القانون الدولي والتحديات المعاصرة
الجريمة السيبرانية نموذجا

دكتور
محمد محمود فياله
دكتوراه القانون الدولي العام
مدرس زائر - الجامعة الأمريكية الدولية

ملخص البحث :
تعد الجريمة السيبرانية إحدى أكبر التحديات التي تواجه قواعد القانون الدولي، لا لشيء الإ لخصوصية المجرم الذي يقوم بتنفيذها، ذلك المجرم الذي يحرص على إمتلاكه للتكنولوجيا تماما كحرصه على التخفي والهروب من الملاحقة، والحق يقال فقد وفرت له هذه الجريمة بطبيعتها هذا المسعى، فمنحت المجرم فرصة إرتكاب الجريمة عن بعد، فلم يعد من الضروري وجود المجرم في مسرح الحادث ولا حتى بالقرب منه، فقد ترتكب الجريمة في قارة وفاعلها في قارة أخرى.
إن خصوصية هذه الجريمة لم تجعل أحد بمنأى عن وقوعه فريسة في يد هذه الطائفة من المجرمين، فيمكن أن تصبح الدولة بأجهزتها ومؤسساتها فريسة، كما يمكن أن تصبح المنظمات، والشركات الخاصة، بل وحتى الفرد ذاته، في إشارة لاتخطأها العين إلى المجهود الخاص الواجب بذله لصد هذه الهجمات، ولعل ذلك مايفسر حرص المجتمع الدولي والمشرع الوطني على توفير قبة دفاعية قانونية يمكن معها صد هذه الهجمات، بل والتعرف على مرتكبيها وملاحقتهم من خلال تعاون الأجهزة المختصة، بما يضفي على البيئة الإفتراضية حماية إضافية تتناسب مع خصوصية العصر الحديث.
الكلمات الدالة :
الجريمة السيبرانية، الأمم المتحدة، الإتفاقيات الدولية، المشرع الوطني.
أهمية البحث :
تأتي أهمية هذا البحث من أنه يدق ناقوس الخطر، وينبه الأذهان ويشحذ الهمم من أجل إعمال الأقلام وتوفير النص القانوني الذي يمكن معه التعامل مع هذا النوع الجديد من الجرائم، وذلك من خلال عرض لطبيعة الجريمة وآلية التصدي لها على المستويين الوطني والدولي.
إشكالية البحث :
لاشك ان خصوصية الموضوع فرضت على الباحث ضرورة قراءة المشهد من زاوية اخرى، فكثرة الإتفاقيات وتعدد المؤتمرات، لم تفلح حتى الآن في منع إرتكاب هذه الجريمة، فمازال المجرم السيبراني ينتظر كل ظرف خاص ليعظم منهجه وليس أدل على ذلك من جائحة كورونا التي اثبتت ذلك، لذلك فقد جاء هذا البحث ليؤكد عدم ضرورة تقوية النصوص القانونية لتتمكن من ردع ومواجهة هذه الجريمة، الامر الذي يفرض ضرورة تغليظ العقوبة وانشاء محاكم خاصة من اجل المحاكمة عن هذه الطائفة الخاصة من الجرائم.
منهج البحث :
إعتمد الباحث في هذا البحث على المنهج التحليلي المقارن، حيث فضّل الباحث أن يقوم بتحليل هذه الجريمة من خلال عرض سريع لتعريفها وإجتهادات المتخصصين بشأنها، خصوصا أنها تمس الجانب القانوني والجناب التقني في آن معا، كما أنس الباحث إلى عقد المقارنات بين نصوص الإتفاقيات الدولية والتشريعات الوطنية حتى يمكِنه ذلك من فهم أوسع لطبيعة الجهود الدولية المبذولة بصدد هذه الجريمة.

Abstract;
Cybercrime is considered one of the greatest challenges facing the rules of international law, for the sole reason that the privacy of the criminal who commits it, the criminal who desires to possess technology just as he desires to hide and escape prosecution.
It must be said that this crime, by its nature, allowed this class of criminals to do this work, by giving them the opportunity. Crimes are committed remotely. It is no longer necessary for the criminal to be present at the scene of the incident, not even close to it. The crime may be committed on one continent and its perpetrator may be on another continent.
The specificity of this crime does not prevent anyone from falling prey to this group of criminals. The state, with its agencies and institutions, can fall prey, as can organizations, private companies and even the individual himself, which is an unmistakable indication. special efforts that must be made to repel these attacks, and this perhaps explains the desire of the international community and the national legislator to provide a legal defense capable of repelling these attacks, and even of identifying and prosecuting their perpetrators through to cooperation. competent agencies, so as to give the virtual environment additional protection commensurate with the respect for private life of the modern era.
Keywords;
Cybercrime, the United Nations, international Conventions, the national legislator.

مقدمة

لطالما قدٌر على فقهاء القانون الدولي أن يبقوا في حالة ترقب مستمر، ذلك الترقب والحرص على حماية منتجات حقولهم من كل إعتداء محتمل، ولما لا وقد أصبحت هناك ضرورة ملِحة لحماية وتحديث القاعدة القانونية بشكل مستمر حتى تكون قادرة على مواجهة آفات العصر القديم منها والحديث، وليس هذا فحسب بل مايزيد الأمر مشقا وتعقيدا، هو أن هذه الآفة قد تتجدد مع كل تطور يحدث فتتغير معالمها وملامحها مايعني إستحداث وسائل حماية جديدة.

ذلك هو قدر القانون الدولي المحتوم بفروعه المختلفة.

فقد واجه القانون الدولي للبحار في قديم الزمان - وحتى في العصر الحالي - جريمة القرصنة البحرية، تلك الجريمة التي فرضت على رجال القانون الدولي ضرورة الحرص المستمر على توفير القاعدة القانونية الدولية المناسبة التي تقيم المسؤولية في رقبة مرتكبيها، الامر الذي دفعهم الى تعريف هذه الجريمة وتوصيفها بتحديد أركانها من أجل توفير التدابير القانونية المناسبة لها، سواء كانت تدبير وقائية تمنع وقوع هذه الجريمة عن طريق الحرص على بذل الجهود وتشريع النصوص وانشاء الاتفاقيات الدولية التي تضمن حالة التعاون الدولي بين حكومات الدول المختلفة، او التدبير العلاجية التي تعالج هذة الازمة حال وقوعها.

ومع ذلك فلم يتوقف الأمر عن هذا الحد، بل ساهمت التكنولوجيا في ظهور جرائم حديثة، الأمر الذي فرض مرة اخرى على رجال القانون ضرورة شحذ هممهم وإعمال اقلامهم من أجل الحفاظ على حالة التوازن بين مايستجد من أوضاع ومايتطلبه الواقع من نصوص قانونية جديدة، لذلك فقد جاءت النصوص القانونية لتواجه صورة حديثة من هذه الجرائم، وهى الجرائم السيبرانية، تلك الجريمة التي اختلفت في كل شيء عن جريمة القرصنة البحرية الا في هدف واحد، وهو السرقة والإستيلاء بغير حق على مايقع في يد هولاء الطائفة من الخارجين عن القانون.

فقد أصبحنا اليوم أمام نمط جديدة من الفعل الإجرامي وأمام صورة جديدة من المنفذين، بل وأصبح المجرم حريص على إمتلاك التكنولوجيا كحرصه على مخالفة القاعدة القانونية، الأمر الذي أفرز نوعا من التحديات ربما لم يكن موجودا في عصر القرصنة البحرية بمعناها الكلاسيكي.

ومرة أخرى فإن الأمر لم يقف عند هذا الحد، فقد فتحت هذه الجريمة بظهورها بابا جديدا وجب على رجال القانون ضرورة سده وهو أن حكومات الدول ذاتها أصبحت - وفي بعض الحالات - تنفذ هجمات سيبرانية ضد حكومات دول أخرى، وتستخدم هذه التكنولوجيا بما يتعارض مع مبادىء هامة ومختلفة في القانون الدولي الإنساني وهو فرع أخر من فروع القانون الدولي - والذي تأثر بالتطورات التكنولوجية الحديثة - الأمر الذي أدى الى إعادة تعريف العمليات الحربية وطبيعة الأسلحة المسموح بإستخدامها، ومحاربة إستغلال السفن التجارية لأغراض حربية وماقد يترتب على كل ذلك من نتائج وآثار.

وفي ضوء ماتقدم فقد تم تقسيم هذا البحث على النحو التالي :

المبحث الاول : المنهج الدولي في مواجهة الجريمة السيبرانية
المطلب الأول : دور الأمم المتحدة في مواجهة الجريمة السيبرانية
المطلب الثاني : صور التعاون الدولي في مواجهة الجريمة السيبرانية

المبحث الثاني : الآلية القانونية في مواجهة الجريمة السيرانية
المطلب الأول : دور المشرع الوطني في مواجهة الجريمة السيبرانية
المطلب الثاني : دور الإتفاقيات الدولية في مواجهة الجريمة السيبرانية

المبحث الأول
المنهج الدولي في مواجهة الجريمة السيبرانية

ماهى الجريمة السيبرانية، وماهو المقصود بها، وماهى الخلفية التي جاءت منها، وهل يمكن إختزالها في تعريف واحد، أم أن طبيعتها الخاصة فرضت ضرورة تعريفها من أكثر من زاوية، وماهى طبيعة الجهود الدولية لمواجهة هذا النوع من الجرائم، وإذا كنا نتحدث عن الجريمة السيبرانية فلاشك من ضرورة البحث عن تعريف للمجرم السيبراني.

إن البحث عن إجابات واضحة لكل هذه التساؤلات يقتضي ضرورة تعريفها إبتداء، ذلك التعريف الذي يوضح ماهيتها فيسهل مواجهتها والتصدي لها، ذلك أنه كيف يمكن مواجهة شيء دون تحديده والتعرف عليه مسبقا.

وبالإطلاع على المراجع العلمية وتحديدا في عام 1948 نجد أن أول إستخدام لمصصلح Cyber يرجع الى عالم الرياضيات Norbert wiener، وذلك أثناء دراسته لبعض الموضوعات المتعلقة بالهندسة الميكانيكية، أما مايتعلق بتأصيل كلمة Cyber فإن جذورها تعود إلى المعاجم اليونانية، والذي تم أخذه من مصطلح kybernetes والذي يعني القيادة والتحكم عن بعد، تلك المفاهيم التي أستخدمت إبتداء في مؤلفات الخيال العلمي. [1]

الأمر الذي جعل William Gibson يستخدم مصطلح الجريمة السيبرانية لأول مرة في روايته الشهيرة Neuromancer والتي تم نشرها في عام 1982، حيث كان الكاتب يشير بهذا الوصف عن الجريمة السيرانية إلى العالم الإفتراضي والبيئة الخاصة التي يحدث فيها تواصل أجهزة الحاسوب عبر الإنترنت، وإنعدام الأمن وزيادة المخاطر في هذه البيئة الإستثنائية. [2]

أما مايدعو إلى الدهشة فهو أن الجريمة السيبرانية رغم خصوصيتها فإنها ضاربة بجذورها في القدم، فقد وقعت أول جريمة إلكترونية مسجلة في عام 1820، بعد وقت قصير من قيام شركة Joseph-Marie Jacquard، وهي شركة تصنيع نسيج في فرنسا، بإنتاج أول نول قابل للبرمجة، وقد كانت دوافع هذه الجريمة الأولى تتلخص في قلق موظفي الشركة من إحتمالية تعرض وظائفهم التقليدية وسبل عيشهم للتهديد، مما أدى بهم إلى إرتكاب أعمالًا تخريبية لثني الشركة عن إستخدام هذه التكنولوجيا الحديثة. [3]

---

[1]: احمد عبيس الفتلاوي، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق للعلوم القانونية والانسانية، العدد4، 2016، ص614 - 615

[2] : Artur Appazov, Legal Aspects of Cybersecurity, University of Copenhagen, Denmark, 2014, P3

[3] : Animesh Sarmah, Roshmi Sarma, Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Law's of India, Assam Kaziranga University, India, 2017, p1634

وبعد فترة قصيرة من إرتكاب أول جريمة وتحديدا في عام 1834، قامت مجموعة من اللصوص بإختراق نظام التلغراف الفرنسي وسرقة معلومات السوق المالية، مما أدى فعليًا إلى تنفيذ ثاني أخطر هجوم إلكتروني في العالم. [1]

وبحلول عام 1878 وبعد عامين فقط من إختراع Alexander Graham Bell للهاتف، طردت شركة بيل للهاتف الناشئة مجموعة من المراهقين من نظام الهاتف في نيويورك بسبب قيامهم بشكل متكرر ومتعمد بتضليل مكالمات العملاء وقطعها. [2]

وفي عام 1962 أعلن معهد ماساتشوستس للتكنولوجيا بالولايات المتحدة الأمريكية أنه تعرض لهجوم سيبراني عندما قام Allen Scherr بشن هجوم على موقع المعهد، وقام بسرقة كلمات المرورمن قاعدة البيانات الخاصة بالمعهد. [3]

حتى الآن يبدوا أن الجريمة السيبرانية قد ظهرت ملامحها ويمكن تعريفها والوقوف على حقيقتها، ولكن الأمر ليس بهذه السهولة، فعند غياب تعريف قانوني واضح ومحدد، تتكاثر المفاهيم وتتعدد التعاريف وتتعاظم الإجتهادات، وكما هو معلوم أنه عندما توجد حقيقة واحدة، فإن هناك الف نظرية تتواجد معها.

لذلك فهناك من يرى أنه لافرق بين الجريمة السيبرانية وبين الجريمة الإليكترونية، لأن الأداة الحقيقية المستخدمة في إرتكابها هى الحاسب الآلي، وعلى ذلك فالجريمة السيبرانية هى كل سلوك إجرامي وغير قانوني يقوم على إستخدام الأجهزة الإليكترونية للحصول على منفعة مادية ومعنوية وذلك من خلال إختراق الأنظمة المعلوماتية. [4]

وهناك من يرى أنه غالبًا ما يتم استخدام مصطلحات جرائم الكمبيوتر، وجرائم تكنولوجيا المعلومات، والجرائم الإلكترونية، وجرائم التكنولوجيا المتقدمة بالتبادل للإشارة إلى فئتين رئيسيتين من الجرائم، الأول يشمل تلك الجرائم التي يكون فيها الكمبيوتر هدفًا للجريمة، مثل الهجمات على سرية الشبكة وتوافرها، بالإضافة إلى الوصول غير المصرح به إلى الأنظمة أو البرامج أو البيانات والتلاعب بها بشكل غير مشروع. [5]

في حين أن الفئة الثانية تشمل الجرائم التقليدية مثل الاحتيال والتزوير والسرقة التي ترتكب بمساعدة أو عن طريق أجهزة الكمبيوتر وشبكات الكمبيوتر وما يتصل بها من تكنولوجيا الاتصالات والمعلومات. [6]

أما Sussman and Heuston فقد عرفا الجريمة السيبرانية بأنها عبارة عن المخالفات أو الجرائم التي تحدث عبر الاتصالات الإلكترونية، أو أنظمة المعلومات،

---

[1] : Animesh Sarmah, Roshmi Sarma, Amlan Jyoti Baruah, ibid, p1643

[2] : Ibid, p1643

[3] : وللمزيد من الجرائم السيبرانية برجاء الاطلاع على الرابط التالي
https://arcticwolf.com/resources/blog/decade-of-cybercrime/

[4]: قادري نور الهدى، الجريمة السيبرانية وآليات مكافحتها : مواجهة تحديات الامن السيبراني، المجلة للحقوق والعلوم السياسية، العدد1، 2023، ص5

[5] : Artur Appazov, ibid, P22 Abdelmonem Mohamed Magdy, Overcoming the conflict of jurisdiction in cybercrime, Master thesis, American University in Cairo, 2020, P2

[6] : Abdelmonem Mohamed Magdy, ibid, p2

كما يمكن وصف الجريمة السيبرانية بأنها الجرائم الإلكترونية، والجرائم المتعلقة بالكمبيوتر، وجرائم التكنولوجيا المتقدمة، وجرائم عصر المعلومات. [1]

وفيما يتعلق ب Susan Brenner فقد ذهبت إلى القول بأن الجريمة السيبرانية هى جزء من العدوان السيبراني، وعلى ذلك فيمكن تقسيم العدوان السيبراني إلى ثلاث فئات، هى الجريمة السيبرانية، والإرهاب السيبراني، والحرب السيبرانية. [2]

وفيما يتعلق ب Tom Forester فقد عرفها بأنها فعل إجرامي يقوم على إستخدام الكمبيوتر كأداة رئيسية في تنفيذ الفعل، كما جاء تعريف آخر لهذه الجريمة نتيجة الإستبيان الذي أجرته منظمة التعاون الإقتصادي والتنمية في عام 1982 حول طبيعة الغش المعلوماتي، بأنها كل فعل أو إمتناع يتعلق بالإعتداء على الأموال المادية أو المعنوية، يكون إستخدام التقنية المعلوماتية فيه أمرا ضروريا سواء تم ذلك بشكل مباشر أو غير مباشر.[3]

أما المجرم السيبراني فيمكن تعريفه بأنه الشخص الذي لديه المقدرة على تحويل لغته الخاصة إلى لغة رقمية يمكنه تخزينها وإسترجاعها بإستخدام أجهزة الحاسب الآلي، وذلك عن طريق القيام بفعل أو الإمتناع عن فعل، كما يعرف بأنه الشخص الذي يتمتع بقدرة عالية من المهارات، بحيث تمكنه هذه القدرات من إختراق الأنظمة المعلوماتية والتلاعب بالبيانات والمعلومات الشخصية لجمهور المتعاملين للبيئة الإفتراضية. [4]

وبناء على ماتقدم فيمكن تقسيم هذا المبحث على النحو التالي :

المطلب الأول : دور الأمم المتحدة في مواجهة الجرائم السيبرانية

المطلب الثاني : صور التعاون الدولي في مواجهة الجريمة السيبرانية

---

[1] : Animesh Sarmah, Roshmi Sarma, Amlan Jyoti Baruah, ibid, p1633

[2] : William M. Stahl, the uncharted water of cyberspace; applying the principles of international maritime law to the problem of cybersecurity, University of Georgia, 2010, p270

[3]: حاتم احمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، العدد1، 2021، ص15

[4]: قادري نور الهدى، مرجع سابق، ص 8

المطلب الأول
دور الأمم المتحدة في مواجهة الجرائم السيبرانية

لايمكن لأحد أن ينكر الدور المحوري الذي تقوم به الأمم المتحدة في مواجهة الجريمة السيبرانية نظرا لما لهذه الجريمة من نتائج سلبية ومباشرة على جميع أعضاء الجماعة الدولية، الأمر الذي دفع الأمم المتحدة إلى عقد إتفاقيات دولية وإصدار قرارات دورية سواء من خلال الجمعية العامة أو مجلس الأمن، أو تقديم كل أوجه المساعدة لاي دولة من دول العالم.

فمع بداية العقد العاشر من القرن العشرين وتحديدا في عام 1990 عقدت الأمم المتحدة المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين والذي جرى انعقاده في هافانا، حيث ناشدت فيه الدول الأعضاء إلى ضرورة الأخذ في الإعتبار الجرائم ذات الصلة بالحاسب الآلي، وأن تكثف جهودها من أجل سن المزيد من التشريعات والقوانين التي تواجه به هذه الطائفة من الجرائم، بما في ذلك - النظر متى دعت الحاجة إلى - تعديل القواعد والنصوص المطبقة، وأن تعقد الدول من الإتفاقيات الدولية مايمكنها من تفعيل مبدأ تسليم المجرمين المتورطين في إرتكاب هذا النوع من الجرائم. [1]

وفي عام 1991 بدأ الحديث الجدي عن ظهور الشبكة الدولية للمعلومات، بحيث يرجع الفضل في إكتشافها إلى العالم البريطاني Tim Berners-Lee وذلك أثناء فترة عمله في المنظمة الأوروبية للبحوث النووية. [2]

ومع منتصف العقد العاشر وتحديدا في عام 1994 أصدرت الأمم المتحدة الدليل الخاص بمنع ومكافحة الجرائم المتصلة بالحاسوب United Nations Guide to Preventing and Combating Computer-Related Crimes 1995 بحيث يكون هذا الدليل عاملا مساعدا يقدم للدول السبل والوسائل القانونية، ويوفر النهج المشترك لدول العالم، من أجل المساعدة في مواجهة الجرائم المتصلة بالحاسب الآلي والتعرف عليها وتوفير كافة وسائل الدعم من أجل تحقيق نتائج مناسبة.

ومع نهاية العقد العاشر وتحديدا في عام 1998 بدأت الأمم المتحدة تدرك جيدا معنى الدور الحقيقي الذي يمكن أن تلعبه شبكة المعلومات، وكذا حجم التأثير الذي يمكن أن تقوم به في إطار العلاقات الدولية، ومايمكن أن يعده ذلك تهديدا يمكن أن يلحق بالسلم والأمن الدوليين نتيجة ذلك، خصوصا مع وقوع حادثة شهيرة، نفذتها مجموعة من الخارجين عن القانون يحملون الجنسية الصينية أطلقت على نفسها مسمى مركز الرد السريع للقراصنة الصينيين، والذي تكون من 3000 قرصان إليكتروني، نفذوا هذه الهجمات ضد مواقع إليكترونية للحكومة الأندونسية كرد على المظاهرات التي شهدتها الشوارع الأندونسية ضد الحكومة الصينية، عند هذه المرحلة إنتبهت الأمم المتحدة وأدركت أن هناك أمر إستثنائي يستوجب التدخل والرد السريع. [3]

---

[1] : هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، طبعة 1994 ، ص 49

[2] : سامر محيي حمزة، مدى مساهمة الامم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني : دراسة في ضوء تقرير فريق الخبراء الدولي لعام 2021، مجلة مركز دراسات الكوفة، العدد 76، 2022، ص328

[3]: المرجع نفسه، ص328

وعلى الفور تم طرح الموضوع للنقاش في إجتماع عقد أمام الجمعية العامة للأمم المتحدة في العام نفسه، بمبادرة روسية حيث ناقش الإجتماع علاقة تطورات الأنترنت بالأمن الدولي، وطلبت فيه من الدول الأعضاء إبداء أرائهم في هذا الصدد. [1]

وبعد عدة مناقشات بين وفود الدول الأعضاء، رأت الجمعية العامة للأمم المتحدة ضرورة تشكيل فريق من الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية ضمن الأمن الدولي، [2] كما قامت الجمعية العامة بإصدار العديد من القرارات التي تواجه بها كافة صور الجريمة السيبرانية. [3]

وفي عام 2000 إعتمدت الجمعية العامة للأمم المتحدة بموجب القرار رقم 25/55 المؤرخ في 15 تشرين الثاني/نوفمبر 2000 إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، بحيث تعد هذه الإتفاقية الصك الدولي الرئيسي في مكافحة الجريمة المنظمة عبر الوطنية.

---

[1]: المرجع نفسه، ص328

[2]: المرجع نفسه، ص329

[3]:

1. القرار 121/45 العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

2. القرارات 70/53 في 4 كانون الأول/ديسمبر 1998، و49/54 في 1 كانون الاول/ديسمبر 1999، 28/55 في 20 تشرين الثاني/نوفمبر 2000 و19/56 في 29 تشرين الثاني/نوفمبر 2001 و53/57 في 22 تشرين الثاني/نوفمبر 2002 و32/58 في 18 كانون الأول/ديسمبر 2003 حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي.
3. القرارات 63/55 في 4 كانون الأول/ديسمبر 2000، و121/56 في 19 كانون الأول/ديسمبر 2001 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.
4. القرار 239/57 في 20 كانون الاول/ديسمبر 2002 بشأن «إنشاء ثقافة عالمية للأمن السيبراني.
5. قرارات الجمعية العامة 239/57 في 31 كانون الثاني/يناير 2003 و199/58 في 30 كانون الثاني/يناير 2004 بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

من ناحية أخرى، هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل:

1. القرار CCPCJ 16/2/2007 من نيسان/أبريل 2007 «المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال» (الفقرات 7، 16).
2. قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ 26 تموز/يوليو 2007 بعنوان «التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية (E/2007/30 و.(E/2007/SR.45)
3. قرار المجلس الاقتصادي والاجتماعي 26/2004 بتاريخ 21 تموز/يوليو 2004 بعنوان «التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة».

وللمزيد برجاء الاطلاع على الموقع التالي.

https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA

وقد تم فتح باب التوقيع على الإتفاقية من قبل الدول الأعضاء في مؤتمر سياسي رفيع المستوى والذي إنعقد لهذا الغرض في باليرمو، إيطاليا، في الفترة من 12-15 ديسمبر 2000 ودخلت الإتفاقية حيز التنفيذ في 29 سبتمبر 2003 وألحق بالإتفاقية ثلاث بروتوكولات تستهدف مجالات ومظاهر محددة للجريمة المنظمة حيث تضمن الآتي :

بروتوكول منع وقمع ومعاقبة الإتجار بالأشخاص، وخاصة النساء والأطفال؛ بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو، وبروتوكول مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والإتجار بها بصورة غير مشروعة، ولابد أن تكون البلدان أطرافا في الإتفاقية نفسها قبل أن تصبح أطرافا في أي من البروتوكولات.

وفي نفس العام صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فينا، إعلان فيينا بشأن الجريمة والعدالة مواجهة تحديات القرن الحادي والعشرين، حيث أكدت الأمم المتحدة فيه أن منع الجريمة وتحقيق العدالة الجنائية يتطلب إشراك الحكومات والمؤسسات الوطنية والإقليمية والأقاليمية والدولية والمنظمات الدولية الحكومية وغير الحكومية ومختلف قطاعات المجتمع الأهلي، بما فيها وسائط الإعلام الجماهيرية والقطاع الخاص، وكذلك الإعتراف بدور ومساهمة كل منها، باعتبارها جهات شريكة وفعالة.

ونتيجة لذلك فقد تقدم الجانب الروسي بمشروع قرار يتعلق بوجوب توفير مجموعة من المبادئ التي تكفل أمن المعلومات الدولية، بهدف حماية بيئة المعلومات وتجريم ما يسمى بأسلحة المعلومات، ولاشك أن كان لهذه المبادرة دوافع خاصة، فقد ظهرت هذه المبادرة على خلفية المخاوف الروسية بشأن الهيمنة الغربية المتصورة على قطاع تكنولوجيا المعلومات.[1]

وفي نفس العام أوصت الجمعية العامة للأمم المتحدة بإصدار أول قانون لتكنولوجيا المعلومات في الهند، وقد صدر هذا القانون بناء على قانون الأمم المتحدة النموذجي بشأن التجارة الإلكترونية الأونسيترال النموذجي، كما تم إجراء بعض التعديلات على هذا القانون في عام 2008؛ وبذلك تم إقرار قانون تكنولوجيا المعلومات لعام 2008 الذي يغطي مجموعة واسعة من المجالات مثل المعاملات التجارية عبر الإنترنت والتوقيعات الرقمية والتجارة الإلكترونية وما إلى ذلك. [2]

وفي عام 2005 عقدت الأمم المتحدة المؤتمر الحادي عشر حول الجريمة والعدالة الجنائية والذي عقد في بانكوك، حيث تضمنت أجندة المؤتمر عدة موضوعات تناولت سبل التعاون الدولي في التصدي للإرهاب وللعلاقات بين الإرهاب والانشطة الإجرامية الأخرى في سياق عمل مكتب الأمم المتحدة المعني بالمخدرات والجريمة، وتعزيز

[1] : The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century, UNIDIR, 2017, p15

[2] : Pallavi Kapila, Cyber Crimes and Cyber Laws in India: An Overview, MCM DAV College for Women, Chandigarh, India, 2020, p3

التعاون الدولي في إنفاذ القانون بما في ذلك تدبير تسليم المجرمين، و طبيعة الجرائم المالية والإقتصادية بإعتبارها تحديات تواجه التنمية المستدامة.[1]

وفي عام 2006 تزايدات الهجمات السيبرانية والتي أدت إلى وقوع خسائر كبيرة تعرضت لها استونيا ثم تلتها جورجيا في عام 2008، الأمر الذي دفع الأمم المتحدة إلى إعطاء أولوية قصوى للهجمات السيبرانية، عن طريق إنشاء فريق متخصص يتكون من 15 عضوا حيث ظل هذا الفريق يعمل من عام 2009 حتى عام 2010 تم تابعه فريق آخر بدأ العمل من عام 2012 وحتى عام 2013 ، وقد عقد الفريقين عدة إجتماعات مطولة، لكن لم تحقق هذه الإجتماعات الغاية المنشودة منها، فلم تفلح الإ في التأكيد على بذل المزيد من الجهد لمناقشة المعايير المتعلقة بإستخدام الدول للتكنولوجيا والإتصالات. [2]

وفي عام 2011، قدم بعض أعضاء منظمة شنغهاي للتعاون " الصين والإتحاد الروسي وطاجيكستان وأوزبكستان " مدونة قواعد السلوك الدولية لأمن المعلومات إلى الجمعية العامة، وتضمنت مدونة قواعد السلوك المقترحة أحكاماً طوعية تحظر إستخدام الإنترنت للأغراض العسكرية، وخاصة للقيام بأنشطة عدائية أو أعمال عدوانية عن طريق إنتشار أسلحة المعلومات أو التكنولوجيات ذات الصلة، كما دعا إلى إحترام المعايير القائمة مثل السيادة والسلامة الإقليمية والإستقلال السياسي وضمان سلامة سلسلة التوريد.[3]

وبحلول عام 2014 تم تشكيل فريق آخر حيث نجح هذا الفريق في التوصل إلى مجموعة من المبادىء التي تؤكد على ضرورة إنطباق القانون الدولي على الفضاء السيبراني، كما أكد الفريق على أن الدولة التي تقوم بعمل عدائي تقوم مسؤوليتها متى ثبت علاقتها بإرتكاب هذا الفعل. [4]

وفي عام 2019 حرص الأمين العام للأمم المتحدة على القيام - وتحت إشرافه الخاص - بجمع آراء الدول الأعضاء حول التحديات التي تواجهها في مكافحة استخدام تكنولوجيات المعلومات والإتصالات لأغراض إجرامية، وحول التحديات التي تواجه هذه الدول عند إنفاذ القوانين الوطنية. [5]

وفي نفس العام سمح قرار الجمعية العامة للأمم المتحدة رقم 247/74، الذي تم إعتماده في ديسمبر 2019، بتشكيل لجنة حكومية دولية مخصصة مفتوحة العضوية لتعزيز مسألة وضع صك عالمي جديد للتعامل مع الجرائم السيبرانية، وقد تأخرت

---

[1]: مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، أوجه التآزر والاستجابات – التحالفات والاستراتيجيات في مجال الجريمة والعدالة الجنائية، بانكوك، 2005

[2] : سامر محي حمزة، مرجع سابق، ص 330

[3]: The United Nations, Cyberspace and International Peace, ibid, p26

[4]: سامر محي حمزة، مرجع سابق، ص330

[5] : The UN cybercrime debate enters a new phase, Global Initiative Against Transnational Organized Crime, Geneva, 2021, P9

الخطوات التالية للعملية - بما في ذلك الإتفاق على العضوية والرئاسة - بسبب جائحة فيروس كورونا 2019 (COVID-19).[1]

ومما يمكن قوله في هذا الصدد أنه، كان هناك تأثير كبير سببه فيروس كورونا 2019 (COVID-19)، حيث أدت ظروف إنتشار هذا الفيروس إلى تراجع معدلات الجريمة التقليدية، وفي نفس الوقت تزايد معدلات الجريمة السيبرانية [2]، خصوصا مع إعتماد حركة المال والأعمال من خلال شبكة الإنترنت، فقد جعلت هذه الأزمة الإعتماد الكامل على هذه الشبكة، الأمر الذي وفر بيئة خصبة للخارجين عن القانون من المجرمين السيبرانيين.

وفي عام 2022 نظم مكتب الأمم المتحدة المعني بالمخدرات والجريمة the United Nations Office on Drugs and Crime (UNODC) في فيينا الدورة الحادية والثلاثين لمنع الجريمة والعدالة الجنائية، وقد هدفت هذه الفعالية إلى تعزيز المشاركة بين الممارسين ومنظمات المجتمع المدني وأصحاب المصلحة الآخرين، ومعالجة عدد من القضايا الرئيسية، مع أكثر من 80 حدثًا جانبيًا مسجلًا، من أجل منع ومكافحة مختلف أشكال الجريمة، وتعزيز العدالة، وحماية الضحايا.[3]

وقد أوصت السيدة ريتا ثيودورو سوبرمان، عضو الوفد القبرصي في كلمتها أن تنفيذ آلية مراجعة إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية " إتفاقية باليرمو " وبروتوكولاتها من قبل مكتب الأمم المتحدة المعني بالمخدرات والجريمة يتيح الفرصة، على المستوى التشريعي، لتحديد مدى صحة الأحكام الحالية، مستمدة من تطبيق الإتفاقية وبروتوكولاتها، مع مراعاة تكنولوجيا المعلومات الحديثة والتكنولوجيات الرقمية التي تستخدمها الشبكات الإجرامية العالمية لتنفيذ أنشطتها الخبيثة.[4]

أما فيما يتعلق بمجلس الأمن فقد أكد في قراره (2014) S/RES/2178 على أنه - بالنسبة للمقاتلين الإرهابيين - للدول الأعضاء منع وقمع تجنيد أو تنظيم أو نقل أو تجهيزهم، وكذلك منع وقمع تمويل أو سفر هؤلاء الأفراد، كما أكد على ضرورة إدراج أسماء كافة الأفراد المشتركين في هذه العمليات في القائمة وذلك بموجب القرار (2014) 2161 . [5]

كما أكد مجلس الأمن في القرار رقم (2016) 2322 والخاص بتعزيز التعاون القضائي، على التزام الدول الأعضاء بمنع تحركات الإرهابيين والجماعات الإرهابية وفقا للقانون الدولي، مع إعتماد عدة ضوابط وطرق منها فرض إجراءات خاصة و

---

[1] : ibid, p18

[2] : عماد الدين محمد كامل، الجرائم السيبرانية في زمن كورونا وآثارها على الامن القومي الاقتصادي : دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة، بنك دبي الاسلامي، العدد 500، 2022، ص627 - 626

[3]: للمزيد برجاء الإطلاع على الموقع التالي

https://www.pam.int/ar/press-releases/pam-contributes-general-debate-31st-session-unodc-commission-crime-prevention-and

[4] :ibid

[5]: https://www.un.org/securitycouncil/ar/s/res/2178-%282014%29

فعالة على الحدود، وتبادل المعلومات على وجه السرعة، وتحسين التعاون بين السلطات المختصة، لمنع دخول الارهابيين والجماعات الإرهابية إلى أراضيها أو خروجهم منها. [1]

وفي قراره رقم S/RES/2396 (2017) أكد مجلس الأمن على أنه يجب على الدول الأعضاء ضرورة تعزيز جهودها الرامية إلى وقف التهديد الذي يشكله المقاتلون الإرهابيون الأجانب من خلال تدابير تتعلق بمراقبة الحدود وبالعدالة الجنائية وتبادل المعلومات ومكافحة التطرف، ودعوة الدول الأعضاء إلى إتخاذ الإجراءات المناسبة فيما يتعلق بالإرهابيين المشتبه بهم وأفراد أسرهم المرافقين لهم الذين يدخلون أراضيها، بما في ذلك عن طريق النظر في إتخاذ تدابير مناسبة للملاحقة القضائية وإعادة التأهيل وإعادة الإدماج إمتثالا للقانون المحلي والدولي. [2]

وفيما يتعلق بإتخاذ التدابير المناسبة من أجل تحقيق العدالة الجنائية بصورة فعالة فقد تقدم القاضي Stein Schjolberg في عام 2015 بمشروع قانون إلى الأمم المتحدة يتضمن إنشاء محكمة جنائية دولية أو محكمة للفضاء السيبراني تختص بالمحاكمة عن هذه الطائفة من الجرائم، كما يرى القاضي أن من حق مجلس الأمن إنشاء هذه المحكمة تطبيقا لسلطاته التي اعطاها له الفصل السابع من ميثاق الأمم المتحدة، بحيث تشكل هذه الجريمة السيبرانية تهديد للأمن والسلم الدوليين. [3]

وفي ذات السياق فقد أعلن المدعي العام للمحكمة الجنائية الدولية كريم خان على أن المحكمة الجنائية الدولية تدرس في الوقت الحالي إمكانية ضم طائفة الجرائم السيبرانية لدائرة الجرائم التي تدخل في إختصاص المحكمة الجنائية الدولية، الأمر الذي يعني إمكانية تعديل ميثاق روما الأساسي المنشىء للمحكمة حتى يستوعب هذه النمط الجديد من الجرائم، ولعل حجة خان في هذا الصدد هى أن الجريمة السيبرانية يصدق عليها وصف الدولية مما يجعل المحكمة مستحقة للفصل في الدعاوى الناشئة عن هذه الجرائم. [4]

وبالعودة إلى مجلس الأمن فنجد حرصه وبصفة مستمرة على تنبيه الدول الأعضاء على منع تحركات الإرهابيين من خلال المراقبة الوطنية الفعالة للحدود ومن خلال تدابير لمنع تزوير وثائق الهوية أو تزييفها أو استخدامها بطرق احتيالية، ويقرر أن تقوم الدول الأعضاء بتنفيذ نظم لجمع وإعداد وتبادل المعلومات المتعلقة بقوائم المراقبة أو قواعد بيانات الإرهابيين المعروفين والمشتبه بهم، بمن فيهم المقاتلون الإرهابيون الأجانب، كما يدعو إلى إتخاذ إجراءات على الصعيد العالمي والإقليمي والوطني لرفع

[1] : راجع قرار مجلس الأمن رقم 2322 (2016) ، والذي اتخذه في جلسته رقم 7831 المنعقدة بتاريخ 12 ديسمبر 2016

[2] : https://www.un.org/securitycouncil/ar/content/sres23962017

[3] : Stein Schjolberg, The Third Pillar for Cyberspace, An International Court or Tribunal, Geneva, 2015
for Cyberspace,

[4] : https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC

مستوى التنفيذ الفعال للخطة العالمية لأمن الطيران الجديدة الخاصة بمنظمة الطيران المدني الدولي، التي تسعى إلى تعزيز أمن الطيران في جميع أنحاء العالم.[1]

وبعد كل ماتقدم فيمكن القول بأن الأمم المتحدة كانت ومازالت حريصة دائما على تنفيذ العديد من البرامج والمشاريع المتعددة بشأن الجرائم السيبرانية، وذلك من خلال وكلاتها المتخصصة، فعلى سبيل المثال، يقدم مكتب الأمم المتحدة المعني بالمخدرات والجريمة the United Nations Office on Drugs and Crime (UNODC)'s المساعدة الفنية للدول الأعضاء ويقدم العديد من الدورات المتخصصة مثل التعلم الإلكتروني في الطب الشرعي الرقمي، وكذلك الحال فيما يتعلق بمعهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة The United Nations Interregional Crime and Justice Research Institute فقد قام بإنشاء مبادرة الذكاء الإصطناعي من أجل أطفال أكثر أمانًا، والتي تهدف إلى أن تكون بمثابة مركز عالمي للإستفادة من الذكاء الإصطناعي لمكافحة مواد الإعتداء الجنسي على الأطفال. [2]

[1] : https://www.un.org/securitycouncil/ar/content/sres23962017

[2] : The UN cybercrime debate, ibid, p11

المطلب الثاني
صور التعاون الدولي في مواجهة الجريمة السيبرانية

فرضت الطبيعة الخاصة للجريمة السيبرانية، منهجا خاصة لمواجهتها، ذلك المنهج الذي جاء في صورة التعاون الدولي وإن إختلفت مظاهره واتحدت مقاصده، فقد أخذ التعاون الدولي صور كثيرة، منها تفعيل التعاون الحقيقي على مستوى حكومات الدول والمنظمات الدولية والإقليمية - الحكومية وغير الحكومية - وإنشاء منظمات متخصصة، وتسهيل الإتصال بين الأجهزة الوطنية المختلفة لدول العالم ذات الصلة بموضوع الجريمة السيبرانية، ولم يقف الأمر عند هذا الحد، بل تم تنفيذ العديد من المؤتمرات الدورية لمناقشة التحديات المستجدة بين أعضاء الجماعة الدولية، وإعتماد برامج تدريب متقدمة للمتخصصين، وكذا الحرص على توحيد الجهد التشريعي بين العديد من دول العالم، حتى يكون هناك قدر كاف من التنسيق والتعاون مما يؤدي الى تحقيق النتائج المرجوة.

فعلى مستوى الجهود الداخلية للدول وفيما يتعلق بأمريكا الشمالية - تحديدا الولايات المتحدة الأمريكية - فقد أنشأت حكومة الولايات المتحدة المعهد الوطني لتعليم الأمن السيبراني National Institute for Cybersecurity Education (NICE) بالتعاون مع وزارة التعليم ومجموعة من الوكالات الأخرى لإعتماد استراتيجية متعددة المحاور لبناء جيل جديد يتمتع بالذكاء السيبراني من خلال التدريب والتوعية من خلال البرامج التعليمية للدراسات العليا والتطوير المهني لمحترفي الأمن الفيدرالي، كما يعد المعهد الوطني شراكة حقيقية بين الحكومة والأوساط الأكاديمية والقطاع الخاص تركز على دعم قدرة الولايات المتحدة على مواجهة تحديات القوى العاملة الحالية والمستقبلية المتعلقة بتعليم الأمن السيبراني من خلال تبني واعتماد أفضل المعايير و الممارسات. [1]

كما قامت الولايات المتحدة الأمريكية في عام 2000 بإنشاء مركز بلاغات إحتيالات الإنترنت The Internet Crime Complaint Center ليكون همزة الوصل بين مكتب التحقيقات الفيدرالي Federal Bureau of Investigation (FBI) والمركز القومي لجرائم ذوي الياقات البيضاء National white collier crime center وذلك بهدف تلقي البلاغات والتحقيق في الجرائم التي يتم إرتكابها من خلال شبكة الإنترنت وذلك بالتنسيق مع كافة الأجهزة المتخصصة في داخل الولايات المتحدة الامريكية وخارجها. [2]

---

[1] :
وللمزيد برجاء الاطلاع على الموقع التالي :

https://www.nist.gov/itl/applied-cybersecurity/nice

Artur Appazov, ibid, p45

[2] : شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، العدد1، 2020، ص747

وعلى مستوى كندا فقد تم إسناد هذه المهمة إلى مكتب مفوض الخصوصية الكندي Office of the Privacy Commissioner of Canada (OPC) فهو المسؤول عن حماية المعلومات الشخصية والوثائق الإلكترونية وتقديم التقارير الخاصة بها إلى البرلمان. [1]

وفيما يتعلق بالإتحاد الأوربي فقد تم إسناد مهمة حماية الوكالات الحكومية من إمكانية وقوع هجمات سيبرانية إلى وكالة حماية البيانات Data Protection Agency (DPA) فهى الجهة المسئولة عن حماية البيانات لدول الإتحاد الأوربي كما يمكن إعتبارها سلطة عامة مستقلة تشرف على قوانين حماية البيانات وتحقق فيها وتطبقها داخل الإتحاد الأوروبي. [2]

وفيما يتعلق بأمريكا الجنوبية - وتحديدا الأرجنتين - فقد تم إسناد هذه المهمة إلى المديرية الوطنية لحماية البيانات National Data Protection Directorate (NDPD) وتتولى هذه مسؤولية تسجيل قواعد البيانات الوطنية، وهى أداة منظمة تستخدم لتتبع قواعد البيانات المتداولة في جميع أنحاء البلاد والتحكم فيها، وكذلك اتخاذ كافة التدابير المتعلقة بحماية البيانات الشخصية، وهى تعمل تحت إشراف وزارة العدل وحقوق الإنسان. [3]

وفيما يتعلق بأسيا - وتحديدا ماليزيا - فقد تم إسناد هذه المهمة إلى وزارة الإعلام والثقافة والإتصالات Ministry of Information, Culture, and Communications فهى التي تتولى تعيين المفوض الخاص لحماية البيانات الشخصية The Personal Data Protection Commissioner وإنفاذ القوانين الخاصة بها. [4]

وقد يأخذ التعاون صورة أخرى فقد يتمثل في تبادل كافة صور المساعدات والتجهيزات الأمنية بين أجهز إنفاذ القوانين الوطنية المختلفة مثل تبادل البيانات والمعلومات وقد تمثل ذلك في قيام الشرطة النيوزيلندية بتنبيه الشرطة الأسترالية بحدوث تواصل جنسي عبر الإنترنت مع فتاة - وهمية، غير حقيقية إبتدعتها أجهزة الشرطة النيوزيلندية لتتبع الجناة من هذه الطائفة – تدعى Roxanne ويُفترض أنها تبلغ من العمر 14، ورتب ضباط الشرطة الفيدرالية الأسترالية لقاءً في مدينة Canberra بين الفتاة الوهمية والمشتبه به، حيث تم القبض عليه ثم توجيه الإتهام إليه. [5]

وفي عام 1994 قام Vladimir L.Levin روسي الجنسية بسرقة 10.7 مليون دولار من حسابات عملاء سيتي بنك في الولايات المتحدة الأمريكية من خلال التلاعب بنظام تحويل الأموال، وقام بتحويل هذه الأموال عبر حسابات أنشأها شركاءه في الجريمة في فنلندا والولايات المتحدة وهولندا وألمانيا وإسرائيل، وقد صدرت مذكرة

[1]: Artur Appazov, ibid, p43
[2]: Artur Appazov, ibid, p43
[3]: ibid, p43
[4]: ibid, p43
[5]: ibid, p59

إعتقال من محكمة أمريكية ولكن تم رفض تسليمه لعدم وجود معاهدة لتسليم المجرمين في ذلك الوقت بين الولايات المتحدة وروسيا، وفي وقت لاحق، تم القبض على المتهم في إنجلترا وتم تسليمه إلى الولايات المتحدة بناءً على معاهدة تسليم المجرمين المبرمة بينهما. [1]

وفي عام 2000 انتشر فيروس Love Bug في جميع أنحاء العالم تقريبا وأدى إلى تعطل أجهزة الكمبيوتر التجارية والحكومية في أكثر من خمسة وأربعين دولة مما أدى إلى خسائر تقدر بمليارات الدولارات، وقد نسبت هذه الجريمة إلى أحد الأشخاص في الفلبين، الغريب في الأمر أنه لم تتم محكامة هذا الشخص، لان الفلبين رفضت تسليمه على أساس أنه في هذا التوقيت لم يكن لدى الفلبين قانون يجرم هذه الأفعال. [2]

وفي عام 2002، أصدرت الشرطة الألمانية أمر ببدء التحقيق والتتبع لسبعة وثلاثين واقعة إستغلال جنسي ضد الاطفال تديره عصابات منظمة تقوم بتبادل وتنزيل المواد الإباحية لغرض إصطياد الأطفال من عشرة دول مختلفة. [3]

وفي عام 2010 قام Kelly and Mehan بتقديم إحصائية حيث أوضحت أن إجمالي تكلفة الهجمات السيبرانية على المواطنين العاديين في جميع أنحاء العالم - عند احتساب الضرر المالي المباشر والوقت الضائع بسبب التعافي بعد الهجمات السيبرانية - بلغت 388 مليار دولار، بحيث يتجاوز هذا الرقم إجمالي السوق السوداء العالمية للماريجوانا والكوكايين والهيروين مجتمعة.[4]

وفي عام 2018 تعرضت العديد من الشركات للهجمات السيبرانية في الولايات المتحدة الأمريكية والمملكة المتحدة، حيث بلغت نسبة الشركات التي تعرضت للهجوم 59 % من إجمالي الشركات العاملة داخل الولايات المتحدة والمملكة المتحدة. [5]

ومما يمكن قوله في هذا الصدد، أن خبراء الأمن السيبرانيين يتوقعون أن الأمر لن يقف عند هذا الحد، بل سوف تتجاوز قيمة الخسائر نتيجة هذه الجرائم السيبرانية هذه الأرقام بنسبة كبيرة، فعلى حد قولهم سترتفع هذه النسبة إلى 15 % سنويا، لتصل إلى 10.5 تريليون دولار أمريكي بحلول عام 2025 مقارنة ب 3 تريليون دولار أمريكي في عام 2015 ، بحيث يتجاوز هذا الرقم حجم الضرر الناتج عن الكوراث الطبيعية على مستوى العالم في عام واحد. [6]

وتوضح هذه الأمثلة على حجم الثقة في التواصل بين أجهزة ووكالات إنفاذ القوانين الوطنية المختلفة، ومن بين دول مثل أستراليا ونيوزيلندا وكندا والولايات المتحدة

---

[1] : Abdelmonem Mohamed Magdy, ibid, p11

[2] : Abdelmonem Mohamed Magdy, ibid, p10

[3] : Abdelmonem Mohamed Magdy, ibid, p10

[4] : Artur Appazov, ibid, p16

[5] : Juan Ignacio Alcaide, Critical infrastructure cybersecurity and the marine security, University of Cadiz, Spain, 2020, P549

[6] : عماد الدين محمد كامل، الجرائم السيبرانية في زمن كورونا وآثارها على الامن القومي الاقتصادي : دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة، بنك دبي الاسلامي، العدد 500، 2022، ص631

والعديد من الدول الأوروبية، تم إجراء العديد من الاتصالات المكثفة لتسهيل التعاون الفعال للغاية، كما تم إقامة شراكات جديدة مع دول أوروبا الشرقية و الدول النامية.[1]

وعلى مستوى الجهود الخارجية للدول فقد تمثل ذلك في إنشاء العديد من المنظمات الدولية المتخصصة في ملاحقة وتعقب الجناة، وقد بدأت الدعوات الأولى لإنشاء منظمة دولية متخصصة في الأمن الدولي من خلال عدة مؤتمرات، جاء أولها في عام 1914 بناء على دعوة أمير موناكو حيث ضم المؤتمر العديد من ضباط الشرطة ورجال القضاء من 14 دولة حول العالم، والحق يقال فلم يسفر هذا المؤتمر عن نتائج تذكر وإن كان قد فتح الطريق أمام إنعقاد العديد من المؤتمرات الدولية. [2]

ثم تتابعت الدعوات لإنعقاد عدة مؤتمرات، ففي عام 1919 دعا فان هوتين وهو أحد ضباط الشرطة في هولندا إلى عقد مؤتمر لمتابعة الفكرة التي تم طرحها في عام 1914، لكن لم يكتب النجاح لفكرته، ثم جاء عام 1923 وجاءت معه دعوة جديدة على يد يوهانس شوبر رئيس شرطة فيينا، وكان من نتيجة هذا المؤتمر أنه تم إنشاء لجنة دولية للشرطة الجنائية، لكن لم تعمل هذه اللجنة بشكل جيد بسبب ظروف الحرب. [3]

وفي عام 1946 تمت الدعوة الى مؤتمر دولي جديد على يد لوفاج أحد روساء شرطة بلجيكا، حضره مندوبون من 17 دوله وإنتهى المؤتمر إلى إعادة اللجنة المذكورة للعمل مرة أخرى، مع إختيار باريس لتكون مقرا لها، وبحلول عام 1956 تمت الدعوة إلى مؤتمر أخر في فيينا، وكان من نتيجة هذا المؤتمر وضع النظام الاساسي للمنظمة، مع تغيير أسم اللجنة ليصبح المنظمة الدولية للشرطة الجنائية International Criminal Police Organization (INTERPOL) هو الإسم الجديد ومع تغيير مقر المنظمة ليصبح مدينة Lyon بدلا من Paris . [4]

ويعد الإنتربول منظمة حكومية دولية تضم في عضويتها 194 دولة بحيث يهدف الى السماح لسلطات الشرطة في جميع الدول الأعضاء بتبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها، فضلا عن تزويدها بمجموعة واسعة من أشكال الدعم التقني والتشغيلي في مجال مكافحة الجرائم الجنائية والجرائم السيبرانية، كما يساعد على تعزيز التعاون الدولي بين أجهزة إنفاذ القانون لضمان التبادل والتحليل الآمن والسريع للمعلومات المتعلقة بالأنشطة الإجرامية والأشخاص المشتبه بهم، كما أنه يسهل تفعيل طلبات الشرطة الثنائية أو المتعددة الأطراف أو تسليم طلب المساعدة القانونية الرسمي بين الأجهزة المختصة. [5]

وعلى مستوى الولايات المتحدة الأمريكية فقد تمت الدعوة - في عام 1986 - إلى إنشاء شرطة الويب الدولية وهى منظمة شرطية تضم في عضويتها أجهزة إنفاذ القانون

---

[1] : Artur Appazov, ibid, p59

[2]: صالح سعود، الانتربول ودوره في التعاون الامني الدولي، مجلة المنارة للدراسات القانونية والادارية، العدد 21، 2017، ص 137

[3] : المرجع نفسه، ص137

[4] : المرجع نفسه، ص138

[5] : Abdelmonem Mohamed Magdy, ibid, p15

من 61 دولة حول العالم، حيث تسعى هذه المنظمة إلى تشكيل فرق بحثية بغرض تعقب وملاحقة الجناة المرتكبين للجرائم العابرة للحدود وبصفة خاصة الجرائم السيبرانية. [1]

وبغرض التسهيل في تنفيذ إجراءات ملاحقة وتعقب الجناة لغرض تسليمهم ومحاكمتهم، فقد عرفت المحكمة العليا الأمريكية ماهية تسليم المجرمين، بقولها أن عملية تسليم المجرمين عبارة عن إجراء قانوني قائم على مبادىء القانون الوطني، أو يرتكز على مبدأ المعاملة بالمثل، أو معاهدة بين الدول الأطراف، تتسلم على أساس ذلك دولة محددة شخص ما متهم بإرتكاب جريمة أو مخالفة جنائية، بحيث يتم معاقبته على الجريمة المرتكبة في الدول التي طالبت بتسليمه بسبب أن الفعل المرتكب يشكل جريمة جنائية في قانون هذه الدولة. [2]

وعلى المستوى الأوروبي فيمكن القول بأنه - وبحلول عام 1995 – دعا المجلس الأوروبي الدول الاعضاء وعن طريق التوصية رقم 95/13 بضرورة معالجة تحديات الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء على مراجعة قوانين الإجراءات الجنائية بما يتلائم مع طبيعة التطور التكنولوجي الحديث. [3]

وليس هذا فحسب ففي عام 1998 تم إنشاء مكتب الشرطة الأوروبية اليوربول European Police Office (EUROPOL) بهدف تحقيق الأمن في المجتمع الاوروبي وذلك من خلال منع ومكافحة الإرهاب وغيره من أشكال الجريمة المنظمة العابرة للحدود الوطنية، خصوصا تلك التي تقع داخل حدود الإتحاد الأوروبي. [4]

ولم يتوقف الجانب الأوروبي عند هذا الحد بل قام ولأول مرة في عام 2002 - ومن خلال حلف شمال الأطلسي North Atlantic Treaty Organization (NATO) -بإدراج تكنولوجيا المعلومات والإتصالات ضمن مبادىء النزاع المسلح لأول مرة في جدول الأعمال السياسي لحلف شمال الأطلسي خلال قمة براغ، كما قام بإعتماد أول سياسة للدفاع السيبراني للمنظمة في عام 2008، وفي عام 2016 - ومن خلال قمة وارسو - قام الحلف المذكور بدراسة طبيعة التهديدات السيبرانية وسبل مواجهتها وكذلك طبيعة الفضاء الإليكتروني طبقا لمبادىء لميثاق الأمم المتحدة والقانون الإنساني الدولي، وقانون حقوق الإنسان[5].

وليس هذا فحسب بل اعترف حلف شمال الأطلسي بالفضاء السيبراني كمجال عملياتي، وخصص له موارد إضافية للقدرات الدفاعية وتعهد بمواصلة تطوير التعاون بينه والاتحاد الأوروبي في مجال الدفاع السيبراني[6] .

وفيما يتعلق بفرنسا ونيوزيلاندا فقد قدمتا إقتراحا لمجلس الأمن يعطي لأي دولة الحق في أن تطلب المساعدة الفورية من الأمم المتحدة، إذا وقعت ضحية لأي هجوم

---

[1]: شيخة حسين الزهراني، مرجع سابق، ص746

[2]: محمد فخري فرحات، دور الانتربول في ملاحقة المجرمين الدوليين، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2019، ص 55

[3] : شيخة حسين الزهراني، مرجع سابق، ص751

[4] : Abdelmonem Mohamed Magdy, ibid, p16

[5] : The United Nations, Cyberspace and International Peace and Security, ibid, p28

[6] : The United Nations, Cyberspace and International Peace and Security, ibid, p28

سيبراني، كما أنه من حق أي دولة أن تطلب الدعم العاجل إذا كان من شأن إستمرار هذه الهجمات السيبرانية التأثير على السلم والأمن الدوليين.[1]

وفي عام 2013، نجح اليوروبول في انشاء المركز الأوروبي للجرائم الإلكترونية European Cybercrime Centre (EC3) لدعم استجابة سلطات إنفاذ القانون للجرائم الإلكترونية في الإتحاد الأوروبي مما يساهم في حماية المواطنين والشركات والحكومات الأوروبية.[2]

وفي عام 2018 نجح المركز الأوروبي للجرائم الإليكترونية التابع لليوروبول في القاء القبض على واحد من أشهر زعماء العصابة على مستوى العالم، حيث إستهدف أكثر من 100 مؤسسة مالية في أكثر من 40 دولة حول العالم، مما أدى إلى خسائر تزيد عن مليار يورو، وتمت ملاحقة المتهم في عدة دول حول العالم حتى تم القبض عليه في إسبانيا بعد تحقيق دام عدة سنوات بالتنسيق مع فريق العمل المشترك المعني بالجرائم الإليكترونية Joint Cybercrime Action Taskforce (J-CAT). [3]

وقد إشتركت عدة أجهزة وطنية في عملية القبض على المتهم، حيث شمل فريق البحث والتحقيق أعضاء من الشرطة الوطنية الأسبانية، ومفوضون من مكتب التحقيقات الفيدرالي الأمريكي، ووكالات إنفاذ القانون في رومانيا، ومولدوفا، وبيلاروسيا، وتايوان، وعدد من شركات الأمن السيبراني الخاصة التي قدمت جانب من المساعدة للأجهزة الوطنية. [4]

وفي نفس العام، - اي عام 2018 - أعلنت وزارة العدل الأمريكية عن نجاحها في القبض على مجموعة من الخارجين عن القانون يحملون الجنسية الأوكرانية، ينظمون تشيكل عصابي في كلا من بولندا واسبانيا والمانيا تحت مسمى Carbanak Group حيث وجهت لهم السلطات الأمريكية تهمة نشر برنامج Carbanak الضار لإستهداف أكثر من 100 شركة أمريكية وسرقة أكثر من 15 مليون سجل لبطاقات العملاء. [5]

وفي عام 2019 قامت الجمعية البرلمانية للبحر الابيض المتوسط بالإشتراك مع مجلس أوروبا إلى جانب مشروع Cyber South بتنظيم مؤتمر بفرنسا - تحديدا مدينة ستراسبورغ - حمل أسم مكافحة الإرهاب والتكنولوجيا الجديدة، وشارك في الإجتماع أكثر من 50 عضو من 15 دولة من بينهم ممثلين دبلوماسيين وبرلمانيين من أجهزة تشريعية مختلفة، إلى جانب العديد من الخبراء من المنظمات المختلفة، مثل الأمم المتحدة وحلف شمال الأطلسي والجمعية البرلمانية لمجلس أوروبا والبرلمان العربي.[6]

---

[1] : Attila Tanzi and others, international law and cyberspace, Ministry of Foreign Affairs, Italy, 2021, p39-40

[2] : Abdelmonem Mohamed Magdy, ibid, p16

[3] : Allison Peters & Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, Journal of national security law, policy, Vol. 10:487, 2020, p487

[4]: Allison Peters & Amy Jordan, ibid, p487

[5] : Allison Peters & Amy Jordan, ibid, p487

[6]: تقرير المؤتمر المشترك للجمعية البرلمانية للبحر الابيض المتوسط ومجلس اوروبا، فرنسا، 2019

وقد ناقش المؤتمر العديد من الموضوعات ذات الصلة بالجرائم السيبرانية، وطبيعة التهديدات التي تشكلها الإستراتيجيات الإرهابية المتطورة والمتعلقة بإستخدام التكنولوجيا، وكذا الإرهاب السيبراني وكيفية جمع الأدلة الإليكترونية لمنع الأعمال الإرهابية وتتبع وملاحقة الإرهابيين والقبض عليهم. [1]

وعلى المستوى الأسيوي - تحديدا ماليزيا - فقد تمت الدعوة إلى عقد الاجتماع الرسمي الأول لرؤساء شرطة رابطة أمم جنوب شرق آسيا في مانيلا، الفلبين، في عام1981، وذلك لمناقشة المسائل الخاصة بالجرائم العابرة للحدود، وكان هذا الإجتماع السنوي يسمى مؤتمر ASEANAPOL والذي يعني منظمة الشرطة الإقليمية لجنوب شرق آسيا، Regional police organization in the Southeast Asia. [2]

وقد ضمت المنظمة العديد من الدول مثل ماليزيا وسنغافورة وتايلاند وإندونيسيا والفلبين، وتعد هذه الدول هى الأعضاء المؤسسة للمنظمة، ثم تتابع إنضمام الدول الأسيوية بعد ذلك، ففي عام 1984، انضمت شرطة بروناي الملكية، وفي عام 1996، انضمت الشرطة الوطنية لجمهورية فيتنام، وفي عام 1998، انضمت الإدارة العامة لشرطة لاوس وقوة شرطة ميانمار، وفي عام 2000، انضمت الشرطة الوطنية الكمبودية. [3]

وتضم ASEANAPOL رؤساء شرطة رابطة دول جنوب شرق آسيا (ASEAN) الذين يجتمعون سنويًا ويشكلون منصة مهمة لتعزيز التعاون الإقليمي والتآزر والتركيز على أنواع الجرائم ذات الأولوية في المنطقة.[4]

وعلى مستوى المجموعة العربية، فقد تمت الدعوة إلى عقد الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة في القاهرة في عام 2010، وقد كان الهدف الرئيسي من هذه الإتفاقية هو التأكيد على مكافحة جرائم الإنترنت وتقنية المعلومات، وتعزيز سبل التعاون والتواصل بين الأجهزة الوطنية المختلفة، وقد ضمت الإتفاقية في عضويتها العديد من الدول العربية مثل، الامارات العربية المتحدة، والبحرين، والصومال، والكويت، والمغرب، ولبنان، واليمن. [5]

كما تمت الدعوة ومن خلال الأمانة الفنية لمجلس وزراء العدل العرب التابع لجامعة الدول العربية قانون الإمارات العربي الإرشادي لمكافحة جرائم تقنية المعلومات ومافي حكمها من جرائم أخرى، والذي اعتمده مجلس وزراء العرب. [6]

---

[1] : تقرير اعمال المؤتمر المشترك للجمعية البرلمانية ، مرجع سابق

[2] : Joint Standing Committee on Foreign Affairs, Defense and Trade Inquiry into Australia's Relationship with ASEAN, 2008

[3] : http://www.aseanapol.org/about-aseanapol/permanent-secretariat

[4] : ibid

[5] : هند نجيب، التعاون القضائي الدولي في مجال الجرائم الاليكترونية، المجلة الجنائية القومية، العدد 2، 2016، ص119 - 120

[6] : المرجع نفسه، ص 119

إن كل ماتقدم أدى إلى نتيجة منطقية وهى تزايد و تعالي الأصوات التي تطالب بإنشاء جهاز قضائي دولي تكون مهمته الفصل في الجرائم السيبرانية وتنفيذ أقصى العقوبات علي مرتكبيها.

فوجود محكمة دولية ذات ولاية قضائية عالمية على أعمال العدوان السيبراني من شأنه أن يردع مثل هذه الأعمال، مع توفير غطاء قانوني دولي للمحاكمة، حيث ترفض الدول في كثير من الأحيان محاكمة مثل هذه الأعمال، وهذا النوع من المحاكم من شأنه أن يساعد في الحفاظ على الإستقلال الوطني، كما أن من شأنه أن يضمن عدم التعامل مع الجرائم بشكل مختلف عبر خطوط الولاية القضائية، خصوصا مع التوافق حول معايير قانونية دولية واحدة تحكم هذه الممارسات المخالفة. [1]

كما ستوفر هذه المحكمة للدول والجهات الفاعلة الخاصة منتدى دولياً لمعالجة هذه الأنواع من القضايا، وليس هذا فحسب بل ستعطي هذه المحكمة الفرصة للكيانات والمؤسسات الخاصة على المطالبة بالتعويض الدولي عن الأضرار الإقتصادية التي تقع عليها والناجمة عن أعمال الجرائم السيبرانية.[2]

[1] : William M. Stahl, ibid, p271
[2] : ibid, p271

المبحث الثاني
الآلية القانونية في مواجهة الجريمة السيبرانية

حرص المشرع الوطني منذ اللحظة الأولى التي إستشعر فيها الخطر من ظهور جريمة جديدة على إقامة سياج أمني يهدف إلى حماية المواطنين ويعزز من سبل طمأنتهم من هذا الخطر الداهم، وقد تمثلت هذه الجهود والتي قام بها المشرع الوطني في مختلف دول العالم في إصدار تشريعات جديدة لتواجه هذه الظروف المستجدة، وإدخال التعديلات المناسبة التي تسمح للنص القانوني بالمواجهة والفعالية لهذه الطائفة الجديدة من الجرائم، وكذا المشاركة في عقد المؤتمرات الدولية التي ينتج عنها وبصفة دائمة إتفاقيات دولية جديدة يسعى بها ومن خلالها الى مواجهة هذا العدوان على الصعيد الدولي وعبر الحدود الوطنية للدول.

والحق يقال فإن دل ذلك على شيء فإنما يدل على أمرين، أولا على حرص المشرع الوطني على مواكبة التطور التكنولوجي، فليس من باب الإنصاف القول بأن المشرع الوطني بعيد عن باقي المعارف، وثانيا لفهم المشرع الوطني للعلاقة الحقيقية بين القانون والتكنولوجيا، تلك العلاقة التي فرضت على المشرع ضرورة الحرص الدائم على تطوير القاعدة القانونية بشكل يتلائم مع كل مايستجد من أوضاع، ذلك أن علم القانون لاينفصل عن علوم التكنولوجيا، فقد قُدر على رجال القانون أن تدور كتاباتهم وإصداراتهم وجودا وعدما مع كل مايستجد من أحداث وكل مايستحدث من ظروف. [1]

وفي ضوء ماتقدم فقد تم تقسيم هذا المبحث على النحو التالي :

المطلب الأول : دور المشرع الوطني في مواجهة الجريمة السيبرانية.

المطلب الثاني : دور الإتفاقيات الدولية في مواجهة الجريمة السيبرانية.

[1] : محمد محمود فياله، النظام القانوني للسفن غير المأهولة في ضوء القانون الدولي للبحار، مجلة كلية الحقوق، جامعة الاسكندرية، العدد 1، 2023، ص 769

المطلب الأول
دور المشرع الوطني في مواجهة الجريمة السيبرانية

أخذ المشرع الوطني - وكما سبق القول - على عاتقه مهمة التصدي لهذا الفيروس الخطير الذي أصاب رئة المجتمع الحديث، ولم تكن هذه المهمة بالأمر اليسير خصوصا مع ظهور طائفة جديدة من الخارجين عن القانون والحريصين على إمتلاك وإكتساب التكنولوجيا تماما مثلما يحرص عليها رجال الضبط القضائي والأمن الجنائي بصفة عامة.

فعلى مستوى المجموعة العربية - تحديدا جمهورية مصر العربية - فقد كان المشرع المصري حريص على وضع الإطار القانوني المناسب لمواجهة هذه الطائفة من الجرائم، وقد جاء النص صريحا على ذلك في عدة مواضع.

فقد نص الدستور المصري لعام 2019 في المادة 31 على أنه " أمن الفضاء المعلوماتي جزء أساسي من منظومة الإقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون ". [1]

ويلاحظ من قراءة هذا النص أن المشرع المصري عد الفضاء المعلوماتي جزء لايتجزأ من أمن الدولة الإقتصادي والقومي، بما يعطي للدولة حق التدخل في حماية هذا الكيان بأعتباره من أصول الدولة، وكل تهديد له يستوجب التدخل الحازم بما يتوافق وروح القانون.

وليس هذا فحسب بل حرص المشرع المصري - من خلال قانون رقم 175 لسنة 2018 - على أن يكون أكثر وضوحا وتفصيلا عند حديثه عن هذه الطائفة من الجرائم، فحدد المعايير والمحاذير التي يجب الإنتباه اليها خشية الوقوع في إرتكاب فعل مما يعد جريمة طبقا لهذا القانون. [2]

ومرة أخرى فإن الأمر لم يتوقف عند هذا الحد بل أصدر رئيس مجلس الوزراء القرار رقم 1699 لسنة 2020 والخاص بإصدار اللائحة التنفيذية للقانون رقم 175 لسنة 2018 ، حيث صدر بالجريدة الرسمية في العدد 35 بتاريخ 27 / 8 / 2020 فحدد ووضح بعض التعريفات والتفاصيل الفنية التي تظهر معها الأمور بشكل لايمكن فهمه على أكثر من معنى، فحدد ماهية

---

[1]: دستور جمهورية مصر العربية، والذي تم تعديله طبقا للاستفتاء على تعديل الدستور، ابريل 2019.

[2]:

1. تنص المادة 13 على أنه " يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات، بخدمة اتصالات أو خدمات قنوات البث المسموع والمرئى ."
2. تنص المادة 14 على انه " يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه ".
3. تنص المادة 15 على انه " يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول ".
4. تنص المادة 16 على انه " يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلى وما فى حكمها ".
5. تنص المادة 17 على انه " يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة ".

التشفير، وطبيعة البنية التحتية المعلوماتية الحرجة، كما حدد مجموعة من الضوابط والإسترشادات لطائفة المتعاملين في خدمة تقنية المعلومات والإتصالات بضرورة تنفيذ بعض السياسات وإعتمادها من جهات الإدارة العليا مع الإلتزام على المراجعة الدورية لها، ضمانا لمواكبتها لكل مايستجد من أوضاع. [1]

كما أصدر المشرع المصري القانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية. [2]

وفيما يتعلق بدولة فلسطين، فقد أصدر المشرع الفلسطيني قرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية، والذي استند فيه على أحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته، و أحكام قانون العقوبات رقم 16 لسنة 1960م وتعديلاته، و قانون الإتصالات السلكية واللاسلكية رقم 3 لسنة 1996، حيث أوضح فيه العقوبات الواجب توقيعها على كل من يقوم بإرتكاب واحدة او أكثر من الجرائم التقنية. [3]

---

[1] : اللائحة التنفيذية الصادرة عن مجلس الوزراء المصري، والمنشورة في الجريدة الرسمية بتاريخ 27 / 8 / 2020 .

[2]: قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية، المنشور في الجريدة الرسمية بتاريخ 15 يوليو 2020، وتاريخ العمل به 16 اكتوبر 2020، العدد 28 مكرر هـ.

[3]:

1. تنص المادة 1 على انه " 1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرضاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ. 2. يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية: أ. إذا ارتكبت من مواطن فلسطيني. ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية. ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية ".

2. تنص المادة 4 على انه " 1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغاؤه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 4. إذا ارتكب الفعل المذكور في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً ".

3. تنص المادة 8 على انه " 1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. كل من ارتكب جريمة باستخدام أي من الوسائل المذكورة في الفقرة (2) من هذه المادة، يعاقب

وفيما يتعلق بالإمارات العربية المتحدة فقد تم إصدار مرسوم بقانون إتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، والذي تم الإستناد فيه على المرسوم بقانون إتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وتعديلاته، حيث غلظ عقوبة الدخول الى المواقع الإليكترونية بدون وجه حق. [1]

وقد جاء القانون رقم 5 لسنة 2012 كصورة من صور التشديد العقابي التي تبناها المشرع الإماراتي نتيجة للتطور التكنولوجي وبعدما رأى المشرع الإماراتي أن القانون رقم 2 لسنة 2006 غير كاف، لا من ناحية طبيعة الجرائم التي يعالجها، ولا من ناحية تناسب العقوبة مع طبيعة الجريمة المرتكبة، فغلظ العقوبة في القانون الجديد سواء من ناحية العقوبات السالبة للحرية، أو من ناحية الغرامات المالية. [2]

وفيما يتعلق بقطر فإن المشرع القطري أصدر قانون مكافحة الجرائم الإليكترونية رقم 14 لسنة 2014 والذي استند فيه على قانون المعاملات والتجارة الإلكترونية الصادر بالمرسوم بقانون رقم 16 لسنة 2010، حيث أوضح طبيعة هذه الجريمة وطبيعة العقوبات الموقعة عليها. [3]

بالسجن وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً ".

[1] :

1. تنص المادة 5 على انه " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (500,000) خمسمائة ألف درهم ولا تزيد على (3,000,000) ثلاثة ملايين درهم، كل من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية .فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفاً مشدداً ".
2. تنص المادة 16 على انه " يعاقب بالحبس مدة لا تقل عن (2) سنتين والغرامة التي لا تقل عن (200,000) مائتي ألف درهم ولا تزيد على (1,000,000) مليون درهم، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو أعد أو صمم أو أنتج أو استورد أو أتاح أو استخدم أي برنامج معلوماتي أو وسيلة تقنية معلومات أو أكواد مرور أو رموز أو استخدم التشفير بقصد ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون أو إخفاء أدلتها أو آثارها أو الحيلولة دون اكتشافها".

[2] : عبد العزيز سالم السنيدي، السياسة العقابية للمشرع الاماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الإتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، رسالة ماجستير، كلية القانون، جامعة الامارات العربية المتحدة، 2018، ص1

[3] :

1. تنص المادة 1 على انه " تقنية المعلومات: أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام معلوماتي أو شبكة معلوماتية ".
2. تنص المادة 2 على انه " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة.

وفيما يتعلق بسلطنة عمان ، فقد تم إصدار المرسوم السلطاني رقم 12 / 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات، حيث تم الإستناد فيه على قانون تنظيم الإتصالات الصادر بالمرسوم السلطاني رقم 30 / 2002، لتوضيح ظروف الجريمة التقنية ونوع الجزاء المحدد لها. [1]

وفيما يتعلق بالمملكة الأردنية الهاشمية فقد تصدى المشرع الأردني لهذه الطائفة من الجرائم من خلال الاداة التشريعية المتمثلة في قانون جرائم نظم المعلومات رقم 3 لسنة 2010، حيث واجه فيه هذه الطائفة من الجرائم وحدد العقوبات الموقعه عليها. [2]

وفيما يتعلق بالمملكة العربية السعودية فقد تم إصدار مرسوم ملكي رقم م/17 بتاريخ 8 / 3 / 1428 هـ، الموافق 27 / 3 / 2007 ، وقد كان هدف هذا النظام هو الحد من وقوع جرائم المعلوماتية ، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها. [3]

---

[1] :

1. تنص المادة 2 على انه " تسري أحكام هذا القانون على جرائم تقنية المعلومات ولو ارتكبت كليا أو جزئيا خارج السلطنة متى أضرت بأحد مصالحها، أو إذا تحققت النتيجة الإجرامية في إقليمها أو كان يراد لها أن تتحقق فيه ولو لم تتحقق ".
2. تنص المادة 3 على انه " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك، فإذا ترتب على ما ذكر في الفقرة الأولى إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين، فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين ".

[2] :

1. تنص الماد 3 / أ على انه " كل من دخل قصداً الى موقعٍ الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بمايخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقلعن 100 مائة دينار ولا تزيد على 200 مائتي دينار أو بكلتا هاتين العقوبتين ".
2. تنص المادة 15 على انه " تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار ايٍ من الجرائم المنصوص عليها فيها ".

[3] :

تنص المادة 2 على انه " يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية ، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي المساعدة على تحقيق الأمن المعلوماتي، حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، حماية المصلحة العامة ، والأخلاق، والآداب العامة ، حماية الاقتصاد الوطني ".

تنص المادة 3 على انه " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه، الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا ، الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه، المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها ، التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة ".

وعلى مستوى أمريكا الشمالية - تحديدا الولايات المتحدة الأمريكية - فقد تم إصدار قانون التحديث المالي The Gramm-Leach-Bliley Act (GLB Act or GLBA) لعام 1999 وهو قانون إتحادي يلزم المؤسسات المالية والشركات التجارية التي تقدم خدمات مالية للعملاء المتعاملين معها مث القروض، أو المشورة المالية أو الاستثمارية بضرورة شرح ممارساتها وأسلوب التعامل والتواصل عند تبادل المعلومات لعملائها وحماية البيانات الحساسة وذات الأهمية الخاصة. [1]

وفي عام 2002 وقع الرئيس الأمريكي جورج بوش على قانون الأمن الداخلي، حيث تم بموجبه إنشاء وزارة الأمن الداخلي Department of Homeland Security (DHS) كإدارة جديدة في السلطة التنفيذية للحكومة، كما تم وضع عددًا من التدابير التي تهدف إلى حماية الأمن القومي للولايات المتحدة، وقد تمت صياغة القانون في أعقاب هجمات 11 سبتمبر عام 2001. [2]

وفي عام 2018 أقر الكونجرس الأمريكي قانون الإستخدام القانوني الخارجي للبيانات Clarifying Lawful Overseas Use of Data Act (CLOUD Act) 2018 وذلك بغرض تسهيل تبادل البيانات عبر الحدود مباشرة بين شركات التكنولوجيا الأمريكية والحكومات الأجنبية بحيث يسمح هذا القانون للولايات المتحدة الأمريكية بحرية الدخول في إتفاقيات دولية من أجل تحقيق هذا الغرض. [3]

وعلى مستوى أمريكا الجنوبية - تحديدا البرازيل - فقد صدر عن رئاسة الجمهورية قرار بقانون رقم 14.155 الصادر بتاريخ 27 مايو 2021 حيث إستند هذا القرار على المرسوم بالقانون رقم 2848 الصادر بتاريخ 7 ديسمبر 1940 وعلى المرسوم بالقانون رقم 3689 الصادر بتاريخ 3 أكتوبر 1941، حيث غلظ هذا القرار من العقوبة المقررة على الجرائم التقنية التي يرتكبها أحد الأشخاص داخل الأراضي البرازيلية. [4]

---

1 :

Public Law 106–102—NOV. 12, 1999, GRAMM–LEACH–BLILEY ACT.

Sec 501 " It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information ".

Sec 503 " At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, of such financial institution's policies and practices with respect to : (1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed; (2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and (3) protecting the nonpublic personal information of consumers ".

2 : Public Law 107–296; Approved November 25, 2002.

3 : 115th CONGRESS, 2d Session, February 6, 2018.

4 : Art. 154-A " Invading computer device of use of others, whether or not to the computer network, in order to obtain, tamper with or destroy data or information without express permission or tacit of the device user or to install vulnerabilities to obtain an unlawful advantage: imprisonment, from 1 (one) to 4 (four) years, and fine ".

وعلى مستوى المجموعة الأوروبية - تحديدا فرنسا - فإن المشرع لم يصدر قانون واحد بل أصدر عدة قوانين مختلفة، فقد تم إصدار قانون البرمجة العسكرية Military Programming Act of 2013 بحيث أوجب هذا القانون على جميع الشركات والقطاعات المختلفة بضرورة الإبلاغ الفوري للسلطات المختصة عند التعرض للهجمات السيبرانية، مع الأخذ في الإعتبار تنفيذ كافة الوسائل التقنية التي تحمي هذه المؤسسات من خطر التعرض لهذه الهجمات، كما أن هناك التزام مقابل على الدولة بأن تتخذ من الإحتياطات اللازمة التي تمكنها من إضفاء الحماية على البنوك والمستشفيات وكافة القطاعات الحيوية داخل الدولة. [1]

وليس هذا فحسب، بل قاد رئيس الوزراء الفرنسي الأسبق Manuel Valls في عام 2015 حملة توعية كاملة لتثقيف الشعب الفرنسي عن الإستراتيجية الجديدة التي تتبناها الحكومة حول مفهوم الأمن الرقمي Digital security حيث تولت الوكالة الوطنية لأمن أنظمة المعلومات Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) هذه المهمة تحت إشراف رئيس الوزراء. [2]

وفيما يتعلق بروسيا فقد حرص المشرع الروسي على تجريم الوصول الغير قانوني إلى البيانات والمعلومات الرقمية عبر الانترنت وذلك من خلال نصوص قانون العقوبات The Criminal Code Of The Russian Federation No. 63-Fz الصادر بتاريخ 13 يونيو 1996، حيث عاقب المشرع على هذا الوصول الغير قانوني بغرامة تصل إلى 200 ألف روبل، أو أي دخل آخر للشخص المدان لمدة تصل إلى 18 شهرًا، أو العمل الإصلاحي لمدة تصل إلى سنة واحدة، أو الحبس لمدة تصل إلى عامين، أو العمل الإجباري لمدة تصل إلى عامين، وذلك في المواد 28، 273، 274. [3]

وليس هذا فحسب بل أطلق المشرع الروسي القانون الإتحادي بشأن البيانات الشخصية Federal Law on Personal Data (No. 152-FZ) وهو يعد التشريع الأساسي الذي فرض الحماية القانونية على البيانات الشخصية، حيث صدر هذا القانون في عام 2006 وتم إدخال عدة تعديلات عليه، كان أخرها في عام 2023، بحيث يمتد هذا القانون بالتطبيق على نطاق واسع وعلى أي كيان، سواء أفراد أو منظمات، كما انه يشمل التطبيق على جميع المواطنين الروس، بغض النظر عن موقعهم، كما يحمي هذ القانون كافة انواع البيانات على اختلاف صورها مثل، البيانات الأساسية كالاسم والسن، والخصائص الجسدية والبيومترية مثل الجنس والعرق والطول والوزن، والمعلومات المهنية والمالية مثل المسمى الوظيفي والمستوى التعليمي، والبيانات الرقمية مثل طبيعة النشاط على وسائل التواصل الاجتماعي social media activity وبيانات المواقع location data وهكذا. [4]

وفيما يتعلق بمقدونيا، فقد نص المشرع المقدوني في المادة 251 من القانون الجنائي Criminal Code الصادر بتاريخ 2002 على تغليظ العقوبة عند إرتكاب أي فعل من الأفعال

[1] : https://www.lexology.com/library/detail.aspx?g=a412035f-b3af-4fd1-a6f2-17e7c97efd7f

[2] : https://www.upguard.com/blog/cybersecurity-laws-regulations-france

[3] : Dora Arifi, Cybercrime: a challenge to law enforcement, SEEU Review Volume 15 Issue 2, Macedonia, 2020, P50

[4] : Federal Law of 27 July 2006 N 152-FZ ON Personal data, adopted by the State Duma on 8 July 2006, Approved by the Federation Council on 14 July 2006

التي يترتب عليها الحصول بشكل غير مبرر على أي بيانات أو معلومات، أو محاولة الدخول لاي برامج أو مواقع بدون الحصول على أذن بالغرامة والسجن مدة لاتقل عن ثلاث سنوات. [1]

وفيما يتعلق بألمانيا الإتحادية فإن المشرع الألماني قد زاد مقدر العقوبة - في نصوص قانون العقوبات الصادر بتاريخ 1998 والمعدل بتاريخ 22 نوفمبر 2021 - عن نظيره المقدوني بحيث جعل المرتكب للجريمة الإليكترونية مستحقا لعقوبة السجن لمدة لاتزيد عن خمس سنوات أو بالغرامة كما قد تصل هذه المدة الى عشر سنوات في الحالات الخطيرة وذلك طبقا للمادة 303 ب وذلك عند إرتكابه أي فعل من الأفعال التي تشكل في مجموعها جريمة من الجرائم التقنية. [2]

وفيما يتعلق بأسبانيا فإن المشرع الاسباني قد حدد في المادة 278 من نصوص قانون العقوبات الصادر عام 1995 العقوبة المتوقع تطبيقها على كل شخص يرتكب جريمة من جرائم المعلومات بإستخدام جهاز من أجهزة الحاسب الألي أو اي وسيلة أخرى بالسجن لمدة تصل الى أربع سنوات متى كان هدفه الحصول على أي بيانات أو مستندات مكتوبة أو إلكترونية أو وسائط حاسوبية أو غيرها من الأشياء المتعلقة بها بقصد كشف سر مالك هذه المستندات. [3]

---

[1] : Article 251 "A person who in a unauthorized way deletes, alters, damages, conceals or otherwise makes unusable computer data or a program or device for maintenance of the information system or will disable or complicate the use of computer system, data or program or computer communication, shall be punishable by a fine or up to three years in prison".

[2] :

Criminal Code in the version published on 13 November 1998, as last amended by Article 2 of the Act of 22 November 2021.

Sec 303b '' (1) Whoever interferes with data processing operations which are of substantial importance to another by

1. committing an offence under section 303a (1),2. entering or transmitting data (section 202a (2)) with the intention of adversely affecting another or 3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(2) If the data processing operation is of substantial importance for another's business, enterprise or an authority, the penalty is imprisonment for a term not exceeding five years or a fine.

(3) The attempt is punishable.

(4) In especially serious cases under subsection (2), the penalty is imprisonment for a term of between six months and 10 years. An especially serious case typically occurs where the offender

1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage or
3. by committing the offence jeopardises the population's supply with vital goods or services or the security of the Federal Republic of Germany''.

[3] :

Criminal codes - Criminal Code of the Kingdom of Spain (1995 as of 2013),

Article: 278 "Whoever obtains data, written or electronic documents, computer media or other objects related thereto in order to discover a company secret, or who uses any of the

وعلى مستوى المجموعة الأسيوية - تحديدا الهند - فإن المشرع الهندي قد وضح بالتفصيل طبيعة العقوبة الواجب تطبيقها عند إرتكاب جريمة من الجرائم التقنية وذلك في المادة 43 من الفصل التاسع من قانون تكنولوجيا المعلومات رقم 21 لسنة 2000 The Information Technology Act of India حيث حدد العقوبة الواجب تطبيقها على كل من يستخدم أجهزة الحاسب الألي بغرض الوصول الغير مشروع الى اي بيانات أو معلومات والتي يؤدي الكشف عنها الى حدوث ضرر لمالك هذه البيانات. [1]

إن كل ماسبق يؤدي الى نتيجة واحدة وهى معرفة الجهد المبذول الذي يقوم به المشرع الوطني في سبيل صد هذه الطائفة الجديدة من الجرائم، وحماية أفراد المواطنين الذين قد يجدون أنفسهم عرضة للسرقة أو الإحتيال أو الإستغلال وتشويه السمعة في حال وقوع بعض البيانات أو المعلومات السرية، مما يهددهم في شؤون أعمالهم وربما في حياتهم كلها.

---

means or instruments described in Section 1 of Article 197, shall be punished with a sentence of imprisonment of two to four years and a fine of twelve to twenty- four months ".

[1] :

The Information Technology Act, 2000

Article 43. " If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, -

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or
computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected ".

المطلب الثاني
دور الإتفاقيات الدولية في مواجهة الجريمة السيبرانية

تعد الإتفاقيات الدولية، هى اداة التشريع الرئيسية - إلى جانب مصادر أخرى - فيما يتعلق بالقانون الدولي، ولما لا وقد إستطاعت هذه الإتفاقيات أن تنتزع لنفسها هذه المكانة فتصبح هى المصدر الأول للقانون الدولي بعدما إحتل العرف الدولي هذه المكانة لفترة طويلة من الزمن.

ولعل محكمة العدل الدولية بنظامها الأساسي قد حددت هذه المسألة بشىء من الوضوح عندما رتبت المصادر الواجب الرجوع اليها عند الرغبة في فصل في نزاع دولي، فأعترفت للإتفاقيات الدولية بهذه المكانة الخاصة. [1]

فالإتفاقيات الدولية هى المرآة الحقيقية التي تعكس رغبة أعضاء الجماعة الدولية حول موضوع محدد، فعلى اساسها ومن خلالها تظهر الرغبة الحقيقة للدول في الوقوف على أمر ما، ولعل مايمكن قوله في هذا الصدد، ان الإتفاقيات الدولية بهذه الصورة تعتبر هى الصورة المثالية والمناسبة عند الحديث عن الرغبة في حصاد مواقف الدول المختلفة تجاه موضوع محدد بذاته، فكما هو معروف أن الإتفاقيات الدولية تمر بعدة مراحل تبدأ بالمفاوضات وتمر بالتوقيعات وتنتهي بالتصديقات المختلفة من الأجهزة التشريعية أو الرئاسية حسب دستور كل دولة.

فعلى مستوى الأمم المتحدة فقد حرصت منذ اللحظة الأولى على عقد المزيد من المؤتمرات التي تؤكد على وجوب منع الجريمة وتحقيق العدالة الجنائية، وعلى ذلك فقد عقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين في القاهرة بتاريخ 29 مايو 1995، وقد تناول المؤتمر العديد من الموضوعات منها وضع خطط لملاحقة العصابات الإجرامية عبر الوطنية والجرائم الإقتصادية من خلال تدعيم التعاون الدولي والمساعدة التقنية العملية لتعزيز سيادة القانون، وكذلك التدبير الفعالة لمكافحة غسيل الأموال. [2]

وليس هذا فحسب بل تمت الدعوة إلى إنشاء إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والتي تم إعتمادها بموجب قرار الجمعية العامة للأمم المتحدة 25/55 المؤرخ في 15 تشرين الثاني/نوفمبر 2000، الصك الدولي الرئيسي في مكافحة الجريمة المنظمة عبر الوطنية، وقد تم فتح باب التوقيع على الاتفاقية من قبل الدول الأعضاء في مؤتمر سياسي رفيع المستوى والذي انعقد لهذا الغرض في باليرمو، إيطاليا، في الفترة من 12-15 ديسمبر 2000 ودخلت الاتفاقية حيز التنفيذ في 29 سبتمبر 2003. [3]

وأُلحق بالاتفاقية ثلاث بروتوكولات تستهدف مجالات ومظاهر محددة للجريمة المنظمة حيث تضمن الاتي: بروتوكول منع وقمع ومعاقبة الاتجار بالأشخاص، وخاصة النساء والأطفال؛ بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو، وبروتوكول

---

[1]: تنص المادة 38 من النظام الأساسي لمحكمة العدل الدولية على انه " . تُطبق المحكمة، التي تتمثل مهمتها في الفصل وفقًا للقانون الدولي، في النزاعات المعروضة عليها: الاتفاقيات الدولية، سواء كانت عامة أو خاصة، التي تحدد القواعد المعترف بها صراحة من قبل الدول المتنازعة؛ العرف الدولي، كدليل على ممارسة عامة مقبولة كقانون ؛ المبادئ العامة للقانون المعترف به من قبل الدول المتحضرة مع مراعاة أحكام المادة 59 والقرارات القضائية وتعاليم أمهر الدعاة من الدول المختلفة كوسائل فرعية لتقرير أحكام القانون ".

[2] : تقرير الأمين العام للامم المتحدة، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، خمسون سنة من مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية : إنجازات الماضى وآفاق المستقبل، بانكوك، 2005

[3] : https://www.unodc.org/romena/ar/untoc.html

مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة، ولابد ان تكون البلدان أطرافا في الإتفاقية نفسها قبل أن تصبح أطرافا في أي من البروتوكولات. [1]

ومما يمكن قوله في هذا الصدد، أن أحداث الحادي عشر من سبتمبر 2001 التي ضربت الولايات المتحدة الأمريكية كانت علامة فارقة على طريق مواجهة الجرائم السيبرانية، حيث أثبتت الحاجة الملحة إلى ضرورة مواجهة هذا الجرائم وسد كل منافذ تواجدها، خصوصا بعد إستخدام مجموعة من الطائرات التجارية لتنفيذ الهجمات، ولايخفى أن كانت أجهزة الحاسب الآلي أداة رئيسية من تلك الأدوات التي استخدمها الفاعلون في القيام بهذا الفعل، والحق يقال فقد بدأت الجهود لمواجهة هذه الجرائم حتى قبل تاريخ هذا الهجوم.

ففي شهر أكتوبر من عام 1999 اجتمع وزراء العدل والداخلية للدول الثماني الكبار في موسكو للبحث والتشاور حول كيفية مواجهة هذه الجرائم ومحاولة وضع حد لإفلات الجناة من العقاب، بما يتضمن بحث سبل ووسائل التواصل الإليكتروني بين الجناة من أجل تنفيذ أغراضهم الإجرامية، ورغم الرغبة الشديدة في مواجهة هذه الجرائم الخطرة، الإ أن نتائج المؤتمر لم تؤدي بشكل ملحوظ إلى تحقيق الأهداف المرجوة، من أجل ذلك تمت الدعوة إلى مؤتمر أخر في شهر يوليو من عام 2000 ولكن هذه المرة على مستوى الرؤساء الذين اصدروا توصياتهم بضرورة البدء الفعلي في إتخاذ التدابير التي تتضمن إقتفاء أثر المجرمين وتسليمهم للعدالة للمحاكمة عن الجرائم التي أرتكبوها في هذه الفترة.[2]

الأمر الذي دفع الوزراء مرة أخرى إلى تكثيف أعمالهم من خلال عقد عدة مؤتمرات متتابعة، تمت بين عدة دول مثل فرنسا والمانيا واليابان، كما تم توجيه الدعوة الى العديد من الخبراء المتخصصين والمستشارين الفنيين في مجال تكنولوجيا المعلومات من الشركات المتخصصة، وعلى ذلك فقد شارك في هذه المؤتمرات ممثلون عن أكثر من مئة شركة متخصصة في هذا المجال. [3]

ثم جاءت أحداث الحادي عشر من سبتمبر 2001 لتضع هذه الجهود في موضع أخر، ولتثبت للجميع أن مواجهة هذه الجرائم أصبحت ضرورة لامفر منها، خصوصا مع إستخدام الفاعلون أجهزة الإتصال مثل الحاسب الألي والتليفونات المحمولة وكذا الإستعانة برسائل البريد الإليكتروني لتنفيذ الهجمات.

والحق يقال فلم يخطأ الجانب الأوروبي لا في فهم المشهد ولا في قراءة هذا الحدث، فقد كان هذ الحادث الدافع الحقيقي وراء توقيع الإتفاقية الأوروبية لمكافحة جرائم الانترنت " بودابست " بتاريخ 23 / 11 / 2001 . [4]

ويرجع الفضل الى إتفاقية بودابست في إنشائها مظلة جزائية مشتركة تضم تحتها العديد من دول العالم، فقد وقعت 30 دولة على هذه الإتفاقية كان من بينها 26 دولة أوروبية، كما إنضمت الولايات المتحدة الأمريكية، وكندا، واليابان، وجنوب افريقيا، كما امتنعت 17 دولة عن التوقيع

[1] : https://www.unodc.org/romena/ar/untoc.html

[2]: هند نجيب، مرجع سابق، ص107

[3]: هند نجيب، مرجع سابق، ص107

[4] : هند نجيب، مرجع سابق، ص108

كان من بينها أيرلندا والدنمارك، ودخلت هذه الإتفاقية حيز التنفيذ في يوليو 2004 [1]، وتحتوي هذه الإتفاقية على 48 مادة وتقسم على أربعة فصول وتتناول موضوعات عديدة من بينها الجرائم المتصلة بالحاسب الآلي، والجرائم الخاصة بالتعدي على حقوق المؤلف، والمسائل الإجرائية بما فيها تسليم المجرمين وطبيعة التعاون الدولي بين الدول الأعضاء في مواجهة هذه الظاهرة الإجرامية، وموضوعات أخرى كثيرة. [2]

وفي عام 2003 تم وضع بروتوكول إضافي بهدف التأكيد على مضمون إتفاقية بودابست، حيث احتوى هذا البروتوكول على 16 مادة، وحدد هذا البروتوكول طبيعة العلاقة بين الإتفاقية الأم والبروتوكول المكمل لها. [3]

وفي عام 2022 تم وضع البروتوكول الإضافي الثاني للإتفاقية المتعلقة بالجريمة الإليكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإليكترونية، حيث احتوى هذا البرتوكول على 25 مادة، وقد كان من ضمن أهداف هذا البروتوكول حماية ضحايا الهجمات السيبرانية المتزايدة والحرص على إنصافهم وتحقيق العدالة، وكذا التأكيد على حماية المجتمع والفرد من خلال إجراء التحقيقات الجنائية والملاحقات القضائية العفالة. [4]

وليس هذا فحسب ففي عام 2000 أصدر الإتحاد الأوروبي التوجيه رقم EC/31/2000 الصادر عن البرلمان الاوروبي ومجلس أوروبا بشأن الجوانب القانونية المحددة لخدمات مجتمع المعلومات، لاسيما التجارة الإليكترونية في السوق الداخلي، وفي عام 2002 تم إصدار التوجيه رقم EC/58/2002 الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الإتصالات الإليكترونية، وفي عام 2006 تم إصدار التوجيه رقم EC/24/2006 الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الإحتفاظ بالبيانات التي تم إنشاؤها أو معالجتها فيما يتعلق بتوفير خدمات الإتصالات الإليكترونية المتاحة للجمهور أو شبكات الإتصالات العامة، وفي عام 2010 تم إصدار المشروع التوجيهي رقم COM(2010) 517 الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات، وفي عام 2011 تم إصدار التوجيه رقم EU/92/2011 الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن مكافحة الإعتداء الجنسي وإستغلال الاطفال في المواد الإباحية. [5]

وعلى مستوى الدول الأمريكية فقد تم إبرام العديد من الإتفاقيات، ففي عام 1981 تم ابرام اتفاقية البلدان الأمريكية لتسليم المجرمين، وفي عام 1984 تم ابرام اتفاقية البلدان الأمريكية بشأن الاختصاص القضائي في المجال الدولي بشأن فعالية الأحكام الأجنبية خارج الإقليم، وفي عام 1992 تم إبرام اتفاقية البلدان الأمريكية بشأن المساعدة المتبادلة في المسائل

---

[1] : قطاف سليمان، بوقرين عبد الحليم، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، العدد 1، المجلد 6، 2022، ص 337

[2] : شيخة حسين الزهراني، مرجع سابق، ص753

[3]: سلسلة معاهدات مجلس اوروبا، البروتوكول الاضافي لاتفاقية الجريمة الاليكترونية بشأن تجريم الافعال المرتبطة بالتمييز العنصري وكراهية الاجانب التي ترتكب عن طريق انظمة الكمبيوتر، 2003

[4] : سلسلة معاهدات مجلس اوروبا، البروتوكول الاضافي الثاني للاتفاقية المتعلقة بالجريمة الاليكترونية بشأن تعزيز التعاون والكشف عن الادلة الاليكترونية، 2022

[5]: دراسة شاملة عن الجريمة السيبرانية، منشورات مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينا، 2013

الجنائية، وفي عام 1993 تم ابرام اتفاقية البلدان الأمريكية لإنفاذ الأحكام الجنائية في الخارج، وفي العام نفسه تم ابرام البروتوكول الاختياري المتعلق باتفاقية البلدان الأمريكية للمساعدة المتبادلة في المسائل الجنائية، وفي عام 2002 تم ابرام اتفاقية البلدان الأمريكية لمكافحة الإرهاب.

وعلى مستوى الإتحاد الإفريقي فقد تم إبرام اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لعام 2014، حيث جرى إعتمادها في الدورة العادية الثالثة والعشرون، وذلك في مالابو بغينيا الإستوائية، وقد صدرت هذه الإتفاقية بأربع لغات مختلفة هى العربية والإنجليزية والفرنسية والبرتغالية، ولهذه اللغات نفس الحجية القانونية، وقد جاءت هذه الإتفاقية في 38 مادة موزعة على أربعة فصول.

وتهدف إتفاقية مالابو إلى تشكيل نص قانوني استراتيجي قادر على مكافحة الجرائم الإليكترونية في القارة السمراء، حيث ركزت هذه الإتفاقية على علاج موضوعات الأمن السيبراني بتوسع شديد، كما تضمنت سبل وآليات مكافحة الجريمة السيبرانية وكذا حماية البيانات الشخصية والإشراف على المعاملات الإليكترونية، وضمان تناسق التشريعات الوطنية للدول الاعضاء وقدرتها على مواجهة هذه الطائفة الجديدة من الجرائم مع إحترامها لحقوق الإنسان. [1]

وعلى مستوى الدول العربية فقد تم إبرام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث وافق عليها مجلسا وزراء الداخلية والعدل العرب في إجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21 / 21 / 2010، وقد حررت هذه الإتفاقية باللغة العربية فقط، كما جاءت في 43 مادة موزعة على خمسة فصول.

وقد صدر قرار رئيس جمهورية مصر العربية رقم 276 لسنة 2014 بشأن الموافقة على الإنضمام للإتفاقية المذكورة. [2]

ومما يمكن قوله في هذا الصدد أن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، تعد واحدة من أهم الإتفاقيات التي تم إبرامها في المنطقة العربية، ولذلك لانها عالجت العديد من الموضوعات الخاصة بالجرائم السيبرانية والأمن السيبراني، فقد جرمت الإعتداء على سلامة البيانات أو حتى مجرد إساءة إستخدام وسائل تقنية المعلومات، وكذا كل مايتشابه معها من مظاهر مثل التزوير والإحتيال والإباحية والإرهاب ونشر الأفكار المتطرفة والتحريض على الإرهاب والإتجار بالبشر ونشر وتوزيع الأسلحة، مما يؤدي إلى تهديد المنطقة بأسرها. [3]

هذا وإن دلت مجموع هذه الإتفاقيات على شيء، فإنما تدل على حرص المجتمع الدولي على بناء سياج قانوني منيع يهدف إلى حماية المواطن العادي والمؤسسات والشركات بل وحتى الدول ذاتها التي قد تجد نفسها - من خلال مؤساستها وهيئاتها - فريسة لهذه الهجمات.

---

[1]: مريم لوكال، قراءة في اتفاقية الاتحاد الافريقي حول الامن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 4، العدد 2، 2021 ص661

[2]: قرار رئيس الجمهورية رقم 276 الصادر بتاريخ 19 / 8 / 2014 بالموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد نشر هذا القرار بتاريخ 13 / 11 / 2014، وبدأ العمل به بتاريخ 8 / 10 / 2014

[3]: حاتم احمد بطيخ، مرجع سابق، ص 25

الخاتمة.

بذل أعضاء المجموعة الدولية من الجهد في مواجهة هذه الجريمة الخطيرة، مالم يبذل في غيرها، فقد تكاثفت الجهود وتلاحقت المؤتمرات وتتابعت الإتفاقيات، كل ذلك من أجل التأكيد على مدى خطورة هذا الفيروس الحديث، وإثبات النية الحقيقية والرغبة المؤكدة والإصرار المتواصل على مواجهة هذه الظاهرة .

إن خصوصية الجريمة بما تتضمنه من تفاصيل متنوعة، وحدت الجهود على المستوى التقني والأمني والسياسي والقانوني بطبيعة الحال، ولعل هذا يؤكد ماسبق طرحه من حرص المجتمع الدولي بكل فئاته وطوائفه على تفعيل الحماية اللازمة لصد هذه الأخطار التي تعصف بسلامة وإستقرار الدول وأمن وسلامة المواطن العادي.

النتائج :

- جريمة الأمن السيبراني من أخطر جرائم العصر الحديث التي تستوجب جهود خاصة لمواجهتها .
- المشرع الوطني حريص كل الحرص على مواجهة هذه الظاهرة بكل الوسائل وبكل ماأوتي من قوة، من خلال إصدار تشريعات جديدة، ومن خلال إعادة صياغة التشريعات الحالية للتتناسب مع مايستجد من أحداث.
- أثبتت بعض الإتفاقيات الدولية وبالتجربة العملية قدرتها على مواجهة وصد هذه الأخطار، ولم لا فالإتفاقيات الدولية هى المؤشر الحقيقي على رغبة المجتمع الدولي تجاه أمر ما.

التوصيات :

- ضرورة مراجعة الإتفاقيات الدولية، مرتين مرة من ناحية تغليظ النص القانوني حتى يتمكن من مواجهة هذه الظاهرة ومنع تكرارها، ومرة اخرى من خلال إظهار نوع من الجدية - وبصفة خاصة - من خلال سلوك المجموعة العربية فيما يتعلق بالإتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 فكيف يمكن الحديث عن خطورة هذه الظاهرة، وإدراك أثارها السلبية، ومع ذلك لم يصدق على هذه الاتفاقية الإ عدد محدود من الدول العربية.
- ضرورة تشديد العقوبة الواردة في النص القانوني الوطني، حتى يمكن معه تجفيف منابع هذه الجريمة.
- ضرورة انشاء محاكم دولية خاصة للمعاقبة على ارتكاب هذه الظاهرة الإجرامية ووضع حد نهائي لها.
- ضرورة عقد ورش عمل بصفة دائمة للتوعية بخطورة الجريمة السيبرانية، وذلك على مستوى رجال القانون والهندسة والأمن والسياسة .
- ضرورة تضمين مناهج الدراسة والبحث العلمي موضوعات الجرائم السيبرانية والأمن السيبراني على مستوى الجامعات ومراكز الأبحاث، وحتى نشر حملات توعية للمواطن العادي للتعريف بخطورة هذه الظاهرة الإجرامية.

قائمة المراجع :

اولا : اللغة العربية.

أ - المجلات العلمية.

1. احمد عبيس الفتلاوي، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق للعلوم القانونية والانسانية، العدد4، 2016.
2. قادري نور الهدى، الجريمة السيبرانية وآليات مكافحتها : مواجهة تحديات الامن السيبراني، المجلة للحقوق والعلوم السياسية، العدد1، 2023
3. حاتم احمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، العدد1، 2021
4. سامر محيي حمزة، مدى مساهمة الامم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني : دراسة في ضوء تقرير فريق الخبراء الدولي لعام 2021، مجلة مركز دراسات الكوفة، العدد 76، 2022
5. شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، العدد1، 2020
6. صالح سعود، الانتربول ودوره في التعاون الامني الدولي، مجلة المنارة للدراسات القانونية والادارية، العدد 21، 2017
7. عماد الدين محمد كامل، الجرائم السيبرانية في زمن كورونا وآثارها على الامن القومي الاقتصادي : دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة، بنك دبي الاسلامي، العدد 500، 2022
8. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1994
9. قطاف سليمان، بوقرين عبد الحليم، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، العدد 1، المجلد 6، 2022
10. هند نجيب، التعاون القضائي الدولي في مجال الجرائم الاليكترونية، المجلة الجنائية القومية، العدد 2، 2016
11. محمد محمود فياله، النظام القانوني للسفن غير المأهولة في ضوء القانون الدولي للبحار، مجلة كلية الحقوق، جامعة الاسكندرية، العدد 1، 2023
12. مريم لوكال، قراءة في اتفاقية الاتحاد الافريقي حول الامن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 4، العدد 2، 2021

ب - الرسائل العلمية.
1. عبد العزيز سالم السنيدي، السياسة العقابية للمشرع الاماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الإتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، رسالة ماجستير، جامعة الامارات العربية المتحدة، 2018
2. محمد فخري فرحات، دور الانتربول في ملاحقة المجرمين الدوليين، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2019

ج - التشريعات الوطنية والقرارات الرئاسية.
1. دستور جمهورية مصر العربية، والذي تم تعديله طبقا للاستفتاء على تعديل الدستور، ابريل 2019
2. قانون جمهورية مصر العربية رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.
3. قانون جمهورية مصر العربية رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية، المنشور في الجريدة الرسمية بتاريخ 15 يوليو 2020، وتاريخ العمل به 16 اكتوبر 2020، العدد 28 مكرر هـ.
4. قرار رئيس جمهورية مصر العربية رقم 276 لسنة 2014 بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
5. اللائحة التنفيذية الصادرة عن مجلس الوزراء المصري، لقانون مكافحة جرائم تقنية المعلومات، والمنشورة في الجريدة الرسمية بتاريخ 27 / 8 / 2020
6. قرار المشرع الفلسطيني بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية
7. مرسوم الامارات العربية المتحدة بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية
8. قانون المشرع القطري رقم 14 لسنة 2014 لمكافحة الجرائم الإليكترونية
9. المرسوم السلطاني العماني رقم 12 / 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات
10. قانون المشرع الاردني رقم 3 لسنة 2010 بشأن جرائم نظم المعلومات
11. المرسوم الملكي السعودي رقم م/17 بتاريخ 8 / 3 / 1428 هـ، الموافق 27 / 3 / 2007 بشأن مكافحة جرائم المعلوماتية.

د - قرارات ومنشورات الأمم المتحدة والمنظمات الدولية الاخرى.
1. النظام الأساسي لمحكمة العدل الدولية.
2. مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، أوجه التآزر والاستجابات – التحالفات والاستراتيجيات في مجال الجريمة والعدالة الجنائية، بانكوك، 2005

3. قرار مجلس الأمن رقم 2322 (2016) ، والذي اتخذه في جلسته رقم 7831 المنعقدة بتاريخ 12 ديسمبر 2016
4. تقرير اعمال المؤتمر المشترك للجمعية البرلمانية للبحر الابيض المتوسط ومجلس اوروبا، بدعم من مشروع Cyber South ، فرنسا، 2019
5. تقرير الأمين العام للامم المتحدة، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، خمسون سنة من مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية : إنجازات الماضى وآفاق المستقبل، بانكوك، 2005
6. سلسلة معاهدات مجلس اوروبا، البروتوكول الاضافي لاتفاقية الجريمة الاليكترونية بشأن تجريم الافعال المرتبطة بالتمييز العنصري وكراهية الاجانب التي ترتكب عن طريق انظمة الكمبيوتر، 2003
7. سلسلة معاهدات مجلس اوروبا، البروتوكول الاضافي الثاني للاتفاقية المتعلقة بالجريمة الاليكترونية بشأن تعزيز التعاون والكشف عن الادلة الاليكترونية، 2022
8. دراسة شاملة عن الجريمة السيبرانية، منشورات مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينا، 2013

ثانيا : اللغة الإنجليزية.

أ - المجلات العلمية.

1. Artur Appazov, Legal Aspects of Cybersecurity, University of Copenhagen, Denmark, 2014
2. Animesh Sarmah, Roshmi Sarma, Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Law's of India, Assam Kaziranga University, India, 2017
3. Abdelmonem Mohamed Magdy, Overcoming the conflict of jurisdiction in cybercrime, Master thesis, American University in Cairo, 2020
4. Attila Tanzi and others, international law and cyberspace, Ministry of Foreign Affairs, Italy, 2021
5. Allison Peters & Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, Journal of national security law, policy, Vol. 10:487, 2020
6. Dora Arifi, Cybercrime: a challenge to law enforcement, SEEU Review Volume 15 Issue 2, Macedonia, 2020
7. Juan Ignacio Alcaide, Critical infrastructure cybersecurity and the marine security, University of Cadiz, Spain, 2020

8. Joint Standing Committee on Foreign Affairs, Defense and Trade Inquiry into Australia's Relationship with ASEAN, 2008
9. William M. Stahl, the uncharted water of cyberspace; applying the principles of international maritime law to the problem of cybersecurity, University of Georgia, 2010
10. Pallavi Kapila, Cyber Crimes and Cyber Laws in India: An Overview, MCM DAV College for Women, Chandigarh, India, 2020
11. The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century, UNIDIR, 2017
12. The UN cybercrime debate enters a new phase, Global Initiative Against Transnational Organized Crime, Geneva, 2021 .

ب - التشريعات الوطنية.

1. Clarifying Lawful Overseas U.S.A of Data Act (CLOUD Act) 2018
2. Criminal Code of the Kingdom of Spain (1995 as of 2013
3. Decision of the Presidency of the Republic, Brazil, Law No. 14.155 of May 27, 2021
4. German Criminal Code in the version published on 13 November 1998
5. Indian Information Technology Act, 2000
6. Macedonian Criminal Code, 2002
7. Military Programming Act, EU 2013
8. The Gramm-Leach-Bliley Act (GLB Act or GLBA), U.S.A, 1999
9. The Criminal Code of The Russian Federation No. 63-Fz, 1996
10. The Federal Law of The Russian on Personal Data (No. 152-FZ), 2006

ثالثا : المواقع الإليكترونية.

1. https://arcticwolf.com/resources/blog/decade-of-cybercrime/

2. https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9-%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA
3. https://www.pam.int/ar/press-releases/pam-contributes-general-debate-31st-session-unodc-commission-crime-prevention-and
4. https://www.un.org/securitycouncil/ar/s/res/2178-%282014%29
5. https://www.un.org/securitycouncil/ar/content/sres23962017
6. https://www.nist.gov/itl/applied-cybersecurity/nice
7. http://www.aseanapol.org/about-aseanapol/permanent-secretariat
8. https://www.lexology.com/library/detail.aspx?g=a412035f-b3af-4fd1-a6f2-17e7c97efd7f
9. https://www.upguard.com/blog/cybersecurity-laws-regulations-france
10. https://www.unodc.org/romena/ar/untoc.html
11. https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC