الدكتور/ سامـي جاد واصل
أستاذ ورئيس قسم القانون الدولي العام المُساعد بأكاديمية الشرطة

التعاون الدولي في مكافحة الجرائم الإلكترونية

المراسلة: الدكتور/ سامـي جاد واصل
أستاذ ورئيس قسم القانون الدولي العام المُساعد بأكاديمية الشرطة

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v3i1.96

البريد الإلكتروني: waselsamy@yahoo.com

نسق توثيق البحث:
سـامي جاد واصل، التعاون الدولي في مكافحـة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد ٣، العدد ١، إبريل ٢٠٢٣. صفحات 13- 99

التعاون الدولي في مكافحة الجرائم الإلكترونية

الدكتور/ سامي جاد واصل

الملخص:

فـي ظل ثـورة المعلومات التـي يعيشها عالمنـا المعاصـر أصبحنا نعيش حيـاة ملؤها الاتصـالات ونقل وتبـادل المعلومات والبيانـات الدولية والوطنية على حد سـواء؛ الأمر الـذى ساعد كل كيان على التعامل مع مختلف النظم المتقدمة، وأضحى العالم بمثابة قرية صغيرة، وتحرر الإنسان من قيود المكان. إلا أن هذه الثورة المعلوماتية قد صاحبها ظهـور نوع جديد من الجرائم، أطلـق عليها «الجرائـم الإلكترونية»، التي باتت تتصدر معـدلات الجرائم العابرة للحدود، وتهدد الأمن الاقتصادي والاجتماعي والسياسي في كافة دول العالم.

ولمواجهة الخطر المحدق والخسائر الفادحة التي تسببها الجرائم الإلكترونية، اتجهت العديـد من دول العالم إلى سن قوانـين جنائية خاصة أو عدلت قوانين العقوبات لديها، بما يكفل مواجهة هذه الجرائم، بيد أن هذه الدول قد واجهت العديد من الصعوبات في مكافحة تلك الجرائم متعدية الحدود عبر قوانينها الوطنية. وكان من الضروري توحيد جهـود المجتمع الـدولي لمواجهة هذا النوع من الإجرام، حيـث بُذلت العديد من الجهود الدولية الراميـة إلى التوصل لمفاهيم موحدة للمكافحة، وإبرام اتفاقيات دولية لمواجهة هذه الظاهرة الإجرامية.

وإزاء اتسـاع مسـرح ارتكاب الجرائـم الإلكترونية على المستوى الـدولي، وعجز كل دولـة منفردة عن مكافحتها، لجأت الدول إلى التعاون فيما بينها على المستويين الأمني والقضائـي، لمواجهة ضـراوة هذا الإجرام وظواهره المختلفة فـي كافة البلدان. إلا أن الممارسـة الدوليـة قـد أظهرت وجود ثمة معوقـات تواجه التعاون الـدولي في مكافحة الجرائـم الإلكترونية، وتحد مـن فاعليته. وعليه فقد اقترحت بعض التوصيات التي من شأنها تفعيل دور التعاون الدولي في مكافحة هذه الجرائم.

الكلمات الرئيسية: الجرائم الإلكترونية، التعاون الدولي، تسليم المجرمين.

International Cooperation in Combating Cybercrimes

Dr. Samy Gad Wasel
Associate Professor & Head of Public International Law Department,
Police Academy

Abstract

In light of the information revolution experienced by our contemporary world, we are living a life filled with communication, transfer and exchange of information and data, which have helped each entity to deal with the various advanced systems. The world has become a small village, and individuals are liberated from the constraints of place. However, this information revolution has been accompanied by the emergence of a new type of crime, called «Cybercrimes», which has become the leading rate of cross-border crimes, and threatens economic, social and political security in all countries of the world.

In order to confront the imminent danger and heavy losses caused by cybercrimes, many countries of the world have taken to enacting special criminal laws or amending their penal laws to ensure confronting these crimes. Nevertheless, these countries have faced many difficulties in combating these transnational crimes through their national laws. It was necessary to unify the efforts of the international community to confront this type of crimes, as many international efforts were exerted to reach unified concepts for combating, and to conclude international agreements to combat these crimes.

In view of the expanding scene of cybercrimes at the international level, and the inability of each individual country to combat it, countries have resorted to cooperating with each other at the security and judicial levels to confront the ferocity of this crime and its various phenomena in all countries. However, international practice has shown that there are obstacles facing international cooperation in combating cybercrimes, and limiting their effectiveness. Accordingly, some recommendations were suggested that would activate the role of international cooperation in combating these crimes.

Keywords: Cybercrimes, International Cooperation, Extradition

المقدمة:

إن مـن أهـم الإنجـازات العلميـة التى ظهـرت فى العقـود القليلة الماضيـة اختراع الحاسب الآلى والإنترنت، اللذين قدَّما خدمات هائلة للإنسانية فى أغلب مناحى الحياة الاقتصاديـة والاجتماعية والعلمية والعسكرية، وغيرها مـن المجالات. بيد أنه قد رافق هذه الإنجازات بروز خبراء جدد لم تعهدهم الإنسانية من قبل، يتمتعون بقدر كبير من الخـبرة والحرفية التى تمكنهم من تطويع هـذه التقنية للقيام بأعمال إجرامية أفرزت إلى جانـب الجرائم التقليدية جرائم معاصرة تعتمد التقنية فى تنفيذ الفعل الإجرامى بأساليـب مبتكرة وطـرق جديدة لم تكن معروفـة من قبل. وساعد هـؤلاء المجرمين ما يشهـده العصر الحاضر من تطور متسارع للوسائل المعلوماتية التى أسهمت بدورها فى نشـر جرائمهم، حتى باتت هذه الجرائم تهدد النظام المعلوماتى نفسه، بل وتسببت فى إحـداث شلل كامـل للأنظمة المدنية والعسكرية، الأرضيـة والفضائية، وتعطيل المعدات الإلكترونيـة، واختراق النظـم المصرفية، وإربـاك حركة الطيران ومحطـات الطاقة، وغيرهـا مـن الهيئات والمؤسسـات الحيوية، وذلـك بواسطة رسائـل معلوماتية مشفرة ترسلها لوحة مفاتيح الحاسب الآلى من على مسافات بعيدة قد تتعدى آلاف الأميال[١].

وتعـد الجرائم الإلكترونية إحدى صور الجرائم ذات البعـد الدولى العابر للحدود، حيـث لم تعد تلك الحدود تشكل حاجزًا أمام مرتكبـى هذه الجرائم، كما أن نشاط هـؤلاء الجنـاة لم يعد مقصـورًا على إقليم معين بل امتد إلى أكـثر من إقليم، بحيث بـات المجرم يشرع فـى التحضير لارتكاب جريمته في بلد معين، ويُقبل على التنفيذ فـى بلد آخر، ثم يهرب إلى بلد ثالـث للابتعاد عن ملاحقة أجهزة العدالة، فالجريمة أصبح لها طابعٌ دولي، والمجرم أصبح مجرمًا دوليًّا.

وقـد لفتت هـذه الأعمـال الإجرامية أنظـار الدول والهيئـات الدولية التـى أدركت خطورتها وسهولة ارتكابها وتأثيرها المباشر، لتجعل مكافحتها من أهم أولويات المجتمع الـدولى الذي انبرى لوضع اتفاقيات دولية تكفـل قمع هذه الأعمال الإجرامية وملاحقة

(١) د. حسـن بن أحمد الشهرى، قانون دولى موحد لمكافحة الجرائـم الإلكترونية، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، مجلد ٢٧، العدد ٥٣، الرياض، ٢٠١١، ص ٥.

مرتكبيها أينما وجدوا. وللتأكيد على أهمية وخطورة الجرائم الإلكترونية فقد أفرد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين إحدى حلقات عمله الأربع التى وردت على جدول أعماله لدراسة الجرائم المتعلقة بشبكات الحاسب الآلى والإنترنت، حيث أشارت الوفود المشاركة خلال المناقشات إلى أن الجرائم الإلكترونية تمثل إحدى أهم تحديات القرن الحادى والعشرين[١].

من ناحية أخرى، اتجهت العديد من دول العالم إلى سن تشريعات لمكافحة كافة صور وأشكال الجرائم الإلكترونية، بيد أن الممارسة الدولية قد أثبتت أنه من الصعوبة بمكان مكافحة مثل هذه الجرائم بصورة منفردة؛ ذلك لأن الجريمة الإلكترونية قد تنشأ فى بلد ليحدث أثرها فى بلد أو بلدان أخرى، أى أن أدلتها غالبًا ما تكون منتشرة بين عدة دول، وبالتالى فقد صار هناك ضرورة ملحة ومبررات قوية للتعاون الدولي لمكافحة الجرائم الإلكترونية، مع ضرورة النظر إلى التعاون بمفهومه الشامل، بحيث يتسع لاستيعاب الصور المختلفة لمجالات التعاون، التشريعية والقضائية والأمنية، بما يكفل ملاحقة وضبط مرتكبى هذه الجرائم وتقديمهم للعدالة.

أهمية البحث:

تتجلى أهمية هذا البحث فى إلقاء الضوء على موضوع من أهم موضوعات القانون الدولى فى الوقت الراهن وهو التعاون الدولى، والتعرف على الدور الذي يمكن أن يضطلع به فى مكافحة الجرائم الإلكترونية، كون هذه الجرائم تعد من قبيل الجرائم عابرة الحدود التى باتت تمثل تحديًا حقيقيًّا لأجهزة الأمن والقانون فى معظم دول العالم؛ الأمر الذي حدا بهذه الدول إلى التكتل والتعاون من أجل قمع هذه الجرائم وملاحقة مرتكبيها. وكذا التعرف على العقبات التى تواجه التعاون الدولى فى مكافحة هذه الجرائم، وسبل التغلب على تلك العقبات.

منهج وخطة البحث:

نظرًا لطبيعة موضوع البحث والهدف منه وتطرقه إلى العديد من المسائل القانونية،

(١) انعقد المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين بالعاصمة النمساوية (فيينا) خلال الفترة من ١٠ إلى ١٧ أبريل ٢٠٠٠.

فقد اعتمدت على المنهج الوصفى التحليلى لتوضيح وتحليل إجراءات التعاون الدولى فى مكافحــة الجرائم الإلكترونية من خلال الرجوع إلى الدراسات المتعلقة بالقانون الدولى العام، وغيرها من الاتفاقيات والمواثيق الدولية ذات الصلة.

هــذا وقد حاولت عرض كافة الأفـكار المتعلقة بموضوع البحث بطريقة متوازنة تكفل تغطية كافة جوانبه، لذا فقد ثم قسَّمت هذا البحث إلى ثلاثة مباحث على النحو التالى:

- **المبحث الأول: ماهية الجرائم الإلكترونية.**
- **المبحث الثانى: الجهود الدولية المبذولة لمواجهة الجرائم الإلكترونية.**
- **المبحث الثالث: آليات التعاون الدولى فى مكافحة الجرائم الإلكترونية.**

المبحث الأول

ماهية الجرائم الإلكترونية

إذا كانت الثورة الصناعية الأولى قد انطلقت فى أواخر القرن الثامن عشر، فإن الثورة الصناعية الثانية، كما يرى العديد من المفكرين، قد اندلعت شرارتها الأولى مع اختراع الحاسب الآلى والإنترنت فى النصف الثانى من القرن المنصرم. ولا غرو بأنه إذا كان هدف الثورة الصناعية الأولى هو إحلال الآلة محل الجهد البدنى للإنسان، فإن هدف الثورة الصناعية الثانية هو إحلال الآلة (الحاسب الآلى) محل النشاط الذهنى للإنسان. والواقع أن مجالات عدة كالصناعة والتجارة والنقل والطيران والطب والاتصالات، وغيرها الكثير من الأنشطة الحيوية التى يصعب حصرها، ما كانت لتتطور وتزدهر دون الاستعانة بالحاسب الآلى والإنترنت [(١)].

وفى ظل ثورة المعلومات التى يعيشها عالمنا المعاصر أصبحنا نعيش حياة ملؤها الاتصالات ونقل وتبادل المعلومات والبيانات الدولية والوطنية على حد سواء، الأمر الذي ساعد كل كيان على التعامل مع مختلف النظم المتقدمة. فالعالم بأسره قد اندمج مع بعضه البعض، وتحرر الإنسان من قيود المكان، ليبدو وكأنه موجود فى أكثر من مكان فى الوقت نفسه. إلا أن هذه الثورة المعلوماتية قد أدت إلى ظهور نوع جديد من الجرائم، أطلق عليها «الجرائم الإلكترونية»[(٢)]، التى تمثل ظاهرة حديثة النشأة؛ لارتباطها بتكنولوجيا حديثة نسبيًّا، هى تكنولوجيا الحاسبات التى لم تكن مألوفة من قبل، وخاصة في بدايات القرن الماضى.

---

(١) د. أسامة حسين عبد العال، جريمة تزوير المستند الإلكترونى، دراسة تحليلة مقارنة، على الرابط التالى:

- https://jelc.journals.ekb.eg/article_232149_5ac7aca18ebbce21dcd16e019f1623f9.pdf

(٢) لقد شغلت الجرائم الإلكترونية Electronic Crimes حيزًا كبيرًا من الدراسات العلمية من أجل تحديد مفهومها؛ الأمر الذى نتج عنه وضع عدد غير قليل من المصطلحات للدلالة عليها، كالجرائم السيبرانية Cyber Crimes، والجرائم الافتراضية Virtual Crimes، والجرائم الرقمية Digital Crimes، والجرائم المعلوماتية Information Crimes، وجرائم التقنية العالية High Technology Crimes، وجرائم أصحاب الياقات البيضاء White Collar Crimes، وجرائم الكمبيوتر Computer Crimes، وغيرها من المصطلحات.

راجع: د. هالة أحمد الرشيدى، الجهود الدولية فى مجال مكافحة الجرائم الإلكترونية: دراسة للخبرتين الأوروبية والعربية، مجلة الديمقراطية، مؤسسة الأهرام، مجلد ١٩، العدد ٧٥، القاهرة، ٢٠١٩، ص ٢٨.

ولبيـان ماهية الجرائم الإلكترونية، سنقسم هذا المبحث إلى ثلاثة مطالب رئيسية، نتناول فى الأول منها تعريف الجريمة الإلكترونية، ونعالج فى الثانى خصائص الجريمة الإلكترونية وصورها، ونخصص الثالث لأركان الجريمة الإلكترونية وأسبابها.

المطلب الأول

تعريف الجريمة الإلكترونية

لقـد تعـددت آراء الفقهاء بشأن تعريف الجريمة الإلكترونيـة، حيث ذهبوا فى ذلك مذاهـب مختلفة ووضعـوا تعريفات شتى لهذه الجريمة، ويمكـن حصر هذه التعريفات فـى اتجاهين أساسيين: أولهما، الاتجاه المضيق مـن مفهوم الجريمة الإلكترونية، الذي نظـر إليها من الجانب التقنى (الفنى). والاتجـاه الثانى، هو الاتجاه الموسع من مفهوم الجريمة الإلكترونية، الذي نظر إليها من الجانب القانونى.

الاتجـاه الأول: ذهب أنصـاره إلى تضييق نطاق الجريمـة الإلكترونية، حيث عرّفها البعض بأنها «نشـاط إجرامى تُستخـدم فيه تقنيـة الحاسب الآلى بطريقـة مباشرة أو غـير مباشـرة كوسيلـة أو هـدف لتنفيذ الفعل الإجرامـى المقصـود»[١]. كما عرَّفها البعض الآخر بأنها «كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبـير لازم لارتكابها مـن ناحية، ولملاحقته وتحقيقه من ناحية أخـرى»[٢]، وحسب هذا التعريـف يجب أن تتوافر معرفة كبيرة بتقنيـات الحاسب ليس فقط لارتكاب الجريمة، بـل أيضًـا لملاحقتهـا والتحقيق فيها، وهـذا التعريـف يضيق بدرجة كبـيرة من نطاق الجريمـة الإلكترونيـة، بمعنى أنه يجب أن يتوافر قدر كبير مـن العلم بهذه التكنولوجيا لدى الجنـاة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وفى السياق نفسه، عرف فريق ثالث الجريمة الإلكترونية بأنها «الفعل غير المشروع الذي يتورط فى ارتكابـه الحاسب، أو هى الفعل الإجرامى الذي يُستخدم فى اقترافه الحاسب باعتباره أداة رئيسية»[٣].

(1) «Any criminal activity that involves use of computer technology, directly or indirectly, as the instrumentality or object of the commission of a criminal act».
See: Franklin Clark and Ken Diliberto, Investigating Computer Crime, 1st Edition, Routledge and CRC Press, 1996, p. 1.

(٢) د. هلالى عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ١٣.

(٣) د. نهلا عبد القادر المومنى، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع، عمان ، ٢٠٠٨، ص ٤٨. =

الاتجـاه الثاني: إزاء الانتقـادات التي وجهت إلى الاتجـاه السـابـق من أنه قد قصر الجـريمة الإلكترونية على الحالات التى يكون النظام المعلوماتى أداة ارتكابها؛ الأمر الذي مـن شأنه خروج العديـد من الأفعال غير المشروعة من دائـرة التجريم والعقاب، ذهب أنصـار هذا الاتجـاه إلى التوسيع من نطاق الجريمة الإلكترونيـة، حيث عرفها البعض بأنهـا سوء استخدام الحاسب أو تسهيـل استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى الحـالات المتعلقة بالولوج غير المصـرح به لحاسب المجني عليه أو بياناته. كما تمتد الجريمـة لتشمـل الاعتداءات المادية على جهـاز الحاسب ذاته أو المعـدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحاسب الآلية بما تتضمنـه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته[١].

وفى السياق ذاته، عرف الفقيه الألمانى «تيدمان» Tiedemann الجريمة الإلكترونية بأنها «كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يُرتكب بواسطة استخدام الحاسـب»[٢]. كمـا عرفها البعض بأنها «أى دخول غير قانونى أو غـير أخلاقى أو غير مصرح به للمعالجة الآلية للبيانات أو لإرسال هذه البيانات»[٣].

بيـد أن هـذا الاتجـاه لم يسلـم -أيضًا- من النقد، حيـث قيل بأن استمـرار إطلاق

= وفـى المعنـى نفسـه، عرف البعض الجريمـة الإلكترونية بأنها «أى جريمـة ضد المال العام مرتبطة باستخـدام المعالجة الآلية للمعلومات».

راجع: د. أحمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعى، الإسكندرية ، ٢٠٠٦، ص ٨٦.

وعرفها فريق آخر بأنها «كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذى يُرتكب باستخدام الحاسب».

راجـع: د. نائلـة عادل قـورة، جرائم الحاسب الآلى الاقتصاديـة، دراسة نظرية تطبيقية، منشـورات الحلبى الحقوقية، بيروت، ٢٠٠٥، ص ٢٩.

(١) حشيفـة عبـد الهادى، التعاون الـدولى فى مجال مكافحة الجرائم الإلكترونية، رسالة ماجستـير مقدمة لكية الحقوق والعلوم السياسية، جامعة زيان عاشور - الجلفة، الجزائر، ٢٠١٩-٢٠٢٠، ص ١٠- ١١.

(2) Klaus Tiedemann, Fraudes et autres délits d›affaires commis à l›aide d›ordinateurs électroniques, RDPC, No. 7, Bruxelles, 1984, p. 612.

(3) Henri Alterman et Alain Bloch, La Fraude Informatique, Paris, 1988, p.530.

وفـى المعنـى نفسـه، عرف البعض الجرائم الإلكترونية بأنها «تلك الجرائم التـى تُرتكب ضد أفراد أو جماعات من أفراد لديهم دوافـع إجراميـة لإيذاء سمعـة الضحية عمدًا، أو إلحـاق الأذى البدنى أو العقلى بالضحية، بصـورة مباشرة أو غير مباشرة، باستخدام شبكات الاتصالات الحديثة مثل الإنترنت والهواتف المحمولة. راجع:

- Bushra Mohamed Elamin Elnaim, Cyber Crime in Kingdom of Saudi Arabia: The threat today and the expected future, Journal of Information and Knowledge Management, Vol. 3, No. 12, 2013, p. 14.

الجريمة الإلكترونية على كل فعل إجرامى له علاقة بالحاسب الآلى قد يؤدى إلى اعتبار جميع الجرائم من قبيل الجرائم الإلكترونية، بسبب الانتشار المرتقب لاستخدام الحاسب الآلى فى شتى مناحى الحياة. كما أن الخلط بين الجرائم الإلكترونية وغيرها من الجرائم الاعتيادية بهذه الصورة قد يسبب خللاً فى عمليات ضبط وملاحقة الجرائم الإلكترونية الحقيقية؛ الأمر الذي من شأنه أن يعكس أرقامًا غير حقيقية لإحصائيات الجرائم الأخيرة[١].

ويتضح من التعريفات السابقة أن الجريمة الإلكترونية، كونها من الجرائم الحديثة نسبيًّا، لا يوجد إجماع على تعريفها ولا اتفاق بين الفقهاء حول مصطلح للدلالة عليها، باعتبار أن موضوعها يختلف بحسب ما إذا كان الاعتداء موجهًا إلى أحد مكونات النظام المعلوماتى أو كان وسيلة لتنفيذ جرائم معينة. فالجريمة الإلكترونية تعتبر شكلاً من أشكال الجرائم المستحدثة ذات الطبيعة الخاصة، التى تُستخدم فيها التقنية الرقمية لتحقيق أهدافها وترتيب آثارها التى تتعدى الحدود الدولية. وفى هذا الصدد، ذهب البعض إلى القول - بحق- أن الجريمة الإلكترونية جريمة حديثة النمط، وغير معروفة بين صور الإجرام البشرى التقليدى؛ الأمر الذي ميزها بهذه الخصائص حتى عُرفت بأنها الجريمة التى لا تعرف الحدود، وأن شبكة الإنترنت التى ألغت الحدود الجغرافية بين الدول أصبحت ذات فاعلية تفوق قدرة الأجهزة الدولية المختصة بمكافحة الجريمة[٢].

المطلب الثانى

خصائص الجريمة الإلكترونية وصورها

مما لا شك فيه أن تطور تقنية ووسائل الاتصال الإلكترونى بمختلف أنواعه قد صاحبه تطور فى الجريمة يتماشى وهذا التطور التكنولوجى، وأصبحت الجريمة الإلكترونية لا تقل خطورة عن الجريمة التقليدية، فهى تمس الفرد فى حياته الخاصة والمؤسسات فى اقتصادها والبلاد فى أمنها القومى والاقتصادى والسياسى فتسبب أضرارًا وخسائر فى مختلف القطاعات. هذا وقد اكتسبت الجريمة الإلكترونية طابعًا

(1) Russel Fox, Justice in the 21st Century, 1st Edition, Routledge-Cavendish, London, 1999, pp. 21 et seq.

(٢) د. أحمد محمد عبد المعبود، الجريمة الإلكترونية وآلية مكافحتها فى ظل القانون الدولى، مجلة البحوث القانونية والاقتصادية، الصادرة عن كلية الحقوق – جامعة المنوفية، المجلد ٣١، العدد ٢، ٢٠١٩، ص ٨.

خاصًا ميزها عن غيرها من الجرائم العادية، كما اتخذت صورًا وأشكالاً متعددة. وبالتالى سوف نقسم هذا المطلب إلى فرعين، نتناول فى الأول خصائص الجريمة الإلكترونية، وفى الثانى صور هذه الجريمة.

الفرع الأول

خصائص الجريمة الإلكترونية

إن سياق الجريمة الإلكترونية وظروف ارتكابها باستخدام الحاسب الآلى من خلال شبكة الإنترنت، حدا ببعض الفقهاء إلى القول بأن لأفعالها خصائص متفردة، لا تتوافر فى أى من أفعال الجرائم التقليدية، نوجزها فيما يأتي:

١- **الجريمة الإلكترونية جريمة مستحدَثة:** تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الحديثة التى يمكن أن تشكل أخطارًا جسيمة فى ظل العولمة، فلا غرابة أن تعد هذه الجرائم، سواء التى تتعرض لها أجهزة الكمبيوتر أو التى تُسخر تلك الأجهزة فى ارتكابها، من قبيل الجرائم المستحدثة، إذ إن التقدم التكنولوجى الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث تجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها فى تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها. من ناحية أخرى، فإن المجرم الذي يرتكب الجريمة الإلكترونية يختلف اختلافًا جذريًا عن المجرم التقليدى، فالمجرم المعلوماتى يتميز بذكائه وقدرته على التعامل مع جهاز الحاسب الآلى والشبكة العنكبوتية، اللذان يساعدانه على ارتكاب جرائمه بدون أدنى مجهود. فالجريمة الإلكترونية تتم بتقنيات عالية فى ظل عالم افتراضى غير ملموس؛ الأمر الذي يؤدى إلى تشتيت جهود البحث والتحرى والتنسيق الدولى لتعقب وضبط مرتكبى مثل هذه الجرائم وتقديمهم للعدالة[١].

٢- **جريمة عابرة للحدود:** إن من أهم الخصائص التي تميز الجريمة الإلكترونية أنها جريمة تتخطى الحدود الجغرافية للدول لاتصالها بعالم الإنترنت وتقنية المعلومات، وقد تتأثر دول كثيرة بهذه الجريمة فى آن واحد؛ وذلك بسبب السرعة الهائلة فى

(١) د. عبيشات أمينة، الجرائم الإلكترونية بين المواثيق الدولية والتشريعات الوطنية، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد ٦، العدد الأول، الجزائر، ٢٠٢١، ص ٥.

تنفيذهـا وحجم الأمـوال والأشخاص المستهدفة من خلالها. مـن ناحية أخرى، أعطى انتشـار شبكة الإنترنت إمكانية لربط أعداد هائلة مـن أجهزة الحاسب الآلى المرتبطة بالشبكـة العنكبوتية دون أن تخضع لحدود الزمان والمكان، لذا فإنه من السهولة بمكان أن يكـون المجرم فى بلـد ما والمجنى عليه فى بلـد آخر[1]، وفى ظل تفـاوت التشريعات الوطنية من دولة لأخرى، تظهر العديد من المشاكل حول صاحب الاختصاص القضائى بهذه الجريمة، فضلاً عـن إشكاليات أخرى تتعلق بإجراءات الملاحقة القضائية. وهنا تظهـر الحاجة إلى وجود تنظيم قانونى دولى وداخلى يتلاءم مع مكافحة هذا النوع من الجرائم وضبط فاعليها.

٣- صعوبـة اكتشـاف وإثبات الجريمـة الإلكترونيـة: إن إقامة الدليـل وإسناده إلى المتهم هو الأصل فى الجريمة، إلا أنه وبفضل التطورات الهائلة فى التقنيات المعلوماتية وظهور ما يسمى بالدليل الرقمى الذي يتمثل فى مجموعة بيانات مأخوذة من تجهيزات حاسوبية وشبكات معلوماتية، وهذا الدليل يمكن نقله بسرعة فائقة من مكان إلى آخر، كما يمكن إلغاءه والعبث به نظرًا لطبيعته. فالجريمة الإلكترونية لا تترك آثارًا ملموسة، ومـن ثَمَّ لا تترك شهودًا يمكن الاستدلال بأقوالهـم ولا أدلة مادية يمكن فحصها؛ لأنها تقع فى بيئة افتراضية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.

مـن جهة أخرى، فإن وسيلة تنفيذ هذه الجريمـة تتسم فى أغلب الحالات بالطابع التقنـى الذي يضفـى عليها الكثير من التعقيـد، ومن ثَمَّ فإنها تحتـاج إلى خبرة عالية بتقنيـات الكمبيوتر ونظم المعلومـات يصعب على المحقق التقليـدى الإلمام بها. وتتجلى صعوبـة إثبـات الجريمـة الإلكترونية فى أن الجانى عـادة لا يترك خلفـه أى أثر مادى

(١) من أهم القضايا التى تؤكد هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة «إيدز»، وتتلخص وقائعها أنه فى أوائـل عـام ١٩٨٩ قام أحد الأشخاص وهو «جوزيـف بيب» بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الإيدز، لكن هذا البرنامج كان يحتوى على «فيروس» يؤدى إلى تعطيل جهاز الحاسب الآلى المُستقبل عن العمل، فيقوم الجانى بطلـب مبلـغ مالى من المجنى عليه لإعطائه عنوان إلكترونى مضاد للفيروس. وفى ٣ فبراير من العام نفسه، تم تحديد مكان الجانـى وإلقـاء القبض عليه فى ولاية «أوهايو» الأمريكية، وطالبت المملكة المتحـدة بتسليم الجانى للسلطات البريطانية نظرًا لأن معظم الأضرار الناجمة عن هذا الفيروس قد وقعت على أراضيها، وبالفعل تم تسليمه ومحاكمته أمام القضاء البريطانى.
راجـع: د. مخلـد إبراهيم الزعبى، فاعلية القوانين والتشريعات العربية فـى مكافحة الجرائم الإلكترونية، المجلة العربية للنشر العلمى، العدد ٣٧، الأردن، ٢٠٢١، ص ٢٨٤.

ملموس يمكن فحصه؛ مما يصعب إجراءات اكتشافها، فكثير من الجرائم الإلكترونية لا يتم اكتشافها إلا مصادفة، فهى جرائم مخفية لا تتقيد بمكان ولا بزمان[١].

٤- **جريمة سريعة التنفيذ:** تعد الجريمة الإلكترونية من قبيل الجرائم سريعة التنفيذ ؛ حيث إنه فى أغلب الأحيان لا يكون الركن المادى سوى ضغطة على زر معين فى الجهاز، مع إمكانية تنفيذ ذلك عن بعد دون اشتراط التواجد فى مسرح الجريمة، ولذا فإن سهولة ارتكاب الجريمة الإلكترونية قد شكلت عنصر إغراء للعديد من المجرمين فى كافة أنحاء العالم، حيث إن ارتكابها لا يتعدى سوى توفر إمكانية استغلال التكنولوجيا والتقنيات الحديثة، خصوصًا عندما يكون الجانى موظفًا عامًّا أو فى إحدى الشركات الخاصة التى تعتمد على الحاسب الآلى فى عملها المتعلق بالمعلومات أو تداول الأموال، بحيث يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلى فى المؤسسة أو الشركة التابع لها، وتحقيق أرباح طائلة من وراء ذلك[٢].

٥- **الجرائم الإلكترونية من الجرائم الناعمة:** لا تتطلب الجرائم الإلكترونية عنفًا أو مجهودًا بدنيًّا لتنفيذها، فهى تُنفذ بأقل مجهود ممكن وتعتمد على الخبرة فى المجال المعلوماتى بشكل أساسى على عكس الجرائم التقليدية التى كثيرًا ما تتطلب القوة والعنف؛ لأنها تقع فى مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات، وهى بالتالى أقل عنفًا، حيث يمكن نقل كافة المعلومات الخطرة والمحظورة من معلومات استخبارية أو خطط تخريبية أو صور فاضحة بشكل سهل وبسيط عبر ضغطة خفيفة على لوحة مفاتيح الحاسب[٣].

إن الجريمة الإلكترونية تعتمد فى الأساس على الدراية الذهنية والتفكير العلمى المدروس القائم على معرفة واسعة بتقنيات الحاسب الآلى. من ناحية أخرى، ليس هناك ثمة شعور بالخوف وعدم الأمان تجاه مرتكبى الجرائم الإلكترونية؛ لأنهم ليسوا

---

(١) د. صورية بوربابة، التعاون الدولى فى مكافحة الجرائم المعلوماتية، مجلة القانون الدولى للدراسات البحثية، جامعة طاهرى محمد - بشار، العدد الأول، الجزائر، ٢٠١٩، ص ٩٣.

(٢) د. عثمان الصديق أحمد محمد، الجرائم الإلكترونية فى القانون السودانى، دراسة مقارنة على ضوء الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة ٢٠٠٢، رسالة ماجستير مقدمة لكلية القانون - جامعة الخرطوم، بدون سنة نشر، ص ١٠٨.

(٣) د. سامى يس خالد، الجهود الدولية لمكافحة الجرائم المعلوماتية، مجلة الدراسات العليا، جامعة النيلين، المجلد ٤، العدد ١٤، الخرطوم، ٢٠١٦، ص ١١.

محترفـى إجرام. كل ذلـك حدا بالبعض إلى وصـف الجرائم الإلكترونيـة بالجرائم الناعمة[١].

٦- **جريمة تعتمد على الخداع والتضليل:** يتميز مرتكبو الجرائم الإلكترونية بالذكاء والدراية بالأساليب المستخدمة فى أنظمة المعالجة الآلية وطريقة تشغيلها وكيفية تخزين المعلومـات، إذ يعتبر الإجرام الإلكترونى إجرام الأذكيـاء مقارنة مع الإجرام التقليدى الذي يميل إلى استخدام القوة والعنف، كما أن الدافع لارتكابها يكون فى أغلب الحالات هو إثبات الذات فى القدرة على قهر النظام والتغلب على الأنظمة[٢].

٧- **عـدم مواكبـة القوانين الساريـة للجريمة الإلكترونيـة:** إن النصوص القانونية التقليديـة الساريـة لم تعـد تتماشى مـع التطور السريـع للجرائـم الإلكترونية، خاصة مـع ما عرفته من تقنية عاليـة ومواكبة للتطور التكنولوجى؛ الأمـر الذي يتطلب سرعة تدخل المشـرع الوطنى لسن قوانين حديثة لمواجهة هذه الجرائم، وتفعيل مبدأ الشرعية الجنائية، مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين فى المعلوماتية، فضـلاً عـن إبرام اتفاقيات ثنائيـة ومتعددة الأطراف تكفل تعزيـز التعاون الدولى فى مكافحة الجرائم الإلكترونية[٣].

الفرع الثانى

صور وأشكال الجريمة الإلكترونية

مـن الصعوبة بمـكان حصر كافة صور وأشـكال الجرائم الإلكترونيـة، نظرًا لتعدد وتنوع صورها وأشكالها بشكل متسارع فى ظل التطور الهائل الذي تشهده تقنيات الشبكة العنكبوتيـة، فهـى تزداد تنوعًا وتعـدادًا كلما أوغل العالم فى استخـدام الحاسب الآلى وشبكـة الإنترنت وقد أثبتـت الدراسات أن معظم هذه الجرائم يكـون من بين أهدافها الحصول على المعلومات، التى تكون إما محفوظة على أجهزة الحواسيب أو منقولة عبر شبكـة الإنترنت، وأخرى يكون هدفها الاسـتيلاء على الأموال، وثالثة تستهدف الأفـراد

(١) حشيفة عبد الهادى، التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، مرجع سابق، ص ١٧.

(٢) د. صورية بوربابة، التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص ٩٤.

(٣) د. عبـد الفتـاح بيومى حجازى، مبادئ الإجـراءات الجنائية فى جرائم الكمبيوتر والإنترنـت، دار الكتب القانونية، القاهرة، ٢٠٠٧، ص ٤٣.

أو الجهـات بعينها، وأخـيرة تستهدف أجهزة الحاسب الآلى نفسهـا، **ويمكن تلخيصها فيما يأتي**[1]:

١- الجرائـم المتعلقـة بالمعلومـات: ثمـة العديـد من الجرائـم التى ترتكـب بهدف الحصـول علـى المعلومات، أو تغييرهـا، أو حذفها نهائيًّا، وذلك حسـب درجة أهميتها. فمعظـم الجرائـم التى يكون هدفهـا المعلومات هى فـى الغالب جرائـم اقتصادية يتم ارتكابها بغرض الحصول على مزايا أو مكاسب اقتصادية، فالحرب الاقتصادية لا تقل فى ضراوتها وشدتها حاليًا عن الحرب العسكرية، إلا أنها تتم باستخدام الحاسب الآلى وعبر شبكة الإنترنت.

٢- جرائـم الاستيلاء علـى الأموال: تستهدف هـذه الطائفة مـن الجرائم تحديدًا عناصـر الذمة المالية، حيث يكـون الطمع وفكرة المكسب السريع عـن طريق الاستيلاء علـى تلك الأموال هى الدافع الرئيس وراء ارتكابها. وقد تُرتكب أحيانًا لمجرد قهر نظام منشـأة أو مؤسسة اقتصادية، أو الرغبة فى تخطـى حواجز الحماية، أو بدافع الانتقام من صاحب تلك المنشأة أو المؤسسة أو أحد عناصرها.

٣- استهـداف الأشخاص أو الجهات: إن نسبة كبيرة مـن الجرائم التى تُرتكب فـي

---

(١) حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة الجلفة، العدد الأول، الجزائر، ٢٠٠٩، ص ٢٢١-٢٢٢.

كما حصر مكتب الأمم المتحدة المعنى بالمخدرات والجريمة صورالجرائم الإلكترونية فى الفئات التالية:

١- الأفعال ضد السرية والنزاهة وتوافربيانات الحاسب أو النظم:

وتتمثل فى الدخول غير المشروع لنظام الحاسوب، الدخول غير المشروع، اعتراض أو الاستيلاء على بيانات الحاسوب، الاستنتاج غـير المشروع لبيانات الحاسوب أو نظامـه، إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب، واختراق الخصوصية أو أساليب حماية البيانات.

٢- الأفعال ذات الصلة بالحاسب لمصالح شخصية أو مادية أو أذى:

وتتضمـن الاحتيـال المتعلق بالحاسوب أو التزوير، جرائم الحاسوب ذات الصلة بالهوية، حقوق الطبع والنشر أو جرائم العلامة التجاريـة ذات الصلـة بالحاسـوب، إرسال أو السيطـرة على إرسال البريـد المزعج، الأعمال ذات الصلـة بأجهزة الحاسوب الشخصية التى تسبب الضرر، والإغراء أو استمالة الأطفال المتعلق بالحاسوب.

٣- الأفعال ذات الصلة بمحتويات الحاسوب:

وتشمـل الأفعـال ذات الصلـة بالحاسوب التى تنطوى على خطاب الكراهية، الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال المتعلقة بالحاسوب، والأعمال ذات الصلة بأجهزة الكمبيوتر فى دعم جرائم الإرهاب.

راجع:

- UNODC United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, New York, 2013, p. 16.

مجـال المعلوماتية تستهدف إما أشخاص أو جهات بعينها، وغالبًا ما تكون تلك الجرائم مـن قبيل الجرائم المباشرة التى تُرتكب فى صورة ابتزاز أو تهديد أو تشهير. وقد تكون جرائم غير مباشرة تُرتكب من أجل الحصول على البيانات، أو المعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها بعد ذلك فى ارتكاب جرائم مباشرة.

٤- استهـداف أجهـزة الحاسب الآلى: والهـدف من ارتكاب مثل هـذه الجرائم هو اخـتراق أجهزة الحاسـب الآلى، أو تخريب أنظمـة تلك الأجهزة نهائيًّـا، أو على الأقل تعطيلها لأطول فترة ممكنة، ومعظم تلك الجرائم تتم بواسطة استخدام الفيروسات[١].

(١) وقد أثبتت الدراسات أنه غالبًا ما يتم ارتكاب الجرائم الإلكترونية عن طريق استخدام أى من البرمجيات التالية:

- الفيروس Virus: تستعمل الفيروسات بغرض تدمـير المواقع الإلكترونية عبر نشرها، وتتميز بقدرتها الفائقة على الاختراق مهمـا كانـت الحماية الموجهة ضدها، إذ تتخذ شكل شفرات قادرة على التناسـخ وإلصاق نفسها بملفات الحواسب الأخرى، وتتميز هذه الشفرات بآثارها المدمرة، إذ بإمكانها إفراغ محتوى القرص المصاب أو حذف ملفات نظام التشغيل المهمة.
- حصـان طـروادة Trojan Horse: هذا البرنامج يظهر على أنه موجه لأغراض مفيدة فى حين يخفي وراءه وظائفه المدمرة، حيث يتمكن من فتح منافذ الحاسب المستهدف لإتاحة الفرصة للمخترق للسيطرة الكاملة عليه. وهذا البرنامج من الصعب اكتشافه، حيث يقوم بتدمير نفسه بمجرد إتمام مهمته.
- البـاب الخلفـى Back Door: هـذا الفيروس يستخدم للولـوج إلى برامج الحاسب دون حاجة للمرور عـبر الضوابط الأمنية المعتـادة، ولـه شفرات متعددة قادرة علـى الولوج أيضًا وتجاوز الإجراءات الروتينية، كمـا أن هذا البرنامج يقوم بمهامه في الخفاء دون القدرة على اكتشافه.
- برنامـج الـدودة: هذا النوع مـن البرمجيات لديه القـدرة على الانتقال داخل الشبكـة الواحدة دون تدخـل الإنسان، وتتميز الدودة بسرعتها فى الانتشار والتكاثر داخل الشبكة المحلية للإنترنت فى زمن قياسى، وذلك باستخدام البريد الإلكترونى أو باستخدام فرات أمنية فى بعض أنظمة التشغيل.
- برمجيات الويب: تظهر هذه البرمجيات على شكل ملفات يتم تحميلها عبر مواقع الإنترنت، ومنها برمجيات جافاJava التى تتخذ قناع لتسهيل عملية الولوج إلى شبكة الإنترنت، وتهدف لإلحاق الضرر بأجهزة الحاسب.
- برمجيات الاختراق: يعتمد الاختراق على استغلال المنافذ المفتوحة بنظم التشغيل، والتى ترجع لأخطاء مادية بشرية، وذلك للبحـث عـن طريق الشبكات وكسر كلمات المرور واقتحام نظم تشغيل الشبـكات، وقد يتم الاختراق عن طريق تحميل ملفات التسجيل التى توجد بالمواقع الإلكترونية، أو من خلال مرفقات رسائل البريد.
- هجمات حجب الرؤية: يستعمل هذا البرنامج فى حالة فشل اختراق الحاسب، وذلك عن طريق إغراق الذاكرة المؤقتة، ويرمز لهـذا البرنامـج بـ «DOS» والذى يتطلـب حاسبًا واحدًا لتنفيذ الهجوم، وقد ظهر نظام جديـد من هذه الهجمات يطلق عليه «DOS D»أى هجمـات حجـب الخدمة الموزعة، وهذا الأخير يتطلب توزيعه على العديد من الحاسبات، ويتم وضع أداة خاصة بالهجـوم علـى العديد من الأنظمة عبر الإنترنـت، والتى تكون مرتبطة بوصلات سريعة يتم التحكـم فيها عبر أداة برمجية تعمل على توجيه جميع الحاسبات للهجوم، وقد تصل الهجمات إلى الآلاف، مما يُصعب مقاومتها .
- سرقة البيانات وانتحال الهوية الحاسوبية: يتم ذلك عند اختراق الأنظمة والحصول على نسخ من بيانات ذات طابع رسمى=

المطلب الثالث

أركان الجريمة الإلكترونية وأسبابها

لقد اتفقت معظم التشريعات فى العالم على ضرورة توافر ثلاثة أركان لقيام الجريمة، هـى: الشرعى، والمادى، والمعنوى؛ ذلك لأنهـا سلوك إرادى مصدره الإنسان. فالجريمة كأى سلـوك إنسانى لها جانبان، جانـب مادي خارجى نلمسه فى الكون المحيط، وجانب باطنى داخلى يعبر عن نفسية مرتكبها. هذان الجانبان ليسا سوى الركن المادى والركن المعنـوى، ومن ثَـمَّ لابد من توافرهمـا واجتماعهما معًا حتى تقـوم الجريمة، وتخلفهما أو تخلـف أحدهمـا يترتب عليه تخلـف الجريمة. أما الركن الشرعـى[1] سواء تمثل فى الصفـة غير المشروعة للفعل أو فى النص الشرعى المجرم، أى القاعدة الجنائية، فيعد ركنًـا فى الجريمة الإلكترونية؛ لأن الجريمة لا توجد أصلاً دون توافر القاعدة الجنائية التى تحدد الجريمة وترسم حدودها[2]. من ناحية أخرى، فالجريمة الإلكترونية، شأنها شـأن غيرها مـن الجرائم، يقف وراء مرتكبها أسباب ودوافـع وجهت سلوكه الإجرامى نحـو ارتكابها، هذه الأسباب تعد بمثابة القوة النفسية التـى تدفع الإرادة لارتكاب هذه الجريمة ابتغاء تحقيق غاية معينة. وعليه فسوف نقسم هذا المطلب إلى فرعين، نتناول فى الأول أركان الجريمة الإلكترونية، ونعالج فى الثانى أسباب هذه الجريمة.

= أو شخصـي وأخـذ نسخ منها والتلاعب بها وتغيير محتواها، الأمر الذي يؤدى إلى خرق الخصوصية، وكذا الاستيلاء على المعلومات الشخصية لأحد الأفراد عبر انتحال هويته الحاسوبية.

- راجـع: أمـين تجينى، الجرائم المعلوماتية، مجلة استشراف للدراسات والأبحاث القانونية، العدد ٦، المغرب، ٢٠٢٠، ص ١٢٠ وما بعدها.
- د. فريحـة محمد كـريم، الجريمة الإلكترونية، مجلة شئـون اجتماعية، جمعية الاجتماعيين فى الشارقـة، المجلد ٢٨، العدد ١١٠، الإمارات، ٢٠١١، ص ١٤٢ وما بعدها.

- Sylvette Guillemard, Le Droit International Privé face au contrat de vente cyberspatial, Thèse de Doctorat présentée en cotutelle à la Faculté des études supérieures de l›Université LAVAL-Québec, Janvier 2003, p. 22.

(١) تجـدر الإشـارة إلى أن الفقهـاء قد اختلقوا حول تحديد أركان الجريمة الإلكترونية، حيـث رأى بعضهم أن الجريمة تقوم على ركنين اثنين فقط هما الركن المادى والركن المعنوى، ويستبعد هذا الاتجاه الركن الشرعى على اعتبار أن الصفة غير المشروعة للفعـل تتجـدد على ضوء نموذج الجريمة، فهى العلاقـة بين الفعل المرتكب والوصف القانونـى، وبالتالي فهى تكشف عن وقوع الجريمة ولا تعتبر جزءًا فيها، ومن أنصار هذا الرأى الفقيه «ديكوك» والفقيه «جانديدى» حيث قررا أن النص القانونى ليس ركنًا من أركان الجريمة، وإنما هو عامل للردع فقط. فى حين ذهب الاتجاه الغالب فى الفقه إلى القول بأن الركن الشرعى يعد ركنًا أساسيًا فى الجريمة إلى جانب الركنين المادى والمعنوى، وفقًا لمبدأ «لا جريمة ولا عقوبة إلا بنص».

راجع: حشيفة عبد الهادى، التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، مرجع سابق، ص ١٨.

(٢) د. حسن بن أحمد الشهرى، قانون دولى موحد لمكافحة الجرائم الإلكترونية، مرجع سابق، ص ١٦.

الفرع الأول

أركان الجريمة الإلكترونية

سبقت الإشارة إلى أن الجريمة الإلكترونية، شأنها شأن غيرها من الجرائم، تتطلب توافر ثلاثة أركان لقيامها، وهي:

أولًا- الركن الشرعى:

ويعنـى هـذا الركـن أن الفعل أو الامتناع عـن الإتيان بالفعل لا يعتـبر جريمة إلا إذا كان هنـاك نص قانونى يجرم هـذا الفعل ويعاقب عليه، وهـذا تطبيقًا لمبدأ «لا جريمة ولا عقوبـة إلا بنصـ». ومن مقتضيات سيـادة النظام وشرعية الجرائـم والعقوبات أن يطبـق النظام العقابى على الأفعـال المحظورة التى تُرتكب فى ظله، والقاعدة العامة أن النصوص الجنائية لا تسري على الوقائع السابقة على صدورها، أو العلم بها بعد نشرها فـى الجريدة الرسميـة، وأن سلطة الدولة فـى التجريم والعقاب تشمـل إقليمها البري والبحـرى والجوى؛ لأنها تمارس حـق السيادة عليه. وتكمن مشكلة الجريمة الإلكترونية فـى السريـان المكانـى لأنها تكون فى أغلـب الأحيان عابـرة للحدود، أما فـى السريان الزمانـى فإنها تواجه مشكلة التطور السريع، الأمر الـذي يؤدى إلى وجود صعوبة بالغة فى مواكبة التشريعات لهذه الجريمة[١].

ثانيًا- الركن المادى:

الركـن المادى لأية جريمة هو مظهرهـا الخارجى المتمثل فى نشاط الفاعل الإيجابى أو امتناعـه السلبي، وما يترتب علـى ذلك من نتيجة، وقيام علاقة السببية بين النشاط الإجرامـى والنتيجة. والنشاط المادى فـى الجريمة الإلكترونية يتطلب وجود بيئة رقمية واتصـال بالإنترنـت، ومعرفة هدف هذا النشـاط وأسلوبه ونتائجـه، كأن يقوم مرتكب الجريمة بتشغيل الحاسب ووصله بالإنترنت، وإعداد برامج لاختراق الأجهزة المستهدفة، أو إعداد وضخ فيروسات مدمرة بهدف الإضرار بهذه الأجهزة، كما أنه يتعلق بالإتلاف الجزئى أو الكلى للجانب المادى من نظم المعلومات الذي يفقده القدرة على تأدية أعمال المنظمة، ومن ثَمَّ لا يحقق المنفعة التى أوجد من أجلها هذا النظام الإلكترونى[٢].

---

(١) د. سامى يس خالد، الجهود الدولية لمكافحة الجرائم المعلوماتية، مرجع سابق، ص ١٢-١٣.

(٢) د. هدى قشقوش، جرائم الحاسب الآلى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٨.

بيد أن طبيعة الركن المادى فى الجريمة الإلكترونية قد أثار بعض المشكلات العملية، ذلك أن مناط التجريم ينصب على نظام إلكترونى يُساء استعماله أو يتم اقتحامه على نحو غير مشروع، وما يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر فى صورة تدمير للمعلومات، وهذا ما أثار التساؤل عن مدى إمكانية إثبات السرقة عن طريق إساءة استعمال بطاقات الائتمان، أو شبهة التزوير عن طريق التلاعب فى بيانات الحاسب الآلى. كما أثارت النتيجة الإجرامية فى الجريمة الإلكترونية مشاكل عدة، فعلى سبيل المثال مشكلة مكان وزمان تحقيق النتيجة الإجرامية، فلو قام شخص مقيم فى البرازيل باختراق جهاز خادم Server أحد البنوك فى الإمارات، وكان هذا الخادم موجود فى الصين، فكيف يمكن تحديد وقت ارتكاب الجريمة، هل هو توقيت بلد إقامة المجرم، أم توقيت بلد البنك محل الاختراق، أم توقيت بلد الجهاز الخادم. فضلاً عن ذلك، تثور إشكالية القانون الواجب التطبيق، نظرًا لوجود بُعد دولى فى هذه الحالة[1].

ولمعالجة هذه الإشكاليات وغيرها من المسائل المستحدثة، يتعين على الدول السعى نحو إبرام اتفاقيات جماعية أو متعددة الأطراف بشأن مكافحة الجرائم الإلكترونية، تتضمن نصوصًا لمعالجة تلك الإشكاليات، مع إفساح المجال أمام إبرام بروتوكولات أو ملاحق لهذه الاتفاقيات تنطوى على نصوص قانونية تواكب التطورات المتلاحقة فى تقنيات الجرائم الإلكترونية.

ثالثًا- الركن المعنوى:

ليست الجريمة ظاهرة مادية خالصة قوامها الفعل وآثاره، ولكنها كذلك كيان نفسي، ومن ثَمَّ استقر فى القانون الجنائى الحديث ذلك المبدأ الذي يقضى بأن ماديات الجريمة لا تنشئ مسئولية ولا تستوجب عقابًا ما لم تتوافر إلى جانبها العناصر النفسية التى يتطلبها كيان الجريمة. وتجتمع هذه العناصر فى ركن يختص بها ويحمل اسم «الركن المعنوى للجريمة»، ويتمثل هذا الركن فى العلاقة التى تربط بين ماديات الجريمة وشخصية الجانى مرتكبها، وهذه العلاقة هى محل الإذناب فى معنى استحقاق العقاب، ومن ثَمَّ يوجه إليها لوم القانون وعقابه[2].

(١) عبد الله دغش العجمى، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير مقدمة لجامعة الشرق الأوسط، عمان، ٢٠١٤، ص ٢٦-٢٧.

(٢) د. محمود نجيب حسنى، النظرية العامة للقصد الجنائى، دراسة تأصيلية مقارنة للركن المعنوى فى الجرائم العمدية، دار النهضة العربية، القاهرة، ١٩٨٨، ص ٩٠.

ويتطلـب الركـن المعنوى فـى الجريمة الإلكترونيـة وجود قصد جنائـى وإرادة حرة وواعيـة للولوج فى الشبكة المعلوماتية وإحداث أضرار، أو الولوج بقصد السرقة وتدمير البيانات، وغيرها من الجرائم، كالاعتداء على المعلومات الخاصة بالمنظمات الحكومية أو الخاصة أو المملوكة للأفراد بقصد إتلافها كليًّا أو جزئيًّا، أو تقليل منفعتها؛ مما يؤدى إلى إلحـاق الضـرر بمالكى هذه المعلومـات. وتعد مثل هذه الجرائـم من قبيل الجرائم العمديـة فى حالـة تحقق عنصرى العلـم بملكيتها للغير واتجـاه الإرادة نحو تدميرها، الأمر الذي يؤثر سلبيًّا على ممارسة المنظمة لأنشطتها جزئيًّا أو كليًّا[١].

من ناحية أخرى، ذهب جانب من الفقه إلى القول بضرورة التمييز بين جريمة الدخول غـير المشروع على نظام المعالجـة الآلية للبيانات، وبين جريمة تجـاوز الصلاحيات فى الدخول على مثل هذا النظام. ففى جريمة تجاوز صلاحيات الدخول، يلزم لتوافرها أن يكون هناك صلاحية للشخص للدخول على نظام ما، على أن تتوافر داخل هذا النظام أنظمـة معينـة أخرى ليس من حق هـذا الشخص الدخول عليها. وفـى هذه الحالة تعد جريمـة تجاوز صلاحيات الدخول من قبيل الجرائـم التى لا تتطلب توافر ركن معنوي. وهـذا ما حدا بالمشرع الأمريكى إلى التنقل فى تحديد الركن المعنوى للجريمة بين مبدأ الإرادة ومبـدأ العلـم. فهو تارة يستخـدم الإرادة كما هو الشأن فـى القانون الفيدرالى الأمريكـى المتعلـق بالعلامات التجارية، وأحيانًا أخرى يأخـذ بمبدأ العلم فقط، كما هو الحال فى قانون مكافحة الاستنساخ الأمريكى[٢].

---

(١) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت؛ الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١، ص ٣٦.

(٢) لقـد ظهـر ذلـك جليًا فى قضية «موريس» الذى كان متهمًا فى قضية دخول غـير مصرح به على جهاز حاسب فيدرالى، ودفع محاميه بانتفاء الركن المعنوى، الأمر الذى حدا بالمحكمة إلى التعليق بقولها «هل يلزم أن الإدعاء بإثبات القصد الجنائى فى جريمـة الدخـول غير المصرح به، بحيـث تثبت نية المتهم فى الولوج إلى حاسب فيدرالى، ثم يلـزم إثبات نية المتهم فى تحدى الحظـر الوارد علـى استخدام نظم المعلومـات وتحقيق خسائر، فمثل هذا الأمـر يستدعى التوصـل إلى تحديد أركان جريمة الدخـول بدون تصريح». وبذلك ذهبت المحكمـة إلى تبنى معيارين هما: إرادة الدخول غير المصرح به، والعلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح.

بينما تبنى القضاء الفرنسى فكرة سوء النية فى غالبية الجرائم الإلكترونية، حيث اشترط المشرع الفرنسى وجود سوء نية فى الاعتـداء على بريد إلكترونى خاص بأحـد الأشخاص. كما أقر بضرورة توافر الركن المعنوى فى جرائم الإنترنت، ومثال ذلك اشتراط توافر الركن المعنوى فى حالة قيام أحد القراصنة بنسخ برامج كمبيوتر من أحد مواقع الإنترنت، وقيامه بفك شفرة الموقع وتخريبه للحصول على البرمجيات وإيقاع الأذى بالشركة صاحبة الموقع.

راجع: د. سامى يس خالد، الجهود الدولية لمكافحة الجرائم المعلوماتية، مرجع سابق، ص ١٤.

الفرع الثانى

أسباب الجريمة الإلكترونية

مما لا شك فيه أن مرتكبى الجرائم الإلكترونية يختلفون عن مرتكبى الجرائم التقليدية، ويرجع ذلك لاختلاف الأشخاص من حيث السن والجنس والمستوى العلمى، وغير ذلك من المؤثرات الخارجية، كما أن الأسباب أو الدوافع التى تدفعهم لارتكاب الجريمة هى أيضًا تختلف، فهى القوة النفسية التى تدفع الإرادة لارتكاب الجريمة ابتغاء تحقيق غاية معينة. ومن الصعوبة بمكان حصر كافة أسباب ودوافع الجريمة الإلكترونية، **ولعل من أبرز هذه الأسباب ما يأتي:**

١- **التحول الرقمى:** يتميز عصر المعلومات بالعديد من السمات التى من أبرزها اتجاه المجتمع الدولى نحو التحول الرقمي فى شتى شئونه الحياتية، فضلاً عن الزيادة المضطردة فى مقدار المعلومات المتدفقة ونوعيتها، فبفعل تكنولوجيا الاتصالات باتت المعلومات والصور تغطي شتى أرجاء المعمورة بسرعة ودقة فائقة. وأصبح إرسال المعلومات لا يقتصر على الأشخاص، بل امتد إلى المعدات حيث توجه المعلومات القنابل والصواريخ أثناء الحروب. ففى الفضاء الافتراضى، تكونت التفاعلات الافتراضية والسلوكيات الافتراضية والشخصية الافتراضية، كل ذلك مهد الطريق أمام ارتكاب الجرائم الإلكترونية بكل سهولة ويسر[١].

فضلاً عن ذلك، فإن عدد غير قليل من الأشخاص يقضون جزءًا من حياتهم اليومية فى الفضاء الإلكترونى، ينشئون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية، كل هذه الأنشطة خلقت بيئة مواتية لارتكاب ثمة جرائم إلكترونية، خاصة مع ضعف أنظمة تأمين الشبكة المعلوماتية[٢].

٢- **الرغبة فى الاستيلاء على المعلومات:** إن أولئك الذين يرتكبون الجرائم الإلكترونية

---

(١) د. ذياب موسى البداينة، الجرائم الإلكترونية: المفهوم والأسباب، ورقة عمل مقدمة للملتقى العلمى بشأن الجرائم المستحدثة فى ظل المتغيرات والتحولات الإقليمية والدولية، عمان، سبتمبر ٢٠١٤، ص ١٥.

(2) Eric R. Leukfeldt R., S. Veenstra, and Wouter Stol, High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands, International Journal of Cyber Criminology (I.J.C.C.), No. 7 (1), January 2013, pp. 1 et seq.

يُقدمـون على ذلك بغيـة الحصول على الجديد مـن المعلومـات، فالقراصنة Hackers غالبًـا ما يبررون أفعالهم بأن جميع المعلومات المفيدة يجب ألا تكون خاضعة لأية قيود، وأن تتـاح حرية نسخها وجعلهـا تتناسب مع استخدامات الأفراد، وكثـيرًا ما يعلنون أن هدفهم من الوصـول للمعلومات ودخولهم للشبكات والحواسيـب الإلكترونية هو التعلم فقط. ومع التطور التقنى سعى القراصنة للحصول على المعلومة ذاتها والاستيلاء عليها والتصـرف فيها، وذلك من خلال الدخول غير المصرح به على المعلومات المحفوظة فى الحاسـب الآلى أو المنقولة والاستيلاء عليها، أو تغييرهـا أو حذفها أو إلغائها نهائيًّا من النظـام. ويختلف الدافع لهذا التصرف، فقـد يكون دافعًـا تنافسيًا أو بغرض الابتزاز، أو من أجل الحصول على مزايا ومكاسب مادية، وكثيرًا ما يكون هدف هذه الجرائم ذا طابع سياسى أو اقتصادى[١].

٣- إلحـاق الأذى بأشخاصـ أو جهات: بعض المجرمين الذيـن يقدمون على ارتكاب الجريمـة عبر شبكـة المعلومات العالمية وتقنيـة المعلومات بصورة عامـة، يتركز الدافع مـن ورائها على إلحاق الأذى بأشخاص محدديـن أو جهات معينة، وغالبًا ما تكون تلك الجرائـم مباشرة تتمثل فى صورة ابتـزاز أو تهديد أو تشهير بالمجنى عليهم. وقد تكون هذه الجرائم غير مباشرة تتمثل فى الحصول على البيانات والمعلومات الخاصة ببعض الجهات أو الأشخاص لاستخدامها لاحقًا فى ارتكاب جرائم مباشرة[٢].

٤- تهديـد الأمـن القومـى والعسكرى: هنـاك ثمة جرائـم إلكترونيـة ذات أسباب ودوافـع سياسية تهـدف إلى تهديد الأمن القومى والعسكرى للدول، ومن ذلك ما يُعرف بالتجسس الإلكترونـى والإرهاب الإلكترونى والحرب المعلوماتية، وعادة ما يحدث ذلك بـين الدول المتقدمـة إلكترونيًّا، حيث تقوم الدولة بشن هجمـات إلكترونية على أهداف عسكريـة أو استراتيجيـة للدولة أو الدول المعادية بغية تكبيدهـا أكبر قدر من الخسائر

(١) سعيـد بن سالم البـادى وآخرون، الجريمة الإلكترونية فـى المجتمع الخليجى وكيفية مواجهتها، مجمـع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، ٢٠١٦، ص ٢٨.

(٢) فى قضية تم ضبطها بإمارة دبى بالإمارات العربية المتحدة، أقدم الجانى الملقب بـ «قرصان صور الفتيات» فيها بالسطو على البريـد الإلكترونـى لمجموعة من الفتيات بتلك الإمـارة، والاستيلاء غير المشروع على صورهـن الشخصية وتعمد نشرها على موقع خاص بشبكة الإنترنت مع مجموعة من الصور الإباحية.

راجع: سعيد بن سالم البادى وآخرون، الجريمة الإلكترونية فى المجتمع الخليجى وكيفية مواجهتها، مرجع سابق، ص ٢٩.

دون الانخراط فى حرب تقليدية مباشرة، إذ إن هذه الحروب الإلكترونية أقل تكلفة من الحروب العسكرية، فضلاً عن صعوبة الكشف عن هوية الدولة مرتكبة هذا النوع من الحروب[١].

٥- **قهر النظام المعلوماتى وإثبات التفوق:** فى بعض الأحيان يكون الدافع وراء ارتكاب الجرائم الإلكترونية هو قهر النظام المعلوماتى وإثبات قدرة الجانى وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة، حيث يمضى الجانى جل وقته أمام شاشات أجهزته لكسر الحواجز الأمنية للأنظمة الإلكترونية واختراقها، ليثبت براعته فى القدرة على تحدي أي تطور جديد فى عالم التقنية والتكنولوجيا. ويرتفع معدل ارتكاب هذه الجرائم لدى فئات صغار السن[٢].

٦- **ضعف إنفاذ القانون فى الجريمة الإلكترونية:** هناك العديد من الدول التى لم تطور تشريعاتها وأجهزة العدالة لديها لكى تتمكن من مجاراة التطور الهائل فى الجرائم الإلكترونية وأساليبها، وتتعامل مع الأدلة الرقمية على المستوى الوطنى. فالجرائم الإلكترونية تزدهر فى ظل غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية فى ملاحقة هذه الجرائم، وجلب مرتكبيها خلف القضبان وتقديمهم للعدالة[٣].

---

(١) فى ١٥ فبراير ٢٠٢٢، وقبيل غزو روسيا لأوكرنيا بعدة أيام، أعلنت السلطات الأوكرانية عن تعرّض مواقع وزارة الدفاع ومصرفين حكوميين لهجوم إلكتروني. وجاء الإعلان الصادر عن هيئة رقابة الاتصالات الأوكرانية في وقت يخيّم القلق على البلاد من احتمال تعرّضها لهجوم عسكرى تشنه روسيا التى تجرى تدريبات عسكرية واسعة عند حدودها. وطال الهجوم موقعى مصرف الادخار الحكومى «أوشاد بنك» و«بريفات ٢٤»، وهما من أكبر مؤسسات الدولة المالية، الأمر الذى تسبب فى إحداث أضرار بالغة بهذه المؤسسات. كما ظهرت رسالة على موقع وزارة الدفاع تشير إلى أنه معطّل ويخضع لصيانة تقنية. وأفادت هيئة رقابة الاتصالات أن «بريفات٢٤» تعرّض لهجوم ضخم يقوم على حجب الخدمة. وأضافت فى إشارة إلى روسيا «لا يمكن استبعاد أن الجهة المعتدية تلجأ إلى حيل غير مشروعة».
راجع: استهداف موقع وزارة الدفاع الأوكرانية بهجوم إلكتروني جديد، على الرابط التالى:
- https://www.dw.com/ar/%D8%A7%D8%B3%D8%AA%D9%87%D8%AF%D8%A7%D9%81-%D9%85%D9%88%D9%82%D8%AF

(٢) سعيد بن سالم البادى وآخرون، الجريمة الإلكترونية فى المجتمع الخليجى وكيفية مواجهتها، مرجع سابق، ص٢٨-٢٩.

(٣) د. ذياب موسى البداينة، الجرائم الإلكترونية: المفهوم والأسباب، مرجع سابق، ص ١٥.

المبحث الثانى

الجهود الدولية المبذولة لمواجهة الجرائم الإلكترونية

سبقت الإشـارة إلى أن الجريمة الإلكترونية تعد نشاطًا إجراميًّا تُستخدم فيه تقنية الحاسـب الآلى وشبكـة الإنترنـت بطريقة مباشرة أو غـير مباشـرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامى المقصود، وبسبب الطبيعة الخاصة بمعطيات الحاسب الآلى من حيـث كونها غـير مادية، وبفعل ما أثاره التطبيق القضائـى لنصوص القوانين الجنائية على جرائم الحاسب من مشكلات، ولضمان عدم إفلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن الانطباق على مثل هذه الجرائم المستحدثة، وصونًا لمبدأ الشرعية الـذي يقضى بأنه «لا جريمة ولا عقوبـة إلا بنص»، وفى ظل مبدأ حظر القياس بالنسبة للنصوص الجنائية الموضوعية. لكل هذه الأسبـاب ولمواجهة الخطر المحدق والخسائر الفادحة التى تسببها الجرائـم الإلكترونية، سنت العديد من دول العالم قوانين جنائية خاصة أو عدلت قوانين العقوبات لديها، بما يكفل مواجهة هذه الجرائم[1].

بيـد أن الدول قد واجهت العديـد من الصعوبات فى مكافحـة الجريمة الإلكترونية عبر قوانينهـا الداخلية، وفى مواجهة أصعب خاصية لها كونها جريمة متعدية الحدود. ونظرًا للانتشار الواسع للأضرار الناجمة عن الجرائم الإلكترونية، لم يعد بوسع الدول منفـردة أن تواجههـا مهما كانت إمكانياتهـا، وكان من الضرورى توحيـد جهود الدول لمواجهـة هذا النوع من الإجرام، وذلك من أجل الوصول إلى مفاهيم موحدة للمكافحة، وإعـداد مشروعـات القوانين التـى تسير على هديهـا، والاستفادة من تجـارب بعضها البعض فى هذا الشأن، وعقد اتفاقيات دولية لمواجهة هذه الظاهرة.

كما بُذلت العديد من الجهود الدولية لمواجهة الجرائم الإلكترونية فى إطار المنظمات الدولية، خاصة فى إطـار منظمة الأمم المتحدة، وغيرها من المنظمات الإقليمية، حيث تبنـت تلك المنظمـات عقد مؤتمـرات وإبـرام اتفاقيات دوليـة لمكافحة هـذه الظاهرة الإجرامية. ولعل من أهم الاتفاقيات التى تناولت الجرائم الإلكترونية اتفاقية بودابست لعـام ٢٠٠١ المنبثقـة عـن اتفاقيات المجلـس الأوروبـى، والاتفاقية العربيـة المتمثلة فى القانون العربى الاسترشادى لمكافحة جرائم تقنية المعلومات وما فى حكمها لعام ٢٠٠٤.

---

(١) محمـود محمد شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مجلة البحوث القانونية والاقتصادية، الصادرة عن كلية الحقوق – جامعة المنوفية، المجلد ٥٤، العدد ٣، أكتوبر ٢٠٢١، ص ٥٢٧.

ولدراسة الجهود الدولية المبذولة لمواجهة الجرائم الإلكترونية سنقسم هذا المبحث إلى مطلبين، نتناول فى الأول جهود المنظمات الدولية لمواجهة الجرائم الإلكترونية، ونعالج فى الثانى جهود المنظمات الإقليمية لمواجهة الجرائم الإلكترونية.

المطلب الأول

جهود المنظمات الدولية لمواجهة الجرائم الإلكترونية

إزاء عجز الدول منفردة عن مواجهة الجرائم الإلكترونية، بات من الضرورى تضافر الجهود الدولية لمكافحة هذه الجرائم التى انتشرت بسرعة هائلة فى الآونة الأخيرة، وأصبحت تشكل تهديدًا حقيقيًّا لمعظم دول العالم، الأمر الذي حدا بالأمم المتحدة وغيرها من المنظمات الدولية إلى بذل جهود مكثفة للتصدى لهذه الجرائم. وقد كان لمنظمة الأمم المتحدة ومجموعة الثمانية دورًا بارزًا فى مواجهة تلك الجرائم. وعليه فسوف نقسم هذا المطلب إلى ثلاثة فروع، نتناول فيها تباعًا دور الأمم المتحدة، والمنظمة العالمية للملكية الفكرية، ومجموعة الثمانية (G-٨) فى مواجهة هذه الجرائم.

الفرع الأول

دور الأمم المتحدة فى مواجهة الجرائم الإلكترونية

تبذل الأمم المتحدة جهودًا حثيثة لمواجهة الجرائم الإلكترونية، وتؤكد دومًا على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشارها وتعاظم آثارها، وذلك من خلال متابعتها وإشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين[١]، وإصدار العديد من القرارات والتوصيات المتعلقة بمجابهة الجرائم الإلكترونية. وسوف نتعرض بإيجاز لأهم المؤتمرات الدولية، وقرارات الجمعية العامة للأمم المتحدة ذات الصلة بمكافحة الجرائم الإلكترونية.

---

(١) فى عام ١٩٨٣ أجرت منظمة التعاون والإنماء الاقتصادى دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية وسوء استخدام الحاسب الآلى. وفى ميلانو عام ١٩٨٥ انعقد المؤتمر السابع لمنع الجريمة ومعاملة المجرمين، وتم تكليف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلى، وإعداد تقرير بذلك لعرضه على المؤتمر الثامن للأمم المتحدة المنعقد فى كوريا الجنوبية عام ١٩٩٠، والذى خرج بعدد من النتائج منها ضرورة الاستفادة من التطورات العلمية والتكنولوجية فى مواجهة الجريمة الإلكترونية، وتدريب القضاة والمسئولين على كيفية التحقيق والمحاكمة فيها، وكذلك التعاون مع المنظمات المهتمة بهذا الشأن.
راجع: د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، الصادرة عن كلية الحقوق – جامعة عجمان، المجلد ٤، العدد ٨، يوليو ٢٠١٨، ص ١٨٩.

أولًا - المؤتمرات الدولية:

ظلـت مؤتمـرات الأمم المتحدة لمنـع الجريمة ومعاملـة المجرمين تنعقـد كل خمس سنـوات منذ عـام ١٩٥٥، بعد أن حلَّت الجمعيـة العامة للأمم المتحـدة اللجنة الدولية للعقوبـة والإصلاح في عام ١٩٥٠ [١]. ومنـذ عام ٢٠٠٥، أصبحت تلك المؤتمرات تنعقد تحـت مسمى مؤتمر الأمم المتحـدة لمنع الجريمة والعدالة الجنائيـة، وقد عقدت الأمم المتحدة حتى الآن ١٤ مؤتمرًا دوليًّا لمنع الجريمة ومعاملة المجرمين (العدالة الجنائية)، وكان المؤتمر الأول قد انعقد فى جنيف عام ١٩٥٥، غير أن موضوع الجريمة الإلكترونية ناقشتـه الأمم المتحدة لأول مرة فـى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين عام ٢٠٠٠. وسوف نتعرض بإيجاز لأهم هذه المؤتمرات:

١- مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين عام ٢٠٠٠:

انعقـد هـذا المؤتمر فـى فيينا فى الفـترة مـن ١٠ إلى ١٧ أبريـل ٢٠٠٠، ومن أبرز الموضوعات التى ناقشها التعاون الدولى فى مكافحة الجريمة المنظمة عبر الوطنية. وقد صدر إعلان المؤتمر متضمنًا لأول مرة تأكيدًا للحاجة إلى التصدى للموجة المتزايدة من الجرائـم الإلكترونيـة، حيث أكد البند «١٨» من الإعلان علـى ضرورة صياغة توصيات ذات توجـه عملى بشأن منع ومكافحة الجرائم المتعلقة بالحواسب الآلية. كما دعا لجنة منـع الجريمة والعدالة الجنائية إلى الاضطلاع بعمل ما يلزم فى هذا الشأن، آخذة فى الاعتبـار الأعمال الجارية فى محافل أخرى. وأكد على ضرورة التزام الأطراف بالعمل علـى تعزيـز قدراتها على منع الجريمـة المرتبطـة بالتكنولوجيا المتقدمـة والحواسب، والتحرى عن تلك الجرائم وملاحقتها [٢].

(1) The General Assembly dissolved the International Penal and Penitentiary Commission (IPPC) on 1 December 1950, while incorporating its functions and archives within the new Organization›s own operations (see General Assembly resolution 415(V) of 1 December 1950).

(2) «We decide to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime».
See: Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, United Nations, A/CONF.187/15, Vienna, 10-17 April 2000, pp. 2-3. On the following Website: file:///C:/Users/NEW%20VISION/Downloads /A_CONF.187_15-EN.pdf

٢- مؤتمر الأمم المتحدة الثانى عشر لمنع الجريمة والعدالة الجنائية عام ٢٠١٠:

انعقد هذا المؤتمر فى سلفادور، البرازيل فى الفترة من ١٢- ١٩ أبريل ٢٠١٠، تحت عنوان «الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها فى عالم متغير». وقد أكد المؤتمر على أن تطور تكنولوجيا المعلومات والاتصالات وزيادة استخدام الإنترنت يهيئان فرصًا جديد أمام المجرمين وييسران نمو الجريمة. وطلب إلى الدول الأعضاء أن تقوم ببناء وتحسين قدرات سلطاتها الوطنية، وتعزيز الخبرات الفنية المتخصصة القادرة على مجابهة الجرائم السيبرانية. وأوصى بأن يقوم مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، بالتعاون مع الدول الأعضاء والمنظمات الدولية المعنية والقطاع الخاص، بتقديم المساعدة التقنية إلى الدول، التى تطلب ذلك، من أجل وضع تشريعات وطنية فعالة لمكافحة الجرائم الإلكترونية، وتدعيم قدراتها على الكشف عن هذه الجرائم والتحقيق فيها وملاحقتها قضائيًّا، ومقاضاة مرتكبيها، بما يشمل الهجمات الإجرامية على نظم البنية التحتية، والجرائم التقليدية التى تُرتكب باستخدام الفضاء السيبرانى، أو بإساءة استخدام الصور الملتقطة بواسطة الأقمار الاصطناعية[١].

٣- مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية عام ٢٠١٥:

انعقد هذا المؤتمر فى العاصمة القطرية «الدوحة» فى الفترة من ١٢ إلى ١٩ أبريل ٢٠١٥، ومن أبرز الموضوعات التى ناقشها هو إدماج منع الجريمة والعدالة الجنائية فى جدول أعمال الأمم المتحدة الأوسع من أجل التصدى للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطنى والدولى ومشاركة الجمهور. وقد أكد المؤتمرون على ضرورة استكشاف تدابير خاصة تهدف إلى توفير بيئة سيبرانية آمنة، والعمل على منع ومكافحة الأنشطة الإجرامية التى يتم تنفيذها عبر الإنترنت، مع إيلاء اهتمام خاص لسرقة الهوية والتجنيد لغرض الاتجار بالأشخاص، وحماية الأطفال من الاستغلال عبر الإنترنت، وتوطيد التعاون بين أجهزة إنفاذ القانون على الصعيدين الوطنى والدولى؛ بغرض التعرف على الضحايا وحمايتهم من خلال إزالة المواد الإباحية المتعلقة بالأطفال من شبكة الإنترنت، وخصوصًا صور التعدى الجنسى على الأطفال.

---

(١) راجع: مشروع إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها فى عالم متغير، مؤتمر الأمم المتحدة الثانى عشر لمنع الجريمة والعدالة الجنائية، سلفادور – البرازيل، ١٢-١٩ أبريل ٢٠١٠، وثيقة رقم A/CONF.٢١٣/٦.L/١.Rev، ص ١٤-١٥.

وأوصـى المؤتمر الدول الأطراف بضرورة العمـل على تعزيز أمن شبكات المعلومات والحاسبـات، وصـون سلامة البنى التحتيـة ذات الصلة، والسعـى إلى تقديم مساعدة تقنيـة طويلة الأمد، وخدمات لبنـاء قدرات السلطات الوطنية مـن أجل تدعيم قدرتها علـى التصدى للجرائم الإلكترونية، بما فى ذلـك منع كل أشكال تلك الجرائم وكشفها والتحـرى عنها وملاحقـة مرتكبيها. ودعا لجنة منـع الجريمة والعدالـة الجنائية إلى النظـر فى إصـدار توصية بأن يواصل فريـق الخبراء تبادل المعلومات عـن التشريعات الوطنيـة والممارسـات المُثلى والمساعـدة التقنية والتعاون الدولى، بغية دراسة الخيارات المتاحـة لتدعيم التدابـير القانونية أو غـير القانونية المتخذة علـى الصعيدين الوطنى والدولى لمواجهة الجرائم الإلكترونية، واقتراح تدابير جديدة لهذا الغرض[1].

ثانيًا- قرارات الجمعية العامة:

دأبـت الجمعيـة العامة لـلأمم المتحـدة على إصـدار قـرارات تتعلـق بالموضوعات والمسائـل محـل الاهتمام العالمى، وبالرغـم من أن غالبية قراراتها غـير ملزمة إلا أنها تحظى باحترام دولى والتزام أدبي. وإزاء تزايد وانتشار الجرائم الإلكترونية، أصدرت الجمعية العامة للأمم المتحدة العديد من القرارات المتعلقة بمواجهة مثل هذه الجرائم وملاحقة مرتكبيها، **ولعل من أهم هذه القرارات ما يأتي:**

١- قرار الجمعية العامة رقم ٦٣/٥٥:

فـى ٤ ديسمبر ٢٠٠٠، اعتمدت الجمعية العامة للأمم المتحدة، فى دورتها الخامسة والخمسـون، قـرارًا بشـأن مكافحـة إساءة استعمـال تكنولوجيـا المعلومـات لأغراض إجراميـة، حددت فيه مجموعة من التدابير الراميـة إلى مكافحة هذا النوع من إساءة الاستعمال، من بينها ما يأتي:

- ينبغـى على الـدول أن تكفل عدم جعـل قوانينها وممارساتها مـلاذًا آمنًا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية.
- ينبغى أن تتسق جميع الدول المعنية التعاون فى مجال إنفاذ القانون لدى التحقيق

(1) Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Draft Doha Declaration on integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation, A/CONF.222/L.6, Doha, 12-19 April 2015, p. 10.

والمقاضاة فى القضايا الدولية المتعلقة بإساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية.

- ينبغى أن تتبادل الدول المعلومات المتعلقة بالمشاكل التى تواجهها فى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.
- ينبغى تدريب العاملين فى مجال إنفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.
- ينبغى أن تحمى النظم القانونية سرية البيانات ونظم الحواسيب وسلامتها وتوافرها، من أى عرقلة غير مصرح بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية.

الوقت المناسب.

ودعا القرارُ الدولَ إلى أخذ التدابير المذكورة أعلاه فى الاعتبار فى جهودها الرامية إلى مكافحة الجرائم الإلكترونية على الصعيدين الوطنى والدولى، بما فى ذلك سن تشريعات وطنية للقضاء على أي ملاذات آمنة لإساءة استعمال التكنولوجيا لأغراض إجرامية، والعمل على تنمية قدرات أجهزة إنفاذ القانون المنوط بها ملاحقة وضبط مرتكبى الجرائم الإلكترونية، وتعزيز أمن البيانات والأنظمة المعلوماتية، وإنشاء أنظمة للتعاون الدولى والمساعدة المتبادلة، ونشر الوعى العام بالمخاطر التى تسببها هذه الجرائم[1].

٢- قرار الجمعية العامة رقم ١٢١/٥٦:

فى ١٩ ديسمبر ٢٠٠١، اعتمدت الجمعية العامة للأمم المتحدة، فى دورتها السادسة والخمسين، بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وأشار القرار إلى الجهود الدولية القائمة فى مكافحة الجريمة السيبرانية، وسلط الضوء على العمل الذي تضطلع به المنظمات الدولية والإقليمية فى مجال مكافحة الجريمة المتصلة بالتكنولوجيا المتقدمة، بما فى ذلك ما يضطلع به مجلس أوروبا

(١) راجع: قرار الجمعية العامة للأمم المتحدة رقم ٦٣/٥٥ بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وثيقة رقم ٦٣/٥٥/A/RES ، على الرابط التالى:
- https://www.unodc.org/pdf/crime/a_res_55/res5563a.pdf

مـن أعمال لوضع اتفاقيـة بشأن جرائم الفضـاء السيبرانى، فضلاً عمَّـا تقوم به هذه المنظمـات من تشجيع للحوار بين الحكومات والقطاع الخاص بشأن السلامة والثقة فى الفضاء السيبرانى.

وأكـد القرار على ضرورة التعاون بين الـدول فى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجراميـة، ودعا الدول الأعضاء إلى مراعاة التوجيهات المقدمة من لجنة منع الجريمة والعدالـة الجنائية عند وضع التشريعات والسياسات الوطنية، **ومن أهم هذه التوجيهات ما يأتي:**

- يتعـين علـى الـدول الأعضاء عنـد وضـع قوانين وسياسـات وممارسـات وطنية لمكافحة إسـاءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وأن تأخذ فى اعتبارها عند الاقتضاء، أعمال وإنجازات لجنة منع الجريمة والعدالة الجنائية، والمنظمات الدولية والإقليمية الأخرى.
- التأكيد على أهمية التدابير الواردة فى قرار الجمعية العامة رقم ٦٣/٥٥، وتدعو الـدول الأعضاء مـن جديد إلى مراعاة هذه التدابير عند بـذل جهودها الرامية إلى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[١].

الفرع الثانى

دور المنظمة العالمية للملكية الفكرية فى مواجهة الجرائم الإلكترونية

بالرغـم من نشوء نظـام الملكية الفكرية فى أواخر القرن التاسـع عشر، فإن الإطار التنفيذى لقواعد الملكية الفكريـة ظل حتى ستينيات القرن العشرين محصورًا بمكاتب الملكيـة الفكريـة، مثل مكاتب براءات الاخـتراع، إلى أن نشأت المنظمـة العالمية للملكية الفكريـة(WIPO) World Intellectual Property Organization بموجـب اتفاقية تم التوقيـع عليها فى العاصمـة السويدية «استكهولم» فى ١٤ يوليـو ١٩٦٧، وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة لهيئة الأمم المتحدة فى ١٧ ديسمبر ١٩٧٤. وصـارت المنظمة العالميـة للملكية الفكرية هى الجهة الدولية الوحيـدة التى تدير سائر

(١) راجع: قرار الجمعية العامة للأمم المتحدة رقم ١٢١/٥٦ بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وثيقة رقم ١٢١/٥٦/A/RES ، على الرابط التالى:
- https://www.unodc.org/pdf/crime/a_res_56/121a.pdf

اتفاقيات الملكية الفكرية، والقوانين الإرشادية النموذجية التى تصدر عن فرق الخبراء فيها لمساعدة الدول النامية فى اتخاذ التدابير التشريعية لحماية الملكية الفكرية[١].

وحتى عام ١٩٩٥ لم يكن هناك ثمة إطار دولى يشارك أو ينازع المنظمة العالمية للملكية الفكرية فى إدارة نظام الملكية الفكرية، إلى أن دخلت اتفاقية منظمة التجارة العالمية(World Trade Organization (WTO حيز النفاذ فى الأول من يناير ١٩٩٥ [٢]، وبالتالى سريان الاتفاقيات الدولية المنظمة للتجارة الدولية، التى من بينها اتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية (تربس) Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) التى تضمنت قواعد تتصل بكافة فروع وأقسام الملكية الفكرية. ولتجنب احتمالات التنازع بين مركزى إدارة الملكية الفكرية، المنظمة العالمية للملكية الفكرية ومنظمة التجارة العالمية، فقد تم إبرام اتفاق تعاون بينهما فى ٢٢ ديسمبر ١٩٩٥ لتنظيم العلاقة بينهما فيما يتعلق بإدارة نظام الملكية الفكرية دوليًّا[٣].

وقد تبنت المنظمة العالمية للملكية الفكرية وضع نصوص تشريعية لحماية برامج الحاسب الإلكترونى، حيث عرفّت هذه البرامج بأنها «مجموعة تعليمات يمكنها إذا ما وضعت على ركيزة يستوعبها الجهاز، أن تحقق نتيجة ما بواسطة هذه الآلة القادرة على التعامل مع المعلومات». كما قامت بإعداد نصوص نموذجية بمعرفة عدد من الخبراء من شتى أنحاء العالم من أجل مساعدة الدول على استكمال تشريعاتها فى مجال حماية البرامج أو تنقيحها[٤]. وكان الهدف من هذه النصوص التى تم وضعها عام ١٩٧٨ هو تبنيها إما بواسطة تشريعات مستقلة أو فى إطار مراجعة تشريعية قائمة، مثل تشريعات حق المؤلف والتشريعات الأخرى التى تكفل حماية أسرار التجارة وتحظر المنافسة غير المشروعة، إذا كانت عاجزة بحالتها الراهنة عن تقرير هذه الحماية، وذلك من أجل توحيد قواعد الحماية فى جل الدول، حيث تكمن أهمية هذا التوحيد فى القضاء على

(١) محمود محمد شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مرجع سابق، ص٥٣٦-٥٣٧.

(٢) تم توقيع اتفاقية منظمة التجارة العالمية فى مراكش بالمغرب فى ١٥ أبريل ١٩٩٤.

(3) See: WTO-WIPO cooperation agreement, Agreement Between the World Intellectual Property Organization and the World Trade Organization. On the following Website:
- https://www.wto.org/english/tratop_e/trips_e/wtowip_e.htm

(٤) د. محمد حسام لطفى، الحجية القانونية لبرامج الحاسب الإلكترونى، دار النهضة العربية، القاهرة، ١٩٩٨، ص١٦١.

المشـكلات الناجمة عن نقل المعلومات عن بعد، فعادة ما يتواجد مستخدم الحاسب فى بلد ما فى حين يكون الحاسب محل الجريمة فى بلد آخر[١].

وفى المجال المعلوماتى، اهتمت المنظمة بتوفير الحماية القانونية للبرامج المعلوماتية وقواعـد البيانـات، فبعد أن استقر الـرأى لديها بعدم إمكانية توفـير الحماية لهما فى تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات الدولية وخاصة اتفاقيتـى «التربس» و«برن» اللتان حثتا الـدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف، ووضع عقوبات على كل أعمال من شأنها تزوير العلامات التجاريـة والقرصنـة المتعمدة والمرتكبـة فى إطار تجارى، وبالطبـع تعتبر الإنترنت من الأماكـن الخصبة لهذا النوع من التصرفات، والتى وفـرت بموجبها الحماية القانونية للبرامج وقواعد البيانات المعلوماتية[٢].

(١) وإزاء الصعوبـات التـى ثارت حول إثبات محل الجريمة، وضعت المنظمة تسع مواد نموذجية : المادة الأولى من هذه النصوص تبسط حمايتها على برامج الحاسب الإلكترونى، وعلى التقديمات الوصفية التفصيلية للبرامج ومستنداتها الملحقة المستهدفة لتبسيـط الفهـم، ويسرى وصف البرامج المحميـة طبقًا لهذه المادة على العناصر الثلاثة التاليـة: ١- البرنامج بمعناه الضيق. ٢- وصف البرنامج. ٣- المستندات الملحقة بالبرنامج.

إلا أن هذه الصياغة قد تعرضت للنقد، حيث تم وصفها بعدم المرونة، ورأى بعض الخبراء بضرورة استبدال هذا النص الضيق بنصـ واسـع خالٍ مـن أى تحديد لمحل الحمايـة. كما انتقد خبراء حق المؤلـف عند اجتماعهم بمدينـة كانبرا CANBERRA صياغة الفقرة الثالثة من النصوص النموذجية التى جاء نصها صريحًا فى حماية المستندات الملحقة بالبرنامج، ذلك أنه من المؤكد أن هذه المستندات تتمتع بحماية تشريعات حق المؤلف كسائر المصنفات المكتوبة.

راجع: محمود محمد شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مرجع سابق، ص ٥٣٨.

ولمزيد من التفاصيل، راجع: الجهود الدولية فى مواجهة جرائم الإنترنت، على الرابط التالى:
- https://www.startimes.com/?t=31163480

(٢) د. أمجـد حسـن مرشد الدعجة، استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجستير مقدمة لمعهد البحوث والدراسات الاستراتيجية – جامعة أم درمان الإسلامية، السودان، ٢٠١٤، ص ٥٦.

الفرع الثالث

دور مجموعة الثمانية (G-٨)

فى مواجهة الجرائم الإلكترونية

فـى عام ١٩٩٧، أنشأت مجموعة الـدول الثمانية (G-٨)[١] «اللجنة الفرعية المعنية بجرائـم التكنولوجيـا المتقدمة» التى تهتـم بمكافحة الجرائـم الإلكترونية، حيث تمثل الجرائـم التى تتم باستخدام أو ضد الكمبيوتر أهميـة خاصة لمجموعة الدول الثمانية؛ ذلـك لأن هـذه المجموعة تقوم على فكرة تبادل قادة هـذه الدول الرأى فى المسائل ذات الاهتمـام المشترك لبلـورة خطط عملية تسهم فى مكافحة كل ما مـن شأنه تهديد أمن واستقـرار الدول الأعضـاء. وقد اعتمد وزراء العدل والداخلية فـى مجموعة الثمانية، إبـان اجتماعهم فى مدينة واشنطن بالولايـات المتحدة فى ديسمبر ١٩٩٧ مجموعة من السياسات لمكافحة جرائم التكنولوجيا المتقدمة، **استنادًا إلى المبادئ التالية:**

- عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات.
- التنسيق بين جميع الدول المعنية فى ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر.
- تدريب الموظفين المكلفين بتنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية[٢].

وفـى قمة مجموعـة (G-٨) فى موسكو عـام ٢٠٠٦، ناقش وزراء العـدل والداخلية فـى المجموعة قضية الإرهـاب السيبرانى، وصدر بيان موسكو الذي تم فيه التأكيد على

---

(١) مجموعة الثمانية (G-٨) أو مجموعة الدول الصناعية الثمانية كانت منتدىً سياسيًا حكوميًا من عام ١٩٩٧ حتى عام ٢٠١٤، يضم الدول الصناعية الكبرى فى العالم وهى: الولايات المتحدة الأمريكية، اليابان، ألمانيا، روسيا الاتحادية ، إيطاليا، المملكة المتحـدة، فرنسـا، وكندا. وقـد تشكلت من دمج دولة روسيا فـي مجموعة السبع (G-٧) التى تكونت عـام ١٩٧٦، وعادت إلى اسمهـا السابـق (G-٧) بعـد أن تم تعليـق عضوية روسيا فـى عام ٢٠١٤ عقب احتلالهـا لشبه جزيرة القـرم. ويمثل مجموع اقتصـاد هذه الدول الثمانية ٦٥٪ من اقتصاد العـالم وأغلبية القوة العسكرية فى العالم. وتتضمن أنشطة المجموعة مؤتمرات على مدار السنة، ومراكز بحث سياسية تتجمع مخرجاتها فى القمة السنوية التى يحضرها قادة الدول الأعضاء.

راجع: مجموعة الثمانى، على الرابط الآتي:

- https://ar.wikipedia.org/wiki/%D9%85%D8%AC%D9%85%D9%88%D8%B9%D8%A9_%D8%A7%D9%84%D8%AB%D9%85%D8%A7%D9%86%D9%8A

(٢) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مرجع سابق، ص١٨٦.

أنــه «من الضرورى اتخــاذ مجموعة من التدابير لمنع الأعمــال الإجرامية المحتملة، بما فــى ذلك مجــال الاتصالات السلكيــة واللاسلكية، والعمــل ضد بيع البيانــات الخاصة والمعلومــات المزيفة وتطبيقات الفيروسات وبرامج الكمبيوتر الضارة الأخرى. وسنوجه خــبراء المجموعة لتعميم مناهج موحــدة لمكافحة الجريمة الإلكترونيــة، وسوف نحتاج للقواعد القانونية الدولية لهذا العمل، وسوف نطبق كل ذلك لمنع الإرهابيين من استخدام مواقــع الكمبيوتر والإنترنت لتوظيف الإرهابيين الجــدد، وتوظيف الجهات الفاعلة غير القانونية الأخرى»[١].

وفــى قمة مجموعة (G-٨) فى روما عــام ٢٠٠٩، ناقش وزراء العدل والداخلية عدة قضايا متعلقة بالجريمــة السيبرانية، وجاء فى البيان الختامى أنه ينبغى حجب المواقع الإباحيــة التــى يُستغــل فيها الأطفــال، بالاستنــاد إلى قوائم سوداء تحدثهــا وتنشرها منظمــات دولية. وفيمــا يخص الجريمة الجريمة السيبرانية سلــط البيان الضوء على ضــرورة التعــاون بين موردى الخدمات والجهــات المعنية بإنفاذ القانــون، وأنه لابد من تعزيــز أشكال التعاون القائمــة، مثل جهات الاتصال التابعة لمجموعــة الثمانية والمعنية بجرائم التقنيات العالية، والتى تعمل يوميًّا على مدار الساعة[٢].

هذا وقد اعتمدت مجموعة الثمانية (G-٨) مجموعة من التوصيات والمبادئ المتعلقة بمكافحة جرائم التكنولوجيا المتقدمة، **وهى:**

يتعــيّن على الــدول أن تُجرِّم الانتهــاكات على حقــوق الغير الشبكــة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي فيما يتعلّق بمكافحة هذه الانتهاكات.

(1)The participants expressed their intention to strengthen the instruments in the fight against cybercrime: «We discussed the necessity of improving effective countermeas-ures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmfull computer programs. We will instruct our experts to generate unified apptoaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and internet sites for hiring new terrorists and the recruitment of other illegal actors». See: www. G7.utoronto.ca/justice/justice2006.htm.

(2) We believe, in particular, that consideration should be given to aggressive measures such as the creation of a blacklist of sites containing child pornography, aimed at blocking navigation to paedophile sites and/or measures to increase the reporting of child pornography as appropriate in our various legal systems. The blacklist could be run by some international organizations.
See: G-8, Final Declaration, Rome, 30th May, 2009. On the following Website:
https://www.statewatch.org/media/documents/news/2009/jul/g8-jha-may-2009-declaration.pdf

ينبغـى على الدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:

- التعـاون مع القطاع الصناعى لضمـان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الإلكترونية للهجمات.
- سـن قوانين وتدابـير أخـرى، وتنفيذها لضمـان حماية ملائمة لحقـوق الملكية الفكرية ضد التزوير والقرصنة.
- تحديد المشاكل المحتملة ومعالجتها فى المستقبل، التى قد تنتج عن التطورات فى مجال تكنولوجيا المعلومات.
- نشر الوعي العام فيما يتعلق بموضوع الجريمة ذات التقنية العالية.
- يتعـين على الدول العمـل المستمر على اقتنـاء التكنولوجيـات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق والادعاء العام، من أجل ملاحقة المجرمـين الذين يستخدمـون تكنولوجيا الكمبيوتر لارتـكاب جرائمهم. ويتوجّب علـى الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.
- ينبغـي تحسـين التواصل بـين الموظفين المكلّفـين بتطبيق القوانـين فى مختلف الدول، بما فى ذلك تبادل الخبرات فى معالجة هذه المشاكل.
- يتعين على الدول الحفاظ على التوازن المناسب بين حماية الحق فى الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.
- علـى الـدول تشجيع وضع القوانين وتنفيذ تدابير لتوفـير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسى على الإنترنت.

علـى الـدول أن تتعـاون من أجـل التطوير المستمـر للمـوارد والتقنيـات والتدريب للمساعـدة فـى تطبيق القانون ومكافحـة الاستغلال الجنسى للأطفـال عبر الإنترنت. كمـا ينبغى العمل مع مقدمى خدمة الإنترنـت والمنظمات غير الحكومية لتطوير الطرق

التى يمكن أن تساعد هذه المنظمات من أجل تطبيق قوانين مكافحة الاستغلال الجنسى للأطفال على شبكة الإنترنت.

وأخـيرًا، على الـدول أن تشجّع التعاون فـى مجال تطويـر الاستراتيجيات المناسبة لرفـع الوعى العام فـى هذا الشأن، وكذلك التقييم المستمـر لبرامج المكافحة والوسائل القانونية المتبعة[١].

المطلب الثانى

جهود المنظمات الإقليمية لمواجهة الجرائم الإلكترونية

ممـا لا شك فيه أن معاهـدات الجرائـم الإلكترونية الثنائيـة والإقليمية والمتعددة الأطـراف تعد أكثر فعالية فى مكافحة هـذه الجرائم وتعقب مرتكبيها، نظرًا لانطوائها علـى مبدأ التجـريم المزدوج، أي وجود بند فـى هذه المعاهدات يتطلـب اعتبار السلوك المزعـوم غـير قانونـى فى كافة البلـدان المتعاهدة، وتحقيـق ذلك يعد أكـثر سهولة فى المعاهـدات الإقليمية عنه فى المعاهـدات الدولية. فبدون ازدواجيـة التجريم والقوانين المنسقـة، يتم إنشاء مـلاذات آمنة للجرائم الإلكترونية حيـث يتعذر ملاحقة ومقاضاة مرتكبى هذه الجرائم. وقد لوحظ إفلات العديد من مرتكبى تلك الجرائم من الملاحقة والعقاب؛ نظرًا لأن أفعالهم لم تكن مجرمة فى بلدانهم وقت وقوع الحادث، ومثال ذلك قضيـة فيروس «دودة الحب» Love Bug سيئة السمعة لعام ٢٠٠٠، التى لم يتم مقاضاة مبتكرها لأن أفعاله لم تكن تعتبر جريمة فى بلده (الفلبين) وقت وقوع الحادث[٢]. وعليه

---

(١) د. جورج لبكى، المعاهدات الدولية للإنترنت: حقائق وتحديات، على الرابط التالى:
- 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

(٢) راجع: مكتب الأمم المتحدة المعنى بالمخدرات والجريمة (UNODC)، آليات التعاون الدولى الرسمية، على الرابط التالى:
- https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

وترجع وقائع هذه القضية إلى عام ٢٠٠٠، حيث انتشر فيروس يدعى «دودة الحب» Love Bug من خلال تلقى الضحايا بريدًا إلكترونيًـا مرفقًا بنص ملحق بعنوان «رسالة حب إليك» LOVE-LETTER-FOR-YOU، وقد تضمنت الرسالة شفرة ضارة تستبـدل الملفـات على الكمبيوتـر، وتسرق كلمات المرور، وترسل نسخًـا منها تلقائيًا إلى كل جهات الاتصـال فى بريد المتلقى. وخـلال ٢٤ ساعة، كانـت الشفرة قد تسببت بمشاكل كبرى حول العالم، مع إصابتها لنحو ٤٥ مليون حاسب آلى. كذلك أربكت الدودة الرقمية أنظمة البريد الإلكترونى فى المؤسسات، وأجبرت مدراء الأقسام التقنية على فصل أجزاء من بناهم التحتية، لتفـادى انتشـار الفيروس. وقد أدى ذلـك إلى وقوع أضرار وأعطال قـدرت بمليارات الدولارات آنذاك، ففـى المملكة المتحدة أطفـأ البرلمان شبكة البريد الإلكترونى لساعات لحمايـة نفسه، كما تأثر البنتاغون الأمريكى بالفيروس. وتقفى المحققون أثر الفيروس وصولاً إلى أنه انطلق من بريد إلكترونى مسجل فى العاصمة الفلبينية «مانيلا» لشخص يدعى «أونيل دى غوزمن».

فقد بـادرت بعض المنظمات الإقليمية إلى عقد اتفاقيـات لمكافحة الجرائم الإلكترونية فى النطاق الجغرافى للمنظمة؛ الأمر الذي من شأنه المساهمة إلى حد بعيد فى مكافحة هذه الجرائم على المستوى الدولى.

ولبيـان جهـود المنظمات الإقليمية فـى مكافحة الجرائم الإلكترونيـة، سنقسم هذا المطلـب إلى فرعين رئيسيـين، نتناول فى الأول دور مجلس أوروبـا فى مواجهة الجرائم الإلكترونية،وفى الثانى دور جامعة الدول العربية فى مواجهة هذه الجرائم.

الفرع الأول

دور مجلس أوروبا فى مواجهة الجرائم الإلكترونية

منذ نشأته الأولى عام ١٩٤٩، سعى مجلس أوروبا Council of Europe [١] إلى تحقيق الهـدف الذي أنشئ من أجلـه وهو دعم حقوق الإنسان والديمقراطيـة وسيادة القانون فـى أوروبا. وإزاء التطور السريع فى مجال تكنولوجيا الكمبيوتر والإنترنت، وشعور دول المجلس بأهمية إعادة النظر فى الإجراءات الجنائية فى هذا المجال، فقد أصدر المجلس توصيات بشأن المشاكل القانونية المتعلقة بتكنولوجيا المعلومات، كما وضع اتفاقية مجلس أوروبـا بشأن الجريمة السيبرانية (المعرفة باتفاقية بودابست) لعام ٢٠٠١. **وبيان ذلك على النحو التالى:**

أولًا - توصيات مجلس أوروبا:

فـى ١١ سبتمـبر ١٩٩٥، أصدر مجلس أوروبا مجموعة مـن التوصيات بشأن مشاكل

= إلا أن المشتبه به لم يخضع للمحاكمة، لأن القوانين فى الفلبين لم تكن تُجرم قرصنة الكمبيوتر آنذاك.

لمزيد من التفاصيل، راجع: بعد ٢٠ عاماً.. تقفي أثر مبتكر «دودة الحب» الفتاكة، على الرابط التالى:

- https://www.bbc.com/arabic/science-and-tech-52521688

(١) مجلـس أوروبـا Council of Europe هو منظمـة دولية يتجسد هدفها المعلـن فى دعم حقوق الإنسـان والديمقراطية وسيادة القانون في أوروبا. تأسس المجلس عام ١٩٤٩ ويضم ٤٧ دولة أوروبية، ويُعتبر المراقب الرسمي للأمم المتحدة. يختلف المجلس عـن الاتحـاد الأوروبى الـذى تأسس عام ١٩٩٣ ويتألف مـن ٢٧ دولة، على الرغم من تشابكه معه فـى بعض الأحيان، حيث لم تنضـم أى دولـة إلى الاتحاد الأوروبى من دون أن تنتمى أولًا لمجلس أوروبا. كمـا يختلف المجلس عن الاتحاد الأوروبي بأنه غير قادر على إصدار قوانين ملزمة، ولكنه يتمتع بسلطة تطبيق الاتفاقيات الدولية المختارة التى توصلت إليها الدول الأوروبية حول مواضيع مختلفة. وتعد المحكمة الأوروبية لحقوق الإنسان الهيئة الأكثر شهرة فى مجلس أوروبا، والتى تطبق الاتفاقية الأوروبية لحقوق الإنسان. يقع مقر مجلس أوروبا فى ستراسبورغ بفرنسا، بينما يقع مقر الاتحاد الأوروبى فى بروكسل ببلجيكا.

لمزيد من التفاصيل، راجع: مجلس أوروبا Council of Europe على الرابط التالى:

- https://www.britannica.com/topic/Council-of-Europe

الإجراءات الجنائيــة المتعلقة بتكنولوجيا المعلومات لحث الــدول الأعضاء على مراجعة قوانــين الإجراءات الجنائية الوطنية لتلائم التطور الهائل فى هذا المجال، **ومن أهم ما ورد بتوصيات المجلس ما يأتي**[1]:

- أن توضــح القوانــين إجراءات تفتيش أجهزة الكمبيوتر وضبــط المعلومات التى تحويها، ومراقبة المعلومات أثناء انتقالها.
- أن تسمــح الإجــراءات الجنائيــة لجهــات التفتيش بضبــط برامــج الكمبيوتر والمعلومــات الموجودة بالأجهزة وفقًا لذات الشــروط الخاصة بإجراءات التفتيش العاديــة، ويتعين إخطــار الشخص القائم علــى الأجهزة بــأن النظام كان محلاً للتفتيش مع بيــان المعلومات التــى تم ضبطها، ويسمح باتخــاذ إجراءات الطعن العادية فى قرارات الضبط والتفتيش.
- أن يُسمــح أثنــاء عملية تنفيــذ التفتيش للجهات القائمــة بالتنفيذ، ومع احترام الضمانــات المقــررة، بمــد التفتيش إلى أنظمــة الكمبيوتــر الأخرى، فــى دائرة اختصاصهــم التــى تكــون متصلــة بالنظام محــل التفتيش وضبط مــا بها من معلومات.
- أن يوضــح قانون الإجــراءات أن الإجــراءات الخاصة بالوثائق التقليدية تنطبق فى شأن المعلومات الموجودة بأجهزة الكمبيوتر.
- تطبق إجراءات المراقبة والتسجيل فى مجال التحقيق الجنائى فى حالة الضرورة فى مجــال تكنولوجيا المعلومات، ويتعين توفير السرية والاحترام للمعلومات التى يفرض القانون لها حماية خاصة وبصورة مناسبة.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التى توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.
- يتعــين علــى الدول تعديل القوانــين الإجرائية بإصدار أوامر لمــن يحوز معلومات تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.

(١) د. سليمان أحمد محمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، رسالة دكتوراه مقدمة لكلية الدراسات العليا بأكاديمية الشرطة، القاهرة، ٢٠٠٧، ص٤٣٣ وما بعدها.

- يجب أن تكون هناك إجراءات سريعة ومناسبة، ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط. ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها؛ ولذلك يتعين تطوير اتفاقيات التعاون الدولى القائمة[1].

- يجب إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات، أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها، وأن تُخول سلطات التحقيق بإصدار أوامر مماثلة لأى شخص آخر لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

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

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

- قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل مثلُ هذا الأمر اعتداءً على سيادة الدولة أو على القانون الدولى؛ وجب وضع قاعدة صريحة

(١) مما لا شك فيه أن التعاون الأمنى الدولى فى مجال الجرائم الإلكترونية قد شهد تطورًا ملموسًا فى الآونة الأخيرة، وذلك بفضل جهود المنظمة الدولية للشرطة الجنائية «الإنتربول» International Criminal Police Organization (INTERPOL) ، فمثلاً عندما تم توقيف أحد الطلبة فى لبنان من قبل القضاء اللبنانى بتهمة إرسال صورة إباحية لأنثى قاصر دون العاشرة من عمرها من موقعه على الإنترنت، كان ذلك بفضل تلقى النيابة العامة اللبنانية برقية من الإنتربول فى ألمانيا حول هذه الواقعة، التى أحالتها إلى القضاء اللبنانى. فهذه المنظمة تهدف إلى تأكيد التعاون الأمنى بين الدول الأطراف فى المنظمة على نحو فعال فى مكافحة الجرائم الإلكترونية، من حيث تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الموجودة فى الدول الأطراف فى تلك المنظمة.

راجع: د. حسين بن سعيد الغافرى، السياسة الجنائية فى مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٦٣٨ وما بعدها.

تسمـح بمثل هذا الإجراء؛ ولذلك كانـت هناك حاجة ملحة لعمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات[١].

ثانيًا- اتفاقية بودابست بشأن الجرائم السيبرانية لعام ٢٠٠١ [٢]:

فى ٢٣ نوفمبر ٢٠٠١، شهدت العاصمة المجرية بودابست توقيع اتفاقية مجلس أوروبا المتعلقـة بالجرائم السيبرانيـة، المعروفة باتفاقية بودابست بشـأن الجرائم السيبرانية Budapest Convention on Cyber Crimes ، وتهدف هذه الاتفاقية إلى مساعدة الدول الأطـراف فى مكافحة الجرائم الإلكترونية، كما تلزم هذه الدول بسن الحد الأدنى من القوانـين الضروريـة للتعامل مع جرائم الإنترنت وجرائم الدخـول غير المصرح به إلى الإنترنـت، والتلاعب فى البيانات، فضلاً عن جرائـم الاحتيال والتزوير. وقد تم إجراء ٢٧ تعديـلاً على هذه الاتفاقية قبـل الموافقة عليها، وتم تضمين بنودها حق الحكومة فى المراقبة، والتعاون الدولى فى جمع الأدلة وفرض القانون[٣].

وحـددت الاتفاقيـة الجرائم التـى يجـب أن تتضمنهـا التشريعات الوطنيـة للدول الأعضاء، وهي:

١- الجرائـم المتعلقـة بأمـن الشبـكات، ومنها الدخـول والاعتراض غـير المشروع، والتدخل فـى البيانات، وفى نظام الكمبيوتر عن طريـق إدخال بيانات حاسوبية أو إرسالهـا أو إتلافهـا أو حذفها أو إفسادها أو تغييرها أو تدميرها، وكذا إساءة استخدام أجهزة الحاسبات الآلية[٤].

---

(١) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مرجع سابق، ص١٩٥-١٩٦.

(٢) تعـد اتفاقية بودابست بشـأن الجرائم السيبرانية أول وأهم الاتفاقيات الدولية المتعلقـة بمكافحة جرائم الإنترنت، وقد جرى اعتمادهـا بمعرفـة لجنة الوزراء بمجلس أوروبا فى ٨ نوفمـبر ٢٠٠١، وتم فتح الباب للتوقيع عليها فى ٢٣ نوفمبر ٢٠٠١، حيث وقعـت عليهـا ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان وجنوب إفريقيـا والولايات المتحدة، وتضمنت ٤٨ مادة. وترمى هذه الاتفاقيـة إلى توحيـد السياسة الجنائية للـدول الأعضاء فيما يتعلق بالجرائـم المعلوماتية، والتنسيق بـين مختلف السلطات الوطنيـة فـى مجال مكافحة الإجرام المعلوماتي والحد منه. إضافة إلى إرساء قواعـد إجرائية للتعاون الدولى تتميز بالسرعة والفاعلية والدقة.

لمزيـد مـن التفاصيل حول أحـكام الاتفاقية، راجع: الاتفاقية المتعلقة بالجريمة الإلكترونيـة، بودابست، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم ١٨٥، على الرابط التالى:

- https://rm.coe.int/budapest-convention-in-arabic/1680739173

(٣) د. منير محمد الجنبيهى، تزوير التوقيع الإلكترونى، دار الفكر الجامعى، الإسكندرية، ٢٠٠٦، ص ١٨٦.

(٤) راجع: المواد (٢- ٦) من اتفاقية بودابست بشأن الجرائم السيبرانية لعام ٢٠٠١.

٢- الجرائـم ذات الصلـة بالكمبيوتر، مثـل التزوير المرتبـط بالكمبيوتر المتمثل فى إدخـال، أوتغيير أو حذف أو إتلاف بيانـات الكمبيوتر[١]. وكذا الاحتيال المرتبط بالكمبيوتر[٢].

٣- جرائم الأخلاق المتعلقة بنشر مواد إباحية عن الأطفال، أو إنتاج أو توزيع أو عرض أو إتاحة أو بث أو حيازة أو نقل هذه المواد الإباحية عبر أنظمة الكمبيوتر[٣].

٤- الجرائـم المتعلقة بانتهاكات حقـوق النشر والتأليف، والحقـوق ذات الصلة مثل حقوق الملكية الأدبية والفكرية، واستنساخ المصنفات المشمولة بالحماية وغيرها، عندما تُرتكب هذه الأفعال عمدًا على نطاق تجارى، وبواسطة نظام الكمبيوتر[٤].

٥- المسئوليـة الجنائية عن الشروع أو المساعـدة أو التحريض على ارتكاب الجرائم الإلكترونيـة، ومساءلة الأشخاص الاعتباريين عـن الجرائم المنصوص عليها فى الاتفاقيـة. فضلاً عن ضـرورة اعتماد كل دولة لمجموعة مـن العقوبات والتدابير الجنائية وغير الجنائية، لمعاقبة وردع مرتكبى هذه الجرائم[٥].

وقـد حملت هـذه الاتفاقية الطابع التوجيهى للخطوات التـى يلزم اتخاذها فى إطار التشريـع الوطنى فى كل دولـة فيما يتعلق بالأحكام الموضوعيـة والإجرائية، لاسيما فى مرحلـة التحقيق والملاحقـة القضائية، مثـل التحفظ علـى الأدلة والتفتيش والضبط ومـا إلى ذلك. وألزمـت الدول الأعضـاء بمراعاة حقـوق الإنسان وحرياتـه الأساسية التـى تضمنتهـا الاتفاقيات الدولية والتشريعات الوطنية على حـد سواء والالتزام بعدم

(١) نصـت المـادة (٧) مـن اتفاقية بودابست لعام ٢٠٠١ علـى أن «تعتمد كل دولة طرف ما يلزم من تدابـير تشريعية وغيرها من التدابـير لتجـريم الأفعال التالية فى قانونهـا الوطني، إذا ما ارتكبت عمداً وبغير حق: إدخـال، تغيير، حذف أو إتلاف بيانات كمبيوتـر، بشـكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامهـا لأغراض قانونية، بغض النظر عما إذا كانـت تلك البيانات قابلة للقـراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

(٢) نصـت المـادة (٨) مـن اتفاقية بودابست لعـام ٢٠٠١ على أن « تعتمد كل دولة طرف ما يلزم مـن تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق: (أ) أى إدخال، تغيير، حذف أو إتلاف لبيانات الكمبيوتر.

(ب) أى تدخـل فـى وظيفـة نظام الكمبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق، على منفعة اقتصادية ذاتية أو لفائدة شخص آخر».

(٣) راجع: المادة (٩) من اتفاقية بودابست بشأن الجرائم السيبرانية لعام ٢٠٠١.

(٤) راجع: المادة (١٠) من اتفاقية بودابست بشأن الجرائم السيبرانية لعام ٢٠٠١.

(٥) راجع: المواد (١١- ١٣) من اتفاقية بودابست بشأن الجرائم السيبرانية لعام ٢٠٠١.

انتهاكهـا، مع إمكانية استعانة الدول الأخرى غير الأعضاء في الاتفاقية بهذه الاتفاقية عنـد إعداد التشريعات الوطنية باعتبارهـا مصدر أساسى فى مجال مكافحة الجرائم الإلكترونيـة[١]. كمـا أكـدت الاتفاقية علـى أهمية تعاون الـدول الأطراف فـى المسائل الجنائيـة، وفـى الترتيبات المتفـق عليها بمقتضـى التشريعات الموحـدة أو ذات الصلة بالمعاملة بالمثل أو القوانين الوطنية[٢].

هـذا وقد ثار خلاف بـين الموقعين على الاتفاقية حـول مسألة مكافحـة العنصرية، حيـث إن الـدول الأوروبية كانت تعتبر التحريض على الكراهيـة العنصرية جريمة، أما الولايـات المتحدة الأمريكية فكانت ترى أن حريـة التعبير المنصوص عليها فى الدستور الأمريكى تتعارض مع ما ذهبت إليه الدول الأوروبية، وبالتالى ترى عدم ضرورة النص فى الاتفاقية على العمل على إزالة المواقع التى تقوم بالتعبير عن هذا الأمر. وأخيرًا، تم الاتفـاق بين جميع الأطراف على عدم تضمين الاتفاقية هـذه المسألة بهدف تقليل حدة الخـلاف بين الدول الأعضاء الموقعة على الاتفاقية آنـذاك، إلى أن يتم دراسة الموضوع من كافة جوانبه ومحاولة التوصل إلى حل وسط ترتضيه كافة الأطراف[٣].

الفرع الثانى

دور جامعة الدول العربية فى مواجهة الجرائم الإلكترونية

نظـرًا لارتفاع معدلات الجرائم الإلكترونية وتضاعـف أعدادها وتطور أساليبها فى المنطقـة العربيـة فى الآونـة الأخيرة، وما صاحب ذلـك من استحـداث أشكال جديدة مـن الجرائم لم تكن معروفة من قبـل، بسبب التطور المضطرد والمتسارع فى تكنولوجيا المعلومـات، تبنت الأمانة العامـة لمجلسَ وزراء الداخلية والعـدل العرب بجامعة الدول العربية استراتيجية لمكافحة هذه الجرائم، أسفرت عن إبرام «الاتفاقية العربية لمكافحة جرائم تقنيـة المعلومات» التى وقعها الوزراء السابقين نيابة عن دولهم بالقاهرة فى ٢١

(١) محمود محمد شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مرجع سابق، ص٥٤٧.

(٢) نصت المادة (٢٣) من اتفاقية بودابست لعام ٢٠٠١ على أن «تتعاون الدول الأطراف فيما بينها، وفقًا لأحكام هذا الباب، ومن خـلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولى فى المسائل الجنائية وبالترتيبات المتفق عليها بمقتضى التشريعـات الموحـدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية، على أوسع نطـاق ممكن لأغراض إجراءات التحقيقات أو المتابعـات التـى تتعلق بالجرائـم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر، أو من أجـل جمع أدلة بشأن جريمة جنائية فى شكل إلكترونى».

(٣) د. منير محمد الجنبيهى، تزوير التوقيع الإلكترونى، مرجع سابق، ص ١٨٣.

ديسمبر ٢٠١٠. وتهدف هذه الاتفاقية بصفة أساسية إلى تعزيز التعاون وتدعيمه بين الدول العربية فى مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[١].

وقد انطوت الاتفاقية على مجموعة من الأفعال التى تشكل جرائم إلكترونية، وألزمت كل دولة طرف بتجريم هذه الأفعال وفقًا لتشريعاتها وأنظمتها الداخلية[٢]. والجرائم الإلكترونية التى وردت بالاتفاقية هى: جريمة الدخول غير المشروع على نظام تقنية المعلومات، وجريمة الاعتراض غير المشروع لخط سير البيانات، والاعتداء على سلامة البيانات، وجريمة إساءة استخدام وسائل تقنية المعلومات، وجريمة التزوير باستخدام وسائل تقنية المعلومات، وجريمة الاحتيال، وجريمة الإباحية[٣]، والجرائم الأخرى المرتبطة بالإباحية كالمقامرة والاستغلال الجنسى، وجريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات، والجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، والاستخدام غير المشروع لأدوات الدفع الإلكترونية، والشروع أو الاشتراك فى ارتكاب هذه الجرائم. كما عالجت الاتفاقية المسئولية الجنائية للأشخاص الطبيعية والمعنوية، وتشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات[٤].

---

(١) المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

وجاء فى ديباجتها «إن الدول العربية الموقعة، رغبة منها فى تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التى تهدد أمنها ومصالحها وسلامة مجتماعتها، واقتناعًا منها بضرورة الحاجة إلى تبنى سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربى ضد جرائم تقنية المعلومات، وأخذًا بالمبادئ الدينية والأخلاقية السامية ولاسيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنسانى للأمة العربية التى تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزامًا بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، فقد اتفقت على ما يلى..».

راجع: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ على الرابط التالى:
- https://adlm.moj.gov.sa/alqadaeya/attach/882.pdf

(٢) نصت المادة (٥) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠على أن «تلتزم كل دولة بتجريم الأفعال المبينة فى هذا الفصل، وذلك وفقًا لتشريعاتها وأنظمتها الداخلية».

(٣) نصت المادة (١/١٢) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠على أن جريمة الإباحية تتمثل فى «إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات».

(٤) راجع: الفصل الثانى (المواد ٦- ٢١) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

وتضمنـت الاتفاقيـة الأحـكام الإجرائية للاتفاقيـة ونطاق تطبيقها، بمـا فى ذلك التحفـظ العاجل على البيانات المخزنة فى تقنيـة المعلومات، والتحفظ العاجل والكشف الجزئـى لمعلومات تتبع المستخدمين، وأمر تسليم المعلومات، وتفتيش المعلومات المخزنة، وضبـط المعلومـات المخزنة، والجمع الفـورى لمعلومـات تتبع المستخدمـين، واعتراض معلومـات المحتوى[١].

كما عالجـت الاتفاقية كافة صور وأشكال التعاون القضائى والقانونى، بما فى ذلك تسليم المجرمين، والمساعدة المتبادلة، والمعلومات العرضية المتلقاة، والإجراءات المتعلقة بطلبـات التعاون والمساعدة المتبادلـة، ورفض المساعدة، والسرية وحـدود الاستخدام، والحفـظ العاجل للمعلومـات المخزنة على أنظمة المعلومـات، والكشف العاجل لمعلومات تتبع المستخدمين المحفوظة، والتعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنيـة المعلومـات المخزنـة، والوصـول إلى معلومـات تقنيـة المعلومـات عـبر الحدود، والتعـاون والمساعـدة الثنائيـة بخصوص الجمع الفـورى لمعلومات تتبـع المستخدمين، والتعـاون والمساعدة الثنائية فيمـا يخص المعلومات المتعلقة بالمحتـوى، وضرورة وجود جهـاز متخصص لدى كل دولة طرف لضمـان توفير المساعدة الفورية لغايات التحقيق والإجراءات المتعلقة بجرائم تقنية المعلومات[٢].

ويلاحظ أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قد وضعت استراتيجية تكفل التزام الدول الأطراف بسن تشريعات وطنية خاصة بمكافحة جرائم تقنية المعلومات التـى انطوت عليها الاتفاقية، كما حرصت علـى إيجاد آلية وطنية للتعاون والتنسيق بين الجهات المعنية بمكافحة هذه الجرائم، بدءًا من مرحلة تقييم المخاطر، ورصد ومتابعة تلك الجرائم وتبـادل المعلومات فى شأنها، مرورًا بعمليات التحرى والملاحقة والتحقيق وتبادل المعلومات، وانتهاءً بتقديم مرتكبيها إلى المحاكمة، مع التعاون والتنسيق مع جميع وسائـل الإعـلام المرئيـة والمسموعة والمقروءة لتوعيـة المواطنين بأخطـار جرائم تقنية المعلومـات وأضرارها الاقتصاديـة والاجتماعية على الفرد والمجتمـع، وتوعية العاملين بمراكـز المعلومـات والاتصـالات، ومستخدمـي الشبكـة العنكبوتية، ومواقـع التواصل

(١) راجع: الفصل الثالث (المواد ٢٢- ٢٩) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(٢) راجع: الفصل الرابع (المواد ٣٠- ٤٣) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

الاجتماعـي بالأساليب والوسائل التي يتبعها قراصنـة المعلومات لتحقيق أهدافهم غير المشروعة[١].

ومما لا شك فيه أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ تعد بمثابـة خطوة هائلة نحو مكافحة الجرائم الإلكترونية، وقد سارت الدول الأطراف على دربها، ومنها جمهورية مصر العربية التى أصدرت القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، ودولة الإمارات العربية المتحدة التى أصدرت مرسومًا بقانون اتحادى رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية.

(١) راجـع: تكاتف الجهود العربية لمكافحة الجريمـة الإلكترونية وجرائم المعلوماتية وأثرها على العمليات المالية، اتحاد المصارف العربية، على الرابط التالى:- https://uabonline.org/ar/

المبحث الثالث

آليات التعاون الدولى فى مكافحة الجرائم الإلكترونية

التعاون بمفهومه العام يعنى العون المتبادل، أي تبادل المساعدة والعون لتحقيق هدف معـين، فكثيرًا ما يلجأ الأفـراد إلى الاستعانة بالآخرين من أجـل قضاء حوائجهم؛ لأن الإنسـان بطبعـه لا يستطيع العيش بمفـرده[١]. أما مفهوم التعاون الـدولى فى مكافحة الجريمـة فيعد مـن المفاهيم التى يصعب وضع تعريف جامع مانع لها، ويرجع ذلك إلى اتسـاع المجال والصور والأشـكال التى يمكن أن يتخذها هذا التعـاون، إلا أن جانبًا من الفقـه عرفـه بأنه: «ما تقدمه سلطـات دولة لدولة أخرى من مساعـدة وعون فى سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهـة الصبغـة غـير الوطنية للجريمـة، وتستجمع الأدلـة بمختلف الطـرق، وهو ما يستغـرق وقتًا، ويتطلب إمكانات لا تملكها سلطـات قانونية لدولة واحدة، ما لم تدعمها وتساندها جهود السلطات القانونية فى الدول الأخرى»[٢].

وقـد أصبح التعاون الدولى ضرورة ملحة لمكافحة الأفعال الإجرامية عابرة الحدود، حيـث أثبـت الواقـع العملـى أن أى دولة مهما كانـت إمكانياتهـا لا تستطيـع بجهودها المنفـردة مكافحة الجرائم الإلكترونية، خاصة مـع التطور الهائل فى مجال الاتصالات وتكنولوجيـا المعلومـات، فإن كان من الضـرورى أن تمتلك الـدول الإمكانات التشريعية والأمنيـة والقضائيـة لمكافحة الجريمـة الإلكترونية، فإن الأهم من ذلـك أن تكون تلك القوانين متوائمة ومتجانسة بين مختلف الدول كونها تحمى مصلحة مشتركة[٣].

---

(١) د. عادل عبد العال إبراهيم خراشى، إشكاليات التعاون الدولى فى مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون بتفهنا الأشراف، العدد ١٦، الجزء الأول، ٢٠١٤، ص ١٧٩.

(٢) د. سالم محمد سليمان الأوجلى، أحكام المسئولية الجنائية عن الجرائم فى التشريعات الوطنية، رسالة دكتوراه مقدمة لكلية الحقوق – جامعة عين شمس، القاهرة، ١٩٩٧، ص ٤٢٥.

وعرفـه فريـق آخـر بأنـه: «تبـادل العـون والمساعـدة وتضافـر الجهـود المشتركة بـين دولتـين أو أكـثر لتحقيق نفـع أو خدمة أو مصلحـة مشتركـة فـى مجـال التصـدى لمخاطـر الإجـرام، ومـا يرتبـط بـه مـن مجـالات أخـرى مثـل مجـال العدالة الجنائيـة ومجـال الأمـن، أو لتخطـى مشـكلات الحـدود والسيـادة التى قـد تعترض الجهـود الوطنية لملاحقـة المجرمين وتعقب مصادر التهديد، سواء اقتصرت على دولتين فقط أو امتدت إقليميًّا أو عالميًا.

راجـع: د. أحمد إبراهيـم مصطفى سليمان، الإرهاب والجريمة المنظمة: التجريم وسبل المواجهة، دار الطلائع للنشر والتوزيع، القاهرة، ٢٠٠٦، ص ٢٩٤.

(٣) د. صورية بوربابة، التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص ٩٤.

وهنـاك عـدة آليات للتعـاون الدولى فى مجـال مكافحة الجرائـم الإلكترونية، من أبرزهـا آليات التعـاون الأمنى الـدولى، وآليات التعـاون القضائى الـدولى. من ناحية أخـرى، أظهرت الممارسة الدولية وجود ثمة معوقات تواجه التعاون الدولى فى مكافحة الجرائم الإلكترونية وتحد من فاعليته.

ودراسـة آليات التعاون الدولى فى مكافحة الجرائـم الإلكترونية تتطلب تقسيم هذا المبحـث إلى ثلاثة مطالب، نتناول فـى **الأول** آليات التعاون الأمنـى الدولى فى مكافحة الجرائـم الإلكترونيـة، ونعالج فى **الثانى** آليـات التعاون القضائى الـدولى فى مكافحة الجرائـم الإلكترونيـة، ونخصـص **الثالـث** للتحديات التـى تواجه التعـاون الدولى فى مكافحة هذه الجرائم.

المطلب الأول

آليات التعاون الأمنى الدولى فى مكافحة الجرائم الإلكترونية

ممـا لا شـك فيه أن الأجهـزة الأمنية العاملـة داخل الحدود الوطنيـة تعد من أهم أجهـزة العدالـة الجنائية فى مجـال مكافحة الجريمـة بمختلف صورها، بيـد أن هذه الأجهـزة لا يمكنها القيام بإجراءات البحث والتحرى – وغيرها من إجراءات مكافحة الجريمـة – خارج الحـدود الوطنية لتعارض ذلك مع مبدأ السيادة، الأمر الذي استلزم تضافـر الجهود الدوليـة الرامية نحو إيجاد آلية للتعاون الأمنـى الدولى تكفل التصدى للجريمة المنظمة عبر الوطنية ومكافحتها.

وقـد تمخضت هذه الجهـود الدولية عن إنشاء «المنظمة الدوليـة للشرطة الجنائية» International Criminal Police Organiztion، التـى تُعـرف اختصـارًا باسـم «الإنتربـول» Interpol [1]، والتى اضطلعـت بدور فعال فى مكافحة الجريمة الإلكترونية علـى المستـوى الدولى. فضـلاً عن ذلك، فقد قامـت بعض الدول بإنشـاء أجهزة أمنية إقليميـة متخصصـة تكفل التعاون الإجرائى على أقاليمهـا. وعليه سنقسم هذا المطلب إلى فرعـين، نتناول فيهما تباعًا التعاون الأمنى على المستـوى الدولى، والتعاون الأمنى على المستوى الإقليمى.

(١) تجـدر الإشـارة إلى أن مصطلح «الإنتربول» Interpol هـو اختصار لكلمتى «الشرطة الدوليـة» International Police. راجع: موقع المنظمة الدولية للشرطة الجنائية (الإنتربول) على الرابط التالى: https://www.interpol.int/ar/Internet -

الفرع الأول

التعاون الأمني على المستوى الدولي

إن المنظمــة الدوليــة للشرطــة الجنائيــة (الإنتربــول)، التي تمخضــت عنها جهود المجتمع الدولى، تهدف إلى تعزيز وتشجيع التعاون الأمنى الدولى، أي مساعدة الأجهزة الأمنية فى الدول الأعضاء على التعاون فيما بينها فى مجال مكافحة الجريمة بأشكالها المختلفــة، وبصفة خاصة الجرائم ذات الطابع عبر الوطني كالجرائم الإلكترونية، دون التدخل فى الشئون ذات الطابع السياسي أو العسكري أو الديني أو العرقي، أو ممارسة أي نشاط من هذا القبيل[١]. وسوف نتعرض بإيجاز لنشأة منظمة الإنتربول، وأهدافها، واختصاصاتها، ونشاطها فى مجال مكافحة الجرائم الإلكترونية.

أولًا- نشأة منظمة الإنتربول:

بدأت منظمة الإنتربول كفكرة منذ مطلع القرن العشرين، وبالتحديد فى عام ١٩١٤ عندمــا عقد أول اجتمــاع دولى للقانون الجنائى، تحت رعاية الجمعيــة الدولية للقانون الجنائى International Commission of Criminal Law فى مدينة موناكو الفرنسية، وضم الاجتماع عددًا من ضباط الشرطة والمحامين وأساتذة القانون من أربعة عشر بلد، وتمت مناقشة العديد من المواضيع المتعلقة بالتعاون الأمنى بين الدول، ومن بينها كيفية تبــادل المعلومات وتوثيقها وملاحقة المجرمين وتعقبهــم، وإلقاء القبض عليهم، وتسليم المجرمــين، وبحث الاجتماع أيضًا إمكانية إنشــاء مركز دولى لتبادل المعلومات الجنائية المتعلقــة بالجريمة والمجرمين بين الدول، وكذا إنشاء مكتب دولى للتسجيل الجنائى، إلا أن هذه الجهــود قد توقفــت بسبب اندلاع الحــرب العالمية الأولى[٢].

---

(١) د. عادل عبد العال إبراهيم، إشكاليات التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص١٩١.

(٢) بينمــا يــرى البعض أن بداية التعاون الــدولى فى المجال الأمنى ترجع إلى عام ١٩٠٤، وذلك بمناسبــة تطبيق الاتفاقية الدولية الخاصــة بمكافحــة الاتجــار بالرقيق الأبيض المبرمة فى ١٨ مايــو ١٩٠٤، والتى نصت المادة الأولى منها علــى أنه: « تتعهد كل الحكومــات المتعاقــدة بأن تنشئ أو تعين سلطة تركز لديها المعلومات الخاصة باستخــدام النساء والفتيات لغرض الدعارة فى الخــارج، ولهــذه السلطة الحق فى أن تخاطب مباشرة الإدارة الممثلة لها فى كل الدول الأطراف المتعاقدة». وتطبيقاً لنص هذه المــادة أنشــئ جهاز لتبادل المعلومات بين مجموعة مــن دول أمريكا اللاتينية عام ١٩٠٥، خاصــة المعلومات المتعلقة باستخدام النســاء والفتيــات لغرض الدعارة فى الخــارج ، وكانت مهام هذا الجهاز تشبــه إلى حد كبير المهام التــى تقوم بها منظمة=

وبعد أن وضعت الحرب العالمية الأولى أوزارها، كان من بين نتائجها اضمحلال الإمبراطورية النمساوية المجرية، حيث أصبح بحوزة مديرية الشرطة بمدينة فيينا بين عشية وضحاها مجموعة كبيرة من الوثائق المتعلقة بالإجرام، والتى تهم كلاً من المجر وإيطاليا ويوغوسلافيا ورومانيا وتشيكوسلوفاكيا وبولونيا، ونتج عنها تبادل كم هائل من المعلومات بين هذه الدول، واستغل مدير شرطة فيينا آنذاك السيد «يوهانس شوبار» Johanz Chober هذه الظروف، ليقترح عام ١٩٢٣ انعقاد مؤتمر دولى للشرطة فى العاصمة النمساوية فيينا، حيث وجهت الدعوات لمديرى الشرطة فى عدد كبير من المدن، وضم هذا المؤتمر مديرى الشرطة الممثلين لسبع عشرة دولة، وكانت مصر من بين الدول المشاركة، وأسفر هذا المؤتمر عن إنشاء «اللجنة الدولية للشرطة الجنائية» International Criminal Police Commission وتمت المصادقة بالإجماع على نظامها الأساسى، وأصبحت فيينا مقرًا لها، وتم انتخاب مدير شرطة فيينا رئيسًا لهذه اللجنة، وكان من بين أهم أهدافها العمل على تنسيق الجهود بين أجهزة الشرطة فى الدول الأعضاء فى مجال التعاون فى مكافحة الجريمة، وقد بدأت الدول فى الانضمام إليها تباعًا[١]. وبالرغم من قيام هذه اللجنة بتسيير دوائر متنوعة ذات فائدة دولية بالغة[٢]، إلا أنها تعرضت للعديد من الانتقادات التى من بينها أن اللجنة اقتصرت فى ممارسة نشاطاتها خاصة فيما يتعلق بتنسيق الجهود بين أجهزة الشرطة بين الدول الأوروبية فقط، بحيث لم تصل إلى مرحلة تدويل نشاطاتها عبر مختلف القارات، أى الوصول

= الإنتربول، ولهذا اعتبر هذا الجهاز بداية التعاون الأمنى بين أجهزة الشرطة فى مختلف الدول، وهذا نظراً لوجود تقارب بين أهدافه وأهداف منظمة الإنتربول، خاصة فى مجال تأكيد تشجيع المعونة المتبادلة فى أوسع نطاق ممكن فى حدود القوانين الداخلية للدول المتعاقدة مع الالتزام بالإعلان العالمى لحقوق الإنسان.

راجع: د. عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٣، ص ١٣٦.

(١) د. عبد الوهاب حومد، التعاون الدولى لمكافحة الجريمة، مجلة الحقوق والشريعة، العدد الأول، الكويت، فبراير ١٩٨١، ص ١٩٥.

(٢) قامت اللجنة بإنشاء وتسيير العديد من الدوائر التى من بينها مكتب مركزى دولى لمكافحة الغش والتزوير بدأ عمله منذ عام ١٩٢٣، وعُهد إليه إصدار مجموعة بطاقات عن العملات الأصلية والعملات المزورة، كما شرعت فى إصدار مجلة للشرطة منذ عام ١٩٢٥، كذلك فقد أنشأت جهاز مخابرات لملاحقة المجرمين الدوليين ووضع سجلاً دولياً للشرطة، كما وضعت سجل المجرمين الأشرار الذى ظهر إلى الوجود عام ١٩٢٦، فضلاً عن إقامة سجل لحفظ البصمات، كما أنشأت مكتب مركزى لمكافحة تزوير جوازات السفر عام ١٩٢٦.

راجع: د. كلود فالاكس، المنظمة الدولية للشرطة الجنائية، بحث فى المجلة الدولية للشرطة الجنائية، الطبعة العربية، العدد ٣٨٧، إبريل ١٩٨٥، ص ٩٢.

بهـا إلى العالميـة، وكانت منذ انبعاثهـا تتميز بغموض نظامها الأساسـى الذي أفضى إلى اندماجهـا فى إدارة وطنية للشرطة (شرطة فيينـا)، فضلًا عن تأثرها بالأحداث السياسيـة الجارية آنذاك. وعقب اندلاع الحرب العالميـة الثانية، وانضمام النمسا إلى ألمانيـا، تم نقـل مقر اللجنة إلى برلين عام ١٩٤٠، ولم يعـد لها ذكر طيلة فترة الحرب، ولم يكتب لها الاستمرار بعد ذلك[١].

وعقب انتهاء الحرب العالمية الثانية، التقت وفود سبع عشرة دولة فى مدينة بروكسل ببلجيـكا بناءً على دعوة المفتش العام للشرطة البلجيكية السيد «لوفاج»Louvage، وكان هـدف هـذا المؤتمر هو إحيـاء التعاون من جديـد بين الدول خاصة فـى مجال مكافحة الجريمـة والقضاء عليهـا، وقد توصل هذا المؤتمـر إلى إحياء اللجنـة الدولية للشرطة الجنائيـة، وتم نقـل مقرها إلى باريـس و شكلت لها لجنة تنفيذية مـن خمسة أعضاء، كما تم استحداث منصب الأمين العام الذي عهد به إلى السيد «لوفاج» الذي كان يرأس اللجنة التنفيذية[٢].

بيـد أن نقطة التحـول الحقيقية فى تاريخ هـذه المنظمة جاءت عقب تأسيس منظمة الأمم المتحدة، وبالتحديد فى عام ١٩٥٦، عندما أصدرت الجمعية العامة للأمم المتحدة فـى دورتها الخامسة والعشرين التى انعقدت فى العاصمـة النمساوية فيينا فى الفترة مـن ٧ إلى ١٣ يونيـه ١٩٥٦، قـرارًا خاصًا باعتمـاد النظام الأساسـى للمنظمة الدولية للشرطـة الجنائية (الإنتربول)، الـذي اعتمد هذه التسمية بدلًا عـن التسمية السابقة «اللجنـة الدوليـة للشرطة الجنائيـة»، وأصبح هذا النظـام نافذًا ابتداءً مـن ١٣ يونيه ١٩٥٦، وصـارت المنظمة منذ ذلك التاريخ تعمل بشكل دائم ومستقر، إلى أن وصل عدد أعضائها إلى ١٩٥ دولة حتى الآن[٣].

---

(١) فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، رسالة ماجستير مقدمة لكلية الحقوق بن عكنون – جامعة الجزائر، الجزائر، ٢٠١٢- ٢٠١٣، ص ١٠.

(٢)د. محمد السعيد الدقاق، التنظيم الدولى، الطبعة الثالثة، الدار الجامعية للطباعة والنشر، بيروت، ١٩٨٤، ص١٩٧.

(٣) راجع: موقع المنظمة الدولية للشرطة الجنائية (الإنتربول) على الرابط الإلكترونى السابق.

وقد نصت المادة الأولى من القانون الأساسى للمنظمة الدولية للشرطة الجنائية على أن: تدعى المنظمة المسماة «اللجنة الدولية للشرطة الجنائية» مـن الآن فصـاعدًا «المنظمة الدولية للشرطة الجنائية (الإنتربول)»، ويكون مقرها فى فرنسا.

وتجـدر الإشـارة إلى أن العاصمـة الفرنسية باريس صارت مقرًا للمنظمة الدولية للشرطة الجنائية منذ نشأتها عام ١٩٥٦ حتى انتقلت إلى مقرها الحالى فى مدينة ليون الفرنسية فى عام ١٩٨٩.

وينظم الوضع القانونى لمقر منظمة الإنتربول اتفاقية دولية أبرمت بين المنظمة والحكومة الفرنسية عام ١٩٧٢، منحت المنظمة=

ثانيًا - أهداف منظمة الإنتربول:

تعرضت المادة الثانية من القانون الأساسى للمنظمة الدولية للشرطة الجنائية (الإنتربول) لبيان أهداف المنظمة، حيث نصت على أن أهدافها تتمثل فى:

١- تأكيد وتشجيع التعاون المتبادل على أوسع نطاق ممكن بين كافة سلطات الشرطة الجنائية، فى إطار القوانين القائمة فى مختلف البلدان، والاهتداء بروح الإعلان العالمى لحقوق الإنسان.

٢- إقامة وتنمية كافة المؤسسات التى من شأنها أن تسهم على نحو فعال ومؤثر فى منع ومكافحة جرائم القانون العام.

ويستخلص من نص هذه المادة أن أهداف المنظمة الدولية للشرطة الجنائية (الإنتربول) تتمثل فى تأكيد وتشجيع التعاون الدولي بين سلطات الشرطة فى الدول الأعضاء، نتيجة لما ألَمَّ بالجماعة الدولية من تطورات فى المجالات كافة، وخاصة فى مجال المواصلات والتى كان لها أثرها فى سهولة انتقال المجرمين بين الدول، بعد ارتكابهم لجرائمهم فى البلدان المختلفة، الأمر الذي يتطلب التعاون بين أجهزة الشرطة فى الدول كافة، لمكافحة مثل هذه الأعمال. وأن يفضى هذا التعاون إلى إقامة وتنمية مؤسسات الشرطة والعدالة الجنائية وغيرها من المؤسسات ذات الصلة، التى تعمل فى إطار القوانين النافذة فى كل دولة، والتى من شأنها أن تسهم على نحو فعال ومؤثر فى منع ومكافحة جرائم القانون العام، وهى الجرائم المعروفة عالميًا بانتهاكها للقانون الطبيعى فى أى مجتمع، مثل القتل والسرقة والنصب والاتجار فى المخدرات والاتجار بالبشر وتزييف العملة وغيرها من جرائم القانون العام[1]. فمنظمة الإنتربول

=بموجبها بعض المزايا والحصانات داخل فرنسا، حيث يتمتع مقر المنظمة بالحصانة الدولية، وتوفر له الحماية اللازمة من قبل الحكومة الفرنسية من أى اعتداء يطال المبنى أو العاملين فيه باعتبارهم موظفين دوليين يتمتعون بالحماية والحصانة الدبلوماسية وفقًا للاتفاقية المبرمة بين الطرفين، والاتفاقيات الدولية الأخرى ذات الصلة بموضوع الحصانات.

راجع: د. محمد منصور الصاوى، أحكام القانون الدولى المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دراسة فى القانون الدولى الاجتماعى فى مجال مكافحة الجرائم الدولية للمخدرات وإبادة الأجناس واختطاف الطائرات وجرائم أخرى، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٤، ص ٦٤٩.

د. إبراهيم أحمد خليفة، القانون الدولى الدبلوماسى والقنصلى، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧، ص١٣٠ وما بعدها.

(١) د. محمد منصور الصاوى، أحكام القانون الدولى المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، مرجع سابق، ص ٦٨٥- ٦٨٦.

تهـدف -بصفـة أساسيـة- إلى تأكيد وتشجيع التعـاون بين أجهـزة الشرطة فى الدول الأطراف على نحو فعال فى مكافحة الجريمة، وذلك من خلال جمع البيانات والمعلومات المتعلقة بالمجرم والجريمة عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة فى أقاليم الدول الأعضاء فى المنظمة[١].

كما يجب أن يكون هذا التعاون متوافقًا مع ما ورد بالإعلان العالمى لحقوق الإنسان[٢]، وبعيـدًا عن الأمـور السياسيـة والعسكريـة والدينية والعنصريـة[٣]. فالغايـة الأسمى للإنتربـول هـى العمل على قيـام عالم أكـثر أمنًا وسلامًا، بعـد أن انتشـرت العمليات الإجرامية وامتـدت إلى عدد كبير من الدول، هذا من جانب، ومن جانب آخر ضعف أو محدودية الجهود الأمنية المحلية فى التصدى للإجرام ولا سيما المنظم منه، وهذه هى أهم الأسباب التى دعت إلى ظهور المنظمة.

ثالثًا- دور الإنتربول فى مكافحة الجرائم الإلكترونية:

لقـد أصبح العالم اليـوم أكثر ترابطًا على الصعيد الرقمـى منه فى أي وقت مضى. ويستغـل المجرمون هـذا التحول الإلكترونـى لاستهداف نقاط الضعـف في المنظومات والشبكات والبنى التحتية عبر الإنترنت، الأمر الذي يُخلّف تبعات اقتصادية واجتماعية هائلة على الحكومات والشركات والأفراد فى شتى أنحاء العالم. وما التصيد الاحتيالى وبرمجيات انتزاع الفدية وانتهاكات البيانات سوى أمثلة قليلة على التهديدات السيبرانية الراهنـة، بينما تظهر علـى الدوام أشكال جديـدة من الجرائـم الإلكترونية، فمرتكبو هـذه الجرائم باتوا أكثر مرونة وتنظيمًا، حيث يستغلون التكنولوجيا الجديدة، ويكيفون اعتداءاتهم ويتعاونون فيما بينهم بطرق مبتكرة[٤].

(1) Malcolm Anderson, Policing the World: Interpol and the Politics of International Police Co-operation, Clarendon Press, Oxford, 1989, pp. 168 et seq.

(٢) الإعـلان العالمـي لحقـوق الإنسان هو وثيقة حقوق دولية تبنتهـا الجمعية العامة للأمم المتحدة فـى ١٠ ديسمبر ١٩٤٨، وتتكون مـن ٣٠ مـادة تتضمن طائفة كبيرة من الحقوق التى يجـب كفالتها لجميع الناس دون تفرقة، مثـل الحق فى الحياة والكرامة الإنسانيـة، والمحاكمـة العادلة، وحرية الفكـر والاعتقاد، والمشاركة فى الحكـم، والحق فى العمل والتعليـم والهجرة والتنقل، وغيرها من الحقوق الأساسية.

راجع: د. محمد رضا الديب، حقوق الإنسان، بدون ناشر، القاهرة، ٢٠١٤- ٢٠١٥، ص ٦ وما بعدها.

(3) Feraud H. and Sclanitz E., La Coopération Policière Interna-tionale, Revue Internationale de Droit Pénal, Vol. 45, 1974., p. 483.

(٤) راجع: الإنتربول، الجريمة السيبرانية، على الرابط التالى: - https://www.interpol.int/ar/4/6

وإذا كانت الجرائم الإلكترونية لا تعرف الحدود، والجناة والضحايا والبنى التحتية التقنيــة ينتمــون إلى اختصاصات قضائيــة متعددة، فإن ذلك يضفــى على التحقيقات والملاحقــات القضائية العديــد من التحديــات، والإنتربول، بحضــوره العالمى، يضطلع بــدور أساسى فى إقامــة الشراكات بين القطاعــات والتعاون الدولى بــين أجهزة إنفاذ القانــون، وينسق عمليات إنفاذ القانون، ويوفر منصات مأمونة لتبادل البيانات، ويقدم التحليــل والتدريب لتقليص التهديــدات السيبرانية[١]. بالإضافة إلى ذلك، فإن منظمة الإنتربــول تعمــل على تعزيز قدرة الــدول الأعضاء على مكافحة الجرائــم الإلكترونية، وكشفهــا والتحقيق فيها وتقويضها، مما يساعد على حمايــة المجتمعات، ويجعل العالم أكثر أمنًا[٢].

فضلاً عن ذلك، فإن ملاحقة مرتكبى الجرائم الإلكترونية يستلزم القيام بإجراءات خارج حدود الدولة، حيث ارتكبت الجريمة، ومن هذه الإجراءات معاينة مواقع الإنترنت فى الخارج وضبط الأقراص الصلبة، وتفتيش أنظمة الحاسب الآلى، وهذا كله يصطدم بمشاكل الحدود، ويتعذر علــى الدولة بمفردها القضاء على مثل هذه الجرائم الدولية، لأن جهــاز الشرطة فى هــذه الدولة أو تلك لا يمكنه تعقــب المجرمين وملاحقتهم خارج حدود الدولة. وقد مرت جهود منظمة الإنتربول فى هذا المجال بمراحل عدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية فى كل من طوكيو، ونيوزيلندا، ونيروبى، وأذربيجان، وبوينــس ايرس، بالإضافــة إلى مكتب إقليمى فرعــى فى بانكوك. ونظــرًا لتنوع أنظمة

(١) قاد الإنتربول عدة عمليات فى مناطق مختلفة استهدفت أنشطة جنائية منظمة فى الفضاء السيبرانى. وجمعت هذه العمليات محققــين للعمــل معًا استنــادًا إلى معلومات عن تهديدات جرى كشفهــا بالتعاون مع شركاء من القطــاع الخاص. ففى منطقة رابطــة أمم جنوب شرق آسيــا ASEAN ، جمعت عملية ASEAN بين خبرة الشرطة والقطــاع الخاص لتحديد خوادم القيادة والسيطــرة التى تنشر أنواعًا مختلفة مــن البرمجيات الخبيثة؛ وقد أدى ذلك إلى كشف ما يقرب من ٢٧٠ موقعًا مخترقًا، بما فى ذلك بوابات حكومية. وحُدِّدت أيضًا هوية عدد من مشغلى مواقع التصيّد الاحتيالى، بمن فيهم مشغّل له صلات بنيجيريا. وفــى إندونيسيــا، تم ضبط أحــد المجرمين الذى نشر مجموعــة من أدوات التصيّــد الاحتيالى عبر الشبكــة الخفية، ومقاطع فيديو على موقع يوتيوب، تظهر للزبائن كيفية استخدام البرمجيات غير المشروعة. وفى الأمريكتين، اتخذت البلدان المشاركة إجــراءات ميدانيــة لتعطيل البنى التحتية للجريمــة السيبرانية فى منطقة الأمريكتين بناءً علــى معلومات استخباراتية قدمها الإنتربــول، وأدت التحقيقات إلى كشف ٢٦ موقعًا إلكترونيًا حكوميًا متضــررًا، وست مجموعات من القراصنة، وعدة قراصنة فرادى، ومعلومات عما يقرب من ٤٠ حالة تصيّد احتيالى وبثّ برمجيات خبيثة تتعلق بـ ٣٧٠٠ تهديد سيبرانى نشط.

راجع: الإنتربول، عمليات مكافحة الجريمة السيبرانية، على الرابط التالى:

- https://www.interpol.int/ar/4/6/2

(٢) راجع: الإنتربول، الجريمة السيبرانية، المرجع السابق.

الـدول المختلفة، فقد كان هناك خيـاران لأنظمة الاتصال داخل هـذه الشبكة، أولهما، هـو نموذج يخصص للدول المركزيـة، وتجرى الاتصـالات الدولية للشرطـة فيها من خلال الجمعية العامة واللجنة التنفيذيـة بواسطة السكرتارية العامة. وثانيهما، للدول اللامركزيـة وتجرى الاتصالات فيـه مباشرة بين أجهزة الشرطة فـى الدول المختلفة، حيـث تقوم المنظمة من خلال هـذه المراكز بملاحقة مجرمـى المعلوماتية عامة وشبكة الإنترنـت خاصة، عـن طريق تعقب الأدلـة الرقمية وضبطها، والقيـام بعملية التفتيش العابـر للحدود لمكونات الحاسب الآلى والأنظمة المعلوماتية وشبكات الاتصال بحثًا عما تحويه من معلومات وأدلة وبراهين على ارتكاب الجريمة الإلكترونية[١].

الفرع الثانى

التعاون الأمني على المستوى الإقليمي

علـى غرار المنظمـة الدولية للشرطة الجنائية (الإنتربول)، سعـت الدول إلى إنشاء آليـة للتعاون الأمنى على المستـوى الإقليمى، خاصة مع انتشـار الجرائم الخطيرة عبر الوطنية، وقامت بإبرام اتفاقيات تكفل التعاون الإجرائى على أقاليمها. ومن أبرز آليات التعـاون الأمنـى الإقليمى: التعاون الأمنى على المستوى الأوروبـى، والتعاون الأمنى على المستوى العربى.

أولاً- التعاون الأمنى على المستوى الأوروبى:

تعود فكرة إنشـاء مكتب الشرطة الأوروبى «اليوروبول» Europol إلى قمة لكسمبورج فـى ٢٨ سبتمـبر ١٩٩١ ليكون بمثابـة وكالة الاتحـاد الأوروبى للتعاون فـى مجال إنفاذ القانـون، بهدف جعـل أوروبا أكثر أمنًا لصالح جميع مواطنى الاتحاد الأوروبى، على أن يختص -بصفـة أساسية- بمكافحة الاتجار الدولى بالمخـدرات والجريمة المنظمة[٢]، وليكـون أداة الوصل بين أجهزة الشرطة الوطنية فـى الدول الأعضاء، بما يكفل تحقيق

(١) حيمـر عبد الكريم، منظمـة الإنتربول، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٣- ٢٠١٤، ص ٤٢.

(2) Europol is the European Union Agency for Law Enforcement Cooperation. Its main goal is to achieve a safer Europe for the benefit of all the EU citizens. In 1991, Establishment of a Central European Investigation Office ('Europol') to fight international drug trafficking and organised crime. See: Europol, Europol History, on the following Website: https://www.europol.europa.eu/about-europol/history.

أقصى درجات التعاون وتبادل المعلومات وملاحقة الجناة فى الجرائم المنظمة عابرة الحدود، ومنها بطبيعة الحال الجرائم الإلكترونية[١].

فى عام ٢٠١٣، ومع ارتفاع معدلات الجرائم الإلكترونية وجسامة الخسائر الناجمة عنها، قامت وكالة «االيوروبول» بإنشاء المركز الأوروبى للجرائم الإلكترونية European Cybercrime Centre (EC3) الذي يهدف إلى مكافحة الجرائم الإلكترونية فى الاتحاد الأوروبى، والعمل على حماية مواطنى الاتحاد والحكومات والشركات من مخاطر جرائم الإنترنت. وتركز نشاط المركز -بصفة أساسية- على مكافحة الأنواع التالية من الجرائم الإلكترونية: الجرائم المعتمدة على الإنترنت Cyber-dependent Crimes، واستغلال الأطفال جنسيًّا، والاحتيال المالى عبر الإنترنت. ويمتد اختصاص المركز أيضًا إلى معالجة الإجرام على الشبكة المظلمة والمنصات البديلة.

بالإضافة إلى ذلك، يقوم المركز الأوروبى للجرائم الإلكترونية بتقديم الدعم العملياتى والاستراتيجي وخدمات الطب الشرعى للتحقيقات التى تجريها الأجهزة الأمنية لدول الاتحاد الأوروبى بشأن الجرائم الإلكترونية. **ويقوم أيضًا بالمهام التالية**[٢]:

- يعمل كمحور مركزى للمعلومات والاستخبارات الجنائية.
- يدعم العمليات والتحقيقات التى تقوم بها الدول الأعضاء من خلال تقديم التحليل العملياتى والتنسيق والخبرة.
- يوفر قدرات دعم جنائية رقمية وتقنية عالية التخصص للتحقيقات والعمليات الأمنية.
- يقدم الدعم لأجهزة إدارة الأزمات فى الاتحاد الأوروبى، التى تعمل ضمن نطاق ولاية اليوروبول، ويعمل على تيسير التعاون العملياتى والتقنى والاستراتيجى بين وكالات إنفاذ القانون وغيرها من الكيانات ذات الصلة بالجرائم الإلكترونية.

(١) د. جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى: الأحكام الموضوعية لجرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٢، ص ٧٩.

(2) See: Europol, European Cybercrime Centre - EC3, on the following Website:
- https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- يوفر الدعم اللازم على مدار الساعة لهيئات التعليم المحلية، والاستجابة الفورية للحوادث الإلكترونية الطارئة أو الأزمات الإلكترونية عبر الخدمة الاحتياطية.
- يستضيف وييسر مهام فرق العمل المشتركة لمكافحة الجرائم الإلكترونية.
- يدعم التدريب وبناء القدرات، ولا سيما للسلطات المختصة فى الدول الأعضاء.
- يقـدم مجموعـة متنوعة من نتائج التحليـل الاستراتيجى التى تمكـن القادة من اتخاذ قرارات مستنيرة بشأن مكافحة الجريمة الإلكترونية وقمعها.
- يقـدم توعية شاملة لسلطـات إنفاذ القانون التى تتصـدى للجرائم الإلكترونية، ويعمـل على توثيق الصلـة بينهم وبين القطاعات الخاصـة والأوساط الأكاديمية والشركاء الآخرين غير العاملين فى مجال إنفاذ القانون.
- يسهم فى تقديم أنشطة موحدة للوقاية من مخاطر الجرائم الإلكترونية، وإعداد حملات توعية فى المجالات ذات الصلة بهذه الجرائم[١].

ثانيًا- التعاون الأمنى على المستوى العربى:

منـذ نشأتها الأولى فـى ٢٢ مارس ١٩٤٥، لم تول جامعة الـدول العربية ثمة اهتمام بالمجال الأمنى العربى بالرغم من الإشارة إليه فى ميثاقها، واقتصرت مناقشة الأوضاع الأمنية على الزيارات المتبادلة وتبادل بعض المعلومات. وفى ١٩٦٠، حدث تطور مهم فى موقـف الجامعة تجاه التعاون الأمنى، حيث وافق مجلس الجامعة فى دورته العادية رقم ٥٥ المنعقـدة فى ١٠ إبريل ١٩٦٠ على إنشـاء المنظمة الدولية العربية للدفاع الاجتماعي ضـد الجريمة[٢] بموجب القرار رقـم ١٦٨٥، التى تهدف إلى العمل على دراسة أسباب الجريمـة ومكافحتها، ومعاملة المجرمين، وتأمين التعاون المتبادل بين الشرطة الجنائية فى البلاد العربية، ومكافحة المخدرات[٣]. ونصت الاتفاقية المنشئة للمنظمة على إنشاء

(1) Europol, European Cybercrime Centre - EC3, op. cit.

(٢) بتاريخ ٩ سبتمبر ١٩٧٦ وافق مجلس الجامعة العربية بقراره رقم ٣٥٧٢ على تعديل اسم المنظمة بحذف كلمة «الدولية» ليصبح اسمها « المنظمة العربية للدفاع الاجتماعى ضد الجريمة».

(٣) راجع: المادة الأولى من اتفاقية المنظمة العربية للدفاع الاجتماعى ضد الجريمة لعام ١٩٦٠ على الرابط التالى:
file:///C:/Users/NEW%20VISION/Downloads/Agreement_3879-1.pdf -

مكتب لمكافحة الجريمة يتولى تنسيق الجهود بين الأجهزة الأمنية فى الدول العربية، والعمل على تحقيق سياسة عربية موحدة فى مجال مكافحة الجريمة[١].

وفى مؤتمر وزراء الداخلية العرب بمدينة الطائف بالمملكة العربية السعودية عام ١٩٨٠ اتخذ المؤتمر قرارًا بتطوير المؤتمر إلى مجلس دائم لوزراء الداخلية العرب، وتمت المصادقة على مشروع النظام الأساسى للمجلس فى الاجتماع الطارئ لوزراء الداخلية العرب المنعقد فى مدينة الرياض بتاريخ ٢٢ فبراير ١٩٨٢، والذي تم إقراره من مجلس جامعة الدول العربية بموجب القرار رقم ٤٢١٨ بتاريخ ٢٣ سبتمبر ١٩٨٢ [٢]. وفى ديسمبر ١٩٨٣، تم إنشاء «المكتب العربى للشرطة الجنائية» التابع للأمانة العامة لمجلس وزراء الداخلية العرب، ومقره فى دمشق بسوريا[٣].

ويتمتع المكتب العربى للشرطة الجنائية بالشخصية القانونية الدولية، ويهدف إلى تأمين وتنمية التعاون المتبادل بين مختلف إدارات الشرطة الجنائية فى الدول الأعضاء فى مجال مكافحة الجريمة، وملاحقة المجرمين فى حدود القوانين والأنظمة المعمول بها فى كل دولة، بالإضافة إلى تقديم المعونة فى مجال دعم وتطوير أجهزة الشرطة فى الدول الأعضاء. فضلاً عن ذلك، يعمل المكتب على تدعيم جميع المؤسسات الخاصة

---

(١) نصت المادة (١١) من اتفاقية المنظمة العربية للدفاع الاجتماعى ضد الجريمة على إنشاء مكتب لمكافحة الجريمة، تسند إليه المهام التالية:

أ) إجراء الدراسات والبحوث العلمية للجريمة وأسبابها وبواعثها، واستنباط وسائل الوقاية منها وعلاجها.

ب) دراسة العقوبة باعتبارها وسيلة اصلاح وردع، وما يقتضيه ذلك من وضع الأنظمة اللائقة للسجون ومعاملة المسجونين ومعتادى الإجرام والمحبوسين احتياطيًا، ومعالجة شئون المحكوم عليهم بعد انقضاء مدة العقوبة.

ج) دراسة أسباب انحراف الأحداث ووضع الأسس العلمية والعملية لعلاجهم، ووضع الأحداث الجانحين فى مؤسسات خاصة بهم، ووقاية الأطفال المشردين، وغير ذلك من أوجه النشاط المؤدية إلى تحقيق الأغراض التى أنشئ المكتب من أجلها.

د) العمل على تنسيق الجهود التى تبذلها الهيئات الحكومية وغيرها فى مختلف البلاد العربية فى الميادين المذكورة، والعمل على تحقيق سياسة عربية موحدة فى هذه الميادين عن طريق توحيد التشريعات.

(٢) راجع: مجلس وزراء الداخلية العرب، نشأة مجلس وزراء الداخلية العرب، على الرابط التالى:
- https://www.aim-council.org/about/emergence-of-the-council/#

(٣) هذا المكتب هو أحد المكاتب الستة التابعة للأمانة العامة لمجلس وزراء الداخلية العرب، وهى: المكتب العربى لمكافحة الجريمة ومقره بغداد، والمكتب العربى للإعلام الأمنى ومقره القاهرة، والمكتب العربى لمكافحة المخدرات ومقره عمّان، والمكتب العربى للحماية المدنية والإنقاذ ومقره الدار البيضاء، بالإضافة إلى المكتب العربى للدراسات الأمنية ومقره الرياض (حاليًا أكاديمية نايف للعلوم الأمنية).

راجع: مقدر منيرة، التعاون الدولى فى مكافحة الجريمة المنظمة، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٤-٢٠١٥، ص ١٩٩.

ذات الصلـة بمكافحـة الجريمة، كما يتعاون مع المنظمـات والأجهزة الدولية فى مجال مكافحة الجرائم المنظمة، ومنها الجرائم الإلكترونية[١].

ومـع تنامى ظاهـرة الجرائم الإلكترونيـة وتأثيرهـا السلبى على الأوضـاع الأمنية والاقتصاديـة فى المنطقة العربية، شأنها فى ذلك شأن بقية دول العالم، اضطلع المكتب العربـى للشرطة الجنائية بدوره فى التصدى لهـا ومكافحتها، خاصة فى أعقاب توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، حيث قام المكتب بالتنسيق والتعاون مع الأجهزة الأمنية فى الدول العربية من أجل مكافحة هذه الجرائم وملاحقة مرتكبيها، وتقديم الدعم الفنـى والعملياتى اللازم لهذه الأجهزة، وكذا التعاون وتبادل المعلومـات مـع المنظمة الدولية للشرطـة الجنائية (الإنتربول) فى هـذا الشأن. بيد أن أحـداث الأزمـة السوريـة التى بدأت فى مارس ٢٠١١ قد أثرت سلبًا علـى كفاءة وأداء المكتـب العربى للشرطة الجنائية، حيـث إن سوريا دولة المقر، لكنه ما زال يقوم بمهامه التى أنشئ من أجلها.

المطلب الثاني

آليات التعاون القضائى الدولى

فى مكافحة الجرائم الإلكترونية

إن اتساع مسرح الجرائم الإلكترونية وامتداده عبر أكثر من دولة جعل من الصعوبة بمكان جمع أدلة إثباتها، خاصة فى ظل قصور القوانين الجنائية الوطنية وتقيدها بمبدأ الإقليميـة السائد فـى أغلب التشريعات الوطنيـة، الأمر الذي ألجأ الـدول إلى التعاون القضائـى فيمـا بينهـا لتسهيل عملية جمـع الأدلة وملاحقـة المشتبه فيهـم وتسليمهم تمهيدًا لمحاكمتهم.

ويقصـد بالتعـاون القضائى الدولى تنسيـق جهود السلطـات القضائية فى مختلف الـدول لمكافحـة الجريمـة المنظمة من خـلال تيسير جمـع الأدلة وإجـراءات التحقيق والمحاكمـة إلى حين صدور الحكم على الجانـى، وضمان عدم إفلاته من العقاب نتيجة ارتكابـه للجريمة فـى عدة دول. ويعد التعـاون القضائى الدولى مـن مرتكزات النظام

(١) د. محمد فاضل، التعاون الدولى فى مكافحة الإجرام، منشورات جامعة حلب، سوريا، ١٩٩٢، ص ٤١٧-٤١٨.

الدولى، حيث إنه يلعب دورًا جوهريًّا على الساحة الدولية، إذ لا يمكن تجنب التهديدات الأمنيــة دوليا دون وجود علاقات تعاونية بين الدول بمــا يضمن تحقيق هذا التعاون[١]. ومــن أهــم صور التعــاون القضائى الــدولى فى مجــال مكافحة الجرائــم الإلكترونية، المساعدة القضائية المتبادلة، وتسليم المجرمين فى الجرائم الإلكترونية. وعليه سنقسم هذا المطلب إلى فرعين، نتناول فى **الأول** المساعدة القضائية المتبادلة، ونعالج فى **الثانى** تسليم المجرمين.

الفرع الأول

المساعدة القضائية المتبادلة

أولى الفقــه الجنائى الــدولى المساعــدة القضائيــة المتبادلة أهميــة خاصة لدورها الفعــال فى التصدى للإجــرام المنظم عبر الوطنى، وسد أوجــه القصور القانونى التى ساعــدت المنظمــات الإجرامية على اخــتراق النظم القانونية الوطنيــة. وتعد المساعدة القضائيــة المتبادلة فى المسائل الجنائية مــن الصور الشائعة للتعاون القضائى الدولى، والتى تستهدف استظهار وجه الحق، والتوفيق بين حق الدولة فى ممارسة اختصاصها الجنائــى داخل حدود إقليمها وحقها فى توقيع العقاب، وتتــم بمساعدة الدولة الطالبة فى إجراءات تكون قد بدأتها[٢].

والمساعــدة القضائيــة المتبادلــة هــى إجــراء قضائــى من شأنــه تسهيــل ممارسة الاختصاصــ القضائى فى دولــة أخرى بصدد جريمة من الجرائــم، يُلجأ إليه لتحقيق الفعاليــة والسرعــة فى إجــراءات الملاحقة والعقــاب على الجرائم، ويُــبرر بضرورات المصلحة المشــتركة لجميع الدول فى مواجهة المنظمات الإجرامية[٣].

بيــد أن موضوع الحصول على الأدلة والشهود من بلــد آخر يثير تساؤلات وإشكالات

(١) فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مرجع سابق، ص ١٣٤.

(٢) د. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، مرجع سابق، ٢٠٠٦، ص ٣٩٤.

(٣) د. سالم محمد سليمان الأوجلى، أحكام المسئولية الجنائية عن الجرائم فى التشريعات الوطنية، مرجع سابق، ص٤٢٥.
كما يُقصد بالمساعدة القضائية المتبادلة «تقديم الدول الأطراف المساعدة القانونية المتبادلة فى التحقيق والملاحقة والإجراءات القضائية المتعلقة بأى جريمة من تلك الجرائم المشمولة بالاتفاقيات الدولية».
راجــع: د. خالــد بن مبارك القحطانى، التعاون الأمنى الدولى ودوره فــى مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه مقدمة لجامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٦، ص ١٧٤.

قانونيــة كثـيرة ومعقدة حـول الطرق التى يمكن مــن خلالها أن يصاغ هــذا النمط من التعــاون بشكل يسمح بجعل تلك الإجراءات ميســرة لدى الدولة المطلوب إليها، ومقبولة قانونًــا لدى السلطة القضائية المختصة بالدولة الطالبة، وتزداد هذه الصعوبات إذا ما كان التعــاون يجرى بين نظم قانونية مختلفة، مثل النظام الاتهامى السائد فى الولايات المتحدة الأمريكية ونظام التحرى والتحقيق المعروف لدى الدول الأوروبية[١].

هذا وتجد المساعدة القضائيــة المتبادلة مصدرها فى النصوص التشريعية الوطنية والاتفاقيــات الدولية المبرمة بين الدول. ويمكن للدول فــى هذا الإطار الاهتداء بأحكام المعاهــدة النموذجية لتبادل المساعدة فى المسائل الجنائيــة، التى تم اعتمادها بموجب قــرار الجمعية العامة لــلأمم المتحدة رقم ٤٥/١١٨ المؤرخ فى ١٤ ديسمبر ١٩٩٠، والتى قــررت أحكامًا تعالج اتفاق الدول الأطــراف على أن يقدم كل منها للآخر أكبر قدر من المساعــدة المتبادلة فى التحقيقات أو إجراءات المحاكمــة المتعلقة بجرائم يكون العقاب عليهــا وقت طلب المساعدة داخــلًا فى اختصاص السلطة القضائية فى الدولة الطالبة، ويمكن للمساعدة المتبادلة وفقًا لهذه المعاهدة أن تشمل أخذ شهادة الشهود أو الاستماع إلى أقــوال الأشخاص، والمساعدة فى تقديم الأشخاص المحتجزيــن أو غيرهم للإدلاء بالشهــادة، والمعاونة فــى التحريات المتعلقة بإعلان الوثائــق القضائية، وتنفيذ عمليات التفتيش والحجــز، وفحص الأشيــاء والمواقع، وتوفــير المعلومات والمــواد الاستدلالية، وتوفــير الوثائــق والسجــلات بما فى ذلــك سجلات المصــارف أو السجــلات المالية أو سجلات الشركات أو الأعمال[٢].

ولا تؤثــر هــذه المعاهدة فى الالتزامــات القائمة بــين الطرفين عمــلًا بمعاهدات أو اتفاقيــات أخرى أو غير ذلــك، ما لم يقررا خلاف ذلك. وعلــى كل دولة أن تعين سلطة أو سلطــات تتــولى تقديم طلبات المساعدة القضائية أو تلقيهــا[٣]. كما عالجت المعاهدة الحــالات التى يجوز فيها رفض طلــب المساعدة، ومحتويات طلبــات المساعدة، وتنفيذ

(١) ذنايب آسية، الآليات الدولية لمكافحة الجريمة المنظمة عبر الدولية، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة الأخوة منتورى، قسنطينة، الجزائر، ٢٠٠٩- ٢٠١٠، ص ١٩٧.

(٢) راجع: المعاهدة النموذجية لتبادل المساعدة فى المسائل الجنائية لعام ١٩٩٠، على الرابط التالى:
- https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/559/90/IMG/ NR055990.pdf?OpenElement

(٣) المادة (٣) من المعاهدة النموذجية لتبادل المساعدة فى المسائل الجنائية لعام ١٩٩٠.

طلبـات المساعدة[١]. وتتخذ المساعدة القضائيـة المتبادلة العديد من الصور والمظاهر، التى من أهمها ما يأتي:

أولًا- تبادل المعلومات:

يقصـد بتبـادل المعلومات تقـديم المعلومـات والوثائق التـى تطلبها سلطـة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التى وجهت إلى رعاياها فى الخارج، والإجراءات التى اتخذت ضدهم[٢]. وهناك مظهر آخر لتبادل المعلومات يتعلق بالسوابق الجنائية للجناة، التى من خلالها تتعرف الجهات القضائية بدقة على الماضى الجنائى للفرد المحال إليها، حيث تساعد فى تقرير الأحكام الخاصة بالعود ووقف تنفيذ العقوبة، إلا أن تدويـل الصحيفـة الجنائيـة ما زال فى مراحلـه الأولى، وتقوم الـدول بإعدادها بالنسبة لرعايا الدول التى ترتبط معها باتفاقيات تبادل معلومات[٣].

ونظـرًا لما تتميز بـه الجريمة الإلكترونية مـن كونها عابرة للحدود، فـإن مكافحتها لا تتحقـق إلا بوجـود تعـاون دولى علـى مستـوى الإجـراءات الجنائيـة، بحيـث يسمح بالاتصـال المباشـر بين الأجهـزة القضائية والأمنية فى الدول المختلفـة من أجل تبادل المعلومـات المتعلقـة بالجريمـة والمجرمـين[٤]. ولتبـادل المعلومـات كصورة مـن صور المساعـدة القضائيـة المتبادلة صدى كبير فى كثير مـن الاتفاقيات الدولية، حيث وردت فى المادة السابعة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ [٥]. كمـا وردت فـى المادة الأولى مـن اتفاقية الرياض العربيـة للتعاون القضائى

---

(١) المواد (٤، ٥، ٦) من المعاهدة النموذجية لتبادل المساعدة فى المسائل الجنائية لعام ١٩٩٠.

(٢) د. عادل عبد العال إبراهيم، إشكاليات التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص ٢٠٤.

(٣)د. عبـد الرحمـن فتحى سمحان، تسليم المجرمين فى ظل قواعـد القانون الدولى، دار النهضة العربيـة، القاهرة، ٢٠١١، ص ٥٢٧.

(٤) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مرجع سابق، ص٢٠٥.

(٥) نصت المادة (١/٧- ب) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ على أن: «تكفل كل دولة طـرف، دون إخلال بأحكام المادتين (١٨)، (٢٧) من هذه الاتفاقيـة، قدرة الأجهزة الإدارية والرقابية وأجهزة إنفاذ القانون وسائـر الأجهزة المكرسـة لمكافحة غسل الأموال (بما فيهـا السلطات القضائية، حيثما يقضى القانـون الداخلى بذلك) على التعـاون وتبادل المعلومات علـى الصعيدين الوطنى والدولى ضمن نطاق الشروط التى يفرضهـا قانونها الداخلى، وأن تنظر، تحقيقًـا لتلـك الغاية، فى إنشاء وحدة استخبارات مالية تعمل كمركز وطنى لجمع وتحليل وتعميم المعلومات عما يحتمل وقوعه من غسل للأموال».

راجع: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ على الرابط التالى:

- https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20 Convention/TOCebook-a.pdf

لعـام ١٩٨٣ بشـأن ضرورة تبادل المعلومات بين الدول الأطـراف والتنسيق بين الأجهزة القضائية[١]. وفى السياق نفسه، صاغ اتفاق «تشنجن» للاتحاد الأوروبى نظامًا متكاملاً لتبـادل المعلومـات[٢]. كمـا صارت على النهـج نفسه اتفاقيـة الاتحاد الإفريقـى بشأن الأمـن السيبرانى وحماية البيانـات الشخصية لعام ٢٠١٤ التى أكدت على أهمية تبادل المعلومات المتعلقة بالتهديدات السيبرانية[٣].

ثانيًا- نقل الإجراءات:

يقصد بنقل الإجراءات قيام دولة ما، بناء على اتفاقية أو معاهدة، باتخاذ إجراءات جنائيـة، وهى بصدد التحقيق فى جريمة ارتكبـت فى إقليم دولة أخرى، ولمصلحة هذه الدولة متى توافرت مجموعة من الشروط، **أهمها:**

١- التجريم المزدوج، ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة فى الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات.

٢- شرعيـة الإجـراءات المطلـوب اتخاذها، بمعنـى أن تكـون الإجـراءات المطلوب اتخاذها مقررة فى قانون الدولة المطلوب إليها عن الجريمة ذاتها.

٣- أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان، بحيث تؤدى دورا مهما فـى الوصـول إلى الحقيقـة، كأن تكون أدلـة الجريمة موجـودة بالدولة المطلوب إليها[٤].

وقـد أقرت العديـد من الاتفاقيـات الدولية والإقليميـة هذه الصـورة كإحدى صور

---

(١) نصـت المـادة الأولى من اتفاقية الرياض العربية للتعاون القضائى لعـام ١٩٨٣ على أن «تتبـادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التى تنشر فيهـا الأحـكام القضائية، كما تتبادل المعلومات المتعلقة بالتنظيم القضائـى، وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية، والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة حسبما تقتضيه الظروف الخاصة بكل منها». راجع: اتفاقية الرياض العربية للتعاون القضائى لعام ١٩٨٣ على الرابط التالى:
- https://www.pacc.ps/uploads/books/2/book-101-cat-2-d-06-01-15.pdf

(٢) د. صورية بوربابة، التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص ٩٦.

(3) State Parties shall encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs). [Article 28, Para 3]. See: African Union Convention on Cyber Security and Personal Data Protection, 2014, on the following Website:
https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_conven tion_on_cyber_security_and_personal_data_protection _e.pdf

(٤) د. سالم محمد سليمان الأوجلى، أحكام المسئولية الجنائية عن الجرائم فى التشريعات الوطنية، مرجع سابق، ص٤٢٧.

المساعدة القضائية المتبادلة، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات فى المسائل الجنائية لعام ١٩٩٠، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ [١]. وإذا كانت هذه الاتفاقيات تمثل آليات ناجعة فى مكافحة الجرائم العادية وملاحقة مرتكبيها، إلا أنها قد لا تحقق أهدافها فى حالة الجرائم الإلكترونية؛ نظرًا للصعوبات المتعددة التى تتعلق بإقامة الدليل على ارتكاب مثل هذه الجرائم.

ثالثًا- الإنابة القضائية:

ويقصد بها طلب اتخاذ إجراء قضائى من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك فى الفصل فى مسألة معروضة على السلطة القضائية فى الدولة الطالبة، ويتعذر عليها القيام به بنفسها. وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التى تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش أو غيرها [٢].

وبموجب الإنابة القضائية تقوم السلطات القضائية لدولة ما بمباشرة إجراء قضائى يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، بناء على طلب الدولة الأخيرة، ووفقًا لما تقرره بنود الاتفاق المبرم بينهما فى هذا الشأن. وعادة ما يتم إرسال طلبات الإنابة القضائية عبر القنوات الدبلوماسية، إلا أنه، وسعيًا وراء الحد

---

(١) نصت المادة (٢١) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠ على أن: «تنظر الدول الأطراف فى إمكانية أن تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجرم مشمول بهذه الاتفاقية، فى الحالات التى يعتبر فيها ذلك النقل فى صالح سلامة إقامة العدل، وخصوصًا عندما يتعلق الأمر بعدة ولايات قضائية، وذلك بهدف تركيز الملاحقة».

(٢) د. عبد الرءوف مهدى، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٥، ص١٠٢ وما بعدها. وانظر أيضًا: د. عمر سالم، الإنابة القضائية الدولية فى المسائل الجنائية، دار النهضة العربية، القاهرة، ٢٠٠١، ص ١٤ وما بعدها.

وتجدر الإشارة إلى أن فكرة الإنابة القضائية قديمة نسبيًا، حيث وردت فى المادة السادسة من اتفاقية الإعانات والإنابات القضائية التى اعتمدها مجلس جامعة الدول العربية فى ١٤ سبتمبر ١٩٥٢، والتى نصت على أن: «لكل من الدول المرتبطة بهذه الاتفاقية أن تطلب إلى أية دولة منها أن تباشر فى أراضيها نيابة عنها أى إجراء قضائى متعلق بدعوى قيد النظر وفقًا لأحكام المادتين (٧، ٨) من الاتفاقية». راجع: نص الاتفاقية على الرابط التالى:

- http://haqqi.info/ar/haqqi/legislation/convention-ads-and-letters-rogatory

من البطء الذي تتسم بـه الإجراءات الدبلوماسية، يحدث وبدرجة متزايدة أن تشترط المعاهـدات والاتفاقيـات الخاصة بتبادل المساعـدة القضائية على الـدول الأطراف أن تعين سلطة مركزية، عادة ما تكون وزارة العدل، لتُرسل إليها الطلبات مباشرة بدلًا من الولوج إلى القنوات الدبلوماسية، وذلك من شأنه تسهيل الإجراءات[١].

هـذا وقد تم إبرام العديد من الاتفاقيـات المتعلقة بالإنابة القضائية التى تهدف إلى اختصـار الوقت وتبسيط الإجراءات عن طريق الاتصـال المباشر بين السلطات المعنية بالتحقيـق، ومنها الاتفاقية الأمريكية الكندية التـى تنص على إمكانية تبادل المعلومات شفويًا فى حالة الاستعجال، ونفس الشىء نجده فى المادة (٢/٣٠) من معاهدة منظمة المؤتمـر الإسلامـى لمكافحـة الإرهاب الـدولى لعـام ١٩٩٩، والمادة (١٥) مـن اتفاقية الرياضـ العربية للتعاون القضائى لعام ١٩٨٣، والمادة (٥٣) من اتفاقية تشينجن لعام ١٩٩٠ بشأن استخدام الاتصالات المباشرة بين السلطات القضائية فى الدول الأطراف، والمادة (٤٦) من اتفاقية الأمم المتحدة لمكافحة الفساد لعام ٢٠٠٤ [٢].

ومـمـا لا شـك فيـه أن الإنابة القضائية تـؤدى إلى تسهيل الإجـراءات الجنائية بين الـدول، وتسهم فى التغلب علـى عقبة السيادة الإقليمية التى تمنـع الدولة الأجنبية من ممارسـة بعض الأعمال القضائية داخل أقاليـم الدول الأخرى، كسماع الشهود وإجراء التفتيشـ والتحريـات وغيرها. وتحافظ الإنابة على السيـادة الوطنية للدولة، حيث يتم إنجـاز الإجراءات المطلوبة علـى أرض دولة أخرى دون تدخل مباشـر من أجهزتها فى القضيـة محل الإنابـة، كما تسهم فى عدم ضيـاع الأدلة وحفظ حقـوق المجنى عليهم، وتكفل حق المتهمين فى محاكمة ناجزة[٣].

(١) د. عادل عبد العال إبراهيم، إشكاليات التعاون الدولى فى مكافحة الجرائم المعلوماتية، مرجع سابق، ص ٢١٠.
وانظر أيضًا: د. طارق سرور، الاختصاص الجنائى العالمى، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٥.

(٢) فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مرجع سابق، ص ١٤٠- ١٤١.

(٣) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مرجع سابق، ص ٢٠٨.

الفرع الثانى

تسليم المجرمين

إن التسليـم فى الجرائم الإلكترونية ينهض على أساس أن تقوم الدولة التى يوجد على إقليمها المتهم بارتكاب جريمة إلكترونية بمحاكمته إذا كانت تشريعاتها تجيز ذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة. فهو يحقق بذلك مصلحة طرفى التسليم، مصلحة الدولة طالبة التسليم فى معاقبة الجانى الذي أخل بقوانينها وأضر بمصالحها، ومصلحة الدولة المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من شخص خارج عن القانون. لكن يظل تسليم الدولة لمواطنيها المتورطين فى ارتكاب جرائم إلكترونية خارج الوطن من أصعب جوانب التعاون الدولى[١].

من ناحية أخرى، يمثل التسليم آلية للملاحقة الجنائية عبر الوطنية تسد الطريق على المتهمين بارتكاب الجرائم الإلكترونية الذين قد يلوذون بالفرار من الدولة التى ارتكبوا فيها جرائمهم أو من الدولة صاحبة الاختصاص بمحاكمتهم. ونظرًا لأهمية موضوع التسليم فسوف نتعرض بإيجاز لماهيته وشروطه وإجراءاته.

أولًا - ماهية تسليم المجرمين:

يعد نظام تسليم المجرمين خروجًا عن الحدود الجغرافية للدول لملاحقة المجرمين والتصدى للجريمة، وغالبًا ما يتم بناءً على اتفاقية خاصة بين دولتين أو بناءً على اتفاق عام كما هو الحال فى الاتفاقيات والمعاهدات متعددة الأطراف[٢]. وقد تعددت تعريفات «تسليم المجرمين» Extradition، حيث ذهب البعض إلى تعريفه بأنه «عقد بين دولتين أو أكثر يتم بمقتضاه إعادة شخص للدولة التى انتهك حرمة قوانينها حتى تتمكن من معاقبته»[٣]. وعرفه المؤتمر العاشر لقانون العقوبات بأنه «إجراء للتعاون القضائى

(1) Jonathan O. Hafen, International Extradition: Issues Arising Under Dual Criminality Requirement, BYU Law Review, U.S.A., 1992, pp. 191 et seq.

(٢) د. صالح مصطفى البرغثى، قضية لوكربى، دراسة فى القانون الدولى، رسالة دكتوراه مقدمة لكلية الحقوق- جامعة عين شمس، ١٩٩٨، ص ١٤٩.

(٣) كما عرف البعض تسليم المجرمين بأنه «مجموعة من الإجراءات القانونية التى تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى، لكى يحاكم بها أو ينفذ فيها الحكم الصادر عليه من محاكمها».
راجع: د. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، مرجع سابق، ص ٣٣٢.

بـين الدول فى المسائل الجنائية يرمى إلى نقـل شخص يكون محلًا للملاحقة الجنائية أو محكومًا عليه جنائيًّا من نطاق السيادة القضائية لدولة إلى سيادة دولة أخرى»[١].

بينما ذهب الاتجاه الغالب فى الفقه الدولى إلى تعريف تسليم المجرمين بأنه «إجراء بمقتضـاه تتخلـى الدولة عن شخص موجـود على إقليمها لسلطـات دولة أخرى تطالب بتسليمه إليها لمحاكمته عن جريمة منسوب إليه ارتكابها، أو لتنفيذ عقوبة مقضى عليه بها من محاكم الدولة طالبة التسليم»[٢].

ثانيًا- شروط تسليم المجرمين:

دعـت العديد مـن المؤتمـرات الدوليـة إلى ضـرورة إبـرام معاهدة عالميـة لتسليم المجرمـين، ومن بينها المؤتمر الأول للشرطة القضائية فـى موناكو عام ١٩٢٤، والمؤتمر الـدولى للعقاب فـى لندن سنة ١٩٤٥، ولكـن تلك الدعوات لم تتحقق حتـى الآن؛ نظرًا لاختـلاف وجهات النظر الدولية حول نظـام التسليم باعتباره أمرًا يتعلق بسيادة الدول ومصالحهـا السياسية. غـير أن الأحكام المتعلقة بتسليم المجرمين قد تبلورت من خلال قيـام الدول بإبرام اتفاقيات ثنائية ومتعددة الأطراف لمنع وقمع بعض الجرائم الدولية ذات الخطورة على المجتمع الدولى. هذا وقد أسهمت كل من الاتفاقية الأوروبية لتسليم المجرمين لعام ١٩٥٧، ومعاهدة Benelux لتسليم المجرمين لعام ١٩٦٢ بدور ملموس فى تطوير قواعد تسليم المجرمين، حيث أبرمت على ضوئهما العديد من الاتفاقيات الثنائية، وأصدرت العديد من الدول تشريعات داخلية خاصة تحكم نظام تسليم المجرمين[٣].

---

(١) د. صالح مصطفى البرغثى، قضية لوكربى مرجع سابق، ص ١٥٢.

وفى المعنى نفسه، عرفه البعض بأنه «إجراء تعاون دولى تقوم بمقتضاه دولة تسمى بالدولة الطالبة بتسليم شخص يوجد فى إقليمهـا إلى دولـة ثانية تسمى بالدولة المطلوب إليها أو جهة قضائية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكـم جنائـى ضده». راجـع: د. عبد المنعم سليمان، الجوانـب الإشكالية فى النظام القانونى لتسليـم المجرمين، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧، ص ٣٢.

(٢)د. حامد سلطان، القانون الدولى العام فى وقت السلم، دار النهضة العربية، القاهرة، ١٩٦٢، ص٤٠٠.

- Kurt Von Schuschnigg, International Law: An Introduction to the Law of Peace, the Bruce Publishing Co., Milwaukee, 1959, p. 223.
- Michael Akehurst, A Modern Interoduction to International Law, Third Edition, George Allen and Unwin Ltd., London, 1977, p. 133.
- Jean Pradel, Droit Pénal Général, 19e edition, Cujas, Paris, 2012, p. 254.

(٣) د. سالم الأوجلى، أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوطنية، مرجع سابق، ص ٤٣٦.

ووضعت الدول شروطًا وقواعد معينة يتعين مراعاتها حين ممارستها للتسليم، وذلك من خلال الاتفاقيات الدولية والتشريعات الوطنية، وتتمثل هذه الشروط فيما يأتي[١]:

١- التجريم المزدوج Double Criminality: تشترط العديد من الدول أن يكون الفعل الـذي يُطالب بالتسليم مـن أجله يشكل جريمة مُعاقب عليها فـى قانون الدولة الطالبة والدولة المطلوب إليها، وذلك تطبيقًا لقاعدة «لا عقوبة إلا بقانون».

٢- أن تكـون الجريمـة علـى درجـة مـن الخطـورة: تشـترط الاتفاقيـات الدوليـة والتشريعـات الوطنية أن يكـون التسليم فى الجرائم ذات الخطـورة فقط، كالجنايات والجنـح المهمة التى لا يقـل العقاب فيها عن حد أدنى معين تحدده الاتفاقيات، ذلك أن إجراءات التسليـم معقدة وباهظة التكاليف، فلا ينبغى أن تشغل الدولة نفسها بجرائم تافهة كالجنح البسيطة أو المخالفات.

٣- ألا تكـون الجريمـة أو العقوبـة قـد سقطت بالتقـادم: فلا يجـوز تسليم المجرم الهـارب -كقاعدة عامـة- إذا انقضت الدعـوى الجنائية أو العقوبة بمضـى المدة وفقًا لقانون إحدى الدولتين طالبة التسليم أو المطلوب إليها التسليم.

٤- الاختصاص القضائى للدولة طالبة التسليم: ويعد ذلك أمـرًا بديهيًا، إذ يُشترط لتسليـم المجرم الهارب للدولة التى تطلبه أن تكون هذه الدولة مختصة بمحاكمته وفقًا لمـا تقضى به المعاهـدات الدولية الخاصة بتسليم المجرمين، فـإذا كانت الدولة الطالبة غير مختصة أصلًا بمحاكمته كما لو ارتكبت الجريمة خارج حدودها الإقليمية أو كانت الجريمة مما يدخل فى اختصاص محاكم الدولة المطلوب إليها التسليم، فلا محل هنا للتسليم[٢].

---

(١) د. عبـد الغنـى محمـود، تسليم المجرمين على أساس المعاملة بالمثل، الطبعـة الأولى، دار النهضة العربيـة، القاهرة، ١٩٩١، ص ٢٣ وما بعدها.

- د. عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دراسة تحليلية تأصيلية، رسالة دكتوراه مقدمة لكلية الحقوق- جامعة المنصورة، ١٩٩٩، ص ٣٢٠ وما بعدها.

- د. إيهـاب يوسـف، اتفاقيات تسليم المجرمين ودورها فى تحقيق التعاون الدولى لمكافحة الإرهاب، رسالة دكتوراه مقدمة لكلية الدراسات العليا بأكاديمية الشرطة، ٢٠٠٣، ص ٤١.

-Starke ,J .G ,.Introduction to International Law10 ,th ed ,.Butterworths ,London ,1989 ,pp 294 .et seq.

- José Francisco Rezek, Reciprocity as a basis of Extradition, B.Y.B.I.L, Vol. 52, Issue 1, 1981, pp. 171 et seq.

(٢) وقـد عالجـت الاتفاقيات الدولية حالة انعقاد الاختصاص لأكثر من دولة وتعدد طلبـات التسليم التى تستهدف مجرماً واحداً بعينه، ومثال ذلك ما تضمنته اتفاقية تسليم المجرمين لدول الجامعة العربية لعام ١٩٥٣، حيث نصت المادة (١٣) منها على أنه=

٥- ألا يكـون الشخص المطلوب تسليمه من رعايا الدولـة المطلوب إليها التسليم: إن المبدأ السائد فى القانون الدولى يقضى بعدم إجبار الدولة على تسليم رعاياها، كما أن غالبيـة المعاهـدات والقوانين الداخلية المتعلقة بتسليم المجرمـين تكاد تُجمع على الأخذ بهذا المبدأ، بينما تأخذ بعض الدول الأنجلوسكونية بمبدأ تسليم الرعايا.

٦- أن تكون الجريمة المطلوب من أجلها التسليم جريمة عادية: يقصد هنا بالجريمة العاديـة تلك التى لا تقع ضمن مجموعة معينة من الجرائم لا ينطبق عليها نظام تسليم المجرمـين فيما بين الدول.. حيث جرى العـرف على عدم جواز التسليم بالنسبة لبعض الجرائم، كالجرائم السياسية والجرائم العسكرية والجرائم الموجهة ضد الأديان.

٧- توافـر أدلـة كافية لمحاكمة الشخص المطلوب أو لتبريـر الحكم الصادر عليه: لا توافق العديد من الدول على تسليم الشخص المطلوب إلى الدولة الطالبة، إلا إذا أرفقت بطلب التسليم الأوراق القضائية المشتملة على الأدلة الكافية لاتهام الشخص الهارب أو لتبرير الحكم الصادر عليه، ويعد ذلك أحد الضمانات المكفولة للشخص المطلوب، على أساسـ أن الحرية الشخصية للإنسان قد كفلتها المواثيـق الدولية والدساتير الوطنية، ومـن ثَـمَّ فإنه لا يجوز الاعتـداء على حرية هذا الشخص إلا بعـد التأكد من وجود أدلة دامغة تبرر تسليمه للدولة الطالبة.

ثالثًا- إجراءات تسليم المجرمين:

إن إجـراءات تسليم المجرمـين تختلف من دولة لأخرى وفقًا للنظـام الذي تتبعه كل دولـة، ففى معظم الدول تتم إجراءات التسليم عن طريق سلطتها التنفيذية التى تتولى البـت فى طلبات التسليم، بينمـا يتم إسناد تلك الإجـراءات إلى السلطة القضائية فى بعض الدول، وتأخذ دول أخرى بالنظام الإدارى القضائى أو المختلط[١]. إلا أنه بالرغم

= «إذا تقدمـت للدولـة المطلوب إليهـا التسليم عدة طلبات من دول مختلفة بشأن تسليم متهـم بذاته من أجل نفس الجريمة، فتكـون الأولوية فـى التسليم للدولة التى أضرت الجريمة بمصالحها، ثم للدولة التى ارتكبـت الجريمة فى إقليمها، ثم للدولة التـى ينتمـى إليهـا المطلوب تسليمه. أما إذا كانـت طلبات التسليم خاصـة بجرائم مختلفة فتكون الأولويـة للدولة التى طلبت التسليم قبل غيرها».

راجع: اتفاقية تسليم المجرمين بين دول جامعة الدول العربية لعام ١٩٥٣، على الرابط التالى:

- https://dftp.gov.ps/uploads/1623136174.pdf

(١) د. محمد فاضل، التعاون الدولى فى مكافحة الإجرام، مرجع سابق، ص ١٧٠.

مـن اختلاف نظم التسليم فإن هناك قواعد متعارف عليها فى إجراءات التسليم تُجمع الدول على الأخذ بها **وتتمثل فى:**

١- طلـب التسليم: إن التسليم عمل مـن أعمال السيادة لا تباشره إلا حكومة الدولة الطالبـة، حيث تتقدم بطلـب التسليم إلى حكومة الدولة المطلـوب إليها التسليم لكونها المكلفـة بملاحظـة واستعمال حق السيادة علـى إقليمها، ووسيلـة الاتصال المعترف بها دوليًّـا بين الحكومات هى الطريق الدبلوماسى، وقد جـرى العرف على قبول هذا المبدأ بـين الدول ونصـت عليه أغلـب المعاهـدات والاتفاقيـات الدولية، وتعتـبر بعض الدول - كفرنسـا- تقديم الطلب بالطريق الدبلوماسى ضمانًـا لرسمية الوثائق، بينما تذهب دول أخـرى - كالولايات المتحـدة - إلى التشدد فى رسمية الوثائق فتشترط توقيعها من عدة جهات رسمية حتى يتم قبولها لدى القضاء[١].

وقـد نصـت العديد مـن الاتفاقيـات على أنه يجـب على الدولـة الطالبـة أن ترفق بطلـب التسليم كافة البيانات الخاصة بالشخص المـراد تسليمه، والتى تتضمن صورته الفوتوغرافيـة وعلاماته المميزة وأوصافه وأمر القبض الصادر ضده والأدلة التى تثبت إدانتـه مـع بيان نوع الجريمة التـى ارتكبها والنصوص القانونية التـى تنطبق على هذه الجريمـة. وفى حالة صـدور حكم ضده فيجـب إرسال الحكم القضائـى الذي يقضى بإدانته أو صورة رسمية منه مع بيان مدة العقوبة التى حكم عليه بها[٢].

٢- الإجـراءات التـى تتخذها الدولـة المطلوب إليهـا التسليم: بمجـرد وصول طلب التسليـم إلى الدولـة المطلوب إليها التسليم فإنها تقـوم بالتحرى عن الشخص المطلوب وإلقاء القبـض عليه، وفى حالة الاستعجال تستعين الدولة المطلوب إليها التسليم بما تم إرسالـه إليها من مستندات وتصدر أمر القبـض بناءً على هذه المستندات لحين وصول ملـف التسليم، وفى جميع الحالات فإن معظم الاتفاقيات قد حددت مدة معينة للقبض المؤقـت أقصاها ستون يومًا، كما حـددت مدة معينة لعملية التسليـم يتعين على الدولة

(١) د. عبـد الرحيـم صدقى، تسليم المجرمين فى القانون الـدولى، المجلة المصرية للقانون الدولى، المجلـد ٣٩، القاهرة، ١٩٨٣، ص ١٠٤ وما بعدها.

(٢) إلهـام محمد حسن العاقل، مبدأ عدم تسليم المجرمين فـى الجرائم السياسية، دراسة مقارنة، رسالة ماجستير مقدمة لكلية الحقوق - جامعة القاهرة، ١٩٩٢، ص ١٦٣.

الطالبــة أن تتسلم خلالها الشخصــ المطلوب، وهى غالبًا شهر واحد من تاريخ إبلاغها بالموافقــة علــى التسليم، فــإذا لم تتم عمليــة التسليم خلال هذه المدة فــإن على الدولة المطلــوب إليها التسليــم أن تطلق سراح المتهم، ولا تقبل النظر فــى طلب جديد للتسليم للشخص نفسه وللجريمة نفسها ومن الدولة الطالبة نفسها.

كمــا أجازت الاتفاقيات للدولة المطلوب إليها التسليم أن تطلب تأجيل التسليم لفترة معينــة يكون خلالها الشخص المطلوب ماثلًا أمام إحدى محاكمها لمحاكمته عن جريمة ارتكبها، أو يكون محكومًا عليه بعقوبة يتعين عليه قضاؤها. وفى بعض الحالات، قد يتعين أن يمــر الشخص المطلوب أثناء تسليمه عبر إقليم دولــة ثالثة، فيجب وفقًا للاتفاقيات الدولية أن يتم إخطار هذه الدولة رسميًا بإرسال صورة من المستندات مع قرار التسليم لكى تسهل مروره عبر إقليمها وتتخذ كافة الإجراءات اللازمة لذلك[١].

٣- الآثار المترتبة على تسليم المجرمين:

بمجــرد قيــام الدولة المطلــوب إليها التسليــم بتسليم الشخص المطلــوب إلى الدولة الطالبة فإنه يترتب على ذلك أثر مهم يتمثل فى عدم جواز قيام الدولة الأخيرة بمعاقبة الشخصــ المسلــم إليهــا إلا عن الجريمة التــى سُلم مــن أجلها، وهو ما يعــرف «بمبدأ التخصيــص» Principe de Spécialité. والغرض الأساسى مــن هذا المبدأ هو الحيلولة دون لجوء الدولة الطالبة إلى التحايل وإخفاء ظروف معينة مرتبطة بالجريمة المطلوب مــن أجلهــا التسليم قد تحول دون التسليــم إذا عرفتها الدولة المطلــوب إليها[٢]. وعليه فإنه لا يجوز للدولة الطالبة أن تحاكم الشخص المسلم إليها عن أى جريمة اقترفها قبل التسليم ما لم تكن هى الجريمة التى من أجلها تم التسليم، إذ يجب على الدولة أن تلتزم بما ورد فى طلب التسليم من وقائع.

وقــد تضمنت أغلب الاتفاقيات الدولية الخاصة بتسليم المجرمين بعض الاستثناءات لمبــدأ التخصيص، حيث أجازت ملاحقة الشخصــ أو معاقبته عن جرائم ارتكبها قبل التسليم فى حالتين: أولاهما، إذا كان هذا الشخص قد أتيحت له حرية ووسيلة الخروج

(١) إلهام العاقل، مبدأ عدم تسليم المجرمين فى الجرائم السياسية، مرجع سابق، ص ١٦٥ وما بعدها.
(2) José Francisco Rezek, Reciprocity as a basis of Extradition, op. cit., p. 195.

من إقليم الدولة المسُلم إليها ولم يغادره خلال ثلاثين يومًا بعد الإفراج النهائى عنه، أو خـرج منه وعاد إليه باختياره. والحالة الثانية: إذا وافقت الدولة التى سلمته على ذلك، بشرط الحصول على موافقتها وفقًا للإجراءات المتبعة فى طلبات التسليم[١].

ويتبين مما سبق أن نظام تسليم المجرمين هو نظام حيوى تسعى الدول من خلاله إلى تفعيـل التعاون القضائى فيما بينها لمكافحة الجرائـم الإلكترونية، والحد قدر الإمكان من آثارها الوخيمة، إلا أن هذا النظام ما زال يعاني من معوقات وصعوبات من الناحية التطبيقيـة، من أبرزها تمسك الدول بمبدأ السيـادة الوطنية، وعدم توحيد التشريعات الجنائية ذات الصلة بتسليم المجرمين، وغيرها.

المطلب الثالث

التحديات التى تواجه التعاون الدولى فى مكافحة الجرائم الإلكترونية

فـى ظـل عالم متخـم بشبـكات الاتصـال والتواصل المتطـورة التى تغطـى أرجاء المعمـورة، وتنقل وتديـر المعلومات والبيانات مـن مسافات بعيدة باستخـدام تقنيات لا تكفـل لها أمنًـا كاملاً، أصبحت الجرائم الإلكترونية تتصـدر معدلات الجرائم العابرة للحـدود، وباتت تهـدد الأمن الاقتصادى والاجتماعى والسياسـى فى شتى بقاع العالم. وعلـى الرغم من تطوير وتغيير المفاهيم القانونيـة فى سبيل مكافحة هذه الجرائم فما زالـت هناك مجموعة من المعوقات والصعوبات التى تعرقل الجهود الدولية الرامية إلى وضع حد لتلك الجرائم، **وتتمثل هذه المعوقات فيما يأتي:**

أولًا- عدم وجود نموذج موحد للنشاط الإجرامى:

إن مـن أكثر الصعوبات التى تواجه التعاون الدولى فى مكافحة الجرائم الإلكترونية هـى عدم وجود توافق بين الأنظمة القانونية فى مختلف بلدان العالم حول نموذج موحد للنشاط الإجرامى المكون للجرائم الإلكترونية، فما يكون مجرمًا فى بعض الأنظمة قد لا يكـون كذلك فى أنظمة أخرى؛ مما يؤدى إلى اختلاف عناصر الجريمة الإلكترونية من

(١) د. سلامـة إسماعيـل محمـد، تعريض وسائل المواصلات للخطـر فى القانون الجنائـى، مع دراسة تحليليـة لظاهرتى خطف الطائرات والإرهاب، دار النهضة العربية، القاهرة، ١٩٩٨، ص ٥٥٨.

دولة لأخرى. ومرد ذلك إلى عدة أسباب وعوامل أهمها اختلاف البيئات والثقافات من مجتمـع لآخر، وبالتالى اختلاف السياسة الجنائية من دولـة لأخرى؛ الأمر الذي يغرى قراصنة الحاسبات على ارتكاب جرائمهم دون خشية من الملاحقة والعقاب[١].

ثانيًا- صعوبة إثبات الجرائم الإلكترونية:

مـن أهم ما يميز الجرائم الإلكترونية أنها غير ظاهـرة، أى لا يلحظها المجني عليه غالبًـا أو يدري حتى بوقوعها، فهـى غالبًا ما تُكشف بمحض الصدفة أو بعد مضى وقت طويـل على ارتكابها؛ ولذلـك توصف بالجريمة غير المرئية، ومما يزيد الأمر تعقيدًا هو أن الجريمة الإلكترونية تتم عن بُعد حيث لا يوجد الفاعل على مسرح الجريمة. كما أن المجـرم فى هذه الجرائم يحاول قدر الإمكان إعاقة الوصول إلى الدليل بشتى الوسائل، أو يلجأ إلى تشفير البيانات ومحو دليل الإدانة فى زمن قياسى؛ الأمر الذي يصعب معه الوصول إلى دليل إدانته[٢].

فالفعـل الإجرامـى فى هذه الجرائم ليس لـه آثار مادية، حيث يكـون الدليل مجرد نبضـات إلكترونيـة غير محسوسة، ممـا يتطلب من المحقق أن تكـون لديه دراية علمية كافية بأنظمة الحاسـب وتقنية تشغيلها، حتى يتسنى له التعامل معها والبحث عن أدلة والمحافظـة عليهـا، هذا مـن ناحية. ومن ناحيـة أخرى، غالبًا ما يعمـد الجناة فى تلك الجرائـم إلى استخـدام أسمـاء مستعارة، والولـوج إلى الشبكـة المعلوماتية عن طريق حاسبـات عموميـة، كتلك المتاحة فى محـال الإنترنت؛ الأمر الذي يجعـل من الصعوبة بمكان تحديد هويتهم[٣].

ثالثًا- اختلاف النظم القانونية الإجرائية:

إن تنـوع واختـلاف النظم القانونية الإجرائية بين دولـة وأخرى قد يؤدى إلى إفلات الجناة من الملاحقة والعقاب، فطرق التحرى والتحقيق والمحاكمة التى يثبت فاعليتها فى دولة ما قد تكون عديمة الجدوى فى دولة أخرى، أو قد لا يُسمح بإجرائها من الأساس،

(١) هنـد نجيـب، إشكاليات التعـاون القضائى فى مجال الجرائم الإلكترونيـة، المجلة الجنائية القوميـة، المركز القومى للبحوث الاجتماعية والجنائية، المجلد ٥٩، العدد الثانى، يوليو ٢٠١٦، ص ١٤٣.

(٢) خالـد عيـاد الحلبى، إجراءات التحرى والتحقيق فى جرائم الحاسوب والإنترنـت، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١١، ص ٢٦٠.

(٣) حشيفة عبد الهادى، التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، مرجع سابق، ص ٤٩.

كما هـو الحال بالنسبة للمراقبـة الإلكترونية، والتسليم المراقـب، والعمليات المستترة، وغيرها من الإجراءات المشابهة. فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية فى دولة معينة، فقد تكون الطريقة ذاتها غير مشروعة فى دولة أخرى. وهذا يعنى صعوبة التنسيق بين الدول المختلفة فيما يتعلق بالإجراءات الجنائية المتبعة بشأن الجرائم الإلكترونية[١].

رابعًا- تنازع الاختصاص القضائى الدولي[٢]:

تعـد الجرائم الإلكترونية، لمـا تتميز به من سمات وخصائـص وكونها من الجرائم العابـرة للحدود، من أكـثر الجرائم التى يثار بشأنها تنـازع الاختصاص القضائى بين الـدول، الـذي ينشأ نتيجة اختـلاف التشريعات والنظم القانونية بـين هذه الدول فيما يتعلـق بالجرائـم الإلكترونية. فقد يحدث أن تُرتكب الجريمـة فى إقليم دولة معينة من قبل شخـص أجنبى، فهنا تكون الجريمة خاضعة للاختصاص الجنائى للدولة الأولى استنـادًا إلى مبـدأ الإقليميـة، وتخضع كذلـك لاختصاص الدولة الثانيـة التى يحمل الجانى جنسيتها استنادًا إلى مبدأ الاختصاص الشخصى، وقد تكون هذه الجريمة من الجرائـم التى تهدد أمن دولـة ثالثة وسلامتها، فتدخل عندئذ فى اختصاصها استنادًا إلى مبدأ العينية[٣].

خامسًا- تمسك الدول بمبدأ السيادة الوطنية:

ويعنـى هـذا المبـدأ أن الدولة هى السلطـة العليا التـى لا تعلوها سلطـة فى الداخل والخارج، بما يعنيه ذلك من استئثار جهة الحكم فى الدولة بكافة اختصاصات السلطة ومظاهرهـا، دون أن تخضـع فى ذلك لأى جهـة أعلى، ودون أن تشـارك معها فى ذلك سلطة أو جهة مماثلة[٤].

---

(١) د. عـادل عبد العال إبراهيم خراشى، إشكاليات التعـاون الدولى فى مكافحة الجرائم الإلكترونية وسبل التغلب عليها، مرجع سابق، ص ٢٣٧-٢٣٨.

(٢) يقصـد بالاختصاص القضائى تلـك السلطة التى يقررها القانون للقضاء فى أن ينظر فى دعاوى من نوع معين حدده المشرع، والأصـل أن ينسـب هذا الاختصاص إلى قضاء الحكم، وأن يكون موضوعه تخويـل القضاء سلطة الفصل فى الدعوى. راجع: د. محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، ١٩٨٨، ص ٨٢٣.

(٣) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مرجع سابق، ص٢١١.
د. جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى، مرجع سابق، ص ٧٣.

(٤) د. أحمد شوقى أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٨٥ وما بعدها.

فعندمـا يرتكـب فرد جريمة ما مـن الجرائـم الإلكترونية فى دولـة معينة، وتجرى محاكمتـه فـى دولة أخرى، فمن البديهى البحث عن كافـة أدلة الجريمة فى البلد محل الواقعـة بحسبـان أنها البلد التى كانت مسرحًا لتلك الجريمـة، وذلك فى إطار التعاون القضائى بين الدول، غير أن هذا التعاون قد يصطدم بمبدأ السيادة الوطنية الذي كان سائدًا فى ظل القانون الدولى التقليدى، حيث ما زالت بعض الدول تتمسك بالفصل فى كافـة المنازعات التى تثـار على أراضيها لاعتبارات ترتبط بفكـرة السيادة؛ الأمر الذي يعوق التعاون القضائى بين الدول فى مكافحة الجرائم الإلكترونية[١].

سادسًا- قصور التشريعات الجنائية:

بالرغـم مـن إصـدار الـدول للعديد مـن التشريعـات الجنائية المتعلقـة بالجرائم الإلكترونيـة، وانضمامهـا للاتفاقيات الدوليـة ذات الصلة بهذه الجرائـم، إلا أن هذه التشريعـات مـا زالت قاصـرة وغير كافيـة البتة لمعالجـة سائر الجرائـم الإلكترونية التـى تتسـم بالانتشار والتطور السريـع، الأمر الذي يؤدى إلى خـروج بعضها من نطاق التجريم[٢].

ولئـن كانـت العديد من التشريعـات تنطوى علـى قواعد عامة يمكـن تطبيقها على الجرائـم التقليديـة، إلا أنه نظرًا لاختـلاف أركان وشروط الجرائـم الإلكترونية عنها فـى التقليديـة، فإنه يترتب على ذلـك عدم إمكانية تطبيق هـذه القواعد على الجرائم الإلكترونيـة، الأمر الذي من شأنـه إعاقة مهام الأجهزة الأمنيـة والقضائية فى ضبط هذه الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة[٣].

(١) د. فتـوح عبـد الله الشاذلى، القانون الدولى الجنائى، أوليات القانون الـدولى الجنائى، النظرية العامة للجريمة الدولية، دار النهضة العربية، القاهرة، ٢٠٠٢، ص ٢٠٣.

(٢) حشيفة عبد الهادى، التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، مرجع سابق، ص ٤٨.

(٣) د. عـادل عبد العال إبراهيم خراشى، إشكاليات التعـاون الدولى فى مكافحة الجرائم الإلكترونية وسبل التغلب عليها، مرجع سابق، ص ٢٤٠.

الخاتمة

فـــى ظـل ثورة المعلومـــات التى يعيشهـــا عالمنا المعاصـــر أصبحنا نعيش حيـــاة ملؤها الاتصـــالات ونقل وتبـــادل المعلومات والبيانـــات الدولية والوطنية على حـد سواء؛ الأمر الـذي ساعد كل كيان على التعامل مع مختلف النظم المتقدمة، وأضحى العالم بمثابة قرية صغيرة، وتحرر الإنسـان من قيـود المكان. إلا أن هذه الثورة المعلوماتية قد صاحبها ظهـور نوع جديد من الجرائم، أطلـق عليهـا «الجرائم الإلكترونية»، التى باتت تتصدر معـدلات الجرائم العابـرة للحدود، وتهدد الأمـن الاقتصادى والاجتماعـى والسياسى والعسكرى فى كافة دول العالم، وتسبب أضرارًا وخسائر فادحة فى مختلف القطاعات.

ولمواجهة الخطر المحدق والخسائر التى تسببها الجرائم الإلكترونية، اتجهت العديد من دول العالم إلى سن قوانين جنائية خاصة أو عدلت قوانين العقوبات لديها، بما يكفل مواجهة هذه الجرائم، بيد أن هذه الدول قد واجهت العديد من الصعوبات فى مكافحة تلـك الجرائم متعدية الحدود عبر قوانينها الوطنية. ونظـرًا للانتشار الواسع والسريع للأضـرار الناجمة عن الجرائـم الإلكترونية، لم يعد بوسع الدول منفـردة أن تواجهها مهمـا كانت إمكانياتها، وكان من الضرورى توحيد جهـود الدول لمواجهة هذا النوع من الإجـرام، وذلـك من أجل الوصـول إلى مفاهيم موحدة للمكافحـة، وإعداد مشروعات القوانـين التى تسير على هديها، والاستفادة من تجارب بعضها البعض فى هذا الشأن، وإبرام اتفاقيات دولية لمواجهة هذه الظاهرة.

وقـد بُذلـت بالفعل العديـد من الجهـود الدولية لمواجهـة الجرائـم الإلكترونية فى إطـار المنظمات الدولية، خاصة فى إطار منظمـة الأمم المتحدة، وغيرها من المنظمات الإقليمية، حيث تبنت تلك المنظمات عقد مؤتمرات وإبرام اتفاقيات دولية لمكافحة هذه الظاهرة الإجرامية. ولعل من أهم الاتفاقيات التى تناولت الجرائم الإلكترونية اتفاقية بودابسـت لعـام ٢٠٠١ بشأن الجرائم السيبرانية المنبثقة عـن اتفاقيات مجلس أوروبا، والتـى تهدف إلى مساعدة الدول الأطراف فى مكافحة الجرائم الإلكترونية. والاتفاقية العربيـة لمكافحـة جرائم تقنيـة المعلومات لعـام ٢٠١٠ التى تهـدف إلى تعزيز وتدعيم التعـاون بين الدول العربية فى مجـال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

وإزاء اتساع مسرح ارتكاب الجرائم الإلكترونية على المستوى الدولى، وسهولة حركة العناصر الإجرامية وتنقلها وهروبها أواختفائها، لجأت الدول إلى تبنى عدة آليات للتعاون الدولى، من أهمها التعاون الأمنى الدولى والتعاون القضائى الدولى، لمواجهة ضراوة الإجرام وظواهره المختلفة فى كافة البلدان. إلا أن الممارسة الدولية قد أظهرت وجود معوقات تواجه التعاون الدولى فى مكافحة الجرائم الإلكترونية وتحد من فاعليته.

فى ضوء ما تقدم، ومن أجل تفعيل دور التعاون الدولى فى مكافحة الجرائم الإلكترونية، أقترحُ التوصيات التالية:

١- يتعين على الدول الأعضاء فى منظمة الأمم المتحدة دعوة الجمعية العامة إلى تبنى اتفاقية دولية بشأن مكافحة الجرائم الإلكترونية، من خلال إصدارها قرارًا تكلف بموجبه لجنة القانون الدولى التابعة للأمم المتحدة بإعداد مشروع اتفاقية فى هذا الشأن، ثم الدعوة لعقد مؤتمر دولى تحت رعاية الأمم المتحدة لاعتماد هذه الاتفاقية.

٢- ضرورة سعى الدول إلى إبرام اتفاقيات متعددة الأطراف بهدف توحيد أنماط وأشكال الجريمة الإلكترونية على مستوى القوانين الوطنية، وتسليم المجرمين، وتعزيز التعاون الدولى فيما بينهم، بحسبان أن التعاون الدولى هو السبيل الوحيد لمعالجة المشكلات القائمة ذات الصلة بمكافحة الجرائم الإلكترونية.

٣- تشجيع الدول على الانضمام للاتفاقيات الدولية القائمة ذات الصلة بمكافحة الجرائم الإلكترونية، والعمل على دمج أحكام هذه الاتفاقيات ضمن قوانينها الوطنية.

٤- حث الدول على سرعة الاستجابة لمكافحة الجرائم الإلكترونية، والعمل على سرعة حفظ الأدلة المعلوماتية للجريمة، خاصة وأن الجناة غالبًا ما يعمدون إلى إتلافها أو إخفائها أو طمس معالمها.

٥- تشجيع الدول المتقدمة على دعم ومساعدة الدول النامية فى بناء وتعزيز مؤسساتها المتخصصة فى التحرى والملاحقة والتحقيق والمحاكمة، فضلاً

عـن إمدادها بالتقنيـات الحديثة وتدريب أفرادها علـى كشف وضبط الجرائم الإلكترونية.

٦- حـث الدول علـى تبنى مبـدأ الاختصاص الجنائى العالمى فـى مواجهة الجرائم الإلكترونية عبر الوطنية، حيث تتم معاقبة الجانى أينما يُلقى القبض عليه، بغض النظـر عن مـكان ارتكاب الجريمة، أو جنسية الجانـى أو المجنى عليه، أو طبيعة المصالـح المعتدى عليها، إذ إن إعمال هـذا المبدأ من شأنه تمكين سلطات الدولة مـن ملاحقة مرتكبى هذه الجرائم أينما وجـدوا، متجاوزة بذلك مبدأ الإقليمية والخلافات الناشئة عن تنازع الاختصاص.

٧- عقـد نـدوات ومؤتمـرات علميـة حول مخاطـر الجرائـم الإلكترونية علـى أمن الأشخاص والمؤسسـات والـدول، ونشر الوعـى بين المواطنين من خـلال وسائل الإعلام، وتفعيل دور المجتمع المدنى والمنظمات غير الحكومية فى هذا الشأن.

قائمة المراجع

أولًا - المراجع العربية:

- **إبراهيـم أحمد خليفـة**، القانون الـدولى الدبلوماسى والقنصلـى، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧.
- **أحمـد إبراهيم مصطفـى سليمان**، الإرهاب والجريمة المنظمـة: التجريم وسُبل المواجهة، دار الطلائع للنشر والتوزيع، القاهرة، ٢٠٠٦.
- **أحمـد خليفـة الملط**، الجرائـم المعلوماتيـة ، دار الفكر الجامعـى، الإسكندرية ، ٢٠٠٦.
- **أحمـد شوقـى أبو خطوة**، شـرح الأحكام العامـة لقانون العقوبـات، دار النهضة العربية، القاهرة، ٢٠٠٧.
- **أحمـد محمد عبد المعبود**، الجريمة الإلكترونية وآليـة مكافحتها فى ظل القانون الـدولى، مجلة البحـوث القانونيـة والاقتصادية، الصادرة عـن كلية الحقوق – جامعة المنوفية، المجلد ٣١، العدد ٢، ٢٠١٩.
- **أمجد حسن مرشـد الدعجة**، استراتيجية مكافحة الجرائـم المعلوماتية، رسالة ماجستـير مقدمة لمعهـد البحوث والدراسات الاستراتيجيـة – جامعة أم درمان الإسلامية، السودان، ٢٠١٤.
- **إلهام محمـد حسن العاقل**، مبدأ عدم تسليم المجرمـين فى الجرائم السياسية، دراسة مقارنة، رسالة ماجستير مقدمة لكلية الحقوق – جامعة القاهرة، ١٩٩٢.
- **أمـين تجينـى**، الجرائـم المعلوماتيـة، مجلـة استشـراف للدراسـات والأبحاث القانونية، العدد ٦، المغرب، ٢٠٢٠.
- **إيهـاب يوسـف**، اتفاقيـات تسليم المجرمين ودورهـا فى تحقيق التعـاون الدولى لمكافحـة الإرهـاب، رسالة دكتـوراه مقدمـة لكلية الدراسـات العليـا بأكاديمية الشرطة، ٢٠٠٣.

- **جميل عبد الباقى الصغير**، الإنترنت والقانون الجنائى: الأحكام الموضوعية لجرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٢.
- **حامد سلطان**، القانون الدولى العام فى وقت السلم، دار النهضة العربية، القاهرة، ١٩٦٢.
- **حسن بن أحمد الشهرى**، قانون دولى موحد لمكافحة الجرائم الإلكترونية، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، مجلد ٢٧، العدد ٥٣، الرياض، ٢٠١١.
- **حسين بن سعيد الغافرى**، السياسة الجنائية فى مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩.
- **حشيفة عبد الهادى**،التعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، رسالة ماجستير مقدمة لكية الحقوق والعلوم السياسية، جامعة زيان عاشور – الجلفة، الجزائر، ٢٠١٩-٢٠٢٠.
- **حكيم سياب**، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، جامعة الجلفة، العدد الأول، الجزائر، ٢٠٠٩.
- **حيمر عبد الكريم**، منظمة الإنتربول، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٣- ٢٠١٤.
- **خالد بن مبارك القحطانى**، التعاون الأمنى الدولى ودوره فى مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه مقدمة لجامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٦.
- **خالد عياد الحلبى**، إجراءات التحرى والتحقيق فى جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١١.
- **ذياب موسى البداينة**، الجرائم الإلكترونية: المفهوم والأسباب، ورقة عمل مقدمة للملتقى العلمى بشأن الجرائم المستحدثة فى ظل المتغيرات والتحولات الإقليمية والدولية،عمان، ٢٠١٤.

- **ذنايب آسية**، الآليات الدولية لمكافحة الجريمة المنظمة عبر الدولية، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة الأخوة منتورى، قسنطينة، الجزائر، ٢٠٠٩- ٢٠١٠.
- **سالم محمد سليمان الأوجلى**، أحكام المسئولية الجنائية عن الجرائم فى التشريعات الوطنية، رسالة دكتوراه مقدمة لكلية الحقوق – جامعة عين شمس، القاهرة، ١٩٩٧.
- **سامى يس خالد**، الجهود الدولية لمكافحة الجرائم المعلوماتية، مجلة الدراسات العليا، جامعة النيلين، المجلد ٤، العدد ١٤، الخرطوم، ٢٠١٦.
- **سعيد بن سالم البادى وآخرون**، الجريمة الإلكترونية فى المجتمع الخليجى وكيفية مواجهتها، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، ٢٠١٦.
- **سلامة إسماعيل محمد**، تعريض وسائل المواصلات للخطر فى القانون الجنائى، مع دراسة تحليلية لظاهرتى خطف الطائرات والإرهاب، دار النهضة العربية، القاهرة، ١٩٩٨.
- **سليمان أحمد محمد فضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، رسالة دكتوراه مقدمة لكلية الدراسات العليا بأكاديمية الشرطة، القاهرة، ٢٠٠٧.
- **صالح مصطفى البرغثى**، قضية لوكربى، دراسة فى القانون الدولى، رسالة دكتوراه مقدمة لكلية الحقوق- جامعة عين شمس، ١٩٩٨.
- **صورية بوربابة**، التعاون الدولى فى مكافحة الجرائم المعلوماتية، مجلة القانون الدولى للدراسات البحثية، جامعة طاهرى محمد - بشار، العدد الأول، الجزائر، ٢٠١٩.
- **طارق سرور**، الاختصاص الجنائى العالمى، دار النهضة العربية، القاهرة، ٢٠٠٦.
- **عادل عبد العال إبراهيم خراشى**، إشكاليات التعاون الدولى فى مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون بتفهنا الأشراف، العدد ١٦، الجزء الأول، ٢٠١٤.

- **عبد الرءوف مهدى،** شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠١٥.
- **عبد الرحمن فتحى سمحان،** تسليم المجرمين فى ظل قواعد القانون الدولى، دار النهضة العربية، القاهرة، ٢٠١١.
- **عبد الرحيم صدقى،** تسليم المجرمين فى القانون الدولى، المجلة المصرية للقانون الدولى، المجلد ٣٩، القاهرة، ١٩٨٣.
- **عبد الغنى محمود،** تسليم المجرمين على أساس المعاملة بالمثل، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩١.
- **عبد الفتاح بيومى حجازى،** مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧.
- **عبد الفتاح محمد سراج،** النظرية العامة لتسليم المجرمين، دراسة تحليلية تأصيلية، رسالة دكتوراه مقدمة لكلية الحقوق - جامعة المنصورة، ١٩٩٩.
- **عبد المنعم سليمان،** الجوانب الإشكالية فى النظام القانونى لتسليم المجرمين، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧.
- **عبد الوهاب حومد،** التعاون الدولى لمكافحة الجريمة، مجلة الحقوق والشريعة، العدد الأول، الكويت، فبراير ١٩٨١.
- **عبيشات أمينة،** الجرائم الإلكترونية بين المواثيق الدولية والتشريعات الوطنية، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد ٦، العدد الأول، الجزائر، ٢٠٢١.
- **عثمان الصديق أحمد محمد،** الجرائم الإلكترونية فى القانون السودانى، دراسة مقارنة على ضوء الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة ٢٠٠٢، رسالة ماجستير مقدمة لكلية القانون - جامعة الخرطوم، بدون سنة نشر.
- **عكروم عادل،** المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٣.

- **عمـر سالم،** الإنابة القضائية الدولية فى المسائل الجنائية، دار النهضة العربية، القاهرة، ٢٠٠١.
- **فتوح عبد الله الشاذلى،** القانون الدولى الجنائى، أوليات القانون الدولى الجنائى، النظرية العامة للجريمة الدولية، دار النهضة العربية، القاهرة، ٢٠٠٢.
- **فريحـة محمد كـريم،** الجريمـة الإلكترونيـة، مجلة شئـون اجتماعيـة، جمعية الاجتماعيين فى الشارقة، المجلد ٢٨، العدد ١١٠، الإمارات، ٢٠١١.
- **فنـور حاسـين،** المنظمـة الدوليـة للشرطة الجنائيـة والجريمة المنظمـة، رسالة ماجستـير مقدمة لكلية الحقوق بن عكنون – جامعة الجزائر، الجزائر، ٢٠١٢-٢٠١٣.
- **كلود فالاكس،** المنظمة الدولية للشرطة الجنائية، بحث فى المجلة الدولية للشرطة الجنائية، الطبعة العربية، العدد ٣٨٧، أبريل ١٩٨٥.
- **محمـد أحمـد سليمـان عيسـى،** الجهـود الدوليـة الإقليميـة لمواجهـة الجرائم الإلكترونية، مجلة العلوم القانونية، الصادرة عن كلية الحقوق – جامعة عجمان، المجلد ٤، العدد ٨، يوليو ٢٠١٨.
- **محمد السعيد الدقاق،** التنظيم الدولى، الطبعة الثالثة، الدار الجامعية للطباعة والنشر، بيروت، ١٩٨٤.
- **محمد أمـين الشوابكة،** جرائـم الحاسوب والإنترنت؛ الجريمـة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١.
- **محمد حسام لطفى،** الحجية القانونية لبرامج الحاسب الإلكترونى، دار النهضة العربية، القاهرة، ١٩٩٨.
- **محمد رضا الديب،** حقوق الإنسان، بدون ناشر، القاهرة، ٢٠١٤- ٢٠١٥.
- **محمـد فاضل،** التعاون الـدولى فى مكافحـة الإجرام، منشـورات جامعة حلب، سوريا، ١٩٩٢.

- **محمد منصور الصاوى**، أحكام القانون الدولى المتعلقة بمكافحة الجرائم ذات الطبيعة الدولية، دراسة فى القانون الدولى الاجتماعى فى مجال مكافحة الجرائم الدولية للمخدرات وإبادة الأجناس واختطاف الطائرات وجرائم أخرى، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٤.
- **محمود محمد شرشر**، الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مجلة البحوث القانونية والاقتصادية، الصادرة عن كلية الحقوق – جامعة المنوفية، المجلد ٥٤، العدد ٣، أكتوبر ٢٠٢١.
- **محمود نجيب حسنى**، النظرية العامة للقصد الجنائى، دراسة تأصيلية مقارنة للركن المعنوى فى الجرائم العمدية، دار النهضة العربية، القاهرة، ١٩٨٨.
- شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، ١٩٨٨.
- **مخلد إبراهيم الزعبى**، فاعلية القوانين والتشريعات العربية فى مكافحة الجرائم الإلكترونية، المجلة العربية للنشر العلمى، العدد ٣٧، الأردن، ٢٠٢١.
- **مقدر منيرة**، التعاون الدولى فى مكافحة الجريمة المنظمة، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٤-٢٠١٥.
- **منير محمد الجنبيهى**، تزوير التوقيع الإلكترونى، دار الفكر الجامعى، الإسكندرية، ٢٠٠٦.
- **نائلة عادل قورة**، جرائم الحاسب الآلى الاقتصادية، دراسة نظرية تطبيقية، منشورات الحلبى الحقوقية، بيروت، ٢٠٠٥.
- **نهلا عبد القادر المومنى**، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨.
- **هالة أحمد الرشيدى**، الجهود الدولية فى مجال مكافحة الجرائم الإلكترونية: دراسة للخبرتين الأوروبية والعربية، مجلة الديمقراطية، مؤسسة الأهرام، مجلد ١٩، العدد ٧٥، القاهرة، ٢٠١٩.

- **هـدى قشقوش**، جرائم الحاسب الآلى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.
- **هنـد نجيب**، إشكاليات التعاون القضائـى فى مجال الجرائم الإلكترونية، المجلة الجنائيـة القوميـة، المركز القومى للبحـوث الاجتماعية والجنائيـة، المجلد ٥٩، العدد الثانى، يوليو ٢٠١٦.

ثانيًا- مواقع إلكترونية:

مكتب الأمم المتحدة المعنى بالمخدرات والجريمة (UNODC)، على الرابط التالى:

- https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-nternational-cooperation-mechanisms.html

- مجلس أوروبا Council of Europe على الرابط التالى:

- https://www.britannica.com/topic/Council-of-Europe

- الاتفاقيـة المتعلقة بالجريمة الإلكترونية، بودابسـت، مجلس أوروبا، على الرابط التالى:

- https://rm.coe.int/budapest-convention-in-arabic/1680739173

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ على الرابط التالى:

- https://adlm.moj.gov.sa/alqadaeya/attach/882.pdf

- موقع المنظمة الدولية للشرطة الجنائية (الإنتربول) على الرابط التالى:

- https://www.interpol.int/ar/Internet

- مجلس وزراء الداخلية العرب، على الرابط التالى:

- https://www.aim-council.org/about/emergence-of-the-council/#

- المعاهـدة النموذجيـة لتبـادل المساعدة فى المسائـل الجنائية لعـام ١٩٩٠، على الرابط التالى:

- https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR090/559// IMG/NR055990.pdf?OpenElement

- اتفاقيـة الأمم المتحـدة لمكافحة الجريمة المنظمة عـبر الوطنية لعام ٢٠٠٠ على الرابط التالى:

- https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-a.pdf

- اتفاقية الرياض العربية للتعاون القضائى لعام ١٩٨٣ على الرابط التالى:

- https://www.pacc.ps/uploads/books/2/book-101-cat-2-d-0615-01-.pdf

ثالثًا- المراجع الأجنبية:

- Bushra Mohamed Elamin Elnaim، Cyber Crime in Kingdom of Saudi Arabia: The threat today and the expected future، Journal of Information and Knowledge Management، Vol. 3، No. 12، 2013.

- Eric R. Leukfeldt R.، S. Veenstra، and Wouter Stol، High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands، International Journal of Cyber Criminology (I.J.C.C.)، No. 7 (1)، January 2013.

- Feraud H. and Sclanitz E.، La Coopération Policière Internationale، Revue Internationale de Droit Pénal، Vol. 45، 1974.

- Franklin Clark and Ken Diliberto، Investigating Computer Crime، 1st Edition، Routledge and CRC Press، 1996.

- Henri Alterman et Alain Bloch، La Fraude Informatique، Paris، 1988.

- Jean Pradel، Droit Pénal Général، 19e edition، Cujas، Paris، 2012.

- Jonathan O. Hafen، International Extradition: Issues Arising Under Dual Criminality Requirement، BYU Law Review، U.S.A.، 1992.

- José Francisco Rezek، Reciprocity as a basis of Extradition، B.Y.B.I.L، Vol. 52، Issue 1، 1981

- Klaus Tiedemann، Fraudes et autres délits d'affaires commis à l'aide d'ordinateurs électroniques، RDPC، No. 7، Bruxelles، 1984.
- Kurt Von Schuschnigg، International Law: An Introduction to the Law of Peace، the Bruce Publishing Co.، Milwaukee، 1959.
- Malcolm Anderson، Policing the World: Interpol and the Politics of International Police Co-operation، Clarendon Press، Oxford، 1989.
- Michael Akehurst، A Modern Interoduction to International Law، Third Edition، George Allen and Unwin Ltd.، London، 1977.
- Russel Fox، Justice in the 21st Century، 1st Edition، Routledge-Cavendish، London، 1999.
- Starke، J. G.، Introduction to International Law، 10th ed.، Butter-worths، London، 1989،
- Sylvette Guillemard، Le Droit International Privé face au contrat de vente cyberspatial، Thèse de Doctorat présentée en cotutelle à la Faculté des études supérieures de l'Université LAVAL-Québec، Janvier 2003.

Reports & Studies:

- UNODC United Nations Office on Drugs and Crime، Comprehen-sive Study on Cybercrime، United Nations، New York، 2013.
- Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders، United Nations، A/CONF.18715/، Vienna، 1017-April 2000.