترك بين الأنتربول واليوروبول في مقر اليوروبول بمدينة لاهاي، حيث ناقش المشاركون الجوانب المالية للجرائم السيبرانية، والتحديات الراهنة والناشئة، بالإضافة إلى الإبتكارات في العمل الشرطي التي ترسم معالم المستقبل في هذا المجال.[1]

وقد تصدّر جدول أعمال المؤتمر اعتماد مناهج منسقة، وأتاحت المداولات للمشاركين تكوين رؤية شاملة حول أبرز الأنشطة العملياتية لمواجهة التهديدات السيبرانية الكبرى، لا سيما التهديد المتزايد الذي تطرحه برمجيات انتزاع الفدية، كما ناقش المؤتمر كيفية استفادة أجهزة إنفاذ القانون من التطورات التكنولوجية الجديدة التي يوظفها المجرمون.[2]

وقد شكل المؤتمر فرصة للمندوبين لتوضيح أن أجهزة إنفاذ القانون، إذا ما أرادت مواكبة التحولات التكنولوجية السريعة، فينبغي عليها إمتلاك الكفاءات والمهارات المناسبة لمواجهة الجريمة الرقمية على المستويات الوطنية والإقليمية والدولية. كما شدد على ضرورة بناء قدرات متخصصة ومصمّمة وفقًا للإحتياجات الخاصة، مع التركيز على الإبتكار في العمل الشرطي.

(1)–بدري فيصل،مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراة، كلية الحقوق، جامعة الجزائر،2018 ، ص150.

(2)–بدري فيصل، المرجع نفسه،ص 152.

وأبرزت المناقشات كيف يمكن للتطورات المجتمعية والتكنولوجية أن تسهم في دعم جهود مكافحة الجريمة السيبرانية، من خلال حلول مبتكرة مثل فك تشفير الأدلة الرقمية التي تم الحصول عليها بصورة قانونية ضمن التحقيقات الجنائية، ودور المختبرات الجنائية المتقدمة في دعم الإبتكار في مجال إنفاذ القانون.[1]

وقد واجه المشاركون تحديًا هامًا تمثّل في ضرورة وضع نماذج تعاون عالمي جديدة، وإقامة شراكات فاعلة، بالنظر إلى أن الجريمة السيبرانية تمثل تهديدًا عالميًا يستدعي إستجابة دولية منسقة.

وفي السياق ذاته، أعلنت منظمة الأنتربول عن نتائج عملية عالمية استغرقت أربع سنوات، وأسفرت عن تفكيك عصابة متخصصة في ارتكاب جرائم سيبرانية باستخدام برمجيات إنتزاع الفدية، وإعتقال سبعة أشخاص. ويُشتبه في أن هؤلاء الأشخاص، الذين أُلقي القبض عليهم ضمن هذه العملية التي نُفذت بالتنسيق مع اليوروبول، قد نفّذوا عشرات الآلاف من الهجمات السيبرانية باستخدام تلك البرمجيات، مطالبين بفدى تجاوزت قيمتها 200 مليون يورو.[2]

الفرع الثاني: آلية الإنابة القضائية الدولية في جمع الأدلة الإلكترونية عبر الحدود

تعتبر الإنابة القضائية الدولية الخاصة بجمع الأدلة الإلكترونية عبر الحدود إحدى صور التعاون القضائي الدولي بين الدول، وتُعد آلية هامة لتقديم المساعدة القانونية المتبادلة في إطار التحقيقات والمحاكمات المتعلقة بجرائم العنف السيبراني، ويهدف هذا التعاون من خلال هذه الآلية إلى تعزيز الجهود الدولية في مكافحة الجرائم السيبرانية، عبر توفير الدعم

(1)-بدري فيصل، المرجع نفسه،ص 160 .

(2)-موقع الأنتربول ،www.interpol.int

القانوني المتبادل بين الدول، بما يضمن تقديم الجناة إلى العدالة في هذا المجال، وسنستعرض في هذا السياق أولاً مفهوم الإنابة القضائية الدولية، ثم إجراءات تنفيذ الإنابة القضائية الدولية في مجال جمع الأدلة الإلكترونية.

أولا : مفهوم الإنابة القضائية الدولية

يقصد بالإنابة القضائية الدولية طلبًا من دولة إلى دولة أخرى لإتخاذ إجراء قضائي معين ضمن إجراءات الدعوى الجنائية، وذلك بغرض الفصل في مسألة معروضة على السلطة القضائية للدولة الطالبة، ويتعذر على هذه الدولة القيام بها بنفسها.[1]

وتهدف هذه الآلية إلى تسهيل التعاون القضائي الجنائي بين الدول، بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على مشكلة السيادة التي تحول دون تمكّن الدولة الأجنبية من ممارسة بعض الإجراءات القضائية داخل أراضي الدول الأخرى، مثل سماع الشهود، وإستجواب المتهمين، وإجراء عمليات التفتيش، وغيرها.

ثانيا : إجراءات الإنابة القضائية الدولية لجمع الأدلة والبيانات الرقمية

تستلزم إجراءات الإنابة القضائية الدولية إرسال ملف الدعوى الجنائية مرفقًا بالمستندات والوثائق ومحاضر التحقيق التي أجريت بمعرفة السلطة القضائية في الدولة الطالبة، إلى السلطات القضائية المختصة في الدولة المطلوب إليها إتخاذ إجراءات التحقيق.[2]

وعادةً ما يتم إرسال طلب الإنابة القضائية الدولية عبر القنوات الدبلوماسية، فمثلاً، عند طلب الحصول على دليل إثبات رقمي، يتم إرسال الطلب عن طريق وزارة الخارجية إلى

(1)- خراشي عادل عبد العالي إبراهيم ، المرجع نفسه، ص 36 .

(2)- خراشي عادل عبد العالي إبراهيم ، المرجع نفسه ، ص40 .

سفارة الدولة محل الطلب، حيث تقوم الأخيرة بإحالته إلى السلطات القضائية المختصة في الدولة المتلقية.[1]

غير أن إعتماد إجراءات التعاون القضائي الدولي على القنوات الدبلوماسية يُعيق سرعة التنفيذ بسبب بطئ الإجراءات وكثرة الشكليات، وهو أمر يتعارض مع طبيعة شبكة الأنترنت التي تتميز بسرعة تبادل المعلومات، لذا، فإن مكافحة العنف السيبراني تتطلب تعاملاً سريعًا لتجنب التلاعب في البيانات التي قد تشكل أدلة ضد المتهمين.[2]

ومن الأمثلة البارزة على الإتفاقيات الدولية التي نصّت على الإنابة القضائية الدولية في مجال الأدلة الرقمية العابرة للحدود، إتفاقية بودابست لمكافحة الجرائم السيبرانية، والتي أكدت على ضرورة التعاون الدولي القضائي وتقديم المساعدة القانونية المتبادلة بين الدول الأعضاء.[3]

كما نصّت إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام 2024 على إلزامية تعزيز التعاون الدولي لمكافحة الجرائم السيبرانية عبر تبادل الأدلة الإلكترونية، وطرحت المبادئ العامة للمساعدة القانونية المتبادلة، لاسيما في مجال إعتراض بيانات المحتوى، كما حدّدت هذه الإتفاقية الإجراءات القانونية الواجب إتباعها من قِبل الدولة صاحبة الطلب لتنفيذ الإنابة القضائية الدولية لجمع الأدلة والبيانات الإلكترونية المخزنة، والإحتفاظ بها ضمن إطار التحقيقات المتعلقة بالجرائم السيبرانية.[4]

(1)–أسامة العبيدي، المرجع نفسه ، ص131 .

(2)–أسامة العبيدي، المرجع نفسه، الصفحة 131 .

(3)–أسامة العبيدي، المرجع نفسه ، ص 132 .

(4)–أنظر: المواد 40 وما يليها من اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لسنة 2024 ، تعزيز التعاون الدولي لمكافحة جرائم معينة مرتكبة بواسطة نظام تكنولوجيا المعلومات والاتصالات وتبادل الأدلة في شكل الكتروني على الجرائم الخطيرة .

خاتمة

خاتمة:

مع التطور المتسارع في تقنيات الإتصال والاعتماد المتزايد على الفضاء الرقمي في مختلف مناحي الحياة، برزت تحديات جديدة أمام المجتمع الدولي، في مقدمتها ظاهرة العنف السيبراني، التي لم تعد مجرّد مسألة أمنية داخلية، بل أصبحت تمسّ صميم السيادة الوطنية وتثير إشكالات قانونية عابرة للحدود.

ولقد كشفت هذه الظاهرة عن ثغرات واضحة في المنظومة القانونية الدولية، سواء من حيث ضعف الإطار المفاهيمي المحدد لها، أو من حيث محدودية آليات الردع والمساءلة المتاحة.

لقد حاول هذا البحث من خلال معالجة موضوع الحماية من العنف السيبراني في القانون الدولي، الإحاطة بأبرز الإشكاليات التي تعترض التصدي لهذا النمط المستجد من التهديدات، خاصة ما تعلق بغياب تعريف قانوني جامع للعنف السيبراني، وتفاوت الرؤى بين الدول حول كيفية تكييفه، إضافة إلى تعقيد الإجراءات القضائية الدولية المتعلقة بجمع الأدلة الرقمية وتبادل المعلومات في هذا السياق.

وأظهرت الدراسة أن إتفاقية بودابست تُعدّ من أبرز الإطارات القانونية المتاحة حاليًا، غير أن إعتمادها يظلّ محدودًا جغرافيًا، كما أن مضامينها أصبحت تحتاج إلى تحديث لمواكبة طبيعة التهديدات الرقمية الراهنة، وبالمثل، فإن ما تم التوصل إليه مؤخرًا في إطار الأمم المتحدة من مبادئ عامة لمكافحة الجرائم السيبرانية لا يرقى بعد إلى مستوى المعايير الملزمة التي تضمن التطبيق الفعلي والفعّال على الصعيد العالمي.

وفي ظل هذا الواقع، لا يمكن مواجهة هذا النوع من العنف إلا من خلال تطوير تعاون دولي فعّال يقوم على تبادل فوري للمعلومات، وتنسيق مستمر بين السلطات القضائية، مع ضرورة إعادة النظر في الآليات التقليدية للتعاون كالإجراءات الدبلوماسية البطيئة التي تعيق الإستجابة الفورية للهجمات السيبرانية التي تُنفذ في لحظات وقد تُطمس آثارها بسرعة،وعليه فإن أبرز النتائج المتوصّل إليها من خلال البحث:

-إنعدام وجود إتفاقية دولية شاملة وملزمة تعالج العنف السيبراني بمختلف أشكاله وتُحدّد مسؤوليات الفاعلين بدقة.

-تفاوت مستويات الحماية القانونية بين الدول وتضارب التشريعات الوطنية، مما يخلق ملاذات آمنة للمجرمين السيبرانيين.

-الإختلاف في نسبة التطور التكنولوجي والرقمي بين الدول المتقدمة وبين الدول النامية ، أدى إلى إنتشار ظاهرة العنف السيبراني في هذه الأخيرة ، نتيجة التفاوت في الإمكانيات الرقمية لمحاربة هذه الظاهرة .

-ضعف آليات التعاون القضائي الدولي، خاصة في ما يخص الإنابات القضائية وجمع الأدلة الرقمية العابرة للحدود.

-عدم كفاية الأطر القانونية القائمة، سواء في القانون الدولي العام أو الإنساني، لتأطير هذا النوع من الجرائم المعقدة .

-الحاجة الملحة إلى إدماج الحقوق الرقمية ضمن منظومة حقوق الإنسان المعترف بها دوليًا، لمواكبة التحول الرقمي العالمي.

وإنطلاقا مما سبق، يمكن أن نقدم بعض التوصيات التي تتمثل في مايلي:

-ضرورة وضع إتفاقية دولية متخصصة في مكافحة العنف السيبراني، على غرار اتفاقيات مكافحة الإرهاب والجريمة المنظمة، تتضمن تعريفات دقيقة، وإجراءات قانونية واضحة، وآليات تنفيذ فعّالة.

-إعادة صياغة وتطوير آليات التعاون القضائي الدولي، وخاصة تسريع إجراءات الإنابة القضائية الرقمية وتيسير تبادل الأدلة الإلكترونية، دون الإخلال بالضمانات القانونية للمتهمين.

-تعزيز القدرات التقنية والقضائية للدول النامية من خلال برامج دعم وبناء قدرات تتيح لها التصدي الفعّال للتهديدات السيبرانية المتزايدة.

-العمل على إنشاء شبكة دولية للخبراء والقضاة والمدعين العامين المختصين بالجرائم السيبرانية لتبادل الممارسات الفضلى والتجارب القانونية.

-دعم البحث العلمي الأكاديمي المتخصص في القانون السيبراني وتحديث المناهج الجامعية بما يواكب التطورات التقنية المستجدة.

-الإعتراف بحقوق الإنسان الرقمية، خصوصًا ما يتعلق بحماية الحياة الخاصة والبيانات الشخصية وحرية التعبير، مع ضمان عدم إستغلال الحرب على العنف السيبراني في تقييد الحريات الأساسية.

قائمة المراجع

أولاً: باللغة العربية

1- الكتب :

1- أبو الفضل ابن منظور، لسان العرب ، مجلد 9 ، دار صادر للطباعة والنشر، لبنان ، 1956 .

2- أحمد هلالي عبد اللاه احمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية، دار النهضة العربية ، القاهرة ، 2008 .

3- إيهاب الحضري: الفضاء البديل، الممارسات السياسية والاجتماعية للشباب العربي على شبكة الأنترنت، مركز الحضارة العربية، الجيزة، 2010.

4- حسين محمود هتيمي، العلاقات العامة وشبكات التواصل الاجتماعي ، دار أسامة للنشر ، الأردن ، 2015 .

5- خراشي عادل عبد العال إبراهيم، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها ، دار الجامعة الجديدة ، الإسكندرية، 2015

6- دحان حزام القرطبي، الأمن السيبيراني وحماية أمن المعلومات، دار الفكر الجامعي ، الإسكندرية ،2024.

7- الدسوقي عطية طارق، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية ، دار الدامعة الجديدة للنشر، مصر ،2009.

8- رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية ، الطبعة 01 ، دار النهضة العربية ، القاهرة ، 2011 .

9- الرشيدي محمود كامل ، العنف في جرائم الأنترنت أهم القضايا، الحماية والتامين ، الدار اللبنانية ، القاهرة ،2011 .

10- سليمان أحمد فضل المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية ، دار النهضة العربية ، القاهرة ، 2008 . .

11- شريفة كلاع ، الأمن السيبيراني وأشكال التهديد ، تحديات عالمية ، ألفا للوثائق للنشر والتوزيع ، الجزائر ، 2023.

12- عادل عبد الصادق، الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق ، العدد 23 ، مكتبة الإسكندرية ، مصر، 2016 .

13- عادل عبد العال إبراهيم خراشي،جرائم الاستغلال الجنسي للأطفال عبر شبكة الإنترنت وطرق مكافحتها في التشريعات الجنائية والفقه الجنائي الإسلامي" دار الجامعة الجديدة للنشر ، 2015 ، الإسكندرية، 2015.

14- عادل عزام سقف الحيط، جرام الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، شبكة الانترنت وشبكة الهواتف النقالة وعبر الوسائط التقليدية والالية ، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع ، الأردن ، 2011 .

15- العربي بوعمامة ،رقاد حليمة ،العنف في الفضاء السيبيراني، منشورات ألفا للوثائق والنشر والتوزيع ، الجزائر، 2023 .

16- علي حسن الطوالبة ، الجرائم الإلكترونية ، جامعة العلوم التطبيقية ،سلسلة الكتب القانونية،الطبعة الأولى ، البحرين ،2008 .

17- علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية، دراسة في إستراتيجيات الاشتباك الرقمي، دار أمجد للنشر والتوزيع، عمان، 2012 .

18- فارس محمد العمارات، إبراهيم الحمامصة، الأمن السيبيراني ، وتحديات العصر، دار الخليج للنشر والتوزيع ،الجزائر ، 2022.

19- فهدعبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة ، الإسكندرية ،2016.

20- كوثر مازوني، الجريمة المعلوماتية، أعمال ندوة وطنية ، دار الخلدونية ، الجزائر ، سنة 2019 .

21- محمد عبد الله أبوبكر سلامة، موسوعة الجرائم المعلوماتية وجرائم الكومبيوتر والانترنت ، منشاة المعارف ،الإسكندرية ، 2006 .

22- المكاوي محمد محمود ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت)، المكتبة العصرية للنشر والتوزيع ، المنصورة ، مصر، 2015 .

23- نبيل رمزي ،علم إجتماع المعرفة ، دراسة مقارنة الوعي والإيديولوجية ، دار الفكر العربي،الإسكندرية ، 1991

24- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، دار الفكر العربي ،الإسكندرية، 2008 .

25- نسرين عبد الحميد نبيه، الجريمة المنظمة عبر الوطنية ، دار الفكر الجامعي ، الإسكندرية ،2016.

26- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافةوالتوزيع،الطبعة01، الأردن ، 2008.

27- يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات ، القاهرة ، 2011.

2- الأطروحات الجامعية والمذكرات:

أ-أطروحة الدكتوراه:

1-بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراة، كلية الحقوق، جامعة الجزائر، 2018

ب-مذكراتالماجستير:

1- صغير يوسف، الجريمة المرتكبة عبر الانترنت ، مذكرة ماجستير، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو، 2013.

2- عمرعباس خضير العبيدي ،الإرهاب الإلكتروني في نطاق القانون الدولي ، مذكرة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2019.

3- فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة ، مذكرة ماجستير، جامعة الجزائر ، كلية الحقوق بن عكنون ، 2013.

4- مريم ناريمان نومار،استخدام مواقع الشبكات الاجتماعية وأثره على العلاقات الإجتماعية ، مذكرة ماجستير ، كلية علوم الاتصال والإعلام ، جامعة باتنة ، 2012.

ج-مذكرات الماستر:

1- سليمان ابو نمر، يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، السنة الجامعية 2020-2021 .

2- طماطمي سالم ،الصحافة الإلكترونية و الأمن السيبراني دراسة حالة الجزائر، مذكرة ماستر، كلية العلوم الإنسانية والاجتماعية، جامعة أدرار، السنة الجامعية 2021-2022 .

3- فريدة طاجين،تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى،مذكرة ماستر،جامعة ورقلة ، السنة الجامعية 218-2019.

03-المقالات العلمية والمداخلات:

1- بن علية بن جدو، "تحديات الامن السيبيراني لمواجهة الجريمة الإلكترونية" ، المجلة الجزائرية للامن السيبيراني، جامعة باتنة، المجلد 07، العدد 02 ، 2022 ،الجزائر، ص 299-319 .

2- وردة دلال، "السياسة التشريعية المتبعة في تجريم التحرش الجنسي: التشريع الجزائري والتشريع السعودي نموذجا"،مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، المجلد4 ، العدد 7، الجزائر،2017 ، ص89-136.

3- سي عبد القادر حنان، "الأمن السيبيراني وأثره على دول العالم"،مجلة الدراسات القانونية والاقتصادية، كلية الحقوق والعلوم السياسية"، المجلد4،العدد7، تونس، 2024، ص21-37.

4- حسين بن احمد الشهري ، "الإرهاب الالكتروني ، -حرب الشبكات – "، المجلة العربية الدولية للمعلوماتية، السعودية، 2015، ص30-55 .

5- أحمد عيسى الفتلاوي، "الهجمات السيبيرانية ، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع ، كلية القانون، جامعة بابل، 2016، ص610-687.

6- إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية المدرسة العليا العسكرية للإعلام والاتصال،المجلد 1، العدد 1،الجزائر، 2019، ص100-121.

7- أسامة بن غانم العبيدي، "الجهود الدولية في مكافحة الجرائم المعلوماتية "، مجلة الحقوق، المملكة العربية السعودية، العدد 04، 2015،ص112-153.

8- علاء الرواشدة، أسماء ربحي، "الجريمة في ظل العولمة، دراسة تحليلية للبنية وسياسات المواجهة"، مجلة الحقيقة للعلوم الاجتماعية والإنسانية ، جامعة أدرار، مجلد 18 ، عدد 12، الجزائر،2019،ص220-230.

9- دخلافي سفيان، "العدوان في القانون الدولي والهجمات السيبيرانية بين الدول"، مجلة العلوم القانونية والسياسية، جامعة تيزي وزو، المجلد 14، العدد 02، 2023، الجزائر، ص.82-103.

10- العلي ناصر، "الجهود الدولية في مكافحة الإرهاب الالكتروني"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، العدد 08، 2021، ص.27-45.

11- إسماعيل زروقة، "الفضاء السيبيراني والتحول في مفاهيم القوة والصراع"، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 10 ،العدد 01، 2019،ص1016-1031 .

12- زاهي رضا، "إستخدام مواقع التواصل الاجتماعي في العالم العربي"، مجلة التربية، جامعة عمان،العدد 15 ، عمان ، ص20-30.

13- بارة سمير، "الأمن السيبراني في الجزائر"،المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح ورقلة، المجلد 2 ، العدد 2 ، 2017 ،ص 255-280.

14- بيدي آمال، "جهود الأمم المتحدة في مكافحة الجريمة السيبيرانية"، مجلة البحوث في الحقوق والعلومالسياسية، جامعة الجلفة، مجلد 8، العدد1،الجزائر،2022 ،ص299-316.

15- جبور منى الأشقر، "الأمن السيبراني" هاجس عصرنا"، المركز العربي للبحوث القانونية والقضائية،جامعة الدول العربية، المجلد 1، بيروت، لبنان ،2018 ، ص218-250.

16- رغدة البهي، "الردع السيبيراني، المفهوم والإشكالات والمتطلبات"، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الإستراتيجية والاقتصادية، العدد 01،ألمانيا، 2007،ص50-70 .

17- روانبنت عطية الله،"الجرائم السيبيرانية"، المجلة الإلكترونية الشاملة متعددة الإختصاصات،العدد 24، المملكة العربية السعودية،2020،ص1-53.

18- سعيدة عباس ، "التنمر الالكتروني (ماهيته وأسبابه واليات حماية أبنائنا منه)"، مجلة الربئة،جامعة باتنة 01، العدد الأول، ص. 10-15.

19- شريفة كلاع،"الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"،مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر 03، المجلد 15، العدد 01، 2022، ص 292-314.

20- شيخة حسين الزهراني، "التعاون الدولي في مواجهة الهجمات الالكترونية"، مجلة جامعة الشارقة للعلوم القانونية،المجلد،17، العدد 01، الإمارات العربية المتحدة، 2020، ص 740-772.

21- طواهير عبد الجليل، "استراتيجيات الأمن السيبيراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة إلى تجربة الإمارات العربية المتحدة"، مجلة الرسالة للدراسات الإعلامية، جامعة ورقلة، المجلد 07 ، العدد 01،الجزائر، 2023، ص 279-291.

22- قطاف سليمان، بوقرين عبد الحليم،"مواجهة الجرائم السيبيرانية في ضوء الاتفاقيات الدولية"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، جامعة الأغواط، المجلد 05، العدد 02 ، 2022 ، ص62-82.

23- منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية"، مجلة كلية التربية، جامعة المنصورة ،المجلد111،العدد 1،المملكة العربية السعودية،2022، ص2-28.

24- يقرو خالدية ، "الإستغلال الجنسي عبر شبكة الانترنت"، مجلة القانون،كلية الحقوق، المركز الجامعي غليزان، العدد 3، الجزائر،2012،.ص 328-342.

25- صغير يوسف، "جرائم الانترنت جرائم حقيقية في عالم إفتراضي"، مجلة المعارف، جامعة البويرة،المجلد 17،العدد2،الجزائر، 2022، ص210-230.

26- محمد نذير بن عرفة،يوسف حوري،"اليوروبول كآلية لمكافحة الجريمة الإلكترونية"، مجلة الدراسات القانونية والسياسية، جامعة الجزائر، المجلد11، العدد1، 2025،ص36-48.

27- منصور بن صالح الجهني، الجرائم المعلوماتية ، أنواعها وصفات مرتكبيها، مداخلة إلى المؤتمر الدولي الرابع للعلوم الإجتماعية ، كلية العلوم الاجتماعية ، جامعة الكويت، الكويت، 2010 ، ص01-08 .

4-النصوص القانونية:

1-إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكلات الملحقة بها، معتمدة من طرف الجمعية العامة للأمم المتحدة بموجب القرار رقم 55/25 مؤرخ في 15 نوفمبر 2000، مصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 55/02 مؤرخ في 5 فيفري 2002 .

2-الإتفاقية الدولية لقمع تمويل الإرهاب، معتمدة من طرف الجمعية العامة للأمم المتحدة بموجب القرار رقم 109/54 مؤرخ في 09ديسمبر 1999، مصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 2000/445 مؤرخ في 23 ديسمبر 2000.

3-الإتفاقية المتعلقة بالجريمة الالكترونية بودابست2001، مجموعة المعاهدات الأوروبية رقم 180.

4-إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية 2024،الجمعية العامة للأمم المتحدة.

7-المواقع الإلكترونية:

1-مكتب الأمم المتحدة المعني بالمخدرات WW.UNODC.ORG، تاريخ الإطلاع 2025/05/02.

3-موقع الانتربول www.interpol.int، تاريخ الاطلاع 2025/06/01 ،18:10 .

4-موقع الأمم المتحدة بجنيفwww.geneva.un.org .، تاريخ الاطلاع 2025/06/03 ، 21:30.

5-موقع الوكالة الأوروبية للأمن السيبيراني:// http: www.enisa.europa.euتاريخ الإطلاع 2025/06/04 ، 12.35.

6–ميتيهان دورماز،إتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية ، الأهداف والثغرات، مقال منشور في موقع www.smex.org، تاريخ الإطلاع 205/06/10 ، 22.00.

7–هشام بشير، "مستقبل إلارهاب الالكتروني ، تحديات وأساليب المواجهة"، مداخلة بندوة المركز الدولي للدراسات المستقبلية والاستراتيجية ، 2112 ،على الرابط :

http://www.siyassa.org.eg، تاريخ الإطلاع 2025/05/20 ، 15:06 .

8–سلمى موضوع ،تاريخ الأمن السيبراني، متاح على الموقع:www.mawdoo.com، تاريخ الإطلاع 2025/05/25 ،18:55 .

9–إتفاقية الأمم المتحدة لمكافحة الجريمة السيبيرانية ، مقال منشور في موقع الأمم المتحدة ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، https://www.unodc.org

ثانيًا: المراجع باللغة الأجنبية :

I-Les ouvrages:

01- Nancy E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* Eugene, OR: Research Press, 2007.

-Les Articles:

16- Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. “Defining Cybersecurity.” Technology Innovation Management Review 4, no. 10 (October 2014): 13–21.

2- Jack Brown, "Jurisdiction to Prosecute Crimes Committed by Use of the Internet," Jurimetrics 38 (1998).

3- Kim Barker and Ola Juras,online violence against women as an obstacle to gender equality a critical view from Europe,European Equality law Review,2020.

الفهرس