تاريخ الإرسال: 2023/06/18 تاريخ القبول: 2024/01/14

التهديدات السيبرانية وجرائم المعلومات

Cyber threats and information crimes

العيداني محمد*
المركز الجامعي الشريف بوشوشة آفلو (الجزائر)، m-laidani@cu-aflou.edu.dz

الملخص:
باتت الجريمة السيبرانية في الوقت الراهن أحد سمات الحروب الحديثة والتي تفرض تحديات لعموم الدول المتقدمة والنامية خصوصا، فكل الدول تهتم في ضمان أمنها الوطني بالدرجة الأولى، ولا يمكن لها أن تحقق ذلك دون حماية فضائها السيبراني، فالحروب والهجمات أصبحت تحدث بشكل إلكتروني وتستهدف البنية التحتية للدول، ومما يميّز تلك الحروب أنها تتميز بالسهولة وقليلة التكلفة، كما أنها تسبب أضرار بالغة للدولة المستهدفة، وعليه أصبحت كل الدول تضع استراتيجيات لمواجهتها.
الكلمات المفتاحية: الجريمة المنظمة-التهديدات السيبرانية-الجرائم الإلكترونية-جرائم المعلومات-التعاون الدولي.

Abstract:
Cybercrime has now become one of the features of modern wars, which poses challenges to all developed and developing countries in particular, as all countries are interested in ensuring their national security in the first place, and they cannot achieve this without protecting their cyberspace, as wars and attacks have become electronic and target the infrastructure of countries, and what distinguishes these wars is that they are easy and low-cost, and they cause severe damage to the target country, and therefore all countries are developing strategies to confront them.

Keywords: Organized crime - Cyber threats - Cybercrime - Information crimes- International cooperation.

* المؤلف المرسل

مقدمة:

لا يختلف اثنان في أن التطور الحاصل في تكنولوجيا المعلومات وشبكة الأنترنت عموما وما صاحبها من تحديات وتهديدات ومع ظهور الثورة المعلوماتية أصبحت التكنولوجيا في الوقت الراهن إحدى أنماط القوة التي اكتسبت أهمية كبيرة ومضاعفة، لأنها استطاعت إلغاء المسافات بين الدول وأصبح العالم متسقا ومتقاربا، ومع هذا التطور الهائل من تهديدات من نوع جديد تضمنت أبعاد وخصائص وفواعل من نوع آخر، إذ عده المختصون في المجال الأمني والاستراتيجي والسياسي ضمن الجيل الخامس من الحروب بعد الحروب البرية والبحرية والجوية والفضائية وأصبح بمثابة جيل جديد من الحروب على صعيد الاستراتيجيات الدولية وهذا ما جعل الدول تبحث عن تحصينات وحلول وضمانات أمنية ضمن هذه البيئة الرقمية.

أدى ظهور الجرائم السيبرانية كنمط جديد من أنماط الجريمة وما تتميز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول إلى توجه المجتمع الدولي للتعاون من أجل تصد فعال لتلك الجرائم التي لها بالغ الآثار السلبية، إذا ما تركت على الأمن القومي للدول في جميع النواحي: الاقتصادية منها والعسكرية والاجتماعية، لذلك سعت دول العالم المتقدمة منها والنامية إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها ولعل أبرزها اتفاقية بودابست لمكافحة الجرائم المعلوماتية وغيرها من الاتفاقيات والآليات الدولية.

من خلال ما سبق تظهر بذلك أهمية طرح الإشكالية التالية: ما مدى كفاية الآليات الدولية في مجابهة التهديدات السيبرانية للحد من آثارها؟

إجابة على الإشكالية المطروحة وإحاطة بالموضوع من مختلف الجوانب اعتمدنا الخطة التالية:

المحور الأول: الإطار المفاهيمي للتهديدات السيبرانية

يتم التطرق في الإطار المفاهيمي للتهديدات السيبرانية أولا لتحديد المفاهيم المشابهة وذات الصلة بالجريمة السيبرانية وبيان الخصائص التي تتميز بها الجريمة والمجرم السيبراني.

الفرع الأول: تحديد المفاهيم المتعلقة بالتهديدات السيبرانية

-الهجمات السيبرانية: تعرف بأنها فعلا يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام،[1]كما تختلف الهجمة السيبرانية بشكل جوهري عن الجريمة السيبرانية في كون الهجمة السيبرانية صادرة عن الدولة أو إحدى مؤسساتها بهدف إضعاف الوظيفة التي تقوم بها أجهزة الحاسوب المستهدفة.[2]

-الجريمة: حسب القانونيون الجريمة هي كل سلوك تحرمه الدولة لضرره وترد عليه بعقوبة وهي عندهم أعم من الجناية شمولا، إذ تتضمن المخالفة والجنحة والجناية بحسب تقسيم القوانين.(3)

-السيبرانية: إن أساس نشأة كلمة السيبرانية (cybernetic) ارتبطت باللغة اليونانية والذي يعني التوجيه والسيطرة ومشتقة من كلمة (cybernetes) أي الشخص الذي يدير دفة السفينة، إذ تستخدم مجازا للمتحكم (govemor)، وبذلك بإمكاننا القول أن السيبرانية هي التحكم عن بعد، فهي عندما تأتي مع كلمة أخرى تعني التحكم بها أو إدارتها كما في الأمن السيبراني.(4)

-الجريمة السيبرانية: هي كل فعل غير مشروع يستهدف تغيير البيانات أو المعلومات بالحذف أو الإضافة أو المعالجة أو السرقة أو تحويل المعلومات أو تعديلها لغايات غير مشروعة بواسطة الكمبيوتر أو أية وسيلة تكنولوجية أخرى، هذا التعريف يشمل كل الأفعال الضارة بما فيها التجسس أو الاستغلال الإلكتروني تحت مفهوم الفعل غير المشروع الموصوف بالأمثلة المتعددة الشاملة لكل أنواع الضرر الذي يمكن أن تسببه الجريمة الالكترونية.(5)

-الجريمة السيبرانية فقهيا: يعرفها عمر الدبور بأنها كل سلوك غير مشروع يتم بالتدخل في العمليات الإلكترونية أو المساس بأمن النظم المعلوماتية والمعطيات التي تعالجها.(6)

-الصراع السيبراني: يأخذ الصراع السيبراني طابعا تنافيا من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول ولكن دون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية، والتي تتمثل في هجمات قرصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون لذلك من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي يحدثها تفجير تقليدي مدمر، وقد أضحى الصراع السيبراني أحد أوجه التفاعلات الدولية الجديدة شأنه شأن الهجمات السيبرانية والحرب السيبرانية.(7)

-الأمن السيبراني: يعتبر الأمن السيبراني وفقا لما صدر عن وزارة الدفاع الأمريكية أنه: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بشتى أشكالها (الالكترونية والمادية) من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث، في حين اعتبره الإعلان الأوروبي بأنه: قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة والتي تستهدف البيانات.(8)

-الحرب الالكترونية : هي مستوى من التسلح العسكري المتقدم والذي من شأنه أن يتفوق على الخصم باستخدام وسائل عديدة كتقنية الاختفاء في الطائرات المقاتلة الحديثة

ومنظومة الرصد الجوي (S400) ومنظومة (Thad) الأمريكية وهي تكتيك يهدف إلى تعطيل فاعلية منظومات الدفاع والهجوم عن طريق التشويش والإعاقة الإلكترونية.

-القوة السيبرانية: مع ثورة تكنولوجيا المعلومات ظهر شكل جديد من أشكال القوة هي القوة السيبرانية Power Cyber والتي بدأ تأثيرها واضحا على المستويين الدولي والمحلي فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة القوة وهذا يعني تغيرا في علاقات القوى في السياسة الدولية.(9)

-الردع السيبراني: ويعرف بأنه: منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية.

الهجوم السيبراني: يعد مفهوم الهجوم السيبراني أو بما يسمى بالحرب الافتراضية أو حرب الإنترنت والساحات الرقمية بحد ذاته مفهوما جديدا على صعيد النزاعات الدولية، وهي تشير إلى أساليب للحرب تعتمد على تكنولوجيا المعلومات وتستهدف الحاسبات والمواقع الإلكترونية، وتشمل عمليات تسلل إلى أنظمة الحاسب الآلي، وجمع البيانات أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، كما تشمل عمليات زرع برمجيات ضارة للتجسس، وغير ذلك من العمليات السيبرانية أو الإلكترونية، أو ما يطلق عليه بعمليات اختراق أو القرصنة الإلكترونية.(10)

البنية التحتية الحيوية للمعلومات: إن البنية التحتية ينظر إليها عموما باعتبارها الأنظمة والخدمات والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار على الصحة العامة والسلامة أو التجارة أو الأمن القومي أو على أي مجموعة من هذه الأمور في أن واحد، ويتألف الأمن السيبراني من عناصر مادية تقنية وتأمين مراكز المعلومات والأزمات مثل: المرافق والمباني وغرف البيانات وعناصر افتراضية ذكية مثل الأنظمة والبيانات.(11)

ثانيا: خصائص الجريمة السيبرانية والمجرم السيبراني

تتميز الجريمة السيبرانية والمجرم السيبراني بمجموعة من الخصائص التي تميزهم عن الجرائم المنظمة الأخرى التي هي كذلك تشكل خطرا داهما يستوجب مجابهته والتصدي له وندرجها فيما يلي:

1- خصائص الجريمة السيبرانية:

-الجريمة السيبرانية ترتكب عبر شبكة الإنترنت: فهذه الشبكة هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالبا ما تكون الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن والحماية الإلكترونية في محاولة منها لحماية نفسها أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم.

-تتسم بالخطورة البالغة: فالجرائم لن ترتكب بواسطة شبكة الأنترنت تتسم بالخطورة لبلدة من عدة نواحي، الأولى جسامة الخسائر الناجمة عنها قياسا بالجرائم التقليدية خاصة في جرائم الأموال، والثانية فهي ترتكب من فئات متعددة تجعل من التنبؤ بالمشتبه فيه أمرا صعبا، أما الثالثة فتنطوي على سلوكيات غير مألوفة.

-الجريمة السيبرانية عابرة للحدود الوطنية: ذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجنى عليه في بلد آخر، وهكذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة[12]، وهذه الصفة غالبة للجرائم الالكترونية، فهي تتجاوز حدود الدولة الواحدة وعادة تشمل كل الدول، وكثيرا ما يؤدي ذلك إلى الحاجة للتعاون الدولي من خلال الاتفاقيات الدولية من أجل تحديد المسؤولية واتخاذ الإجراءات القانونية اللازمة.

-الجريمة السيبرانية يصعب إثباتها: أن وسيلة ارتكابها ليست مادية وتسمى بالجريمة الناعمة فهيي تعتمد على أنشطة إلكترونية يمكن إلغائها أو تغييرها ، وليس سهلا إثبات مصدرها إلا من قبل متخصصين، وتقتضي إجراءات محاكمتها لقضاة مؤهلين علميا وتقنيا في هذا النوع من الجرائم.[13]

-صعوبة اكتشاف الجريمة السيبرانية: توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم، وبالتالي فإن هذه الجرائم وفي الغالب لا تترك اثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها.[14]

2- خصائص مرتكبي الجرائم السيبرانية:

-المجرم لا يتواجد على مسرح الجريمة: بل يرتكب جريمته عن بعد وهو ما يعني عدم التو اجد المادي للمجرم السيبراني فقد يوجد الجاني في بلد ما ويستطيع الدخول الى ذاكرة الحاسب الآلي الموجود في بلد آخر، ويظهر أكثر في البرامج الخبيئة (Viruses) حيث يتم نسخها في بلد وترسل الى دول مختلفة من العالم.[15]

-المجرم الإلكتروني ذكي ومتخصص: في الغالب يتميز المجرم الإلكتروني بالذكاء، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة

الأمنية الإلكترونية، حيث يستطيع المجرم الإلكتروني أن يكون تصور كاملا لجريمته حتى لا يتمكن من ملاحقته وتتبع أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكمبيوتر، فالمجرم الإلكتروني عادة يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به، لتجنب ما من شأنه ضبط أفعاله والكشف عنه، كما أنه يتمتع بقدرة ومهارة تقنية يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة في أجهزة الكمبيوتر ومن خلال الشبكات.

-المجرم الإلكتروني شخص سوي واجتماعي: يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال أو بهدف الانتقام.(16)

الفرع الثاني: أنواع التهديدات السيبرانية ومجالات ارتكابها

صحيح أن التهديد السيبراني لا يحدث إلا عبر الحاسب الآلي وشبكة النت، لكنه يختلف من شكل لأخر حسب نوع ارتكابه، كما أن له عدة مجالات يمكن أن يقع فيها ويرتكب في حقها وهذا ما سيأتي معنا فيما يلي:

أولا: أنواع التهديدات السيبرانية

-التهديدات التي تلحق بمكونات الكمبيوتر: وتشمل مكونات الكمبيوتر؛ المادية مثل: وحدات الإدخال والإخراج والتخزين الأقراص المرنة والصلبة والشاشة والطابعة، ومكونات معنوية (بيانات ، معلومات مخزنة في الكمبيوتر) وتتسبب هذه الجرائم بالضرر على هذه المكونات ويمكن أن تدمرها كليا أو جزئيا أو قد تنتقل الى حواسيب أخرى أو قد تمحو أثرها أو تفسدها ومثال ذلك فيروس الفدية.

-التهديدات التي تمس بشبكة المعلومات: وهي أفعال غير قانونية تستهدف المواقع الالكترونية بقصد تعطيلها أو التشويش عليها أو تعديلها أو الدخول الى مواقع خاصة . وتستخدم عناوين غير حقيقية للدخول الى الشبكة ، ويتم نقل الفيروسات وإرسال الرسائل المؤذية وترويج أشياء غير مشروعة.

-التهديدات التي تقع على البيانات والمعلومات: وهي أفعال غير قانونية (دخول أو اعتراض) تستهدف وثيقة أو نص موجود في شبكة الكومبيوترات بقصد سرقتها أو تعديلها أو إتلافها أو نشرها، ومن أمثلتها انتهاك الملكية الفكرية للبرامج أو الإنتاج الفني أو الأدبي أو العلمي، وبإمكان المتطفلين المراقبة والتنصت على الاتصالات الالكترونية. ويوجد الآن مكتبات إلكترونية هائلة في الدول المتقدمة تتضمن البيانات والنصوص التي تم اعتراضها وتسجيلها في كل أنحاء العالم.(17)

ثانيا: المجالات التي تقع عليها التهديدات السيبرانية

يتسع نطاق مجال الجريمة السيبرانية ليشمل جميع مناح حياة الأفراد والمجتمع على سواء، بداية من التدخل في حياته الخاصة وصولاً إلى أمنه، فنطاق الجريمة السيبرانية يطال حياة الأشخاص الخاصة ويقع على أموال الأفراد والمؤسسات، وأخرى تطال أمن الدولة وسلامتها:

-التهديدات السيبرانية تمس بحياة الأشخاص الخاصة:

من المتعارف عليه أن المشرع في مختلف النظم القانونية يسن قوانين بغرض حماية الأشخاص من كل اعتداء قد يطالهم، وبظهور العالم الإلكتروني أصبحت حياة الأشخاص الخاصة في خطورة نتيجة توافر إمكانية السطو والاطلاع على أدق تفاصيل المعلومات عنهم والاستخدام السيئ لها كالتهديد والمضايقة وانتحال شخصية الغير والاستدراج ونشر الإباحة.

- التهديدات السيبرانية تمس الأموال:

من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الإلكترونية، مما زاد من تطور وسائل الدفع الإلكتروني، الأمر الذي أدى إلى تطور الجريمة الإلكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة، كالجريمة التي تلحق ببطاقات الائتمان والتحويلات المالية الإلكترونية، والاحتيال (بطاقات الدفع الإلكتروني، سرقة أموال البنوك، غسيل الأموال...)

- التهديدات السيبرانية تلحق بأمن الدولة:

يعتبر الأمن القومي للدولة من بين الخطوط الحمراء التي لا يجوز المساس بها، وإلا فذلك يعني زوال مؤسساتها وزوال كيانها، وتعد جرائم الإرهاب والتجسس والجوسسة المضادة وغيرها من الجرائم المنظمة من الجرائم السيبرانية التي تمس بالأمن القومي للدولة وتهدد وجوده.[18]

المحور الثاني: دور المجتمع الدولي في التصدي للتهديدات السيبرانية

أثارت الجريمة المنظمة عموما والتهديدات السيبرانية خصوصا قلق المجتمع الدولي نظرا لانتشارها وصعوبة تحديد مرتكبيها، ولهذا فقد اهتم المجتمع الدولي من خلال تحقيق التعاون الدولي من أجل مكافحة هذا النوع من الجرائم والتصدي لها، فضلا عن دور الأجهزة الدولية لمجابهتها.

الفرع الأول: التعاون الدولي لمكافحة التهديدات السيبرانية

-معاهدة بودابست 2001:

تعد معاهدة بودابست لمكافحة جرائم الإنترنت من أولى المعاهدات المتعلقة بتلك الجرائم التي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين

التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيء لها، هذا وقد تناولت تلك المعاهدة الجرائم التي تعتبر من أكثر الجرائم شيوعا على مستوى العالم مثل الإرهاب الإلكتروني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال، كما حددت المعاهدة الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة،[19]وتناولت أيضا أنواع الجرائم الالكترونية وهي الدخول غير القانوني المتعمد والاعتراض غير القانوني المتعمد والتدخل المتعمد على البيانات والمعلومات بهدف تدميرها أو حذفها أو إفسادها أو تغييرها أو تعديلها أو كبتها أو إخمادها، والتدخل المتعمد في الأنظمة بهدف تعطيلها أو تدميرها، وإساءة استخدام الأجهزة واستخدام الكومبيوتر في التزوير أو الاحتيال، وجرائم دعارة الأطفال والجرائم المرتبطة بحق المؤلف.

كانت اتفاقية بودابست وما زالت متقدمة على الجهود الدولية الأخرى في دقة تحديد الجرائم الالكترونية وكذلك رسمت إجراءات عملية وحددت نوعية الأدلة التي تثبت ارتكابها بما يراعي خصوصية هذه الجريمة وأن إثباتها يعتمد على أدلة من نوعية خاصة ذات طبيعة إلكترونية، واستطاعت الاتفاقية أن تثبت جدواها للدول من خارج الاتحاد الأوروبي التي انضمت إليها، فقد صادقت المغرب عليها في عام 2018 وكذلك الولايات المتحدة الأمريكية وكندا وجنوب إفريقيا، ليصل عدد الدول المصدقة عليها إلى 55 دولة أخرى، فضلا عن أنها تضمنت إجراءات رادعة من حيث جسامة الغرامات التي تفرضها.[20]

-توصيات المجلس الأوروبي:

تضمنت توصية المجلس الأوروبي رقم 13/95 الذي أصدرها في 11-09-1995 مجموعة من الأحكام التوجيهية التي تتعلق بإعادة النظر في قوانين الإجراءات الجزائية الداخلية للدول الأعضاء فيه ولاسيما فيما يخص المشاكل المرتبطة بتكنولوجيا المعلومات لمواكبة التطور التكنولوجي التي آلت إليه الحياة الاجتماعية، فنذكر على سبيل المثال:

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

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

-يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
-يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.(21)

-النظام الأوروبي العام لحماية البيانات GDPR:

أنشأت أوروبا هذا النظام في 2016 الذي تعهد إليه مهام حماية البيانات والخصوصية لجميع الأفراد داخل الاتحاد الأوروبي، إذ يهدف إلى تمكين المواطنين من التحكم والسيطرة على البيانات الشخصية وتبسيط بيئة التنظيمات والقوانين للمشاريع التجارية الدولية من خلال توحيدها داخل الاتحاد الأوروبي وهو نظام تنظيمي ولا يتطلب أن تصدر الدول أي تشريع لأن النظام ملزم وقابل للتطبيق مباشرة، كما ويؤمن هذا النظام وجود معرف شخصي (اسم ورقم الضمان الاجتماعي وبيانات الموقع والتعريف عبر الأنترنيت) وأحد العوامل الخاصة بالهوية المدنية أو الفيزيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لكل شخص بهدف تحكمه الكامل في بياناته، ولن يسمح لأية جهة الحصول عليها بدون موافقة، كما تشمل البيانات الشخصية حتى الجنسية والأصل العرقي والتوجه الجنسي والحالة الصحية، ويسمح النظام أيضا للمستخدم أن يطلب مسح بياناته الموجودة لدى أية جهة إلا اذا كانت تتعلق بالتزامات مالية وذلك وفق المادة 17، يجوز كذلك حسب هذا النظام للأشخاص معرفة المعلومات المخزونة عنهم ولا يجوز استخدامها إلا بعد موافقتهم، وبالرغم من أن النظام مصمم لحماية مواطني الاتحاد الأوروبي، إلا أنه أصبح يؤثر بشكل أساسي على جميع مستخدمي مواقع الأنترنت بلا استثناء بغض النظر عن مكان تأسيس النشاط التجاري أو مكان الأنشطة عبر الأنترنيت اذا كان يعالج بيانات أو يجمعها من مواطني الاتحاد الأوروبي فيجب أن يلتزم الآخرين بهذا النظام.

-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010:

تناولت هذه الاتفاقية مجموعة من الفصول ويتعلق الأمر بالتجريم، الأحكام الإجرائية، التعاون القانوني والقضائي، حيث لم تكن الجرائم الموصوفة في الاتفاقية تتناسب مع واقع المعلومات والاتصالات (المادتين 6 و9) وكان التجريم واسعا جدا ويمكن أن يشمل تطبيقات وبرمجيات ضرورية، وتناولت أيضا الاتفاقية جريمة الإباحية المتعلقة بالأطفال، إلا أنها فسحت المجال للدول أن تفسرها بدون تحديد أو قيود (المادة 62)، وتطرقت أيضا إلى الجرائم المتعلقة بالإرهاب واستعمال تقنية المعلومات، وفي الفصل الإجرائي نصت على عبارة غامضة (أية جرائم أخرى) يسمح للدول أن تجرم أي فعل خارج نصوص الاتفاقية وهو أسلوب يتناقض مع مبادئ القانون الجنائي الذي لا

يسمح بالتجريم إلا بموجب نص قطعي وصريح استنادا لمبدأ لا جريمة ولا عقوبة إلا بناءً على نص (المادة 22)، ولم تنص الاتفاقية بشكل واضح على حماية خصوصية المستخدمين وبياناتهم وحقوقهم (المادة 14)، كما تنص هذه الاتفاقية على حرمة الحياة الخاصة دون الإشارة للبيانات الالكترونية، وتسمح للدول الأطراف باتخاذ الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر على أي شخص أو جهة مختصة بتسليم المعلومات دون تحديد ضوابط قانونية لهذه الأوامر (المادتين 24و25)، أي أن الاتفاقية لم تكن تتضمن تفاصيل وافية تسهل تطبيقها على الوقائع المختلفة مثلما تضمنته اتفاقية بودابست مما أدى إلى انحسار عدد الدول العربية المصدقة عليها لعدم ثقتها بجدواها.[22]

-اتفاقية الاتحاد الإفريقي بشان أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي (اتفاقية مالابو2014):

تشكل اتفاقية مالابو نص قانوني استراتيجي في مجال مكافحة الجرائم الالكترونية في إفريقيا، بحيث تعالج مسألة الأمن السيبراني بتوسع، حيث تضمنت مكافحة الجريمة السيبرانية وحماية البيانات الشخصية والإشراف على المعاملات الإلكترونية، وفيما يلي مجموعة من الأهداف على سبيل المثال:

-تعزيز ومواءمة التشريعات الحالية للدول الأعضاء والمجموعات الاقتصادية الإقليمية في مجال تكنولوجيا المعلومات والاتصال مع احترام الحريات الأساسية وحقوق الإنسان والشعوب.

-يجب أن تحترم أي معالجة للبيانات الشخصية التوازن بين الحريات الأسية ومصالح الجهات الفاعلة العامة والخاصة.

-تعزيز استخدام تكنولوجيا المعلومات والاتصال وزيادة التدفق وتخفيض أسعار الأنترنت.[23]

كما وتغطي هذه الاتفاقية نطاقا واسعا من أنشطة الأنترنت بما فيها التجارة الالكترونية، وحماية البيانات والجرائم الالكترونية، والتركيز على العنصرية وكراهية الأجانب، واستغلال الأطفال في المواد الإباحية، والأمن الإلكتروني الوطني (المواد 2-7)، ويفرض على الدول المصدقة عليها سن قوانين لحماية البيانات الشخصية المواد (8-23) وإنشاء سلطة عامة مستقلة (سلطة حماية البيانات الوطنية) وأن تضع كل دولة استراتيجية وطنية للأمن الإلكتروني وإصدار قوانين للجرائم الالكترونية وضمان ممارسة التجارة الالكترونية بحرية، وأن تتم معالجة البيانات فقط في غرض مشروع (المواد 24-31) ولكن لم يتم تعريف الغرض المشروع.

كما أقرت الاتفاقية استثناءً في معالجة البيانات عند وجود (لأغراض تاريخية أو إحصائية أو علمية) وهو استثناء واسع يمكن استغلاله في انتهاك خصوصية المعلومات، بشكل عام

فإن الاتفاقية الإفريقية متكاملة أكثر من الاتفاقية العربية وتجاوزت الانتقادات الموجهة للأخيرة، وأنها أقرب الاتفاقيات للاتفاقية الأوروبية، وكان يرتجى منها مواجهة ظاهرة تفاقم الجرائم الالكترونية في القارة الإفريقية على أسس قانونية فعالة تعتمد على وسائل مبتكرة تتناسب وواقع الدول الإفريقية معتمدة منهجا واسعا في تنظيم وحماية المعلومات والبيانات الالكترونية.

-تقرير الخبراء الدوليين لعام 2019:

منذ 1990 واجهت الأمم المتحدة الجريمة الالكترونية المتعلقة بالكومبيوتر والأنترنيت وكان آخرها تقرير لجنة الخبراء الحكوميين لعام 2019، الذي يهدف الى دراسة شاملة للجريمة الالكترونية واتخاذ التدابير الدولية للتصدي لها وتبادل المعلومات عن التشريعات الوطنية والإجراءات الفضلى والمساعدة التقنية والتعاون الدولي والتفاوض على صك قانوني عالمي جديد بشأن الجريمة الالكترونية في إطار الأمم المتحدة ومراعاة الحاجة إلى تدابير فعالة في إطار إنفاذ القانون ومراعاة السيادة وتعديل قواعد الإثبات لكفالة جمع الأدلة الالكترونية وحفظها والتأكد من صحتها واستخدامها في الإجراءات الجنائية، فضلا عن اعتماد قواعد وطنية لتتبع الاتصالات، تنظيم عمليات التفتيش الوطنية والدولية، وسن قوانين موضوعية وإجرائية محايدة تكنولوجيًا لتمكين الدول من التصدي للأشكال الجديدة والمستجدة للجريمة الالكترونية، وإنشاء هيئة دولية للتحقق من أدوات التحليل الجنائي الرقمية واعتمادها وإعداد الأدلة الإرشادية وتعزيز قدرات إنفاذ القانون والتدابير القضائية للتصدي للجريمة الالكترونية؛ إذ تمثل هذه التدابير تطورا كبيرا في مدى اهتمام الأمم المتحدة نحو تدويل الجريمة الالكترونية وأن تكون منبرا أمميا لأجل ضمان قوة وقانونية الإجراءات ووضع حجر الأساس لإنشاء اتفاقية دولية أممية تواجه هذه الجريمة. (24)

-لجنة خبراء دولية مخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام مكافحة تكنولوجيا للمعلومات والاتصالات للأغراض الإجرامية:

تبنت الجمعية العامة للأمم المتحدة القرار رقم 74/247 في 2019 لصياغة اتفاقية دولية جديدة لمكافحة الجرائم السيبرانية، إذ ينص القرار التي تم تبنيه على إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية لوضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، كما وعقدت اللجنة المخصصة دورة تنظيمية مدتها 3 أيام في أوت 2020 بنيويورك من أجل الاتفاق على مخطط وطرائق أنشطتها الأخرى لتقديمها إلى الجمعية العامة للنظر فيها والموافقة عليها،(25)ومما تجدر الإشارة إليه أنه قد أثار قرار إنشاء اللجنة قلق المجموعات الحقوقية والقوى الغربية التي تخشى أن يفضي إلى تقييد الحريات ويقمع حرية التعبير كما ذهب إليه كل من الصين وايران والعراق، ويرون أن توسيع اتفاقية بودابست والمشاركة فيها

في مواجهة انتهاكات حق النشر والتأليف والاستغلال الجنسي للأطفال أفضل من العمل على اتفاقية أخرى.[26]

الفرع الثاني: الأجهزة الدولية للتصدي للتهديدات السيبرانية

1- المنظمة الدولية للشرطة الجنائية (الإنتربول):

المنظمة الدولية للشرطة الجنائية هي منظمة حكومية دولية فيها 195 بلداً عضواً مهمتها مساعدة أجهزة الشرطة في جميع هذه الدول على العمل معاً لجعل العالم مكاناً أكثر أماناً، ولهذا فإنها تمكن البلدان من تبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها، وتقدم الدعم الفني والميداني بمختلف أشكاله، تتولى الأمانة العامة للإنتربول تنسيق الأنشطة اليومية لمكافحة مجموعة من الجرائم يديرها الأمين العام، يعمل في الأمانة العامة ضباط الشرطة والمدنيين وتتخذ من ليون مقراً لها، كما ولها مجمّع عالمي للابتكار في سنغافورة والعديد من المكاتب الفرعية في مناطق مختلفة من العالم.

توفر الأمانة العامة للبلدان الأعضاء مجموعة من الخبرات والخدمات والإنتربول يتضمن 19 قاعدة بيانات شرطية تحتوي على معلومات عن الجرائم والمجرمين (كالأسماء وبصمات الأصابع وجوازات السفر المسروقة...) والتي يمكن للبلدان الاستفادة منها بشكل آني، كما ويقدم الدعم في التحقيقات عن طريق تحليل الأدلة الجنائية، والمساعدة في تحديد مكان الفارّين من العدالة في جميع أنحاء العالم، ويُعد التدريب جزءاً بارزاً من عمله في الكثير من المجالات حتى يصبح الموظفون ملمّين بكيفية الاستفادة من خدماته بشكل فعال، تُخصص خبراته لدعم الجهود الوطنية في مكافحة الجرائم في ثلاثة مجالات عالمية يعتبرها الأكثر إلحاحاً اليوم وهي: الإرهاب، والجريمة السيبرانية، والجريمة المنظمة.

يتولى الموظفون العاملون في كل من مجالات الجريمة المتخصصة هذه إدارة مجموعة غنية من مختلف الأنشطة مع البلدان الأعضاء، نذكر منها إسناد التحقيقات والعمليات الميدانية والتدريب والتشبيك، والأهم من ذلك هو أنه نظراً إلى تطور الجرائم وتغيرها، يستشرف الإنتربول المستقبل من خلال البحث في الجرائم الدولية واتجاهاتها ومتابعة آخر المستجدات المتصلة بها.[27]

2- شرطة الويب الدولية:

أنشئت هذه المنظمة في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم، ونظرا لاتساع نشاط هذه المنظمة وما تقوم به من إجراءات

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

3- مركز بلاغات احتيالات الإنترنت:

تم إنشاء هذا المركز في الولايات المتحدة الأمريكية بتاريخ 2000/05/18 ليتعاون مع مكتب التحقيقات الفيدرالي والمركز القومي لجرائم ذوي الياقات البيضاء، وذلك بهدف تلقي البلاغات وتتبع الجرائم والاحتيالات التي ترتكب من خلال شبكة الإنترنت بالتنسيق مع أجهزة المكافحة والضبط المعنية داخل الولايات المتحدة الأمريكية وخارجها من خلال موقع المركز على الشبكة الدولية، فمثلا من أجل إحكام الرقابة على شبكة الإنترنت طبقت معظم الدول ما يعرف بنظام الرقيب proxyالذي يقوم بمراجعة نوعية الخدمات المقدمة عبر شبكة الإنترنت، فعندما يطلب المشترك موقعا على الشبكة الأم تصل الإشارة إلى الرقيب الذي يقوم بدوره بعرض الموضوع على قائمة كبيرة جدا من المواقع الممنوعة فإذا تبين له أن الموقع المطلوب يدخل ضمن هذه القائمة المحظورة فلا يستطيع المشترك الحصول على هذا الموقع وتظهر له على الشاشة رسالة بعنوان (تم منع هذا الموقع بواسطة رقيب الأنترنت).[28]

الخاتمة:

تشكل التهديدات السيبرانية ظاهرة عبر وطنية معقدة وسريعة التطور وتشكل تهديدًا كبيرًا لحقوق الإنسان والديمقراطية وسيادة القانون وكذلك للأمن الوطني والدولي، علاوة على ذلك مع الاستخدام المتزايد لتقنيات المعلومات والاتصالات، قد يترتب على أي نوع من الجرائم أدلة على أنظمة الكمبيوتر وغالبًا ما يتم تخزين هذه الأدلة الإلكترونية في ولايات قضائية أجنبية أو متعددة أو متغيرة أو غير معروفة ؛ يشكل الحصول على الأدلة الإلكترونية تحديات كبيرة لسلطات العدالة الجنائية.

ومع تطور استخدام الإنترنت وانتشار استعمالها بلغ عدد مستخدمي الإنترنت في إفريقيا مثلا حوالي 570 مليون مستخدم في سنة 2022 وهو رقم زاد بأكثر من الضعف مقارنة بسنة 2015، مما جعل المنطقة تتقدم على مناطق أخرى مثل أمريكا الشمالية وأمريكا الجنوبية والشرق الأوسط اعتبارًا من جانفي 2022.

أصبح التصدي للجرائم الإلكترونية أولوية بالنسبة للعديد من دول العالم -إن لم نقل كلهم- التي اعتمدت تشريعات محلية واتخذت خطوات نحو الالتزام باتفاقيات مثل بودابست بشأن الجرائم الإلكترونية واتفاقية مالابو بشأن الأمن السيبراني وحماية البيانات الشخصية من أجل تسهيل التعاون الدولي.

لم يكن التعاون الدولي الفعال أكثر أهمية من أي وقت مضى، فهناك حاجة إلى مزيد من التعاون المعزز بين جميع الدول ساء على المستوى الإقليمي أو الدولي، فنجد على سبيل المثال: النهج التعاوني الذي أقرته إفريقيا بمناسبة المنتدى الأفريقي الأول المعني بالجرائم الإلكترونية والمنتدى الأفريقي الثاني الذي نظمته مفوضية الاتحاد الأفريقي ومجلس أوروبا وبدعم من الإنتربول والاتحاد الأوروبي ومكتب الأمم المتحدة المعني بالمخدرات والجريمة وأمانة الكومنولث، ووزارة العدل الأمريكية، والمنتدى العالمي للخبرة الإلكترونية، والمجموعة الاقتصادية لدول غرب أفريقيا (ECOWAS) من أجل إضافة المزيد من الزخم للجهود المتعلقة بالجرائم الإلكترونية من قبل البلدان الأفريقية.

التوصيات:

وفي ختام هذا المقال ندرج مجموعة من المقترحات التي ندرجها في النقاط التالية:

-تطوير وتعزيز ثقافة الأمن السيبراني لتستجيب بفعالية للتهديدات والتحديات العالمية المتعلقة بالتقنيات الحديثة.

-التوعية بالقوانين والتشريعات المتعلقة بالجرائم السيبرانية عبر وسائل الإعلام الجديد والعقوبات التي تقع على مرتكبيها وتفعيل دور مؤسسات المجتمع المدني في مجال التوعية ونشر الوعي.

-التوعية بأخطار الجرائم السيبرانية والتعريف بالعوامل الشخصية التي تسهل الوقوع كضحية لمثل هذه الجرائم- خاصةً وأن نتائج الدراسة الحالية أظهرت اتساع انتشارها في الفضاء السيبراني نظراً لتوفر شروط ارتكابها.

-الاهتمام بمختلف أنماط الجريمة المنظمة في مؤسسات التشريع الوطني وإدراجها ضمن مختلف النصوص القانونية بما يتلاءم والمتغيرات الدولية.

-إنشاء مركز معلومات مشترك يهتم برصد وتحليل الجرائم المنظمة وسبل ضبطها وملاحقة مرتكبيها.

المراجع:

(1) مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد 111، جويلية 2021، ص 11.

(2) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، ديسمبر 2018، ص 346.

(3) بوخنوش أمال، مصطلح الجريمة في قانون العقوبات الجزائري بين الصيغة والمفهوم-دراسة لغوية، مجلة الحكمة للدراسات الإسلامية، المجلد 08، العدد 01، 2021، ص34.

(4) إسراء شريف جيجان، الأمن السيبراني الصيني: دراسة في الدوافع والتحديات ، قضايا سياسية، العدد 56، ص35.

(5) إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية (السيبرانية) في القانون الدولي، مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد 6، العدد 2، 2022، ص 146.

(6) شعاع عبد الرحمن الجاسر، الجرائم السيبرانية الممارسة ضد المرأة السعودية وعلاقتها بالسمات الشخصية للضحية المستخدمة لوسائل الإعلام الجديد، مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية، المجلد 18، العدد1، يونيو 2021، ص 202.

(7) إسراء شريف جيجان، المرجع السابق، ص36-37.

(8) بن عربية رياض، التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا، دفاتر البحوث العلمية، المجلد 10، العدد 1، 2022، ص 463.

(9) إسراء شريف جيجان، المرجع السابق، ص37-38.

(10) البابلي عمار ياسر زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، الفكر الشرطي القيادة العامة لشرطة الشارقة - مركز بحوث الشرطة ، المجلد 30، العدد 118، 2021، ص 27.

(11) البابلي عمار ياسر زهير، المرجع السابق، ص 31.

(12) رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018، ص441و 443.

(13) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 147.

(14) رحموني محمد، المرجع السابق، ص441.

(15) كوثر حازم سلطان موقف لقانون والقضاء من الجريمة الالكترونية (السيبرانية) دراسة مقارنة، مجلة كلية التربية الأساسية، المجلد 22، العدد 96، 2016،ص 973.

(16) رحموني محمد، المرجع السابق، ص 443-444.

(17) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 147.

(18) رحموني محمد، المرجع السابق، ص 444-449.

(19) شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1، يونيو 2020، ص753-755.

(20) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 148.

(21) شيخه حسين الزهراني، المرجع السابق، ص751-752.

(22) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 148.
(23) مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 04، العدد 03، 2021، ص 661.
(24) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 149.
(25) وكالة الأنباء الليبية، الأمم المتحدة تعتزم صياغة اتفاقية دولية لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، 28-12-2019، على الرابط: https://lana.gov.ly/post.php?lang=ar&id=161104 ، تاريخ الاطلاع: 06-04-2023، وقت الزيارة: 15:40.
(26) إبراهيم أحمد عبد السامرائي، المرجع السابق، ص 149.
(27) ما هو الإنتربول؟ ، على الرابط: https://www.interpol.int/ar/3/3 ، تاريخ الاطلاع: 06-04-2023، وقت الزيارة: 16:07.
(28) شيخه حسين الزهراني، المرجع السابق، ص 746-747.