آليات التعاون الدولي في مكافحة الجرائم الإلكترونية

International Mechanisms and Cooperation in Combating Cybercrime

فريد ناشف ♦
جامعة البليدة 02 - الجزائر
farid.nachef1011@gmail.com

تاريخ الإرسال: 2022/01/13	تاريخ القبول: 2022/05/09	تاريخ النشر: 2022/06/03

الملخص:

إن مكافحة الجرائم الإلكترونية اصبح من أهمية بمكان أن نبحث في السبل التي يجب اتباعها للتصدي لتلك الجرائم العابرة للحدود والتي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مرتكبيها وكيفية مساءلتهم جنائيا ومدنيا، وبالنظر إلى الطبيعة الخاصة للجرائم الالكترونية التي تنشأ وتقع في بيئة شبكة الإنترنت فإن التعاون الأمني والقضائي الدولي في سبيل مكافحة هذه الأنماط الإجرامية يجب أن يعتمد على آليات متطورة تواكب تطور هذه الجرائم وطبيعتها الخاصة، ويجب أن يتم هذا التعاون الدولي على أسس معينة تكفل في نهاية الأمر مكافحة هذه الجرائم بصورة بناءة.

لأجل ذلك كان لابد ان تكون تلك الأجهزة الوطنية والدولية على مختلف أنواعها على درجة كبيرة من الكفاءة و المعرفة والقدرة على كشف غموض تلك الجرائم المستحدثة.

الكلمات المفتاحية: الآليات، التعاون الدولي، مكافحة، الجرائم الالكترونية.

Abstract:

Combating cybercrime has become important to address these cross-border crimes, which require identifying their nature, characteristics, the specificities of perpetrators and their criminal and civil accountability. Taking into account the particular nature of cybercrime that happen through the Internet Network, international security cooperation to fight such types of crimes must be based on sophisticated mechanisms in accordance with the development and nature of such crimes . This international cooperation should be carried out on a specific basis that will ultimately ensure that these crimes are effectively combated.

♦ المؤلف المرسل

For this reason, national and international bodies had to be highly competent, knowledgeable and able to detect the ambiguity of these crimes.

Keywords: Mechanisms, International cooperation, combating, cybercrime

مقدمة:

يعاني المجتمع الدولي من ظاهرة خطيرة ومقلقة، تتمثل في التنامي المتزايد لعصابات الجريمة المنظمة العابرة للأوطان، والتي تطورت بصورة رهيبة واستفادت من التطورات التكنولوجية المتلاحقة والمتغيرات الكبيرة التي أفرزتها الظروف السياسية والاقتصادية والثقافية العالمية، بحيث عجزت الأجهزة الأمنية الدولية المتطورة عن ملاحقتها والحد من سلطانها، وذلك بالنظر لما أصبحت تشكله الجرائم الالكترونية من مخاطر على جميع مناحي الحياة وخاصة على الجانب الاقتصادي للدول، ويبدو أن الشعوب ليست ببعيدة عن استشعار الأخطار المحدقة الهائلة التي تواجهها من جراء الانتشار الواسع لهذه الجرائم.[1]

وعلى اعتبار أن الجريمة صنو للحياة ظهرت بوجودها وتستمر بدوامها، وهي ثمر لظروف المجتمع ونبت من غرس معطياته وإفراز لذاتية أشخاصه، فالجريمة إذن وجدت بوجود بني أدم على الأرض، وفي ذلك يقول الله تعالى:**(وَإِذْ قَالَ رَبُّكَ لِلْمَلَائِكَةِ إِنِّي جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً ۖ قَالُوا أَتَجْعَلُ فِيهَا مَن يُفْسِدُ فِيهَا وَيَسْفِكُ الدِّمَاءَ وَنَحْنُ نُسَبِّحُ بِحَمْدِكَ وَنُقَدِّسُ لَكَ ۖ قَالَ إِنِّي أَعْلَمُ مَا لَا تَعْلَمُونَ)** .[2]

وبما أن عالم اليوم يتسم بأشكال جديدة من الإجرام لم تكن مألوفة من قبل، أو لم يكن قد استفحل خطرها بعد، فهناك الإجرام المنظم أو الإجرام العابر للحدود والأوطان أو القارات أو الإجرام العالمي، والجرائم السياسية، والجرائم الإرهابية، والجرائم الإلكترونية، الأمر الذي يتطلب تعاونا وتضامنا دوليا لمكافحته و الوقاية منه، لأنه قد يكون خارج عن قدرة وإمكانيات - قانونية ومادية - لأي دولة منفردة التحكم فيه أو احتوائه والسيطرة عليه، وعلى اعتبار أن الجريمة الإلكترونية مشكلة معقدة عابرة للحدود الوطنية لا تستطيع أي دول معالجتها بمعزل عن باقي الدول الأخرى المكونة للمجتمع الدولي، وإذا أردنا فهم الجريمة الالكترونية وأسبابها و طرق وأساليب مكافحتها، علينا أن ننظر إليها ضمن نطاقها العالمي. الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم وطبيعتها، وتطوير الوسائل التقليدية بما يكفل تضامن جهود الدول وأجهزتها القائمة بمهمة مكافحة الجرائم عموما ، والجريمة ً الالكترونية على وجه الخصوص.

1 راجع: عوض محمد يحيى يعيش، دور التشريع في مكافحة الجريمة من منظور أمني (دراسة مقارنة)، الناشر الكتب الجامعي الحديث، مصر، دون طبعة 2006، ص 08

2 راجع: القرآن الكريم، سورة البقرة، الآية 30

المبحث الأول: مفاهيـــم عـامـة للجريمة الالكترونية

لقد تعددت ألفاظ ومفردات وصيغ ومصطلحات التعريف بالجريمة الالكترونية: " فقد أطلق عليها، جرائم الكمبيوتر والإنترنت وجرائم الحاسب الآلي (Computer crims)، والجرائم الرقمية (digital crims)، والجرائم الناعمة (Crims Soft)، وجرائم التقنية العالية (High -Tech Crims)، والسيبر كرايم (Cyber Crims)، وجريمة أصحاب الياقات البيضاء (White collar)، والجرائم النظيفة (Clean Crims) ".[1]

المطلب الأول: مفهوم الجريمة الالكترونية

ذهب خبراء متخصصون من دول الإتحاد الأوروبي أن جريمة الكمبيوتر هي: "كل فعل عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأملاك المادية أو المعنوية".[2] في حين أن منظمة التعاون الاقتصادي والتنمية (OCDE) وضعت تعريف للجريمة الالكترونية في اجتماع باريس 1983 والذي يعتبر أقدم التعاريف بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها".[3]

ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا"، كما عرفها "David Tnompson" بأنها: "أية جريمة يكون متطلبًا لاقترافها أن تتوافر لدى فاعلها معرفة تقنية للحاسب الآلي" .

ويرى "Massa" أن المقصود بها: " الاعتداءات غير القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"، وفي الغالب ترتكب الجريمة الالكترونية ليس بغرض تحقيق الربح وإنما بدافع المتعة النفسية أو الانتقام والسخرية من المنافسين أو غير ذلك من الدوافع الأخرى.[4]

و تعرف الجريمة الإلكترونية على أساس الاتفاقية العربية وقانون الجرائم الامريكية واتفاقية بودابست والاتحاد الدولي للاتصالات بأنها:"كل جناية أو جنحة ترتكب ضد فرد أو جماعة بدافع جرمي ونية الإساءة لسمعة الضحية أو جسده أو فكره أو ماله أو حياته، سواءً كان ذلك بطريقة مباشرة أم طريقة غير مباشرة باستخدام وسائل الاتصالات الحديثة الانترنيت"، ومع تزايد الانفتاح العالمي في مجتمع متحول من النظام الاجتماعي الطبيعي الى النظام الاجتماعي المنفتح على العالم والأكثر تطوراً وسرعة واندماجاً بالعالم الخارجي والمجتمعات

1 أنظر: أحمد بن عبد الرحمن البعادي، دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، 25/22 سبتمبر 2012، إدارة الدراسات والبحوث، الخرطوم، ص 04.

2 عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية دور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003، ط1، ص 32.

3-Sieber, Ulrich (1998). Legal Aspects Of Computer-related Crime in the Information Society. [Online]. Available: http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc [04-11-2002] .

4 إيمان فاضل السمرائي، هيثم محمد الزغبي، نظم المعلومات الإدارية، الطبعة الأولى، دار صفاء للنشر والتوزيع. عمان 2005. ص 259.

الداخلية المحلية بتقنيات ووسائل التواصل الاجتماعي المتاحة والمباحة وبحرية مطلقة دون قيود او ضوابط أو قوانين واضحة تحدد نطاق العقوبات الجرمية في حالة انتهاك الخصوصية أو الحقوق والحريات[1].

وبالرجوع الى مؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، يتضح أنه تبنى تعريف منضبط لجريمة تقنية المعلومات بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسبي أو شبكة حاسبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية."

وأما من منظور التشريع الجزائري فقد نصت المادة (02 أ) من القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال على أنها: "كل جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[2] وبالتالي فمفهوم الجريمة الالكترونية مرتبط أشد الارتباط بالنظم المعلوماتية، ولا يمكن الوصول للجريمة الالكترونية إلا من خلال أنظمة المعلومات وهو المنفذ الوحيد (النظام المعلوماتي) الذي يوجد في جميع الحواسيب وهو الذي يتم الربط فيه بشبكة الاتصال العالمية .

ويقصد بالمعلومات التي تعد أساسا للجريمة المعلوماتية ما نصت عليه المادة 02 فقرة ج من القانون رقم (09-04) المؤرخ في 05-08-2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها على أنه: " أي عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تجعل من المنظومة المعلوماتية تؤدي وظيفتها".

المطلب الثاني: المجرم المعلوماتي وخصائص الجرائم الإلكترونية

المُجرم المعلوماتي، يطلق على ذلك الفاعل الرئيس في العملية الجُرمية الإلكترونية، حيث يتمتع هذا الأخير بذكاء ودراية معلوماتية ناتجة عن تعلم وخبرة ميدانية في عالم الإلكترون،. إذ أن الجريمة الإلكترونية لا تقع على الأرض ولا بالوسائل المادية والأدوات المستعملة في الجريمة التقليدية ولا تثبتها مساحات الدماء ولا كسر الأعضاء، إنما تقع في فضاء رقمي بواسطة التقنيات الحديثة المرتبطة بالشبكة العالمية مما يصح أن تسمى بالجريمة العابرة للحدود، يتميز الفاعلين فيها بصفات وسمات لم تكن موجودة عند المجرمين التقليديين إن صحت العبارة، لذلك أُطلق عليهم بأصحاب المهارة، المعرفة، الوسائل السلطة، الباعث.[2]

ويتوفر المجرم الإلكتروني على مهارة عالية في مجال المعلومياتية والبرمجة، حيث يمكنه اختراق الشبكات بمهارات فائقة في كسر الشفرات وكلمات المرور للحصول على أدق المعلومات، ويُشَغّل أجهزة عن بُعد بكل سرية من خلال ارتباطه بشبكة الإنترنت مستغلا تجربته وذكاؤه في تطوير الأنظمة الأمنية المعلوماتية وتعديلها.[3]

---

[1] محمد محي الدين عوض، الجريمة المنظمة"، مقال بالمجلة العربية للدراسات الأمنية و التدريب، المركز العربي للدراسات الأمنية و التدريب، المجلد 10، العدد 19، الرياض 1995. ص 56.

2 "دون باركر" واضع أول قانون لجرائم الحاسوب لولاية فلوريدا الأمريكية عام 1987.

3 عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنيت في القانون العربي النموذجي،دار الكتب القديمة،مصر، 2007، ص 83.

وتأسيسا على ما سبق، فإن المجرم المعلوماتي يتصف بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية، فهي جرائم فنية تقنية في الغالب، والأشخاص الذين يقومون يكونون من ذوي بارتكابها عادة الاختصاص في مجال تقنية المعلومات الالكترونية أو على الأقل شخص لديه حد أدنى من المعرفة و القدرة على استعمال جهاز الحاسوب، والتعامل مع شبكة الإنترنت، كما أن الباعث إلى ارتكاب المجرم لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.[1] وعلى هذا سوف ندرس من خلال هذا المطلب سمات المجرم المعلوماتي في الفرع الأول ونتناول في الفرع الثاني خصائص الجرائم الالكترونية.

الفرع الأول: سمات المجرم المعلوماتي

يتميز المجرم الالكتروني بعدد من السمات والخصائص التي تجعله مختلفا عن المجرم التقليدي والتي منها:

1/ مجرم ذكي: يعتبر الذكاء من أهم صفات المجرم المعلوماتي لأنه يتطلب منه الإلمام التام بتقنية بتكنولوجيا المعلومات والقدرة على تعديل وتغيير برامج الحاسب الآلي، وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، فتنفيذ بعض الجرائم الإلكترونية يتطلب قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين[2]

2/ مجرم محترف: يتصف مرتكب الجريمة الالكترونية بأنه على درجة عالية من الخبرة والمهارة في استخدام الحاسب الآلي، والتكنولوجيا الحديثة.

3/ مجرم غير عنيف: يرتكب المجرم المعلوماتي نوعاً من الجرائم ينتمي إلى إجرام الحيلة، فهو لا يلجأ إلى استخدام القوة والعنف في ارتكاب جريمته، لا سيما وأنه لا يتعامل مع اشخاص حقيقين، بل يتعامل في مقومات غير مادية ممثلة في البيانات والمعلومات المخزنة في جهاز الحاسب الآلي، ولهذا فليس هناك مبرر للجوئه إلى العنف[1]

4/ مجرم متكيف اجتماعيا: فلا يضع المجرم الالكتروني نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إن ذكاءه يدفعه للتكيف مع المجتمع، و كلما ازداد تكيفه مع المجتمع كلما زادت خطورته الإجرامية.

5/ الميل إلى ارتكاب الجرائم: يتميز مرتكبو الجرائم الالكترونية بفرط في النزعة الإجرامية والميل إلى ارتكاب الجرائم.

---

1 طارق إبراهيم الدسوقي عطية، الأمن ألمعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009 ، ص322،322.

2 Vladimir Golubev, Criminal in Computer Related Crimes, Computer Crime Research center, http://www.polcyb.org,12/10/2009

[1] إسراء جبريل رشاد مرعي، الجرائم الإلكترونية" الأهداف، الأسباب، طرق الجريمة ومعالجتها"، المركز الديمقراطي 09 أوت 2016 الموقع التالي: https-//democraticac.de/?p=35426

6/ الميل إلى التقليد: أغلب الجرائم الالكترونية تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي لارتكابه للجريمة.[1]

الفرع الأول: خصائص الجرائم الالكترونية

تتميز الجرائم المرتبكة بواسطة الحاسب عبر شبكة الانترنت بالخصائص التالية:

1/ الجريمة الالكترونية جريمة مستحدثة: إن التقدم العلمي والتكنولوجي في ظل العولمة تجاوز قدرات الدولة الرقابية وإمكانيتها بل وأضعف قدرتها على تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وسلامتها،[1] لهذا تعد الجريمة الالكترونية جريمة مستحدثة تفرز إشكالات عديدة وتحديات كبرى على الدول من اجل التصدي لها.

2/ سرعة التنفيذ: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكثير، وبضغطه واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى أخر.

3/ التنفيذ عن بعد: لا تتطلب جرائم الحاسب في أغلبها وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة عن الفاعل.

4/ إخفاء الجريمة: إن الجرائم التي تقع عن طريق شبكة الانترنت مخفية، إلا أن أثارها تبقى وتلاحظ.[2]

5/ الجاذبية: نظرا لما تمثله سوق الحاسب والانترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها".[3]

6/ عابرة للدول: يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، فمن بين خصوصية هذا النوع من الجرائم هو إمكانية ارتكابها عن بعد، و من ثم اكتسابها طبيعة دولية ، أو كما يطلق عليها البعض الجرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. ويعد ذلك من بين الأسباب التي تستدعي ضرورة تفعيل التعاون الدولي بشأن مكافحة الجريمة المعلوماتية.[4]

7/ جرائم ناعمة: الجريمة المعلوماتية تستهدف المعنويات لا الماديات فهي تمتاز بأنها جرائم ناعمة لا تتطلب جهدا عضليا أو عنفا، فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي

---

1 أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دن، 2005، ص 36.

2 نبيلة هروال، الجوانب الاجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006، ص35.

2 Cohen Frederick: Protection and security on the information super high way,Wiley&sons,Inc,1995,p36.

3 عباس أبو شامة، التعريف بالظواهر الإجرامية المستحدثة، حجمها ، أبعادها، ونشاطها في الدول العربية، أكاديمية نايف العربية للعلوم الأمنية، ندوة علمية عقدت في تونس، 28-30 /06 /1999، ص 110.

4 ذياب البداينة، الجريمة المنظمة وأساليب مواجهتها في الوطن العربي، الندوة العلمية السابعة و الأربعون، مصر، 18-1998/05/20، ص 6.

عنف أو تبادل لإطلاق نار مع رجال الأمن، بل إلى جهد ذهني وعضلي مع إدراك لتقنيات الحاسوب. وتتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات والسرقة و السطو، إلا أن الجرائم المتصلة بالحاسب تمتاز بأنها ناعمة لا يستعمل فيها العنف"[1].

8/ الجريمة المعلوماتية جريمة يصعب إثباتها: الأصل في الجريمة إقامة الدليل وإسناده إلى المتهم، غير أنه وبفضل التطورات العلمية الحاصلة وظهور ما يسمى بالدليل الرقمي، يجعل إثبات هذا النوع من الجرائم أكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها، إضافة إلى أنها جرائم مخفية وفي كثير من الأحيان لا يتم اكتشافها إلا صدفة – جريمة لا تتقيد بمكان و زمان معين –. وعليه تتميز جرائم الانترنت عن الجرائم التقليدية للجريمة، بغياب الدليل الفيزيقي، وسهولة محو الآثار وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وعدم كفاية القوانين القائمة[2].

المبحث الثاني: أشكال التعاون الدولي لمكافحة الجرائم الإلكترونية

لقد عملت الأمم المتحدة منذ نشأتها على رسم سياسة ناجعة في مجال منع الجريمة وتحقيق العدالة الجنائية، عبر إقرار العديد من التوصيات وإنشاء اللجنة المتخصصة ومن بينها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين الذي عهد إليها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام، وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة، ومعاملة المجرمين وتعقد مؤتمرات دورية كل خمس سنوات وذلك تعزيز وتبادل المعارف والخبرات بين الأخصائيين من مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، ويعتبر مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده مدين ميلانو بإيطاليا في سنة 1985 م والذي انبثق عن هذا المؤتمر مجموعة من القواعد التوجيهية والتي توجت بالمصادقة على هذه المبادئ في هافانا بكوبا عام 1990 م.[3]

وتلعب منظمة الأمم المتحدة الدور الرئيسي- في مكافحة الإجرام المنظم في جميع مظاهره، وبالنظر إلى طبيعة الجرائم الالكترونية ومرونتها واكتسابها بعدا دوليا متناميا، فإن التعاون الدولي لمكافحة هذه الجرائم أمر لا مناص منه، وشرط هذا التعاون وجود تشريع داخلي متكامل وقضاء وطني فعال واتفاقيات دولية تتوافر على آليات تنفيذية قادرة على مساعدة الدول على التصدي للجرائم المنظمة وتفكيك الجماعات الإجرامية ومعاقبة وملاحقة العاملين فيها والقضاء على البنيات السوسيواقتصادية المولدة للجريمة بصفة عامة.

---

[1] سليم طارق عبد الوهاب، الجرائم المرتكبة بواسطة الانترنت وسبل مكافحتها ، بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة ، مجلس وزراء الداخلية العرب، تونس، 7-9 يوليو 1997 ، ص10.

[2] رستم هشام ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني، مجلة الأمن و القانون، مجلة دورية محكمة تصدرها أكاديمية شرطة دبي، العدد 02، 1999، ص 40 .

3 محمد الأمين ومحسن عبد الحميد أحمد معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية الرياض، الطبعة الأولى 1998، ص 19.

وإذا كان الالـتزام الأخـلاقي بالتعـاون مرهـونا دائمـا بتـوافر الرغبـة في تحقيقـه، فضـلاً عـن اتسـامه بالطـابع الاختياري، بحيث يمكن التخلي عن القيام به في أي وقت دون أن يترتب على ذلك أية مسؤولية في مواجهة الطرف المتخلي، بينما على العكس من ذلك نجد أن الأمر يختلف إذا كان مبعث الالتزام بالتعاون قانونيا متولد عن وثيقة مكتوبة (اتفاقيات دولية)، تولد التزاما على عاتق الدول، ويترتـب بالتـالي مسـؤولياتها في حـالة عـدم وفائها بهذا الالتزام[1].

ونظرا لتعدد الجرائم الالكترونية وتطورها تزايدت صورها، مما أدى إلى ضرورة التعاون الدولي لمواجهتها، ومـن ثم تكثيف الجهود الدولية وعقد الاتفاقيات والمؤتمرات الدولية لوضع استراتيجيات خاصة بمرحلتي الوقاية والمكافحة لهذه الجرائم، وهذا ما سنتناوله في هذا المبحث، مبرزين على ذلك الآليات الدولية والوطنيـة، لمكافحـة الجريمـة الالكترونية بحيث أننا قسمنا هذا المبحث إلى مطلبين:

المطلب الأول : الآليات الأمنية والقضائية لمكافحة الجريمة الالكترونية.

المطلب الثاني : إبرام الاتفاقيات الدولية والإقليمية لمكافحة الجرائم الالكترونية

المطلب الأول : الآليات الأمنية والقضائية لمكافحة الجريمة الالكترونية.

التعاون الدولي في مجال مكافحة الجريمـة المعلوماتيـة قـد يأخـذ مظهـران، الأول يتعلـق بالسـعي إلى اتخـاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ، والثـاني يتعلـق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة، والتي تعتـبر إختصاصـات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي[2].

الفرع الأول: الآليات الأمنية لمكافحة الجريمة الالكترونية.

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ مـن الأمـن والنظـام. وتشكل الجريمة إحدى القضايا الرئيسية في الكثير مـن دول العـالم، وتشـغل بال الحكومـات والمختصـين والأفـراد على حد سواء. ولقـد أثبـت الواقـع العمـلي أن الدولة – أي دولة – لا تسـتطيع بجهودهـا المنفـردة القضـاء علـى الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة. فنتيجة للتطور الملموس والمذهل في الاتصـالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهـور أشـكال وأنمـاط جديـدة

[1] لخضر دهيمي ، النظام القانوني لعمل الشرطة في الجزائر ،أطروحة مقدمة لنيل الدكتوراه في الحقوق، التخصص، القانون الجنائي الدولي، جامعة البليدة 02، السنة الجامعية 2014/ 2015، ص 244.

[2] سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهاد الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر، باتنة، السنة الجامعية: 2012-2013، ص 88.

من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية ، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب ، بل تعدت إلى أمن البنى الأساسية الحرجة.[1]

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة.

أولاً : جهود المنظمة الدولية للشرطة الجنائية، الإنتربول

تهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة. من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها وتتبادلها فيما بينها،[2] بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت، ومن الأمثلة على دور الإنتربول في ما يتعلق بالجرائم المتعلقة بالإنترنت ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت. وذلك أثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص.[1]

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

ومن بين الإنجازات التي حققتها الإنتربول في ظل مواجهة الجرائم المعلوماتية، تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول والمتعلقة بملاحقة الشخص الذي قام بنشر دودة الحب عبر الانترنت في الفلبين، وكذا العملية التي قامت بها شرطة الإنتربول، بالاشتراك مع المباحث الفيدرالية، وكذا

---

1 تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م – وثيقة رقم. A/CONF.203/14

2 Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co- Operation " , Clarendon press.Oxford,1989,p 168

3 محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية الرياض، 1998، ص 19.

الشرطة الإنجليزية عام 1998 والتي أحرزت فيها إنجازات كبيرة، من خلال تفكيك منشور عليه أكثر من 75000 صورة سلبية لدعارة الأطفال، والقبض على 107 أشخاص في 12 دولة، وكذا عملية القبض على شاب ألماني، بتهمة توزيع أحد الفيروسات، وذلك بالتنسيق بين الإنتربول والمباحث الفيدرالية الأمريكية والشرطة الألمانية، وتفكيك موقع منشور للصور الإباحية في 2005/05/02، بالتنسيق مع الأوروبول.[2]

وعلى غرار هذه المنظمة، أنشأ المجلس الأوربي عام 1991م في لكسمبورج، شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول الأطراف، لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالأنترنت.

أما على المستوى العربي، فقد أنشأ المكتب العربي للشرطة الجنائية من قبل مجلس وزراء الداخلية والعدل العرب في سنة 2010، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[3]

ثانياً: شرطة الويب الدولية

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

ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم .ونظرا لاتساع نشاط هذه المنظمة وما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خال شبكة الإنترنت على مستوى العالم .وفي إطار مسألة الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الإنترنت، فهناك من يرى أنه من الضروري وضع ضوابط وقواعد بحيث لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان من ناحية، وإلا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى.[1]

الفرع الثاني: التعاون القضائي على المستوى الدولي

يهدف التعاون القضائي بين الدول إلى التنسيق بين السلطات القضائية، فيما يتعلق

1 عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، جامعة الأزهر، مصر، ص 194.

2 محمد احمد سليمان عيسى-، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2016/02، جامعة المجمعة، المملكة العربية السعودية، ص 54.

3 سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة2007 ، ص 414.

بالإجراءات الجنائية من حيث إجراءات التحقيق والمحاكمة إلى حين صدور الحكم على المحكوم عليه، وضمان عدم إفلاته من العقاب .

وقد تعرضت اتفاقية الأمم المتحدة لمكافحة الجريمة إلى ضرورة تفعيل المساعدة القضائية المتبادلة بين الدول في مرحلة التحقيق أو المحاكمة، والمتعلقة بالجرائم المنصوص عليها في هذه الاتفاقية، حيث نصت المادة 18 منه على أن تقدم الدول الأطراف لبعضها البعض أكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية[1].

وترتبط المساعدة القضائية، بما تقدمه دولة ما من اجراءات من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، وتعتبر الاتفاقيات الدولية منبع الالتزامات بين الدول، على أن يظل ما ليس ملزما ممكنا، وفقا لما ينص عليه القانون الداخلي في كل من الدولتين، وقد أدرجه المشرع الجزائري، ونص عليه في القانون رقم 09.04، في المادة 16، معتبراً أنه في إطار تحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة، في الشكل الكتروني[2]، أما عن صور المساعدة القضائية الدولية فتتمثل فيما يلي:

1/ تبادل المعلومات: ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أو أمنية أجنبية، متى كانت بصدد جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل أيضا السوابق القضائية للجناة، تتعرف من خلاله الجهات القضائية على الماضي الجنائي للفرد المحال إليها، لتقرير الأحكام الخاصة بالعود ووقف تنفيذ العقوبة وغيرها من الإجراءات[3].

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

كما نصت المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي على هذا التبادل بنصها: " تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل لمعلومات المتعلقة بالتنظيم القضائي....."[4].

---

[1] عبد المنعم سليمان ، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين دراسة مقارنة ،دار الجامعة الجديدة الإسكندرية 2007، ص 95.

[2] القانون رقم 09-04 المتعلق بجرائم تكنولوجيا الإعلام و الاتصال ومكافحتها.

[3] علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات (التعاون القضائي الدولي لمكافحة الجريمة المعلوماتية)، دار الكتب والدراسات العربية، دون سنة، ص 5.

[4] عادل عبد العال ابراهيم خراشي، المرجع السابق، ص205.

كما حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، المنعقد في هافانا عام 1990م في قراره المتعلق بالجرائم ذات الصلة بالحاسوب، الدول الأعضاء بكشف جهودها لمكافحة الجرائم المعلوماتية، باتخاذ عدد من الاجراءات، منها مضاعفة الأنشطة التي تبذلها الدول على الصعيد الدولي من أجل مكافحة جرائم المعلوماتية، بما في ذلك دخول الدول أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل المرتبطة بجرائم المعلوماتية، وتطابق تشريعات الدول الأعضاء مع الأشكال الجديدة للإجرام.

وقد نص عليها المشرع الجزائري، في المادة 17 من القانون رقم 04-09، مؤكداً على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية إلزامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل[1].

2/ نقل الإجراءات: أقرت هذه الصورة من صور المساعدة القضائية العديد من الاتفاقيات الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية 2000و، في المادة 21 منها، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999و في المادة 9 منها، وكذا المادة 16 من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.

وتتجسد هذه الصورة في قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الأخيرة، وذلك بتوافر شروط معينة كالتجريم المزدوج، وأن تؤدي الاجراءات المطلوب اتخاذها دورا مهما في الوصول إلى الحقيقة[2].

3/ الانابة القضائية الدولية: تعبر الإنابة القضائية عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن، وتهدف الإنابة القضائية إلى تذليل العقبات التي تعترض سير الإجراءات الجنائية في ظل ما تشهده الظواهر الإجرامية من تطور[3].

ومن شأن الإنابة القضائية تسهيل الاجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كإجراء التفتيش والضبط والمعاينة[4].وتماشيا مع سرعة الجريمة الإلكترونية، وتجنبا لطول إجراءات طلب الإنابة القضائية الدولية، فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في اختصار

---

[1] علي حسن الطوالبة، المرجع السابق، ص06.

[2] محمد احمد سليمان عيسى، المرجع السابق، ص55 و56.

[3] عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 209 و210.

[4] علي حسن الطوالبة، المرجع السابق، ص 11.

الاجراءات عن طريق الا تصال المباشر بين السلطات المعنية بالتحقيق، كالاتفاقية الأمريكية الكندية، التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال[1].

4/ التعاون الدولي من خلال تسليم المجرمين في الجرائم المعلوماتية: يعرف تسليم المجرمين بأنه الإجراء الذي تسلم بموجبه دولة استنادا إلى معاهدة أو تأسيسا على المعاملة بالمثل عادة إلى دولة أخرى شخصا تطلبه الدولة الأخيرة لاتهامه أو لأنه محكوم عليه لعقوبة جنائية وتشترط معظم الدول للتعليم التجريم المزدوج للسلوك الذي يطالب بالتسليم لأجله وأن يكون معاقبا عليه بموجب قوانين الدولة طالبة التسليم والدولة المطلوب إليها.

وتتلخص هذه الصورة من صور التعاون الدولي لمواجهة الجريمة عامة والمعلوماتية خاصة في قيام الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود، كجرائم الأنترنت، بمحاكمة هذا المتهم إذا كان تشريعها يسمح بذلك، وإلا تسليمه لدولة اخرى مختصة من أجل محاكمته، والغرض من وراء ذلك، هو الحيلولة دون إفلات المتهم من العقاب متى كان القانون الداخلي للدولة المتواجد على إقليمها لا يسمح لها بمحاكمته[2].

وقد كانت مسألة تسليم المجرمين في مجال مكافحة الجرائم الإلكترونية موضوع العديد من الاتفاقيات والمعاهدات الدولية، أهمها معاهدة بودابست لمكافحة جرائم الأنترنت، من خلال المواد 12 و23 و24 و25 منها، وتوصيات المجلس المجلس الأوربي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجية المعلومات من خلال التوصية رقم (13/95) بتاريخ 11 سبتمبر 1995[3].

المطلب الثاني : إبرام الاتفاقيات الدولية والإقليمية لمكافحة الجرائم الالكترونية

تظهر أهمية الجهود الإقليمية والدولية في مواجهة الجريمة الالكترونية من خلال العمل على مكافحة هاته الجريمة، والتي رسخت في مساعي عقد وإبرام الاتفاقيات الدولية الثنائية والمتعددة الأطراف، والذي برز بدوره كعنصر فعال في مكافحة الظاهرة، خصوصا المحافظة على الثقة المتبادلة بين الدول في تقديم المساعدة الفنية والتقنية والأمنية والقضائية، الأمر الذي جعلها تضع توصيات وتبرم اتفاقيات تدرج في التشريعات داخلية، وتعالج كل ما هو مستحدث في مجال التقدم العلمي[4].

هذا بالإضافة إلى الجهود التي تبذلها جامعة الدول العربية، من خلال اعتمادها عبر أمانة مجلس الوزراء العدل العرب لما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، لذلك سنتناول في الفرعين التاليين معاهدة بودابست والقانون العربي النموذجي.

---

[1] محمد احمد سليمان عيسى المرجع السابق، ص 56

[2] عبد المنعم سليمان، المرجع سابق، ص275.

[3] عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 216 و217.

[4] بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي أطروحة لنيل شهادة الدكتوراه علوم تخصص، قانون عام ،كلية الحقوق، جامعة الجزائر، يوسف بن خدة، السنة الجامعية 2017- 2018، ص 08.

الفرع الأول: الاتفاقيات الدولية في مجال مكافحة الجرائم الالكترونية

تعد الاتفاقيات الدولية والمعاهدات من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة، ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات[1]، ونبينها فيما يلي:

اتفاقية بودابست: لقد أولى القانون الدولي والفقه الجنائي الدولي، التعاون القانوني اهتماماً بالغاً لتحقيق القدرة على التصدي للإجرام عبر الوطني، وسد أوجه القصور القانوني التي ساعدت المنظمات الإجرامية على اختراق النظم القانونية، وتعد المساعدة القانونية المتبادلة في المسائل الجنائية من الآليات الفعالة لمواجهة الجريمة المنظمة خصوصاً، والإجرام بوجه عام، لما للتعاون - في مجال الإجراءات الجنائية - من دور في التوفيق بين حق الدولة في ممارسة اختصاصها الجنائي داخل حدودها الإقليمية وحقها في توقيع العقاب[2].

تم إبرام أول المعاهدات المتعلقة بمكافحة الجريمة الالكترونية أو جرائم الانترنيت، وكان هذا عام 2001، بعاصمة المجرية بودابست، فقد تم صياغة المعاهدة من طرف عدد كبير من الخبراء المختصين في القانون في مجلس أوروبا، وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطع الكمبيوتر على مستوى العالم، هذا ما أدى في النهاية إلى توقيع عليها من قبل 30 دولة بتاريخ 23 نوفمبر 2001، في العاصمة المجرية بودابست.

لقد وقعت على هذه الاتفاقيات العديد من الدول الغير الأعضاء في مجلس أوروبا مثل كندا واليابان وجنوب إفريقيا كما صادقت عليها الولايات المتحدة الأمريكية، فهي في الأصل أوروبية المنشأ، إلا أنها دولية الطابع لأنها مفتوحة للانضمام لدول الأخرى، غير دول المجموعة الأوروبية طبقاً لنص المادة 48.

تتكون هاته الاتفاقية من 48 مادة، وأكدت الاتفاقية على حاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر، ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة جرائم الكمبيوتر ومخاطرها على الدول كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية واعتبرت مرجعاً لا يستهان به في ميدان محاربة الإجرام سيبيراني، سواءً بالنسبة لبعض الاتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية[3].

---

[1] شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، جامعة الشارقة، الإمارات العربية المتحدة، المجلد 17 ، العدد1 ، ص 751.

[2] لخضر دهيمي ، المرجع السابق ، ص 245.

[3] الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 18 نوفمبر 2001، من طرف المجلس الأوروبي و تم وضعها و التوقيع عليها بتاريخ 23 نوفمبر 2001.

وقد تضمن الفصل الأول، المضمون ب: تعريف للمصطلحات الأساسية في نص المادة 01، أما الفصل الثاني: فقط جاء تحت عنوان الخطوات الواجب اتخاذها على الصعيد الوطني وهو ينقسم إلى قسمين:

- القسم الأول: يضم المواد من 02 إلى 13، التي تعالج النصوص الموضوعية لجرائم الحاسوب.

- القسم الثاني: يضم المواد من 14 إلى 21، وتتعلق بالقواعد الإجرائية

- القسم الثالث: يضم المادة 22، و يتعلق بالاختصاص.

أما الفصل الثالث: و جاء تحت عنوان التعاون الدولي من المادة 23 إلى المادة 35.

أما الفصل الرابع: فتضمن الأحكام الختامية من المادة 36 حتى المادة 48.

وقد صنفت اتفاقية بودابست الجرائم المعلوماتية في خمسة عناوين في القسم الأول من الاتفاقية:

العنوان الأول: ويضم جوهر الجرائم الحاسب أو الجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد السرية أو سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات والنظم.

العنوان الثاني: و يضم الانتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.

العنوان الرابع: ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة 10 من الاتفاقية.

العنوان الخامس: يشمل على أحكام إضافية بخصوص الشروع والاشتراك وأيضا الجزاءات وتدابير طبقاً للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية.

لقد حدد واضعو اتفاقية بودابست الإطار القانوني العام للجرائم معلوماتية، والمتمثل في الدخول الغير مشروع أو الاعتراض الغير مشروع أو الاعتداء على سلامة البيانات أو النظام المعلوماتي وكذلك إساءة استخدام أجهزة الحسابات أو التزوير المعلوماتي أو الغش المعلوماتي، وقد أوجبت اتفاقية بودابست، بعض الشروط حتى تأخذ الأفعال السابقة وصف الجريمة.

تتمثل هذه الشروط في أن ترتكب الجرائم المذكورة في الاتفاقية دون وجه حق، وأن ترتكب الجرائم المذكورة بطريقة عمديه من أجل إقرار المسؤولية الجنائية.

وألزمت اتفاقية بودابست الدول الأطراف عند سن التشريعات الداخلية المتعلقة بالجرائم الالكترونية أن تراعي اتفاقية دولية لحقوق الإنسان. مثل: الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام 1950،

العهد الدولي للحقوق المدنية والسياسية لعام 1966،[1] ويجب على الدول الأطراف الاعتماد على المعايير لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية المتمثلة في مبدأ الإقليمية ومبدأ النسبية الاختصاص المكاني ومبدأ الجنسية.

الفرع الثاني: التعاون العربي لمكافحة الجرائم الالكترونية

إن المجتمعات العربية على غرار بقية المجتمعات الدولية ليست في منأى عن تهديدات الجريمة الالكترونية، تكون هذه الأخيرة جريمة متعدية الحدود، ولقد صدر القانون العربي النموذجي الاسترشادي بخصوص مكافحة الجرائم الالكترونية، أو بالأحرى جرائم الكمبيوتر انتزنيت كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب، في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعاً بخصوص مكافحة الجريمة المعلوماتية.[2]

ولقد حرصت جامعة الدول العربية، منذ إنشائها على تعزيز روابط التعاون القانوني والقضائي والأمني بين أعضائها، في مجال مكافحة الجريمة وتحقيق العدالة الجنائية، من خلال تنسيق سياساتها الجنائية وإرساء آليات قانونية لتنظيم هذا التعاون، كما شاركت بفاعلية جدية في جهود المنتظم الدولي لمكافحة الجريمة المنظمة عبر الوطنية، حيث كان لها إسهام ملحوظ في جميع مراحل صياغة اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها، وذلك من خلال الاقتراحات التي قدمتها في اجتماعات الخبراء الحكوميين.[3]

لقد اعتمدت جامعة الدول العربية ما سمي بقانون الإمارات الاسترشادي لمكافحة جرائم تقنية المعلومات وما فيه حكمها، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات المتحدة، وتم اعتماد هذا القانون النموذجي من قبل مجلس الوزراء العدل العرب في دورته التاسعة عشر- بالقرار رقم 495 الدورة 19، بتاريخ 8 أكتوبر 2003، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين.

إن قانون دولة الإمارات العربية المتحدة يمنع نسخ برامج الكمبيوتر بدون إذن وكل من يقبض عليه متلبسا بقرصنة البرامج سيخضع هو وشركته للمحاكمة، بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب قانون الغرامة المالية بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل 3 سنوات.

ونصت المادة السابقة من القانون العربي النموذجي الموحد، في شأن مكافحة الجرائم إساءة استخدام تقنية المعلومات على معاقبة كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو أسطوانة ممغنطة أو غيرها من الوسائل.

---

1 العهد الدولي للحقوق المدنية و السياسية، لعام 1966. اعتمد وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د-21) المؤرخ في 16 كانون/ ديسمبر1966 تاريخ بدء النفاذ: 23 آذار/مارس 1976، وفقا لأحكام المادة 49.

2 بدري فيصل، المرجع السابق، ص 33/32.

3 لخضر دهيمي ، المرجع السابق ، ص 251.

خاتمة:

إن تطور وسائل الاتصال الحديثة شجع المنظمات الإجرامية لتوسيع نطاق أنشطتها الإجرامية وتنويعها، لاسيما مع ظهور الإنترنت، حيث وجدت عصابات الجريمة المنظمة في الإنترنت ملاذاً أمناً، بما توفره من إمكانات في الاتصال والتخفي وتجاوز الحدود، فأصبحت تشكل لها قواعد في بلدان تعد واحة لها نظراً لضعف الأمن فيها لتنطلق من هذه القواعد عابرة للحدود في الاتصال بين شبكات الجريمة حول العالم لتنسيق أعمالها وترويج نشاطاتها في أسواق جديدة من العالم لم تكن تحلم بالوصول إليها، وقد وظفت عصابات المخدرات والجنس شبكة الإنترنت في إيصال سمومها إلى ضحاياها، وفي غسل الأموال الناجمة عن أعمالها وإظهارها في مظهر شرعي مستغلة مكامن الضعف في الشبكة، ومستعينة بخبراء على درجة عالية جلبتهم بالترغيب أو الترهيب أو بهما معاً.[1]

و اذا كان الاهتمام على المستوى الدولي أخذ منحى ايجابياً كماً وكيفاً، إلا ان الاهتمام على المستوى العربي ما زال ليس بمستوى الطموح، إلا في بعض الدول العربية في اقتحام هذا المجال بعملية ايجابية اكثر تسهم في حل المشكلات القانونية المترتبة على استخدام الكمبيوتر والانترنت في ارتكاب الجرائم، من حيث مواكبة ومواءمة النصوص القانونية والاتفاقيات الدولية، وكذلك من حيث استخدام التقنيات التكولوجيا الحديثة في الوقاية من الجرائم الالكترونية.

بالنظر إلى الطبيعة الخاصة للجرائم الالكترونية التي تنشأ وتقع في بيئة شبكة الإنترنت فإن التعاون الأمني الدولي في سبيل مكافحة هذه الأنماط الإجرامية يجب أن يعتمد على آليات متطورة تواكب تطور هذه الجرائم وطبيعتها الخاصة، ويجب أن يتم هذا التعاون الدولي على أسس معينة تكفل في نهاية الأمر مكافحة هذه الجرائم بصورة بناءة. حيث تةوصلنا إلى جملة النتائج الآتية:

ــ على ما اوضحنا فيما تقدم وبسبب هذه الاهمية المتزايدة لهذه الجريمة الحديثة في الوقت الحاضر فهي تحتاج بلا شك إلى دراسات وأبحاث معمقة لغرض توضيحها والإطلاع على ما يجري بخصوصها في ارجاء العالم معززة ببحوث ودراسات مقارنة للتشريعات العقابية المحلية والعربية والأجنبية.

ــ تتميز الجرائم الإلكترونية بخصائص تميزها عن باقي الجرائم الأخرى، كا ترتب عليه عديد الصعوبات في الإثبات، حيث أنها لا تترك أثر لها لقيام الجناة بمحو ما يدل وعليها بعد ارتكابها .

ــ تتميز جريمة الالكترونية بالطابع العالمى، فهى لا تعترف بحواجز الزمان ولا المكان ولا حتى بالحدود الاقليمية للدول.

1 راجع: علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 54

ــ للتعاون الدولي وسائل متعددة منها تبادل المعلومات وتبادل الخبرات والمساعدة التقنية وغيرها من الأشكال.

ــ سعى المجتمع الدولي إلى إبرام اتفاقيات دولية لمكافحة الهجمات والجرائم الإلكترونية وذلك من خال إبرام معاهدة بودابست لمكافحة جرائم الإنترنت التي تعد أولى المعاهدات التي تعلقت بمكافحة تلك الجرائم.

وتتمثل أهم المقترحات ذات الصلة بموضوع الدراسة في ما يلي:

ــ موائمة التشريعات الجنائية المقارنة والمعايير الدولية المعتمدة في مجال التجريم والحماية والتعاون الدولي واحترام حقوق الإنسان.

ــ اعتماد السياسة الوقائية الفعالة الرامية لدراسة أبعاد الظاهرة الإجرامية الإلكترونية المعاصرة.

ــ تأهيل المختصين بالتحري والتحقيق فى الجرائم الإلكترونية و كيفية إثبات تلك الجرائم وضبط الأدلة المتحصلة منها وكذلك ضبط الجناة.

ــ العمل على إبرام اتفاقيات دولية يتم فيها توحيد وجهات النظر بين الدول في مسألة تنازع الاختصاص القضائي فيما يتعلق بجرائم الإنترنت وتحديث القوانين الجنائية الموضوعية والإجرائية بما يتناسب مع خصوصيات الجرائم الإلكترونية.

قائمة المراجع:

1/ القرآن الكريم.

أ/ الكتب:

1 ــ أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دن، 2005.

2 ــ إيمان فاضل السمرائي، هيثم محمد الزغبي، نظم المعلومات الإدارية، الطبعة الأولى، دار صفاء للنشر والتوزيع. عمان 2005.

3 ــ عوض محمد يحيى يعيش، دور التشريع في مكافحة الجريمة من منظور أمني (دراسة مقارنة)، الناشر الكتب الجامعي الحديث، مصر، دون طبعة 2006.

4 ــ عبد المنعم سليمان ، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين دراسة مقارنة ،دار الجامعة الجديدة الإسكندرية 2007.

5 ــ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية دور الشرطة والقانون، دراسة مقارنة،، ط1. منشورات الحلبي الحقوقية، بيروت، 2003.

6 ــ عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنيت في القانون العربي النموذجي،دار الكتب القديمة،مصر، 2007.

7 ــ علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات(التعاون القضائي الدولي لمكافحة الجريمة المعلوماتية)، دار الكتب والدراسات العربية، دون سنة.

8 ــ عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، جامعة الأزهر، مصر.

9 ــ علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004.

10 ــ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009.

11 ــ سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة2007 .

12 ــ محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية الرياض، 1998.

13 ــ محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية الرياض، الطبعة الأولى 1998.

14 ــ نبيلة هروال، الجوانب الاجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006.

ب/ المجلات والدوريات:

1 ــ أحمد بن عبد الرحمن البعادي، دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية، 25/22 سبتمبر 2012، إدارة الدراسات والبحوث، الخرطوم.

2 ــ ذياب البداينة، الجريمة المنظمة وأساليب مواجهتها في الوطن العربي، الندوة العلمية السابعة و الأربعون، مصر، 18-1998/05/20.

3 ــ سليم طارق عبد الوهاب، الجرائم المرتكبة بواسطة الانترنت وسبل مكافحتها ، بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة ، مجلس وزراء الداخلية العرب، تونس، 7-9 يوليو 1997.

4 ــ عباس أبو شامة، التعريف بالظواهر الإجرامية المستحدثة، حجمها ، أبعادها، ونشاطها في الدول العربية، أكاديمية نايف العربية للعلوم الأمنية، ندوة علمية عقدت في تونس، 28-30 /06 /1999.

5 ــ رستم هشام ،الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني، مجلة الأمن و القانون، مجلة دورية محكمة تصدرها أكاديمية شرطة دبي، دبي العدد2 ، 1999.

6 ــ محمد محي الدين عوض، الجريمة المنظمة"، مقال بالمجلة العربية للدراسات الأمنية و التدريب، المركز العربي للدراسات الأمنية و التدريب، المجلد 10، العدد 19، الرياض 1995.

7 ــ شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، جامعة الشارقة، الإمارات العربية المتحدة، المجلد 17 ، العدد1 .

ج/ النصوص التشريعية:

1 ــ قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق لـ 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر عدد 47 مؤرخة في 16 غشت 2009.

2 ــ القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات ،ج.ر .عدد 71.

3 ــ القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل و المتمم لقانون العقوبات ،ج.ر .عدد 84.

4 ــ القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل و المتمم لقانون العقوبات ،ج.ر .عدد 37.

د/ الأطروحات والرسائل الجامعية:

1 ــ بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي أطروحة لنيل شهادة الدكتوراه علوم تخصص، قانون عام ، كلية الحقوق، جامعة الجزائر، يوسف بن خدة، السنة الجامعية 2017- 2018.

2 ــ لخضر دهيمي ، النظام القانوني لعمل الشرطة في الجزائر ،أطروحة مقدمة لنيل الدكتوراه في الحقوق، التخصص، القانون الجنائي الدولي، جامعة البليدة 02، السنة الجامعية 2014/ 2015.

3 ــ سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهاد الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر، باتنة، السنة الجامعية: 2012-2013.

4 ــ محمد احمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2016/02، جامعة المجمعة، المملكة العربية السعودية.

ه/ الاتفاقيات الدولية:

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر2000.

تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م – وثيقة رقم. A/CONF.203/14

الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 18 نوفمبر 2001، من طرف المجلس الأوروبي و تم وضعها و التوقيع عليها بتاريخ 23 نوفمبر 2001.

الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية. بتاريخ 2010/12/21

و/ المراجع باللغة الأجنبية:

1— Cohen Frederick, Protection and security on the information super high way,Wiley&sons,Inc,1995 .

2— Sieber, Ulrich (1998). Legal Aspects Of Computer-related Crime in the Information Society. [Online]. Available: http://europa.eu.int /ISPO/legal /en/ comcrime /sieber.doc [04-11-2002].

3— Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co- Operation " , Clarendon press.Oxford,1989.

4— Vladimir Golubev, Criminal in Computer Related Crimes, Computer Crime Research center, http://www.polcyb.org,12/10/2009