التعاون الوطني والدولي في الجرائم الإلكترونية
المشكلات والحلول

د.جمال محمد خلفان محمد النقبي [1]
د. سلطان محمد سالم عوض هيسان المصعبي[2]

الملخص:

تسعى الدراسة إلى التعرف على التعاون الوطني والدولي في الجرائم الإلكترونية، والمشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية وسبل مواجهتها.

ومن أهم نتائجها: من الأجهزة المختصة في التعاون الأمني في مكافحة الجرائم الإلكترونية بدولة الإمارات العربية المتحدة: المباحث الإلكترونية بشرطة دبي، وإدارة الأدلة الجنائية الإلكترونية بشرطة دبي، ويتعاون معهما مركز دبي للأمن الإلكتروني. وعلى المستوى الاتحادي: الهيئة الوطنية للأمن الإلكتروني، والهيئة العامة لتنظيم قطاع الاتصالات. وتعمل الأجهزة المختصة بالدولة على التعاون الأمني فيما بينهم للحد من الجرائم الإلكترونية، وذلك من خلال جمع البيانات والمعلومات الخاصة بالجريمة عن طريق مأموري الضبط القضائي، وقيامهم بالبحث والتحري والمراقبة عن الجرائم ومرتكبيها، وجمع الأدلة التي تؤدي إلى كشف الحقيقة؛ لتقديمها إلى جهة التحقيق.

وتعد الاتفاقية الأوروبية بودابست لمكافحة الجرائم الإلكترونية لعام 2001م هي الاتفاقية الوحيدة على مستوى العالم التي عملت على تحقيق الحماية الإجرائية والعقابية

(1) دكتوراه في القانون العام
(2) دكتوراه في القانون العام

للنظم الإلكترونية، ولا توجد أيُّ اتفاقياتٍ أخري على مستوى العالم سواها، وتستطيع جميعُ دول العالم الانضمامَ إليها. وعلى مستوى الدول العربية والإقليمية؛ فلا توجد إلا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م. وهناك معوِّقاتٌ تواجه التعاونَ الدولي في الجرائم الإلكترونية، ومن أهمها: اختلال التشريعات الوطنية وتطبيق القواعد التقليدية في الجرائم الإلكترونية، واختلاف النظم القانونية الإجرائية الجنائية، وتنازع الاختصاص القضائي الدولي وهاجس المساس بالسيادة الإقليمية والقومية، فضلًا عن الصعوبات المتعلقة بالمساعدات القضائية الدولية، وعدم وجود قنوات الاتصال المرجوة من التعاون الدولي في مجال الجريمة الإلكترونية. وتواجه التعاون الوطني في الجرائم الإلكترونية معوِّقاتٌ، وتتمثل في: أنها تُرتكب في بيئة النظم الإلكترونية التي تعد هدف المجرم المعلوماتي، وأنها جريمةٌ عابرةٌ للحدود الوطنية، وعدم وجود اتفاقياتٍ ومعاهداتٍ دوليةٍ كافيةٍ للتعاون الدولي في مجال مكافحتها.

الكلمات الدالة: التعاون، الدولي، الجرائم، الإلكترونية، المشكلات، الحلول.

Abstract:

The study seeks to identify national and international cooperation in cybercrimes, the problems facing national and international cooperation in cybercrimes, and ways to confront them.

Among its most important results: Among the agencies specialized in security cooperation in combating cybercrimes in the United Arab Emirates are the Dubai Police Electronic Investigations and the Dubai Police Electronic Forensics Department, with which the Dubai Electronic Security Center cooperates. At the federal level: the National Electronic Security Authority and the General Authority for Regulating the Telecommunications Sector. The competent agencies of the state work on security cooperation among themselves to reduce cybercrimes, by collecting data and information related to the crime through judicial police officers, and by them conducting research, investigation and monitoring of crimes and their perpetrators, and collecting evidence that leads to revealing the truth. To be submitted to the investigation body.

The Budapest European Convention against Cybercrime of 2001 is the only agreement in the world that has worked to achieve procedural and punitive protection for electronic systems. There are no other agreements in the world except it, and all countries of the world can join it. At the level of Arab and regional countries; There is only the Arab Convention on Combating Information Technology Crimes of

2010. There are obstacles facing international cooperation in cybercrimes, the most important of which are: the imbalance of national legislation and the application of traditional rules in cybercrimes, the differences in criminal procedural legal systems, the conflict of international jurisdiction and the obsession with violating regional and national sovereignty, in addition to the difficulties related to international judicial assistance, and the lack of communication channels. Expected international cooperation in the field of cybercrime. National cooperation in cybercrime faces obstacles, which are: that it is committed in the environment of electronic systems that are the target of the information criminal, that it is a crime that crosses national borders, and that there are no sufficient international agreements and treaties for international cooperation in the field of combating it.

Keywords: cooperation, international, diversity, electronics, challenges, solutions.

المقدمة:

تشكل الجريمة إحدى القضايا الرئيسة في دول العالم أجمع، ونتيجة للتطور المذهل في الاتصالات وتكنولوجيا المعلومات، والانتشار الواسع والسريع لها أدى إلى ظهور أشكالٍ وأنماطٍ جديدةٍ من الجرائم لا سيما المتعلقة منها بالشبكة الإلكترونية التي باتت تشكل خطرًا ليس على سرية النظم الحاسوبية أو سلامتها فحسب؛ بل تعدت إلى أمن النظم المعلوماتية، وقد فطن المجتمع الدولي إلى أن مرتكبيها أصبحوا يبسطون نفوذهم إلى جميع أرجاء العالم، بفضل ما يملكونه من قوةٍ ونفوذٍ ودهاءٍ؛ لذا بادر المجتمع الدولي إلى الاهتمام بضرورة التعاون الدولي واتخاذ الإجراءات التي تهدف إلى مكافحتها[1].

وإن الجرائمَ الإلكترونية عابرةٌ للحدود الدولية بين كل دول العالم، ولا بد من التعاون الأمني الدولي بين السلطات في البلد الذي كان مَنْشَأً للجريمة، أو من السلطات في البلد التي عبر من خلالها للنشاط المجرّم، وهو في طريقه إلى الهدف؛ فلا بد من التعاون الأمني الدولي لمكافحة هذه الجرائم، وقد أثبت الواقعُ العملي أن الدولة لا تستطيع – بجهودها المنفردة – القضاءَ على الجرائم الإلكترونية، وبخاصةٍ مع هذا التطور المذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الشبكة الإلكترونية. ومع تميزها بالعالمية، وبكونها عابرةً للحدود؛ فإن مكافحتها لا تتحقق إلا بوجود تعاونٍ دوليٍّ

[1] د. عادل عبد العال إبراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015م، ص7.

على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة[1].

أولاً: مشكلة الدراسة:

تكمن مشكلة الدراسة في أنه لا يمكن مواجهةُ الجرائم الإلكترونية بدون تعاونٍ دوليٍّ؛ لكونها عابرةً للحدود الوطنية، ولا تستطيع دولةٌ بمفردها مواجهتَها، ولكن هناك معوقات تواجه تلك التعاون، حيث يواجه مأمورو الضبط القضائي وسلطة التحقيق والقضاء إعاقة الوصول إلى الدليل التقني من خلال مشكلات إجراءات الحصول عليه بين الدول؛ لتعارضه مع مبدأ سيادة الدولة على أراضيها، ولاختلاف النظم القانونية الإجرائية، والمشكلات المتعلقة بتنازع الاختصاص القضائي، وبالمساعدات القضائية الدولية، لذا لابد من التغلب على المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية.

ثانياً: أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

1- التعرف على التعاون الوطني والدولي في الجرائم الإلكترونية.

2- التعرف على المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية وسبل مواجهتها.

[1] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009م، ص393-395.

ثالثاً: تساؤلات الدراسة:

التساؤلات الكامنة وراء مشكلة الدراسة:

1- ماهي التعاون الوطني في مواجهة الجرائم الإلكترونية؟

2- ما هي التعاون الدولي في مواجهة الجرائم الإلكترونية؟

3- ماهي المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية؟

4- ما هي سبل مواجهة المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية؟

رابعاً: أهمية الدراسة:

تبرز أهمية الدراسة في إلقاء الضوء على التعاون الوطني والدولي في الجرائم الإلكترونية، كما هي في الواقع بطريقةٍ علميةٍ منظمةٍ قائمةٍ على الانتقاء من بين عناصر التعاون الوطني والدولي موضوع الدراسة، ولن نقف عند هذا الحد؛ بل سنعمل على تفسير البيانات، وتحليلها؛ للوقوف على نقاط القوة والضعف في التشريعات والاتفاق والاختلاف بينهم، واستخراج الاستنتاجات ذات الدلالة والمغزى بالنسبة لمشكلة الدراسة، ووضع حلولٍ إجرائيةٍ عمليةٍ للمشكلات المتعلقة بالتعاون الوطني والدولي الجرائم الإلكترونية.

خامساً: منهج الدراسة:

سوف تعتمد الدراسة على منهجية علمية تحليلية وتوصيفية، لرصد وتحليل التعاون الوطني والدولي في الجرائم الإلكترونية، المشكلات والحلول، وذلك من خلال الاعتماد على الكتب والدراسات المختصة ذات الصلة بموضوع الدراسة.

سادساً: خطة الدراسة:

المبحث الأول: التعاون الوطني والدولي في الجرائم الإلكترونية

المطلب الأول: التعاون الوطني في مواجهة الجرائم الإلكترونية.

المطلب الثاني: التعاون الدولي في مواجهة الجرائم الإلكترونية.

المبحث الثاني: المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية وسبل مواجهتها:

المطلب الأول: المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية.

المطلب الثاني: سبل مواجهة المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية.

المبحث الأول

التعاون الوطني والدولي في الجرائم الإلكترونية

تمهيدٌ، فتقسيمٌ:

لا يمكن مواجهةُ الجرائم الإلكترونية بدون تعاونٍ دوليٍّ؛ لكونها عابرةً للحدود الوطنية، ولا تستطيع دولةٌ بمفردها مواجهتَها، وسنتناول في هذا المبحث التعاونَ الوطني والدولي في مواجهتها، وعليه؛ يرى الباحث ضرورة تقسيم هذا المبحث إلى المطلبين الآتييْن:

المطلب الأول: التعاون الوطني في مواجهة الجرائم الإلكترونية.

المطلب الثاني: التعاون الدولي في مواجهة الجرائم الإلكترونية.

المطلب الأول

التعاون الوطني في مواجهة الجرائم الإلكترونية

سنتعرف في هذا المطلب إلى التعاون الوطني من قبل الأجهزة المختصة في مواجهة الجرائم الإلكترونية، وذلك على النحو الآتي:

تشمل الاستراتيجياتُ الوطنية إنشاءَ أجهزةٍ مختصَّةٍ بمكافحة الجرائم الإلكترونية، وتحقيق الأمن المعلوماتي، وغالبًا ما تعتمد من مجموعة واسعة من أصحاب المصلحة المختلفين، ويشارك أصحاب المصلحة المتنوعون في العملية الأمنية؛ لأن أجزاءً من هذه البنية التحتية تُدار من قبل التعاون بين هذه الأطراف، وهي مفيدةٌ لهم[1].

[1] Neil Robinson and Luke Gribbon, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime, Legal, Regulatory and

ومن هذا المنطلق؛ نشير إلى أنه من الأجهزة المختصة في التعاون الأمني في الجرائم الإلكترونية في دبي، إدارة المباحث الإلكترونية بالقيادة العامة لشرطة دبي، وكانت بدايتها في عام 2002م، حيث تم تشكيل قسم الجرائم الإلكترونية، وفي البداية كان نطاق البلاغات محدودًا، ولم يكن هناك الوعيُ الكافي لدى الجمهور بمدى خطورة التهجم الإلكتروني من خلال مجرمي المعلوماتية، وكيفية التعامل مع أساليبه، وبخاصةٍ عن طريق الاختراقات الإلكترونية، وفي عام 2008م تم تحويل قسم مكافحة جرائم الكمبيوتر إلى إدارة المباحث الإلكترونية، وتقسيمها إلى عدة أقسام من حيث الأساليب والبلاغات الواردة إلى مراكز الشرطة، وفي عام 2009م أُنشِئَتْ الدورياتُ الإلكترونية؛ للتصدي للجرائم الإلكترونية بكل أنواعها، ومحاربتها حتى قبل وقوع الجريمة[1].

وعليه؛ شكَّلت شرطةُ دبي وحداتٍ تحتوي على فرق عمل متخصصةٍ في المجال التقني ضمن إدارة المباحث الإلكترونية، وإدارة الأدلة الإلكترونية، وتعد إدارة المباحث الإلكترونية بشرطة دبي من أهم الإدارات التي تتعامل مع الجرائم الإلكترونية؛ حيث تعتمد آلية العمل لديها على جمع المعلومات وتحليلها، والتَّقَصِّي عن أي أدلةٍ تخص المجرمين؛ فيقوم مأمور الضبط القضائي بإعداد ملفٍ متكاملٍ يعتمد من خلاله على طبيعة مجريات حالة التبليغات والشكاوى المقدمة من المجني عليهم، وذلك عبر

Operational Factors Affecting CERT Co-operation with Other Stakeholders, op, cit, 2012, p29.

[1] الراشد سالم عبيد سالمين ولد راحة: عرض التجارب والخبرات الأمنية المختلفة في التعامل مع جرائم تقنية المعلومات مركز بحوث الشرطة، أكاديمية شرطة دبي، دبي، الطبعة الأولى، 2010م، ص69.

الحصول على إذنٍ رسميٍّ من النيابة العامة أو المحكمة للشروع في العمل، ثم يبدأ – بعد ورود البلاغ عن الجرائم عبر الدوريات الإلكترونية أو أي طُرُقٍ أخرى للبلاغ – بجمع أكبر كَمٍّ من المعلومات والأدلة التي تخص المجرمَ المعلوماتي، سواء أكان ذلك عبر الحاسوب الآلي أم الشبكة الإلكترونية أم الهواتف الذكية أم غيرها من الأجهزة الإلكترونية، ومن ثَمَّ القبض على المجرم، ويكون هذا بالتعاون مع إدارة الأدلة الجنائية بشرطة دبي التي تفحص هذه الأجهزةَ؛ لمعرفة مكان الجاني وهُوِيَّتِه، ثم تحويله إلى النيابة العامة مع الأدلة التي تفيد في التحقيق[1].

ومن هذا المنطلق؛ فإن إدارة المباحث الإلكترونية بشرطة دبي تعمل – من خلال القسم الإداري الذي يتبعه فرع الأرشيف والقضايا – على حفظ كل المعلومات عن مرتكبي الجرائم وتسجيلها، وأسلوب ارتكابهم لها، وكذلك حفظ وتسجيل القضايا، وعمل الإحصائيات الخاصة بها. فضلًا عن فرع الاتصال والمتابعة الذي يختص بعملية الاتصال والمتابعة مع الجهات الأمنية والمؤسسات المختلفة التي تتطلبها عمليات البحث والتحري في متابعة القضايا الإلكترونية المختلفة. فضلًا عن القسم الفني – يتبعه فرع برامج القرصنة وفرع برامج المحادثات – الذي يهدف إلى تحقيق الدقة المطلوبة في مجال متابعة البحث والتحريات في الجرائم الإلكتورنية. فضلًا عن القسم الميداني الذي يتبعه فرع الانتقال والمتابعة، وفرع مقاهي الإنترنت. وتعمل الإدارة وأقسامها على التعاون الأمني، ومكافحة جرائم الاختراق والاحتيال والاستيلاء على مال

[1] د. خالد خلفان أحمد المنصوري: إطلالة معرفية على شبكات التواصل الإجتماعي "الفيسبوك – التويتر – اليوتيوب"، أكاديمية شرطة دبي، دبي، 2013م، ص119–121.

الغير أو الإتلاف أو التدمير وغيرها من الجرائم التي تهدد الأمن المعلوماتي، وبعد ذلك تعمل على البحث والتحري، ثم ملاحقة مرتكبيها، والقبض عليهم، وتقديمهم للعدالة الجنائية[1].

وفي سبيل العمل والتنسيق تتعاون مع إدارة المباحث الإلكترونية إدارة الأدلة الجنائية الإلكترونية بشرطة دبي؛ إذ لها دورٌ كبيرٌ في إثبات الجرائم الإلكترونية، فهي تتسلم الأجهزة المُتَحَصَّلَة من الجرائم مغلقةً ومختومةً بإحكامٍ، ومرفق معها ملف القضية، وتعمل – من خلال خبراء برامج الحاسوب الآلي والشبكة الإلكترونية والهواتف الذكية – على تصويرها، وبعدها يتم استخدام البرامج الخاصة لفحص أجهزة الحاسوب الآلي أو الشبكة الإلكترونية أو الهواتف الذكية بأحدث البرامج المتطورة في هذا الشأن[2].

وتستخدم شرطةُ دبي أحدثَ الأنظمة لحفظ البيانات والمعلومات، وتعد برامج مقاومة الفيروسات من أهم النظم التي تعمل على حماية نظم المعلومات، فضلًا عن التشفير والإخفاء للمعلومات التي يتم تبادلها مع الجهات الأمنية، واستخدام أحدث البرامج لمنع الاختراق والتعدي على البيانات والمعلومات، ووضع أجهزةٍ مُرَاقِبَةٍ؛ لرصد أي تسللٍ ودخولٍ غير مُصَرَّحٍ به لنظم البيانات والمعلومات بشرطة دبي، بالإضافة إلى

---

[1] د. أيمن عبد الحفيظ: مكافحة الجرائم المستحدثة، أكاديمية شرطة دبي، دبي، الطبعة الأولى، 2006م، ص221-222.

[2] مريم عثمان عبد القادر: الحماية الجنائية للطفل من الجرائم الإلكترونية في ضوء القانون الإماراتي، دراسات قانونية، رسالة ماجستير، أكاديمية شرطة دبي، كلية الدراسات العليا، دبي، 2104م، ص217.

استقطاب خبراء حماية نظم المعلومات، ووضع حواجزَ أَمنيةٍ عند مداخل مراكز المعلومات والخطوط والشبكات، وهي من أهم الطرق الكفيلة للحدِّ من التحديات التي تهدد مراكزَ المعلومات والبيانات الأمنية بشرطة دبي[1].

ويتعاون معهم مركز دبي للأمن الإلكتروني الذي يعمل على تأمين وحماية المعلومات وشبكة الاتصالات وأنظمة المعلومات الحكومية بحكومة وإمارة دبي، والجهات الحكومية المختلفة، ومنها: الدوائر الحكومية، والهيئات والمؤسسات العامة، والمجالس، والمناطق الحرة، وجهات حكومة دبي المختلفة. ويتلقى المركزُ الشكاوى والمقترحات المتعلقة بأمن المعلومات الحكومية، ثم يقوم بدوره بمكافحة الجرائم الإلكترونية والشبكة المعلوماتية، وتقنية المعلومات على مختلف أنواعها، فضلًا عن دوره في وضع الخطط الاستراتيجية لمواجهة أي أخطارٍ أو تهديداتٍ أو اعتداءاتٍ على المعلومات الحكومية؛ بالتنسيق مع الجهات الحكومية المعنية، وتطوير استخدام الوسائل الحديثة في مجال الأمن الإلكتروني، ورفع كفاءة طرق حفظ المعلومات، ووضع سياسة إمارة دبي في مجال أمن المعلومات الحكومية وتنفيذها، إضافة إلى إشرافه على التزام الجهات الحكومية بتنفيذ متطلبات الأمن الإلكتروني، وتقديم الدعم الفني والاستشاري لكل الجهات الحكومية بإمارة دبي، ونشر الوعي بأهمية الأمن الإلكتروني بالتنسيق مع الجهات الحكومية والإقليمية والدولية[2].

---

[1] زكي أحمد الجبلي: تأمين المعلومات في الأزمات الأمنية، دراسة تطبيقية لتأمين المعلومات بشرطة دبي، أكاديمية شرطة دبي، دبي، 2013م، ص321-323.

[2] المواد 1 و4 و5 من قانون رقم 11 لسنة 2014 في شأن مركز دبي للأمن الإلكتروني.

ويقوم مركز دبي للأمن الإلكتروني بالمراقبة في سبيل عدم تعرض شبكة الاتصالات وأنظمة المعلومات بإمارة دبي لأي عمليات اختراقٍ غير مشروعةٍ، وله كشف مواقع الخلل في شبكة الاتصالات وأنظمة المعلومات؛ لتجنب حصول أي مخالفاتٍ لأحكام هذا القانون[1].

ولموظفي مركز دبي للأمن الإلكتروني صفة مأموري الضبط القضائي في إثبات الجرائم الواقعة بالمخالفة لأحكام القانون، وتحرير محاضر الضبط اللازمة في شأن الجرائم الإلكترونية التي يتم ضبطها، وإخطار النيابة العامة المختصة بالإجراء الذي اتخذه المركز في الجرائم الواقعة بالمخالفة لأحكام القانون خلال أسبوع؛ لتكملة الإجراءات المناسبة[2].

وفي سبيل التعاون والتنسيق على المستوى الاتحادي تعمل الهيئة الوطنية للأمن الإلكتروني على التعاون والتنسيق مع الأجهزة المحلية المعنية بمكافحة الجرائم الإلكترونية؛ حيث صدر المرسوم بقانون اتحادي رقم (3) لسنة 2012م بإنشاء الهيئة الوطنية للأمن الإلكتروني، وهي تتبع المجلس الأعلى للأمن الوطني بدولة الإمارات العربية المتحدة، وتتمتع بالصلاحيات التنفيذية والرقابية اللازمة لممارسة أعمالها؛ وفقًا لأحكام القانون، ومقرها بمدينة أبوظبي، ولها أن تُنشئ فروعًا داخل دولة الإمارات وخارجها[3].

---

[1] المادة 14 من القانون رقم 11 لسنة 2014 في شأن مركز دبي للأمن الإلكتروني.

[2] المادة 15 و18 من القانون رقم 11 لسنة 2014 في شأن مركز دبي للأمن الإلكتروني.

[3] المادة 2 و3 من المرسوم بقانون اتحادي 3 لسنة 2012 بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني.

وتعمل الهيئة الوطنية للأمن الإلكتروني – التابعة للمجلس الأعلى للأمن الوطني بدولة الإمارات العربية المتحدة بالتعاون مع الجهات الحكومية الاتحادية والمحلية المعنية بشؤون الأمن الإلكتروني داخل الدولة – على حماية شبكة الاتصالات ونظم المعلومات ونظم التحكم الإلكتروني من الوصول غير المصرح به، مع تأمين وحماية الشبكة الإلكترونية وشبكة الاتصالات ونظم المعلومات[1].

وعليه؛ تختص الهيئة بتأمين وحماية الشبكة الإلكترونية وشبكة الاتصالات ونظم المعلومات وعمليات جمع المعلومات باستخدام أيٍّ من الوسائل الإلكترونية لدى كل الجهات بالدولة؛ فهي تتأكد من فاعلية عمل أنظمة حماية شبكة الاتصالات ونظم المعلومات لدى الجهات الحكومية والخاصة، والإشراف على مدى التزام الجهات المعنية بتنفيذ متطلبات الأمن المعلوماتي التي أصدرتها، ومتابعة تنفيذها، وكذلك مكافحة جرائم الحاسوب الآلي والشبكة الإلكترونية وتقنية المعلومات باختلاف أنواعها، والتنسيق مع الجهات المعنية والإقليمية والدولية فيما يتعلق بمجال عملها، وتقديم الدعم الفني لكل الجهات الحكومية والخاصة، وتلقي الشكاوى والمقترحات المتعلقة بالأمن المعلوماتي بالدولة، ويكون لموظفيها صفة مأموري الضبط القضائي في إثبات ما يقع بالمخالفة لأحكام قانون الأمن الإلكتروني[2].

---

[1] المادة 1 من مرسوم بقانون اتحادي 3 لسنة 2012 بشأن إنشاء الهيئة الوطنية للأمن الإلكترونية.

[2] المواد 1 و4 و21 من مرسوم بقانون اتحادي 3 لسنة 2012 بشأن إنشاء الهيئة الوطنية للأمن الإلكترونية.

كما تقوم الهيئة الوطنية للأمن الإلكتروني بدولة الإمارات العربية المتحدة – من خلال مأموري الضبط القضائي – بضبط الجرائم الإلكترونية الواقعة على الأفراد والجهات الحكومية والخاصة، وإخطار النيابة العامة المختصة بالإجراء التي اتخذته خلال أسبوع، لتقوم بدورها بتكملة الإجراءات المناسبة حيالها[1].

وتتعاون معهم الهيئة العامة لتنظيم قطاع الاتصالات؛ فهي السلطة المختصة بالرقابة على قطاع الاتصالات والمرخص لهم، وتأمين خدمات الاتصالات في جميع أنحاء الدولة، وحماية خطوط وشبكات الاتصالات في الدولة، ويكون لموظفيها صفة مأموري الضبط القضائي بالنسبة للجرائم التي تقع بالمخالفة لأحكام قانون تنظيم الاتصالات[2].

وتعمل وزارة الداخلية بدولة الإمارات العربية المتحدة في سبيل التعاون والتنسيق بدورٍ فعَّالٍ في مكافحة "الجرائم الإلكترونية" حيث تمثل هذه الجرائم تحديًا جديدًا يضاف إلى التحديات التي تواجه السلطات الأمنية بالدولة وبكل دول العالم. ويعود بروز هذه الظاهرة إلى شيوع خدمات الإنترنت، وما يصاحبها من استغلال المجرمين لتلك التقنية، وتبرز جهود وزارة الداخلية في إسهامها في تحقيق مكافحة الجريمة، وجعل الإمارات أكثر البلدان أمنًا على مستوى العالم، والمخاطر التي تهدد الأفراد والمؤسسات والدولة

---

[1] المادة 14 و21 من مرسوم بقانون اتحادي 3 لسنة 2012 بشأن إنشاء الهيئة الوطنية للأمن الإلكترونية.

[2] المواد 1 و13 و57 و58 و59 و81 مكرر، من المرسوم بقانون اتحادي رقم 3 لسنة 2003، بشأن تنظيم قطاع الاتصالات.

من قبل مجرمي المعلوماتية[1]. وقد بادرت دولة الإمارات العربية المتحدة – من خلال جهود وزارة الداخلية – بخطواتٍ جريئةٍ؛ لضمان حماية الأفراد والمؤسسات من محاولات استغلال المجرمين للشبكة الإلكترونية في ارتكاب الجرائم الإلكترونية، ومنها:

1- إنشاء قاعدة معلومات متطورة تهتم بحصر عناصر "مجرمي المعلوماتية" التي تستخدم الشبكة الإلكترونية في الداخل والخارج، ومعرفة الجماعات والجهات والخلايا التي تدعمهم وأهدافهم ومخططاتهم.

2- تسهيل إجراءات تبادل المعلومات – بصفةٍ عاجلةٍ – وفق طرقٍ وأساليبَ سريةٍ مُحْكَمَةٍ بين الأجهزة الأمنية المعنية داخل الدولة لمكافحة الجرائم الإلكترونية.

3- إقامة تعاون فعَّال بين الأجهزة المعنية وبين المواطنين، وإيجاد ضماناتٍ وحوافزَ مناسبةٍ؛ لتشجيعهم على الإبلاغ عن أي "جرائم معلوماتية" تستخدم الشبكة الإلكترونية، وتقديم المعلومات التي تساعد في الكشف عنها، والتعاون في القبض على مرتكبيها.

4- تشديد إجراءات المراقبة الداخلية لمعرفة الأشخاص الذين لهم تَوَجُّهَاتٌ وميولٌ تجاه "الجرائم الإلكترونية" في الخارج، واتخاذ جميع التدابير الأمنية اللازمة؛ لتحجيم نشاطهم، ومنعهم من تفعيل هذه النشاطات داخليًّا وخارجيًّا.

---

[1] مريم عثمان عبد القادر: الحماية الجنائية للطفل من الجرائم الإلكترونية، في ضوء القانون الإماراتي، مرجع سابق، ص197.

5- تكثيف اللقاءات والاجتماعات الدورية بين الأجهزة الأمنية، وتبادل وجهات النظر والمعلومات المستجدة، وإعادة تقييم المواقف من آنٍ إلى آخرَ؛ لمنع أي "جرائم معلوماتية" عن طريق الشبكة الإلكترونية.

6- عدم توفير الملاذ الآمن لمن يُمَوِّلُون الأعمال الإرهابية "الإلكترونية"، أو يديرونها، أو يدعمونها، أو يرتكبونها، ولمن يوفرون الملاذ الآمن للإرهابيين.

7- رصد أسماء الأشخاص المتورطين في أعمالٍ إرهابيةٍ عن طريق الشبكة الإلكترونية في القائمة السوداء، وتعميمها على المطارات والموانئ والمنافذ الحدودية.

8- الدورات التدريبية التي تنظمها وزارة الداخلية بصفةٍ دوريةٍ للعاملين لديها لمكافحة الجرائم الإلكترونية؛ لتزويدهم بالوسائل الفنية والتقنية المساعدة لكشف هذه الجرائم.

9- دعم وتشجيع البحوث الأمنية ومراكز البحوث والدراسات، وحَثّها على دراسة الجرائم الإلكترونية وتحليلها؛ للتعرف إلى أسبابها وأساليبها ووسائلها، والآثار الناجمة عنها، وكيفية مواجهتها، ودراسة ما يقع من الإجرام المعلوماتي وتحليله، واستخلاص أوجه القصور في الاستعداد أو المواجهة؛ لتلافيها، وتحقيق تطويرٍ مستمرٍ في هذا المجال.

10- تبادل المعلومات الجنائية مع شُعَب الاتصال بالدول العربية والمكتب العربي للشرطة الجنائية، والتنسيق والتعاون معها في هذا المجال.

11- تبادل المعلومات الجنائية – ومنها المعلومات عن الجرائم الإلكترونية – مع المكاتب المركزية للشرطة الدولية (الإنتربول) في الدول الأعضاء في المنظمة الدولية وأماناتها العامة، والتنسيق والتعاون معها في هذا المجال.

12- تجاوب وزارة الداخلية لطلبات الدول التي تتقدم للحصول على معلومات في شأن "الجرائم الإلكترونية"، وذلك من خلال شُعبة الاتصال بالإنتربول؛ حيث تعمل الأجهزة الأمنية على تبادل المعلومات الجنائية – ومنها المعلومات عن الجرائم "الإلكترونية" – مع المكاتب المركزية للشرطة الدولية (الإنتربول) في الدول الأعضاء في المنظمة الدولية وأماناتها العامة، والتنسيق والتعاون معها في هذا المجال[1].

وعليه؛ فإن الأجهزة الأمنية المختصة "بالجرائم الإلكترونية" بدولة الإمارات العربية المتحدة تعمل في منظومة عملٍ موحدةٍ ومتجانسةٍ، وبالتعاون مع الجهات المعنية، وباقي الأجهزة الحكومية للدولة ومنظمات المجتمع المدني، وذلك من خلال المشاركة المجتمعية للقطاع الجماهيري، وبالتنسيق مع الأجهزة المناظرة للدول الشقيقة والصديقة؛ لتحقيق أعلى معدلات الأمن والاستقرار بما يقابل الأخطار والإفرازات الأمنية السلبية الناجمة عن المتغيرات والتطورات الإقليمية والعالمية في جميع المجالات، ولمواجهة كل أشكال "الجرائم الإلكترونية" الدخيلة على المجتمع؛ بهدف تهيئة المناخ المناسب لتحقيق

[1] د. محمد المتولي: التخطيط الاستراتيجي في مكافحة جرائم الإرهاب الدولي، دراسة مقارنة، مجلس النشر العلمي، جامعة الكويت، الطبعة الأولى، 2006م، ص394-399.

التنمية الشاملة التي تسعى الدولة إلى تحقيقها؛ وصولًا إلى مصافِّ الدول المتقدمة، وتوفير حياةٍ كريمةٍ للمواطنين والمقيمين، وذلك من خلال المراحل الآتية:

1- **المرحلة الأولى: مرحلة درء أو تفادي الجريمة:** في هذه المرحلة تتكاتف جميعُ أجهزة الدولة، وتتعاون – وفقًا لتخطيطٍ مسبقٍ – لاتخاذ كل الإجراءات والسياسات التي من شأنها الكشف المبكر عن بؤر التوتر الأمني، والعمل على سرعة تداركها، والتعامل معها؛ بهدف القضاء على الدوافع والأسباب التي تؤدى إلى وقع الجريمة أو إلى نشوب مخاطر "الجرائم الإلكترونية".

2- **المرحلة الثانية: مرحلة الاحتواء:** في حالة كشف مؤشرات وقوع "الجرائم الإلكترونية" وهي في مراحلها الأولى؛ فإن الجهات الأمنية والجهات المعنية الأخرى تركز جهودها في سرعة التدخل، واتخاذ الإجراءات العاجلة؛ لاحتواء الموقف، ومنعه من الانتشار.

3- **المرحلة الثالثة: مرحلة المكافحة:** في حالة الفشل في احتواء الموقف، أو وقوع الأزمة بصفةٍ غير متوقَّعةٍ، وفي حالة تصاعد القوة الدافعة لها؛ فيتم حشد كل الجهود والإمكانيات التي تتناسب مع طبيعة الموقف الأمني وحجمه؛ بغرض مواجهة الموقف، والانتصار عليه، وذلك من خلال منظومة إدارة أزماتٍ على درجةٍ عاليةٍ من الكفاءة.

4- **المرحلة الرابعة: مرحلة استعادة الأوضاع:** بعد النجاح في مواجهة الموقف أو الأزمة الأمنية "الإلكترونية" ومخاطرها؛ ينبغي اتخاذ كل الإجراءات اللازمة

لإزالة الآثار الناجمة عنها، وإعادة الأوضاع إلى ما كانت عليه، مع عدم إغفال تسجيل الدروس المستفادة والخبرات المكتسبة؛ للاستفادة منها مستقبلًا.

كما تلتزم الاستراتيجيةُ بالضوابط التي حدَّدها صاحب السمو رئيس الدولة التي تتضمن: أن السياسة الخارجية لدولة الإمارات العربية المتحدة ترتكز على قواعدَ ثابتةٍ أساسها الاحترام المتبادل، وحسن الجوار، وعدم التدخل في الشؤون الداخلية للآخرين، وإقامة العلاقات على أساس المصالح المتبادلة، وتنمية روح التعاون، وحل المشكلات والنزاعات بالطرق السلمية، والالتزام بالمواثيق العربية والإسلامية والدولية، والوقوف إلى جانب الحق والعدل، والمشاركة في تحقيق الأمن والسلم الدوليين، والعمل على دعم العمل العربي المشترك من خلال جامعة الدولة العربية ومؤسساتها ومنظماتها المتخصصة، وعلى تعزيز علاقاتها الثنائية مع كل الدول العربية الشقيقة، ونبذ كافة أشكال "الجرائم الإلكترونية" والعنف والتطرف والإرهاب، والالتزام بالقوانين والمواثيق والمعاهدات الدولية، كما أن الدولة تقف مع كل دعوة للسلام يمكنها أن تجنب العالم الوقوف على فوهة بركان يمكن أن ينفجر في أي لحظة[1].

ونخلص إلى القول، إن الأجهزة المختصة في مكافحة الجرائم الإلكترونية بدولة الإمارات العربية المتحدة تعمل على التعاون الأمني فيما بينهم للحدِّ من الجرائم الإلكترونية، من خلال جمع البيانات والمعلومات الخاصة بالجريمة عن طريق مأموري

[1] مروان جمعة بن بيات الفلاسي: انعكاسات الأزمات الإقليمية والعالمية الراهنة على الأمن والاستقرار الداخلي في دولة الإمارات العربية المتحدة، دراسات شرطية، سلسة الرسائل العلمية، أكاديمية شرطة دبي، كلية القانون وعلوم الشرطة، 2011م، ص243-244.

الضبط القضائي، وقيامهم: بالبحث، والتحري، والمراقبة عن الجرائم ومرتكبيها، وجمع الأدلة التي تؤدي إلى كشف الحقيقة؛ لتقديمهم إلى جهة التحقيق.

وفي سبيل التعاون والتنسيق بين الأجهزة المختصة التي تقوم بتأمين الشبكة الإلكترونية وشبكة الاتصالات ونظم المعلومات وحمايتها، كما تعمل على المواجهة الإجرائية للجرائم الإلكترونية، من خلال إنشاء قاعدة معلومات متطورة تهتم بحصر عناصر مجرمي الإلكترونية، فضلًا عن تشديد إجراءات المراقبة الداخلية؛ لمعرفة الأشخاص الذين لديهم توجهاتٌ وميولٌ تجاهها، واتخاذ جميع التدابير الأمنية اللازمة؛ لتحجيم نشاطهم، ومنعهم من تفعيله داخليًّا وخارجيًّا، ورصد أسماء الأشخاص المتورطين فيها في القائمة السوداء، وتعميمها على منافذ الدولة. إضافة إلى إقامة تعاونٍ فعَّالٍ بين الأجهزة المعنية بالدولة لمواجهة الجرائم الإلكترونية، والتنسيق مع الجهات المعنية والإقليمية والدولية فيما يتعلق بمجال الحدِّ منها، ويكون للموظفين في هذه الأجهزة الأمنية صفة مأموري الضبط القضائي في إثبات هذه الجرائم المخالفة لأحكام القانون المعلوماتي، وتتعاون الأجهزة المختصة بالدولة في القبض على المجرمين، وجمع الأدلة الإلكترونية، وإثباتها جنائيًّا على الجاني، ثم تحويله إلى النيابة العامة مع الأدلة التي تفيد في التحقيق.

وتجدر الإشارة إلى أنه من الأجهزة المختصة بالتعاون الأمني على المستوى الوطني في الجرائم الإلكترونية بفرنسا القسم الوطني لقمع جرائم المساس بالأموال والأشخاص الذي أُنشئ في عام 1997م، وهو متخصص في مكافحة جرائم الإنترنت لا سيما الجرائم الإلكترونية. كما أُنشئ المركزُ الوطني لمكافحة جرائم تكنولوجيا

المعلومات والاتصالات بفرنسا في 2000/5/15م لمكافحة هذه الجرائم المستحدثة، ويمارس هذا المكتب أعماله من خلال: وحدة العمليات، ووحدة المساعدة التقنية، ووحدة التحليل والتوثيق العملي، فضلا عن قسم الإنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية بفرنسا، ويختص بجمع الأدلة الرقمية[1].

ومن الأجهزة المختصة بالتعاون الأمني في الجرائم الإلكترونية بمصر إدارة مكافحة الجرائم المستحدثة التي أُنشئت عام 2002م، وهي متخصصة بمكافحة جرائم الحواسيب وشبكات المعلومات، وتتبع الإدارة العامة للمعلومات والتوثيق، وتختص بمكافحة وضبط الجرائم التي تقع على نظم شبكات المعلومات وقواعد البيانات باستخدام الحاسوب الآلي[2]، فضلًا عن "الجهاز القومي لتنظيم الاتصالات"؛ وفقًا للقانون رقم (175) لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات[3].

---

[1] صالح شنين: الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراة، جامعة أبوبكر بلقايد تلمسان، كلية الحقوق، غير منشورة، الجزائر، 2013م، ص215-218.

[2] د. حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، الكتاب الثالث، أكاديمية العلوم الشرطية، الشارقة، الطبعة الأولى، 2009م، ص61.

[3] المادة 1 من قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات المصري.

المطلب الثاني

التعاون الدولي في مواجهة الجرائم الإلكترونية

أولًا- التعاون الأمني الدولي:

تتضح أهمية التعاون الأمني من خلال تبني تقنيةٍ متطورةٍ لإجراء التحريات والتحقيقات في مجال مكافحة الجريمة الإلكترونية، باستخدام التكنولوجيا الحديثة في الاتصال مثل الدوائر التليفزيونية، واستعمال أساليب خاصة بالتحري والمراقبة، واستحداث قنوات للاتصال والتنسيق الأمني والقضائي بين جهات القضاء المختصة عن طريق الأقمار الصناعية، والشبكة الإلكترونية لتبادل المعلومات سريعًا، وانتقال القاضي إلى الدول المعنية للتحقيق، ولاتخاذ ما يراه من إجراءاتٍ ليس فقط في مرحلة التحقيق الابتدائي؛ بل وفي مرحلة الحكم أيضًا، ومراعاة تنفيذ الأحكام الأجنبية وفقًا لضوابطَ تتفق عليها الدولُ فيما بينها، من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتيْن، والاتفاق على معاييرَ موحدةٍ في هذا الشأن، كذلك الاتفاق على كيفية مصادرة الأموال محل الجريمة الإلكترونية عبر الحدود أو إرسال السجناء، وبخاصةٍ أن مرتكبها قد يحمل جنسية دولةٍ ما، ويشن الهجوم الفيروسي من حواسيبَ موجودةٍ بدولةٍ أخرى، وتقع آثاره المدمرة بدولةٍ ثالثةٍ؛ لذا فمن البديهي ألا تقف مشكلات الحدود والولايات القضائية عقبة أمام اكتشافها ومعاقبة مرتكبيها[1].

[1] د. فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2016م، ص471-473.

ومن هذا المنطلق؛ تعد الجرائمُ الإلكترونية عابرةً للحدود الدولية بين كل دول العالم؛ إذ يمكن – عن طريق جهاز الكمبيوتر والشبكة المعلوماتية – ارتكابُ العديد من الجرائم، مثل: جريمة الدخول إلى النظام المعلوماتي والبقاء فيه بدون تصريحٍ، والقرصنة، واعتراض رسائل البريد الإلكتروني والتحريف فيه وتغيير محتوياته، وإتلاف المعلومات، والتلاعب في أنظمة المعالجة الآلية للبيانات، وغيرها. لذا؛ فإنه لا بد من التعاون الأمني الدولي بين السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد التي عبر من خلالها للنشاط المجرَّم، وهو في طريقه إلى الهدف[1]؛ فلا بد إذن من التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية، ولقد أثبت الواقع العملي أن أي دولة لا تستطيع – بجهودها المنفردة – القضاء عليها، وبخاصةٍ مع هذا التطور المذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الشبكة المعلوماتية، ومع تميزها بالعالمية وبكونها عابرةً للحدود؛ فإن مكافحتها لا تتحقق إلا بتعاونٍ دوليٍّ على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتبَ متخصصةٍ لجمع المعلومات عن مرتكبيها، فمثلًا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيبَ موجودةٍ بدولة أخرى، وتقع آثاره المدمرة بدولةٍ ثالثةٍ؛ لذا فمن البديهي ألا تقف مشكلات الحدود والولايات القضائية عقبة أمام اكتشافها ومعاقبة مرتكبيها. وبدأ هذا النوع من التعاون الأمني الدولي عندما أُنشئت المنظمة الدولية

---

[1] أ. حمد عبد الرحمن حمد المظلوم: المواجهة الأمنية للجرائم العابرة للحدود، أكاديمية شرطة دبي، كلية الدراسات العليا، 2013م، ص165.

للشرطة الجنائية "الانتربول"، حيث مثلت دعوة أمير موناكو (ألبرت الأول) إلى عقد مؤتمر دولي للشرطة المبادرة الأولى لإنشاء جهاز دولي في مجال التعاون الأمني الدولي لمكافحة الجريمة، وكان ذلك في عام 1914م، وفي المؤتمر الدولي الثاني للشرطة الذي عُقد بفيينا عام 1923م تقرر إنشاء اللجنة الدولية للشرطة الجنائية، ومقرها مدينة فيينا عاصمة النمسا، وقد تغير اسمها فيما بعد ليصبح "المنظمة الدولية للشرطة الجنائية"، ويطلق عليها اختصارًا "الإنتربول"، ومقرها الحالي مدينة ليون بفرنسا[1].

وهذه المنظمة يشكل أعضاؤها (190) دولة، وهي أكبر منظمة عالمية للشرطة، ويتمثل دورها الفعَّال في تمكين أجهزة الشرطة في جميع بلدان العالم من التكاتف والعمل بروحٍ واحدةٍ؛ لجعل العالم أكثر أمانًا، وتساعد البنية التحتية المتطورة للدعم الفني والميداني التي تملكها المنظمة على مواجهة التحديات المتنامية في مجال مكافحة الجرائم الإلكترونية، لا سيما وأن أجهزة الشرطة لا يمكنها التصدي لجرائم العصر الحديث إلا من خلال التعاون الأمني الدولي. وتسعى هذه المنظمة إلى ضمان تمكين أجهزة الشرطة في العالم أجمع من القيام – بشكلٍ فوريٍّ – بتوفير قاعدة البيانات اللازمة لدعم تحقيقاتها، والاطلاع عليها عبر قنوات اتصالٍ مأمونةٍ؛ مما ييسر التعاون بين أجهزة الشرطة، حتى في غياب العلاقات الدبلوماسية بين بلدانٍ معينةٍ، بما يتماشى مع مبدأ الحياد السياسي للإنتربول، ناهيك عما يوفره الإنتربول من برامجَ تدريبيةٍ محددة الأهداف، وذات دعم متخصص لعمليات التحقيق وشبكات عالمية تساعد أجهزة

[1] المرجع السابق نفسه، ص165.

الشرطة في الميدان على تنسيق جهودها لجعل العالم أكثر أمانًا[1]، ويمكننا بيان جهود الإنتربول في مجال مكافحة الجرائم الإلكترونية على النحو الآتي:

1- الإنتربول منظمةٌ رسمية بين الحكومات، ميزانيتها السنوية (30) مليون دولار، وهو مبلغٌ متواضعٌ بالنسبة لمنظمة دولية يعمل بها (270) شخصًا، ويحقق عدة مهام هامة ومفيدة، وإن كانت متواضعةً، وبخاصةٍ في مجال تبادل المعلومات والتعاون الدولي ضد الجريمة المنظمة عبر الدول، وتشغله شبكة اتصالات لاسلكية مؤمَّنة تغطي كل أنحاء العالم حيث تربط الدول الأعضاء، من خلال مكاتبهم الوطنية الرئيسة بعضها مع البعض ومع سكرتاريته في ليون بفرنسا، وتسهل هذه الشبكة النقل السريع للرسائل الإلكترونية التي تشمل رسائلَ مكتوبةً، الصور الفوتوغرافية، والبصمات وغيرها. وتنقل الشبكة أكثر من مليونيْ رسالة كل عام، وهي توفر التسهيلات الأساسية لتنفيذ عمل المنظمة[2].

2- يرفع الإنتربول من تركيزه على أنشطة المجرمين الذين يستخدمون الإنترنت بشكل همجي لخرق الشبكة الإلكترونية ومواقعها، ومن أمثلة ذلك إغلاق موقع OINK الذي كان يمثل أحد أكثر مصادر التنزيل غير المشروع للموسيقى الأكثر استخدامًا في العالم، وقد أبرز التحقيق – في شأن هذا الموقع – الدور

---

(1) أ. مريم عثمان عبد القادر: الحماية الجنائية للطفل من الجرائم الإلكترونية، في ضوء القانون الإماراتي، دراسات قانونية، مرجع سابق، ص286.

(2) أ. عزيزة علي عبد العزيز جمعدار: الجرائم المنظمة بين التقدم العلمي والمكافحة الأمنية، مطبعة رأس الخيمة الوطنية، رأس الخيمة، الطبعة الأولى، 2012م، ص271-272.

الأساسي الذي يمكن أن يضطلع به الإنتربول في التنسيق بين أجهزة الشرطة والقطاع الخاص؛ لضمان إجراء التحقيقات الشرطية بالتزامن مع عدة بلدان، وهو ما جرى في هذه القضية بين هولندا والمملكة المتحدة، هذا وقد تم تعزيز هذه القدرة خلال سنة 2008م عن طريق تيسير مزيدٍ من الدعم إلى الأطراف المعنية من هيئات القطاع الخاص في سياق التحقيقات المتعلقة بالشبكة الإلكترونية.[1]

3- أصدرت المنظمة الدولية للشرطة الجنائية العديد من القرارات في شأن تنسيق تعاون الشرطة الدولية ضد الجريمة، وبخاصة عبر الوطنية، ومنها بطبيعة الحال الجرائم الإلكترونية.

4- إنشاء فرع للجريمة المنظمة عبر الوطنية، وإنشاء قاعدة معلومات شاملة عن المنظمات الإجرامية وهياكلها التنظيمية.

5- يقوم الإنتربول بدورٍ مهمّ في مكافحة الجرائم الإلكترونية، وقد خصص لها وحداتٍ متخصصةً، وفي إطار مكافحة الجرائم الإلكترونية فقد أعدت الأمانة العامة للإنتربول دفاترَ أو سجلاتٍ خاصةٍ بالأشخاص المطلوبين المنتمين إلى منظمات إجرامية، وتحتوي هذه السجلات على كل ما يتعلق بهؤلاء الأشخاص، من صورٍ وبصماتٍ وأسماء مستعارةٍ وتفاصيل هُوِيَّاتهم، ويتم

---

[1] د. عبد العزيز خنفوسي: الآليات المستحدثة من طرف منظمة الإنتربول بغية التصدي للإجرام الدولي المنظم، الفكر الشرطي، مركز بحوث شرطة الشارقة، القيادة العامة لشرطة الشارقة، الشارقة، المجلد (21) العدد (83)، أكتوبر 2012م، ص104.

توزيع هذه الدفاتر أو السجلات على المكاتب الوطنية المركزية للإنتربول في الدول الأعضاء.

6- يقوم الإنتربول بدور جوهريٍّ في مجال تسليم المجرمين المطلوب محاكمتهم أو المحكوم عليهم في شأن الإجرام الدولي المنظم، ولا يقتصر دوره على تتبع المجرمين الهاربين والقبض عليهم، سواء لتقديمهم للمحاكمة أم لتنفيذ أحكامٍ جنائيةٍ صادرةٍ ضدهم في دولة أخرى؛ بل أنه يتتبع المعلومات التي يوفرها على اتجاهات الجرائم الإلكترونية العابرة للحدود، ويسهم في منع وصول الجريمة إلى دولة ما، ومن ثم فإن للمنظمة الدولية للشرطة الجنائية "الإنتربول" دورًا وقائيًّا لمنع الجرائم الإلكترونية العابرة للحدود[1].

7- خصص الإنتربول مركزًا للشكاوى الخاصة بجرائم الإلكترونية "IC3"، وهو كنايةٌ عن نظام تبليغ وإحالة شكاوى الناس في الولايات المتحدة والعالم أجمع ضد المعلوماتية، ويعمل المركز بواسطة استمارة الشكاوى المرسلة على الإنترنت، وبواسطة فريقٍ من الموظفين والمحللين، ووكالات فرض تطبيق القوانين الأمريكية والدولية التي تحقق في الجرائم الإلكترونية، ونشأ مركز الشكاوى الخاصة بالجرائم الإلكترونية كمفهوم في الإنتربول سنة 1998م[2].

---

[1] أ. حمد عبد الرحمن حمد المظلوم: المواجهة الأمنية للجرائم العابرة للحدود، مرجع سابق، ص165-166.

[2] د. عبد العزيز خنفوسي: الآليات المستحدثة من طرف منظمة الإنتربول بغية التصدي للإجرام الدولي المنظم، مرجع سابق، ص103-104.

وعليه؛ يمارس الإنتربول دوره في مجال مكافحة الجرائم الإلكترونية، عن طريق التعاون والتنسيق مع الدول الأعضاء بملاحقة مجرمي الإلكترونية، وتعقبهم، وتسليمهم. ويستند الإنتربول في ذلك إلى المادة الثانية من دستوره التي تنص على أن الهدف الأساسي من إنشاء المنظمة الدولية للشرطة الجنائية هي: تأكيد وتشجيع المساعدة المتبادلة بين سلطات الشرطة الجنائية في حدود القوانين السائدة في الدول المختلفة، وبروح الإعلان العالمي لحقوق الإنسان، وإنشاء وتطوير النظم التي من شأنها أن تسهم على نحو فعال في منع ومكافحة ظاهرة الإجرام[1].

وقد أكدت المنظمة الدولية للشرطة الجنائية "الإنتربول" في سبيل مكافحة الجرائم الإلكترونية على ما يأتي:

- طبيعة الجرائم الحاسوبية دولية؛ بسبب الاتصالات المتزايدة بشكل مُطَّرِدٍ من قبل الهواتف والأقمار الصناعية وغيرها، بين البلدان المختلفة، ويجب على المنظمات الدولية – مثل الإنتربول – إعطاء هذا الجانب مزيدًا من الاهتمام.
- تطوير وتنسيق قوانين العقوبات المتعلقة بالجرائم الإلكترونية حول العالم، وبالأخص جرائم تعديل البيانات ومحوها، أو التأثير على معالجة البيانات بقصد التدمير، والاستيلاء أو الحصول على بيانات تخصُّ شخصًا آخرَ،

[1] أ. ليندا بن طالب: غسل الأموال وعلاقته بمكافحة الإرهاب "دراسة مقارنة"، دار الجامعة الجديدة، الإسكندرية، 2011م، ص379.

والحصول على خدمات الحاسوب الآلي بدون تفويضٍ، بهدفٍ واحدٍ هو استخدام جهاز حاسوبٍ آليٍّ ينتمي لشخصٍ آخرَ[1].

وتتولى المنظمة الدولية للشرطة الجنائية الإنتربول إقامة العلاقات بين الدول المنضمَّة، وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بالجرائم الإلكترونية، وبخاصةٍ الجرائم المتشعبة في عدة دول، وعلى نمط الإنتربول الدولي أنشأ المجلس الأوروبي في لكسمبورج عام 1991م شرطة أوروبية؛ لتكون حلقة وصل بين أجهزة الشرطة الوطنية في الدول المنضمة، ولملاحقة الجناة في الجرائم العابرة للحدود، ومنها بطبيعة الحال الجرائم الإلكترونية[2].

وفي ضوء ما سبق؛ تمثل المنظمة الدولية للشرطة الجنائية الإنتربول نموذجًا لإرادة الدول في التعاون الأمني الدولي وضبط المجرمين وتسليمهم؛ بغية تحقيق أهدافٍ مشتركةٍ، وتعد نموذجًا جليًّا للتعاون الدولي حيث جمعت معظم الدول تحت مظلة منظمةٍ مختصةٍ اختصاصًا جنائيًّا، بالإشارة إلى تفرد سلطات الدول تشريعيًّا وقضائيًّا وتنفيذًا في مجال الإجرام ضمن سلطتها الجغرافية، فمن أهداف المنظمة تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كل سلطات الشرطة الجنائية، وإنشاء وتنمية كل المؤسسات القادرة على المساهمة الفعالة في الوقاية من الجرائم التي تقع على الجرائم الإلكترونية ومكافحتها، وترجع أهمية هذه المنظمة إلى ما توفره من معلوماتٍ جنائيةٍ

---

(1) Stein Schjolberg, The History of Global Harmonization on Cybercrime, op, cit, p3.

(2) د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009م، ص597.

دوليةٍ، وفرقٍ جنائيةٍ متخصصةٍ على مستوًى عالٍ، ومعاهد ومؤسسات تعليمية وتدريبية متخصصة، وتعد همزةَ وصلٍ بين دول العالم، وتمثل المعاهدات والاتفاقيات الدولية مظهرًا من مظاهر السيادة الخارجية للدول، وهي شرط لسيادتها الداخلية، ومن تلك المعاهدات التعاون الدولي في المسائل الجنائية من المعاهدات الثنائية والإقليمية والدولية[1].

ومن مظاهر التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ما نصت عليه الاتفاقية الأوروبية ببودابست في المادة (29) على سرية حفظ البيانات المعلوماتية المخزنة، وأجازت لكل طرفٍ أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر الذي ينوي الطرف – الطالب المساعدة – أن يقدم طلباً للمساعدة بشأنها؛ بغرض التفتيش أو الدخول بأي طريقةٍ مماثلةٍ، وضبط أو الحصول أو الكشف عن البيانات المشار إليها. كما أكدت المادة (30) من الاتفاقية على الكشف السريع عن البيانات المحفوظة. كما أكدت المادة (32) من الاتفاقية الدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاقٍ، أو أن تكون هذه البياناتُ متاحةً للجمهور. وأكدت المادة (33) من الاتفاقية تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة بالاتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وينظم هذا التعاون الشروط

[1] د. عبد العزيز حسن الحمادي: نشاط المنظمة الدولية للشرطة الجنائية (الانتربول) وأنشطتها في ضوء القانون الدولي، مركز بحوث الشرطة، شرطة الشارقة، الطبعة الأولى، 2013م، ص298.

والإجراءات المنصوص عليها في القانون الدولي. وأكدت المادة (34) من الاتفاقية على التعاون في مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات[1].

أما على المستوى العربي فنجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية؛ بهدف تأمين التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[2].

ومن الأهمية تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناءً على اتفاقياتٍ دوليةٍ، ولهذا التعاون أهميته بحيث إذا اكتشفت الشرطة الوطنية لدولةٍ ما أن إحدى الجرائم الإلكترونية قد تمت ممارستها عبر الشبكة المعلوماتية من خلال موقعٍ موجودٍ في الخارج؛ فإنها تبلغ عن هذه الجريمة إلى سلطات الشرطة بالدولة التي تم منها البث. كما يجب أن تُعَيِّنَ كلُّ دولةٍ الإدارةَ الأمنية المكلفة بمكافحة هذا النوع من النشاط الإجرامي؛ فيوكل إليها تلقي البلاغات التي محورها الجرائم الإلكترونية، ويكون من اختصاصها اتخاذ الإجراءات الأمنية والقانونية المناسبة حسب القوانين الوطنية،

[1] د. فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، مرجع سابق، ص567-568.

[2] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص401.

وتنفيذًا للتدابير الأمنية الواقية من استفحال هذا الخطر الملاصق للتقنية الحديثة، والهادم للاستفادة الصحيحة من الشبكة الإلكترونية[1].

ثانيًا- التعاون القضائي الدولي:

إن لم تتمكن الأجهزة الشرطية، كجهات استدلال، من منع وقوع الجريمة وهو الدور الذي تفرضه عليها الضبطية الإدارية، فيتحول دورها إلى حتمية الضبط الجنائي وتقديمه إلى جهات التحقيق والمحاكمة، وفاعلية التحقيق والملاحقة القضائية في الجرائم الإلكترونية غالباً ما تقتضي تتبع أثر النشاط الإجرامي، وهنا لابد من مساعدة السلطات في البلد الذي كان منشأ الجريمة، ويعد التعاون القضائي الدولي من التدابير المانعة لوقوع الجريمة، وذلك لأن المجرم يجد نفسه محاطاً بجدار مانع من الإفلات من المسؤولية الجرمية التي ارتكبها أو من العقوبة التي حكم عليه بها، ولما كانت هذه الجرائم ذات طابع عالمي، وبالتالي يمكن أن تتعدى آثارها إلى عدة دول، فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة لتوقيع العقاب عليهم يستلزمان القيام بأعمال إجرائية خارج حدود الدولة، مثل معاينة موقع الإنترنت في الخارج، أو القبض على المتهم، أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم معلومات يمكن أن تساهم في تحقيق هذه الجرائم، وكل ذلك لا يمكن تحقيقه بدون تعاون قضائي بين الدول[2].

---

[1] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، 594-595.

[2] عمر عباس خضير العبيدي: مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الوقائي، مركز الدراسات العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2020م، ص143-144.

ومن هذا المنطلق، يلعب القضاءُ في أي دولة دورًا مهمًّا في مواجهة حالات التعدي المؤثم الماس بمصالح المجتمع وأفراده علي حد سواء، وذلك من خلال تطبيق القوانين وتفسيرها بما يتفق والغاية من سَنِّها، والمصالح التي تبتغي حمايتها، وإذا كان من الرؤى البعيدة تصور أن يكون للقضاء دورٌ وقائيٌّ مشابهٌ لدور الشرطة في مكافحة الجرائم الإلكترونية، إلا أنه في الواقع يلعب دورًا مهمًّا في ردع كل من تُسَوِّل له نفسه الاعتداءَ علي المصالح الاجتماعية والاقتصادية محل الحماية القانونية، ولن يتأتى ذلك إلا من خلال المساعدة القضائية الدولية في المواد الجنائية[1]، ويقصد بالمساعدة القضائية كلُّ إجراءٍ قضائيٍّ تقوم به دولةٌ من شأنه تسهيل مهمة المحاكمة في دولة أخرى، بصدد جريمة من الجرائم[2]، وتتخذ المساعدة القضائية في المجال الجنائي صورًا عدةً، ومنها:

1- **تبادل المعلومات:** وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطةٌ قضائيةٌ أجنبيةٌ، وهي بصدد النظر في جريمة ما عن الاتهامات التي وُجِّهَت إلى رعاياها في الخارج، والإجراءات التي أُتُّخِذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة.

2- **نقل الإجراءات:** ويقصد به اتخاذ دولةٍ ما – بناءً على اتفاقيةٍ أو معاهدةٍ – إجراءاتٍ جنائيةٍ وهي بصدد جريمةٍ أُرتكبت في إقليم دولةٍ أخرى ولمصلحة هذه

---

[1] أ. عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، جامعة الإسكندرية، كلية الحقوق، 2000م، ص362.

[2] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص597.

الدولة متى توفرت شروطٌ معينةٌ أهمها التجريم المزدوج، ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمةً في الدولة الطالبة وفي الدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها؛ بمعنى أن تكون الإجراءاتُ المطلوب اتخاذها مقررةً في قانون الدولة المطلوب إليها عن الجريمة ذاتها[1].

وقد أقرَّ المجلسُ الأوروبي اتفاقيةَ نقل الإجراءات الجنائية التي تعطي للأطراف المنضمة إمكانية محاكمة الجاني طبقًا لقوانينها، وبناءً على طلب دولةٍ أخرى طرفٍ في هذه الاتفاقية؛ بشرط أن يكون الفعل معاقبًا عليه في الدولتيْن[2]. كما أقرَّت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة الدولية القضائية الدولية كمعاهدة الأمم المتحدة النموذجية في شأن نقل الإجراءات في المسائل الجنائية (22)، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م[3] في المادة 21 منها، والشيء ذاته نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م

---

[1] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص407-408.

[2] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص599.

[3] وقعت دولة الإمارات العربية المتحدة على هذه الاتفاقية في مايو سنة 2007م، وذلك ضمن جهود المشاركة الدولية التي تبذلها الدولة في نطاق التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية بشتى صورها. انظر: أ. حمد عبد الرحمن حمد المظلوم: المواجهة الأمنية للجرائم العابرة للحدود، مرجع سابق، ص172.

في المادة (9) منها، وأيضًا المادة (16) من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م[1].

3- **الإنابة القضائية الدولية:** يقصد بها طلب اتخاذ إجراءٍ قضائيٍّ من إجراءات الدعوى الجنائية، وتقدمه الدولة الطالبة إلى الدولة المطلوب إليها؛ للفصل في مسألةٍ معروضةٍ على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام به بنفسها. فالإنابة القضائية تسهل إذن الإجراءات الجنائية بين الدول؛ بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدولة الأخرى[2].

وعليه، قد الزمت اتفاقية بودابست الأوروبية لعام 2001م الدول التي دخلت الاتفاقية على ضرورة أن تقوم الدول الأطراف الموقعة على الاتفاقية بإصدار تشريعات وطنية، تعمل على التعاون القضائي[3]، وقد أقرت المادة (32) من الاتفاقية الأوروبية "بودابست" لعام 2001م، بشأن الجرائم المعلوماتية، إمكانية الدخول بغرض التفتيش والضبط للبيانات والمعلومات في أجهزة أو شبكات تابعة

---

(1) د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص408.

(2) د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص601.

(46) Conention on cybercrime, Budapest, 23Xl.2001, Details of Treaty no. 185, Council of Europe, Ibid, p3-4. Date of entry: 15/1/2023
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور، والثانية إذا حصل على موافقة قانونية من الشخص الذي لديه السلطة القانونية للكشف عن البيانات من خلال نظام الكمبيوتر[1].

وقد أقرت المادة (22) من الاتفاقية الأوروبية "بودابست" لعام 2001م، بشأن الجرائم المعلوماتية بتبني كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لوضع الولاية القضائية على أي جريمة منصوص عليها وفقاً للمواد من (2-11) من هذه الاتفاقية عند ارتكاب الجريمة أو في أراضيها، وعندما يدعي أكثر من طرف الاختصاص القضائي بجريمة منصوص عليها وفقاً لهذه الاتفاقية فعلى الأطراف المعنية، عند الاقتضاء، التشاور فيما بينهم بهدف تحديد الولاية القضائية الأنسب للمقاضاة[2].

وعليه، قد حرصت جمهورية مصر العربية على تحقيق التعاون الدولي في أحدث قوانينها المتعلقة بمكافحة الجرائم الإلكترونية، حيث نصت المادة (4) من القانون رقم (175) لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات على أنه: "تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار

(47) Article 32, Conention on cybercrime, Budapest, 23Xl.2001, Details of Treaty no. 185, Council of Europe, Ibid, P.17. Date of entry: 15/1/2023 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

(48) Article 22, Conention on cybercrime, Budapest, 23Xl.2001, Details of Treaty no. 185, Council of Europe, Ibid, P.17. Date of entry: 15/1/2023 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقًا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن"[1].

وكذلك نصت المادة 33 من قانون رقم (17) لسنة 2023 بشأن الجرائم الإلكترونية الأردني على أنه:

أ- للمدعي العام المختص أو للمحكمة المختصة وعند قيام نظام المعلومات أو موقع إلكتروني أو مزود الخدمة داخل المملكة أو خارجها أو منصات التواصل الاجتماعي أو الشخص المسؤول عن أي حساب أو صفحة عامة أو مجموعة عامة أو قناة أو ما يماثلها بنشر أي مواد مخالفة لأحكام هذا القانون أو التشريعات النافذة في المملكة اصدار أمر الى القائمين عليها لاتخاذ ما يلي:

1- إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوي أو منع الوصول اليه أو حظر المستخدم أو الناشر مؤقتاً خلال المدة المحددة في القرار.

2- تزويدهما بجميع البيانات أو المعلومات اللازمة التي تساعد في اظهار الحقيقة ومنها بيانات مالك أو مستخدم الموقع الإلكتروني أو نظام المعلومات التي تساعد في تحديد هويته واجراء الملاحقة القانونية.

[1] المادة 4 من قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، المصري.

3- الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة وتخزينها والمحافظة على سلامتها.

4- الحفاظ على السرية".

ب- في حالة عدم استجابة أو رفض القائمين على نظام المعلومات أو منصة التواصل الاجتماعي أو الموقع الإلكتروني أو مزود الخدمة للأمر المنصوص عليه في البند (1) من الفقرة (أ) من هذه المادة أو إذا اقتضت السرعة ذلك فيجوز للمدعي العام المختص أو المحكمة المختصة وبقرار معلل اصدار أمر الى الجهات المختصة بحظر نظام المعلومات أو الموقع الإلكتروني أو منصة التواصل الاجتماعي أو الخدمة عن الشبكة الوطنية أو حظر الوصول للمحتوي المخالف...."[1].

ويلاحظ الباحث أنه لا يوجد نص يقابل هذا النص في التشريع الإماراتي والمصري والبحريني، فكان الأجدر عليهم أن ينصوا على ذلك في القانون الإلكتروني.

كما حرصت دولة الإمارات العربية المتحدة – منذ نشأتها – على التعاون والتنسيق مع المجتمع الدولي ممثلة في منظمة الأمم المتحدة في إرساء وتعزيز مبادئ وقواعد العدالة الجنائية من خلال المشاركة الفعالة في المؤتمرات والاجتماعات واللقاءات العلمية المعنية بنظم العدالة الجنائية، وقد عزَّزت تلك المشاركاتُ الوعيَ الوطني بمفاهيم العدالة الجنائية، والأخذ بالمعايير والموجهات التي اعتمدتها الأمم المتحدة

[1] المادة 33 من قانون رقم 17 لسنة 2023 بشأن قانون الجرائم الإلكترونية، والمنشور بالجريدة الرسمية، رقم 5874، الصادر بتاريخ 2023/8/13م.

لتكون دولة الإمارات العربية المتحدة في مقدمة الدول المنفذة للمعاهدات والمواثيق الدولية ذات العلاقة بالعدالة الجنائية على الواقع العملي، وذلك وفقًا للآتي:

1- المشاركة الفعَّالة في اجتماعات الجمعية العامة للأمم المتحدة، وهي تعتمد وتصدر القرارات المتصلة بشأن العدالة الجنائية.

2- المشاركة المستمرة في مؤتمرات الأمم المتحدة الخمسية للعدالة الجنائية، ومنع الجريمة التي تعتبر السلطة التشريعية الدولية التي تُعد المواثيق والاتفاقيات الدولية الخاصة بنظام العدالة الجنائية.

3- الإعلان الرسمي عن التزام الدولة باحترام المواثيق الدولية.

4- اعتماد المواثيق الدولية الخاصة بنظام العدالة الجنائية، وترجمتها إلى قوانينَ وطنيةٍ حسب الأصول.

5- اعتماد الاتفاقيات والمواثيق الدولية ذات العلاقة بنظام العدالة الجنائية ضمن مناهج التأهيل والتدريب في كليات القانون وكليات الشرطة ومدارسها، ومعاهد تدريب القضاة والمحامين.

6- تنظيم مؤتمراتٍ وندواتٍ علميةٍ حول مواضيع العدالة الجنائية التي تهدف إلى تعزيز المهارات لدى العاملين في أجهزة العدالة الجنائية.

7- إيلاء البحث العلمي في مجال علوم العدالة الجنائية اهتمامًا خاصًّا.

8- تطوير مناهج كلية الشرطة لتصبح كلية جامعية تمنح ضباط الشرطة درجة البكالوريوس في العدالة الجنائية وعلوم الشرطة، وأيضًا الماجستير؛ لتصبح

دولة الإمارات العربية المتحدة أول دولة عربية توفر تعليمًا متخصصًا في العدالة الجنائية للشرطة، وهي أهم مكونات نظام العدالة الجنائية[1].

وقد أصدرت دولة الإمارات العربية المتحدة – في سبيل تحقيق التعاون الدولي – القانون الاتحادي رقم (39) لسنة 2006م في شأن التعاون القضائي الدولي في المسائل الجنائية. كما اتخذت الدولة مجموعةً من الاتفاقيات في التعاون الأمني الدولي والمساعدة القضائية، على النحو الآتي:

1- اتفاقية التعاون القضائي والإعلانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين مع دولة الإمارات العربية المتحدة بتاريخ 1978/1/18م.

2- اتفاقية تنفيذ الأحكام والإنابات والإعلانات القضائية بدول مجلس التعاون لدول الخليج العربية؛ بالمرسوم الاتحادي رقم (41) لسنة 1996م.

3- اتفاقية الرياض للتعاون القضائي؛ بالمرسوم الاتحادي رقم (53) لسنة 1999م.

4- اتفاقية نقل المحكوم عليهم بين دول مجلس التعاون لدول الخليج العربية؛ بالمرسوم الاتحادي رقم (92) لسنة 2006م.

5- اتفاقية التعاون القضائي وتنفيذ الأحكام وتسليم المجرمين مع الجمهورية التونسية؛ بالمرسوم الاتحادي رقم (32) لسنة 1975م.

---

[1] د. عبد الله علي سعيد بن ساحوه وأ.د محمد الأمين البشري: العدالة الجنائية مفهومها نظمها وتطبيقات دولة الإمارات العربية المتحدة، مركز بحوث الشرطة، شرطة الشارقة، الشارقة، الطبعة الأولى، 2013م، ص173-174.

6- اتفاقية التعاون القانوني والقضائي مع جمهورية الصومال؛ بالمرسوم الاتحادي رقم (95) لسنة 1982م.

7- اتفاقية التعاون الأمني وتسليم المجرمين مع المملكة العربية السعودية؛ بالمرسوم الاتحادي رقم (104) لسنة 1982م.

8- اتفاقية التعاون القضائي مع الجمهورية الجزائرية الديمقراطية الشعبية؛ بالمرسوم الاتحادي رقم (12) لسنة 1984م.

9- اتفاقية التعاون القضائي مع المملكة الأردنية الهاشمية؛ بالمرسوم الاتحادي رقم (106) لسنة 1999م.

10- اتفاقية التعاون القانوني والقضائي في المسائل المدنية والتجارية، واتفاقية المساعدة القانونية المتبادلة في المسائل الجنائية، واتفاقية في شأن تسليم المجرمين مع حكومة جمهورية الهند؛ بالمرسوم الاتحادي رقم (33) لسنة 2000م.

11- اتفاقية التعاون والقانون القضائي مع حكومة جمهورية مصر العربية؛ بالمرسوم الاتحادي رقم (83) لسنة 2000م.

12- اتفاقية تسليم المجرمين مع جمهورية الصين الشعبية؛ بالمرسوم الاتحادي رقم (25) لسنة 2003م.

13- اتفاقية إعلان الأوراق القضائية وغير القضائية، وسماع الشهادة والاعتراف بالأحكام وتنفيذها في المسائل المدنية والتجارية، واتفاقية تسليم المجرمين مع

حكومة جمهورية باكستان الإسلامية؛ بالمرسوم الاتحادي رقم (12) لسنة 2005م.

14- اتفاقيات المساعدة القانونية المتبادلة في المسائل الجنائية وتسليم المجرمين والمساعدة القانونية والقضائية في المسائل المدنية والتجارية مع المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية؛ بالمرسوم الاتحادي رقم (38) لسنة 2007م[1].

وفي سبيل تحقيق الغاية المنشودة في تعزيز التعاون الأمني الدولي، والمساعدة القضائية فيما بين الدول العربية والإقليمية والدولية، وتفعيله فيما بينها وبين أجهزتها المختصة وأجهزة الدول الأخرى النظيرة بقصد مكافحة الجرائم الإلكترونية بحزمٍ وصرامةٍ، وملاحقة الجناة في كل موطن؛ فيجب على الدول العربية والإقليمية والدولية الترحيب بعقد اتفاقياتٍ ثنائيةٍ، والدخول في اتفاقياتٍ متعددة الأطراف؛ لتحقيق التعاون الأمني الدولي والمساعدة القضائية بأفضل ما يمكن فيما بينها؛ لمكافحة الجرائم الإلكترونية؛ بوصفها جريمةً عبر وطنيةٍ، بعد أن أضحت جهود كل دولة بمفردها – مهما بلغت – لا تغنيها عن طلب العون من دول أخرى[2].

---

[1] د. عبد العزيز حسن الحمادي: نشاط المنظمة الدولية للشرطة الجنائية (الإنتربول) وأنشطتها في ضوء القانون الدولي، مرجع سابق، ص354-358.

[2] المستشار. أحمد محمود خليل: الجريمة المنظمة، الإرهاب وغسل الأموال، المكتب الجامعي الحديث، الإسكندرية، 2009م، ص81-82.

المبحث الثاني

المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية وسبل مواجهتها

سنتعرف في هذا المبحث إلى المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية، وسبل مواجهتها. لذا؛ يرى الباحث ضرورة تقسيمه إلى المطلبيْن الآتييْن:

المطلب الأول: المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية

المطلب الثاني: سبل مواجهة المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية

المطلب الأول

المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية

سنتعرف في هذا المطلب إلى المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية، وذلك في الفرعيْن الآتييْن:

الفرع الأول

المشكلات التي تواجه التعاون الوطني في الجرائم الإلكترونية

أولًا- ارتكاب الجريمة الإلكترونية في بيئة النظم المعلوماتية:

إن ما يميز الجريمة الإلكترونية عن الجريمة التقليدية أن أداة ارتكابها هو الحاسوب الآلي والشبكة الإلكترونية ووسائلها، ومحلها هي النظم المعلوماتية المخزنة

فيها، كما أنها قد تُرتكب أثناء إحدى مراحل تشغيل نظام المعالجة الآلية للمعلومات سواء في مرحلة الإدخال أم المعالجة أم الإخراج[1].

ثانيًا– المجرم المعلوماتي هدفه النظم المعلوماتية:

إن هدف المجرم المعلوماتي هو النظم المعلوماتية، حيث أصبح من الممكن – في عصرنا الحاضر – تدميرُ النظم المعلوماتية للأفراد والقطاع العام والخاص، من خلال مجرم المعلوماتية وهو مستترٌ بعيدًا عن أعين الأجهزة الأمنية المختصة، وتزداد هذه الجريمة في الدول التي تُدار بنيتها التحتية بالحاسوب الآلي والشبكة الإلكترونية ووسائلها؛ مما يجعلها هدفًا له؛ فمن خلال الشبكة الإلكترونية يستطيع المخترقون تدميرَ النظم المعلوماتية، وإغلاقَ المواقع، وشلَّ أنظمة القيادة والاتصالات، أو قطعَ شبكة الاتصالات بين الوحدات والقيادات المركزية، أو تعطيلَ أنظمة الدفاع الجوي، أو إخراجَ الصواريخ عن مسارها، أو التحكمَ في خطوط الملاحة الجوية والبرية والبحرية، أو شَلَّ محطات إمداد الطاقة والماء، أو اختراقَ النظام المَصْرِفِيّ؛ مما يؤدي إلى الإضرار بالمصارف والأسواق المالية[2].

تتمثل أبرزُ السلبيات في الجرائم الإلكترونية في الجوانب الأمنية؛ حيث يمكن لقراصنة الحاسوب الآلي والشبكة الإلكترونية ووسائلها: اختراق مواقع التجارة الإلكترونية

---

[1] د. محمد كمال شاهين: الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2018م، ص41.

[2] أ.د. جميل عبد الباقي الصغير: مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الإنترنت، مجلة الأمن والحياة، العدد 329، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009م، ص74–75.

في بعض الأحوال، وسرقة المعلومات الموجودة فيها، وقد يكون من بينها أرقام بطاقات العملاء، وكذلك يمكن تخريب هذه المواقع أو تدميرها عن طريق الفيروسات، أو تغيير محتوياتها، أو تعطيلها عن العمل، أو محو البيانات الموجودة فيها، وتتعدد المخاطر التي تتعرض لها شبكة الإنترنت في تداول البيانات والمعلومات، الأمر الذي يؤثر سلبًا في التجارة الإلكترونية، ويؤدي إلى وجود نوع من التردد في استخدام الشبكة الإلكترونية، وقد تم تصنيف مستخدمي الشبكة – بحسب أسباب إحجامهم عن التعامل بالتجارة الإلكترونية – إلى الأصناف الآتية: (53%) يرجع إلى عدم وجود الأمان Security الكافي بالنسبة للعميل، وتليها صعوبة التجول والاتصال والتعامل بنسبة (35%)، ثم عدم التعامل لعدم وجود اختياراتٍ كافيةٍ بنسبة (27%)، ثم لعامل عدم الثقة بنسبة (24%)، ثم لارتفاع الأسعار بنسبة (20%)، كما أن هناك بعض المشكلات الأخرى التي تتمثل في إمكانية تعطيل مواقع التجارة الإلكترونية، ومن أهم المخاطر التي يمكن أن يتعرض لها أيُّ مشروعٍ مشتركٍ في التجارة الإلكترونية الكشف عن الأسرار، وخسائر مالية مباشرة، وتكاليف غير متوقعة، وفقدان الثقة في التعامل عبر شبكة الإنترنت[1].

[1] المستشار د. محمد عبيد الكعبي: الحماية الجنائية للتجارية الإلكترونية، دار النهضة العربية، القاهرة، 2010م، ص177-179.

وقد تتعرض التطبيقاتُ الحكومية للاختراق؛ حيث يعمل مجرمو المعلوماتية وقراصنة المعلومات على التلاعب في المعلومات الإدارية للحكومة، وإفشائها، أو تدميرها بالفيروسات[1].

وعلى الرغم من حداثة جرائم الحاسوب الآلي والإنترنت نسبيًّا إلا أن الدراسة التي أجرتها منظمة (business software alliance) في الشرق الأوسط في حجم خسائر جرائم الحاسوب الآلي وصلت إلى ثلاثين مليون دولار أمريكي في المملكة العربية السعودية والإمارات العربية المتحدة[2].

ثالثًا– جريمة عابرة للحدود الوطنية:

لم يعد يقتصر مدى الجريمة الإلكترونية على النطاق الوطني فقط؛ بل أخذت بُعْدًا دوليًّا عابرًا للحدود الوطنية؛ لسهولة الاتصالات بين دول العالم بصورةٍ غير مسبوقةٍ؛ نتيجة للشبكة الإلكترونية ووسائلها التي جعلت العالمَ قريةً كونيةً صغيرةً، وباتت الجريمة الإلكترونية لا تخضع لنطاقٍ إقليميٍّ محددٍ، وإنما أصبحت تُرتكب في

(1) د. السيد أحمد محمد مرجان: دور الإدارة العامة الإليكترونية والإدارة المحلية في الارتقاء بالخدمات الجماهيرية، دراسة مقارنة، بين الإدارة المحلية في مصر وبلدية دبي في دولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة، الطبعة الثانية، 2010م، ص134.

(2) د. علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، جرائم الحاسوب والإنترنت، 2009م، ص174–175.

دولةٍ، وتمر عبر دولةٍ أخرى، وتحقق نتيجتها في دولة ثالثة أو عدة دول، كل ذلك في ثوانٍ معدودةٍ[1].

رابعًا- عدم وجود اتفاقياتٍ ومعاهداتٍ دوليةٍ كافيةٍ للتعاون الدولي في مجال الجرائم الإلكترونية:

عدم وجود اتفاقيات ومعاهدات دولية كافية للتسليم والمعاونة – الثنائية أو الجماعية – بين الدول تسمح بالتعاون الدولي في التحريات وتسليم المجرمين والسرعة في الإجراءات؛ فلا توجد سوى اتفاقيةٍ دوليةٍ وحيدةٍ على مستوى العالم وهي الاتفاقية الأوروبية بوادبست لعام 2001م؛ فهي متميزة في مكافحة الجرائم الإلكترونية، وتعد من أهم أدوات التعاون الدولي في هذا الصدد[2].

وعلى المستوى العربي هناك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد وافق عليها مجلسُ وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21م، وجمهورية مصر العربية 2010/12/21م، ودولة الإمارات العربية المتحدة 2011/9/21م[3].

ويرجع عدمُ وجود اتفاقيات ومعاهدات دولية كافية للتعاون الدولي في الجرائم الإلكترونية إلى عدم وجود نموذجٍ واحدٍ متفقٍ عليه فيما يتعلق بالنشاط الإجرامي، ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفقْ على صورةٍ محددةٍ يندرج في

---

[1] د. محمد كمال شاهين: الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، مرجع سابق، ص42.

[2] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص87.

[3] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لعام 2010م.

إطارها ما يسمى "بإساءة استخدام نظم المعلومات الواجب اتباعها". فضلًا عن عدم وجود تنسيقٍ فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجرائم الإلكترونية في الدول المختلفة، وبخاصةٍ فيما يتعلق منها بأعمال الاستدلال والتحقيق، وعدم وجود معاهدات – ثنائيةٍ أو جماعيةٍ – بين الدول على نحوٍ يسمح بالتعاون المثمر في شأنها، بالإضافة إلى مشكلة الاختصاص التي تثيرها؛ فهي من المشكلات التي تعرقل الحصول على الدليل فيها، ذلك أنها من أكثر الجرائم التي تثير مسألة الاختصاص على المستويْن المحلي والدولي؛ بسبب التداخل والترابط بين شبكات المعلومات؛ فقد تقع جريمة الحاسوب الآلي في مكانٍ معينٍ، وتنتج آثارُها في مكانٍ آخرَ داخل الدولة أو خارجها، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على الشبكة الإلكترونية[1].

ونخلص إلى القول، تتمثل المشكلات التي تواجه التعاون الوطني في الجرائم الإلكترونية في أنها تقع في بيئة النظم المعلوماتية، وهو هدف المجرمِ المعلوماتيّ، مع نقص خبرة الأجهزة المختصة على المستوى الوطني، والمهارة الفنية العالية لمجرمي المعلوماتية؛ مما يؤدي إلى صعوبة ملاحقاتهم، وإثبات الجرائم الإلكترونية التي تقع على النظم المعلوماتية. فضلًا عن كونها جريمةً عابرةً للحدود الوطنية، ويصعب التعاون الدولي فيها؛ نظرًا إلى عدم وجود اتفاقياتٍ ومعاهداتٍ دوليةٍ كافيةٍ للتسليم، والتعاون – الثنائي أو الجماعي – بين الدول؛ فالأمر يتطلب تعاونًا دوليًّا؛ لكونها جريمةً تُرتكب في دولةٍ ما، وتتحقق نتيجتُها في دولةٍ أخرى أو عدة دول.

---

[1] المستشار د. عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، 2009م، ص104-107.

الفرع الثاني

المشكلات التي تواجه التعاون الدولي في الجرائم الإلكترونية

أولًا– اختلاف التشريعات الوطنية وتطبيق القواعد التقليدية في الجرائم الإلكترونية:

إن اختلافَ النظم القانونية والتشريعات العقابية له دورٌ بارزٌ في مجال وضع العوائق أمام تحقيق التعاون الدولي في مجال الجرائم الإلكترونية؛ حيث إن اشتراط تجريم الفعل ذاته في التشريعات الوطنية هو أهم الشروط، وبخاصةٍ في نطاق تسليم المجرمين، فضلًا عن أن معظم الدول لم تصدرْ التشريعات التي تعالج الجريمة الإلكترونية أو تضع الآلية المناسبة لمواجهتها، وتطبيق القواعد التقليدية من الناحية الإجرائية والعقابية على الجريمة الإلكترونية[1].

وبنظرةٍ متأنيةٍ للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم الإلكترونية؛ يتضح لنا من خلالها عدم وجود اتفاقٍ عام مشتركٍ بين الدول حول نماذج إساءة استخدام نظم المعلومات والشبكة المعلوماتية الواجب تجريمها، فما يكون مباحًا في أحد الأنظمة قد يكون مجرَّمًا وغير مباحٍ في نظامٍ آخرَ، ويمكن إرجاع ذلك إلى عدة أسبابٍ وعواملَ كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع إلى آخر، وبالتالي اختلاف السياسة التشريعية من مجتمعٍ إلى آخرَ[2].

---

[1] أ. لينا محمد الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، دار الحامد للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2015، ص256.

[2] د. السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2017م، ص447.

ثانيًا– اختلاف النظم القانونية الإجرائية الجنائية:

بسبب تنوع النظم القانونية الإجرائية واختلافها؛ نجد أن طرق التحري والتحقيق والمحاكمة التي تَثْبُت فائدتها وفاعليتها في دولةٍ ما قد تكون عديمة الفائدة في دولة أخرى، أو ربما لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونيةٌ في دولة معينةٍ فقد تكون الطريقة ذاتُها غيرَ مشروعةٍ في دولة أخرى، وبالتالي فإن الدولة الأولى ستشعر بخيبة أملٍ؛ لعدم مقدرة سلطات القانون في الدولة الأخرى علي استخدام ما تعتبره أداةً فعَّالةً، فضلًا عن أن السلطات القضائية لدى الدولة الثانية ربما لا تسمح باستخدام أي دليل إثباتٍ جرى جمعُه بطرقٍ تراها غيرَ مشروعةٍ، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع[1].

وبالنظر إلى الاختلافات التي توجد بين التشريعات المختلفة فيما يتعلق بشروط قبول الأدلة، وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود؛ لذا يجب إعادة النظر في أُطر التعاون القضائي؛ من أجل صياغة شكلٍ جديدٍ له، فمنذ سنة 1993م أدرك المجلس الأوروبي المشكلات التي يمكن أن تثيرها الشبكة المعلوماتية الجديدة في مجال الإجراءات الجنائية؛ حيث إن الاقتراح رقم (17) للتوصية رقم R 95 13 قد أكد

[1] د. السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مرجع سابق، ص448.

بوضوحٍ وجود قصورٍ على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود[1].

وعلاج ذلك أنه يجب على دولة الإمارات العربية المتحدة وجمهورية مصر العربية من التعاون، وتبادل الإنابة الدولية القضائية التي يُقصد بها التفويض الذي يصدر من سلطةٍ قضائيةٍ جنائيةٍ إلى سلطةٍ قضائيةٍ أجنبيةٍ في القيام نيابة عنها بالتحقيق في واقعةٍ إجراميةٍ معينةٍ، ومحاولة الكشف عن أدلة ارتكابها، ونسبتها إلى فاعلها، وبمعنى آخر تتمثل الإنابة القضائية الدولية في الطلب الذي ترسله سلطةٌ قضائيةٌ في إحدى الدول إلى سلطةٍ مناظرةٍ بدولةٍ أجنبيةٍ؛ لتتخذ هذه السلطة الأجنبية إجراءً من إجراءات التحقيق باسم السلطة الطالبة القضائية الوطنية، ولحسابها؛ سواء أكان من إجراءات التفتيش، أم سماع شهود معينين، أم فحص أوراق تفيد في كشف الجريمة، أم مراقبة الشبكة المعلوماتية، أم الإذن لها بالتنصُّت على الهواتف[2].

---

[1] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص601.

[2] المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، في ضوء الأحكام الموضوعية والإجرائية للقانون الدولي والداخلي، "دراسة مقارنة"، دار النهضة العربية، القاهرة، الطبعة الأولى،2011م، ص815.

ثالثًا- تنازع الاختصاص القضائي الدولي وهاجس المساس بالسيادة الإقليمية والقومية:

يثير هذا التنازع مشكلةَ فحصِ البيانات في مراكزَ دول أخرى؛ مما يعني خضوع إجراءات التحقيق – بخصوص هذه البيانات – للقوانين الجنائية النافذة في هذه الدولة؛ على الرغم من إبرام المعاهدات والاتفاقيات الخاصة بتسهيل عمليات الاستدلال والتحقيق في الجرائم الإلكترونية؛ إلا أن ذلك لم يكن بالمستوى المطلوب لحل مشكلات الاختصاص القضائي وتبادل الأدلة الجنائية الرقمية وتسليم المجرمين، حيث إن صعوبة تحديد الاختصاص القضائي للمحكمة التي تنظر في القضية المتعلقة بالجريمة الإلكترونية؛ فهي إحدى أهمِّ المشكلات التي تعرقل عملية مكافحتها؛ إذ تعد من الجرائم الأكثر إثارة لموضوع الاختصاص على المستوى الوطني والدولي نتيجةً للترابط في شبكة المعلومات، وهذه المسالة بدورها ستثير العديد من المشكلات أثناء البحث عن الأدلة اللازمة لإثباتها إذا تمت بين أكثر من دولة واحدة[1].

إن الجرائم المتعلقة بالمعلوماتية من أكبر الجرائم التي تثير مسألة الاختصاص على المستويْن المحلي والدولي، ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي؛ حيث يتم الرجوع إلى المعايير المحددة قانونًا لذلك، ولكن المشكلة تُثار بالنسبة للاختصاص على المستوى الدولي؛ حيث اختلاف التشريعات والنظم القانونية التي قد ينجم عنها تنازعٌ في الاختصاص بين الدول بالنسبة للجرائم المتعلقة

[1] أ. لينا محمد الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، مرجع سابق، ص254-255.

بالشبكة المعلوماتية التي تتميز بكونها عابرةً للحدود؛ فقد يرتكبها أجنبيٌّ في إقليم دولةٍ معينةٍ؛ فهنا تكون الجريمةُ خاضعةً للاختصاص الجنائي للدولة الأولى؛ استنادًا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيسه على مبدأ الإقليمية[1].

وعلى الرغم من أهمية القانون الدولي في مجال مكافحة الجرائم العابرة للحدود الوطنية؛ إلا أن القانون الجنائي ظل مدةً طويلةً أمرًا لا يخص الولاية القضائية غير الوطنية فحسب؛ بل يخصُّ أيضًا أحد الميادين التي تتجسد فيها السيادة الوطنية والتي من مسلماتها الرئيسة أن الدولة لا تعترف بأي سلطةٍ قانونيةٍ أو دستوريةٍ عُليا سواها، وتحتكر الاستخدام المشروع للقوة، ويفسر واجب الدولة في حماية مواطنيها – بصفةٍ عامةٍ – بما مفاده أن المواطنين الذين ينتهكون القانون ينبغي مقاضاتهم بالقانون الخاص بالدولة، ولا ينبغي خضوعهم لولايةٍ قضائيةٍ أجنبيةٍ؛ لذلك تترد الدولة عادة في تسليم مواطنيها إلى ولايةٍ قضائيةٍ أخرى، حتى ولو كان لدى الدولة الأخرى أسبابٌ حقيقيةٌ لمقاضاتهم، وحتى إن رغبت الدولة في تسليم مواطنيها لمقاضاتهم في بلدٍ آخرَ؛ فقد يثير ذلك معارضةً عنيفةً من جانب المنظمات الإجرامية غير الوطنية في الدولة التي تتخذ منها هذه المنظمات قاعدةً لها[2].

---

[1] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص413.

[2] أ.د. محمد سامي الشوا: التعاون الأوربي في مجال مكافحة الجريمة المنظمة، أكاديمية العلوم الشرطية، الشارقة، 2017م، ص14.

وعلى الرغم من تنامي ظاهرة الجرائم المعلوماتية؛ إلا أن كل دولة مازالت تعتزُّ بسيادتها، وتعتبر أن ملاحقة رعاياها أو ملاحقة رعايا على أرضها هو مساسٌ وانتهاكٌ لحقها في السيادة على إقليمها، وهذا من شأنه إعاقة التعاون الدولي لمواجهتها، وعلى وجه الخصوص إعاقة نظام تسليم المجرمين والإنابة القضائية والمساعدة القانونية وغيرها من الإجراءات اللازمة لمكافحتها[1] والمساعدة القانونية وغيرها من الإجراءات اللازمة لمكافحتها هذا من جانب، وتستهدف المصلحة القومية حفظ استقلال الدول ومحاولة إبعاد النفوذ الخارجي، وهذا إذا كان له تأثيرٌ إيجابيٌّ في المحافظة على الأمن القومي للدولة؛ إلا أنه قد يكون له تأثيرٌ سلبي في مجال التعاون الدولي لمكافحة الجرائم المعلوماتية؛ حيث تتحفظ الدول – في مجال التعاون الدولي عادةً – على الإجراءات التي قد تستشعر أنها تَمَسُّ مصلحتَها وأمنَها القومي كوجود رجال أمن تابعين لدولة أخرى مثلًا على أراضيها؛ مما يعيق التعاونَ الدولي في القبض والتفتيش والتسليم وتنفيذ الأحكام من جانب آخر[2].

ومن القضايا التي لفتت النظر إلى هذه المشكلة قضية R.V. Thomp-son: وتتلخص وقائعها في قيام مبرمجٍ إنجليزي يعمل بأحد البنوك بدولة الكويت بالتلاعب في نظام الحاسوب الآلي الخاص بالبنك؛ لإجراء خصوماتٍ من أرصدة العملاء، ثم يودعها في حسابه الخاص، وبعد عودة المتهم إلى إنجلترا يكتب إلى البنك سائلًا إياه

---

(1) المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، مرجع سابق، ص805–806.

(2) أ. عبد العزيز الزدجال: التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2014م، ص208.

تحويل الحساب الخاص به إلى عدة حساباتٍ بنكيةٍ في إنجلترا، وهو ما قام به البنك بالفعل، وبعد ذلك قُدِّم للمحاكمة بتهمة الحصول على أموال الغير بطرق الاحتيال بالمادة (15) من القانون الإنجليزي المُجَرِّم لفعل السرقة لعام 1968م، وحُكِمَ عليه بعقوبة السَّجن؛ إلا أنه طعن في الحكم استنادًا إلى عدم اختصاص القضاء الإنجليزي بالفصل في الجريمة؛ حيث إن فعليْ السحب والإيداع تمَّا بدولة الكويت وليس في إنجلترا، وقد رفضت محكمة الاستئناف الطعن المقدم منه، وجاء في حيثيات رفضها أن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل، وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية[1].

رابعًا- الصعوبات المتعلقة بالمساعدات القضائية الدولية:

نعلم أنَّ الأصل بالنسبة لطلبات الإنابة القضائية الدولية – التي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي – أن تُسَلَّمَ بالطرق الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، ويتعارض مع طبيعة الجرائم الإلكترونية المتميزة بالسرعة[2]، وهو الأمر الذي انعكس عليها. كذلك من الصعوبات الكبيرة – في مجال المساعدات القضائية الدولية المتبادلة – التباطؤ في الرد؛ حيث إن الدولة المتلقية الطلب غالبًا ما تكون متباطئةً في الرد على الطلب؛ سواء بسبب نقص الموظفين

---

[1] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص603-604.

[2] د. السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مرجع سابق، ص450.

المدربين نتيجة الصعوبات اللُّغوية، أو الفوارق في الإجراءات التي تُعَقِّد الاستجابة، وغيرها من الأسباب؛ فكم هو محبطٌ شطب قضيةٍ لعدم تلبية طلب بسيط في الوقت المناسب[1]؛ لذلك تقتضي مكافحة الجرائم الإلكترونية ردودًا سريعة، خشية التلاعب في البيانات التي يمكن أن تشكل دليلًا ضد مجرمي المعلوماتية[2].

خامسًا- عدم وجود قنوات الاتصال المرجوة من التعاون الدولي في مجال الجريمة الإلكترونية:

إن أهمَّ الأهدافِ المرجوة من التعاون الدولي في مجال الجريمة والمجرمين هو الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزامًا أن يكون هناك نظامُ اتصالٍ يسمح للجهات القائمة على التحقيق بالاتصال بجهاتٍ أجنبيةٍ لجمع أدلةٍ معينةٍ أو معلوماتٍ مهمةٍ؛ فعدم وجود مثل هذه النظام يعني عدم المقدرة على جمع الأدلة والمعلومات العملية التي غالبًا ما تكون مفيدةً في التصدي لجرائمَ معينةٍ ولمجرمين معينين، وبالتالي تنعدم الفائدة من هذا التعاون[3].

ونخلص إلى القول، إن من المشكلات التي تواجه التعاون الدولي في الجرائم الإلكترونية اختلاف التشريعات الوطنية حولها، وتطبيق القواعد التقليدية عليها، فضلًا عن اختلاف النظم القانونية الإجرائية الجنائية، وتنازع الاختصاص القضائي الدولي،

---

[1] د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص414-415.

[2] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص602.

[3] د. السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مرجع سابق، ص449.

وهاجس المساس بالسيادة الإقليمية والقومية، والصعوبات المتعلقة بالمساعدات القضائية الدولية، وعدم وجود قنوات الاتصال المرجوة من التعاون الدولي في مجال الجريمة الإلكترونية.

وعليه؛ فالجرائم الإلكترونية بُعْدٌ دوليٌّ، حيث غالبًا ما تمُرُّ عبر عددٍ من البلدان أثناء النقل من المرسِل إلى المُتَسَلِّم، أو تخزين المحتوى غير القانوني خارج الدولة في إطار التحقيقات في الجرائم الإلكترونية، ويعد التعاونُ الوثيقُ بين البلدان المعنية مهمًّا للغاية، وتستند اتفاقيات المساعدة القانونية المتبادلة بين الدول إلى إجراءاتٍ تستغرق وقتًا طويلًا، إضافة إلى ضَعْف إجراءات الاستجابة السريعة للحوادث وطلبات التعاون الدولي[1].

(1) Prof. Dr. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, op, cit, p11.

المطلب الثاني

سبل مواجهة المشكلات التي تواجه التعاون الوطني والدولي في الجرائم الإلكترونية

إن التقدمَ التكنولوجي المتواصلَ يفرض على جهات إنفاذ القانون أن تسير بخطواتٍ متناسقةٍ مع التطورات السريعة التي تشهدها هذه التقنياتُ، والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها هذا من جانب، كما أن إعمال القانون في مواجهة الجرائم الإلكترونية يستلزم اتخاذَ إجراءاتٍ قد تتجاوز المفاهيمَ والمبادئ المستقرة في المدونة الإجرائية التقليدية؛ لما تتسم به هذه الجرائمُ من: حداثة الأسلوب، وسرعة التنفيذ، وسهولة إخفائها، والمقدرة علي محو آثارها؛ لذلك كان لا بد من أن تكون الأجهزة – على مختلف أنواعها – على درجةٍ كبيرةٍ من الكفاءة والمعرفة، والمقدرة على كشف غموض تلك الجرائم، والتعرف إلى مرتكبيها بسرعةٍ ودقةٍ متناهيتيْن، وهذا لن يتحقق إلا بالتدريب المتطور والمواكب لتلك الصور المستحدثة من الجرائم الإلكترونية[1].

ومن الأهمية التفعيل الدولي والإقليمي في المجال الأمني والقضائي، من خلال الاتفاقيات الدولية بين الدول في مجال الجرائم الإلكترونية، حيث نجد أن الصكوك الدولية الصادرة من الأمم المتحدة غالبًا ما تشجع الأطرافَ فيها على السماح باستخدام

[1] المستشار د. فخري محمود خليل: جرائم البلطجة الإلكترونية، تتحدى التشريعات والقضاء وتدعم المجرم والجريمة المستحدثة، دراسة مقارنة، الناشر "المؤلف"، القاهرة، الجزء الأول، 2019م، ص22-23.

بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غُلُوِّ النظم القانونية والإجرائية واختلافها، ويفتح المجال أمام تعاونٍ فعَّالٍ؛ فمثلًا المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الشأن إلى التسليم المراقَب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة التي تعد من أهم التقنيات المستخدمة للتصدي للجماعات الإجرامية المنظمة المحنكة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها، وتجميع المعلومات وأدلة الإثبات؛ لاستخدامها – فيما بعد – في الملاحقات القضائية الوطنية منها أو الدولية في دولٍ أطرافٍ في سياق نظم المساعدة القانونية المتبادلة[1].

وقد أخذ القانون رقم (39) لسنة 2006م الصادر بدولة الإمارات العربية المتحدة بهذا الاتجاه في شأن التعاون القضائي الدولي في المسائل الجنائية؛ فحددت المادة الأولى منه المقصود: بالجهة القضائية الأجنبية، والدولة الطالبة، والدولة المطلوب إليها، والمطلوب تسليمه. وحدَّدت المادة الثانية الأحكام العامة للتعاون القضائي التي نصت على أنه: "مع عدم الإخلال بأحكام الاتفاقيات الدولية التي تكون الدولة طرفًا فيها وبشرط المعاملة بالمثل تتبادل الجهات القضائية في الدولة مع الجهات القضائية الأجنبية التعاون القضائي في المسائل الجنائية طبقًا لأحكام هذا القانون". وحدَّد شروطَ التسليم في المادة السادسة التي نصت على أن: "يكون تسليم الأشخاص المتهمين أو المحكوم عليهم إلى الجهات القضائية الأجنبية للتحقيق معهم أو لمحاكمتهم جزائيًّا أو

[1] د. السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مرجع سابق، ص452-453.

لتنفيذ الأحكام الجزائية الصادرة ضدهم طبقًا للأحكام الواردة في هذا الباب". وحدَّد في المادة (8) الجرائمَ المطلوب بشأنها التسليم. وحدد في المادة التاسعة الحالات التي يتم فيها رفض التسليم وذلك على سبيل الحصر. فضلًا عن نصه في المادة (10) على تأجيل تسليم الشخص حتى ينتهي التحقيق معه أو تنتهي محاكمته في جريمة أو جرائم أخرى في الدولة. وحددت المواد (11، 12، 13، 14) الإجراءات الواجب اتباعها في التسليم للدولة الأجنبية[1].

وعليه؛ فإن مكافحة أساليب مجرمي المعلوماتية – عن طريق الشبكة المعلوماتية ووسائلها – لا يتحقق إلا إذا كان هناك تعاونٌ دوليٌّ على المستوى الإجرائي الجنائي؛ بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتبَ متخصصةٍ لجمع المعلومات من مرتكبيها وتعميمها، حيث يصعب على الدولة بمفردها القضاء على الجرائم الإلكترونية العابرة للحدود الوطنية؛ لأن جهاز الشرطة في هذه الدولة أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عَبَرُوا حدودَها؛ ولذلك فإن الحاجةَ مُلِحَّةٌ إلى تعاون أجهزة الشرطة بين الدول، وتنسيق العمل فيما بينها؛ لضبط مجرمي المعلوماتية، ومكافحة نشاطهم الذي يتم عن طريق الشبكة المعلوماتية ووسائلها، والذي يتجاوز حدود الدولة، وقد تبلور هذا النوعُ من التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية "الإنتربول" التي تستهدف تأكيد وتشجيع التعاون بين سلطات الشرطة في الدول الأطراف على نحوٍ فعَّالٍ يحقق مكافحة

[1] المواد 1–14 من قانون اتحادي رقم 39 لسنة 2006 في شأن التعاون القضائي الدولي في المسائل الجنائية.

الجريمة، وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم وبالجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة بأقاليم الدول المنضمة، وتبادل المعلومات والبيانات فيما بينها، والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدِّها بالمعلومات المتوفرة لديها على إقليمها؛ أي أن عضو الإنتربول لا يقوم بإجراء القبض على المجرم بنفسه؛ بل إن هذا العملَ منوطٌ بجهاز الشرطة الوطنية في الدولة التي يوجد المجرم على إقليمها، الأمر الذي يؤكدُ احترامَ السيادة الوطنية[1].

وعلى ذلك، تكمن أهمية التعاون الأمني الدولي بضرورة شعور المجتمع الدولي بمخاطر الجرائم الإلكترونية، وما يمكن أن تحدثه من آثار سلبية على مصالح المجتمع الدولي المشتركة، وإدراكه للنمو السريع والمتزايد لها والنمط المستجد والخطر من الجرائم الإلكترونية، حيث تمثل هذه الجرائم نقطة مشتركة تتلاقى فيها جهود المجتمع الدولي في بذل الاهتمام لأجل اتخاذ تدابير وآليات وتدعيم سبل التعاون الدولي في مكافحة تلك الجرائم، وهذا التعاون يكون بين أجهزة الشرطة الدولية المتخصصة بمكافحة الجرائم الإلكترونية عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي هذه الجرائم وتعميمها، فينبغي أن يكون هناك تعاون بين أجهزة الشرطة المختلفة في الدول، والتنسيق فيما بينها لضبط المجرمين ومكافحة هذه الجرائم التي تتجاوز حدود الدولة، وذلك على النحو التالي:

---

[1] د. طارق الدسوقي: الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، مرجع سابق، ص565-566.

1- ربط شبكات الاتصال والمعلومات:

تحتاج الأجهزة الشرطية إلى وسائل للاتصال تحقق السرعة الممكنة في أجهزة العدالة الجنائية، من خلال التواصل بين سلطات التحقيق والملاحقة المختلفة، وهذا ما قامت به الدول والمنظمات الدولية لتطوير الاتصال وتبادل المعلومات فيما بينها.

2- القيام ببعض العمليات الشرطية والأمنية المشتركة:

تشترك الدول فيما بينها للقيام بعمليات شرطية وأمنية بما يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم، ووضع حد لها، وذلك من خلال تعقب المجرم وتعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابرة للحدود لمكونات الحاسوب الآلي والأنظمة المعلوماتية وشبكات الاتصال، بحثاً عما قد تحويه من أدلة وبراهين على ارتكاب الجرائم الإلكترونية، فالقيام بهذه الأمور يستدعي هذه العمليات [1].

3- التعاون الأمني من خلال جهود المنظمة الدولية للشرطة الجنائية "الإنتربول" في مكافحة الجرائم الإلكترونية.

قدمنا أن الإنتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم الإلكترونية، فمهمة الإنتربول الأساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق، لضبط وملاحقة المجرمين

[1] عمر عباس خضير العبيدي، مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الوقائي، مرجع سابق، ص138.

الهاربين وتسليمهم إلى الدولة التي تطلب تسلُّمهم، وإنشاء وتطوير كل النظم القادرة على المساهمة بفعالية في الوقاية من الجرائم، والعقاب على جرائم القانون العام، ويعهد بتلك المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو في الإنتربول، وإلى جهاز دائم يتم تعيينه بواسطة السلطة المختصة الوطنية، وبمساعدة فرق الإنتربول للتحرك إزاء الأحداث التي يمكنها تيسير مجموعة من خدمات التحقيق والتحليل في موقع الحدث، فضلاً عن ذلك يستخدم الإنتربول أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها، والتقصي في قواعد البيانات وتقديم الخبرات والدورات التدريبية في مجال مكافحة الجرائم الإلكترونية، وذلك بالاستعانة بمجموعة من الخبراء الدوليين والمختبرات الدولية على الصعيد العالمي، وتيسير تبادل وتحليل وتخزين البيانات الجنائية حيث تقوم المنظمة بتزويد شرطة الدول الأطراف بالمعلومات عن الجرائم الإلكترونية، وكيفية التدريب على مكافحتها والتحقيق فيها، وتعد الجرائم الإلكترونية من الجرائم التي تركز عليها منظمة الإنتربول[1].

وعليه، قد أكدت الاتفاقية الأوروبية بوادبست لسنة 2001م للإجرام المعلوماتي التعاون الدولي على المستوى الإجرائي الجنائي، من خلال إجازتها لكل طرفٍ أن يطلب من الطرف الآخر الحفظَ السريعَ للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر الذي ينوي الطرف الطالب المساعدة أن يقدم طلبًا للمساعدة بشأنها بغرض التفتيش أو الدخول بأي طريقةٍ

[1] شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة، المجلد 17، العدد1، الشارقة، يونيو 2020م، ص745.

مماثلةٍ، وضبط البيانات أو الحصول عليها أو الكشف عنها؛ طبقًا للمادة (29) من الاتفاقية. فضلًا عن المساعدة في الكشف السريع عن البيانات؛ طبقًا للمادة (30) منها. بالإضافة إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة؛ طبقا للمادة (31). كما أجازت المادة (32) الدخول للبيانات المخزنة خارج نطاق الحدود؛ بشرط أن يكون ذلك بموجب اتفاقٍ، أو أن تكون هذه البياناتُ متاحةً للجمهور. كما أجازت المادة (34) التعاون في مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات.

وتعزز الاتفاقيةُ الأوروبية الحمايةَ الجنائية من اختراق النظم المعلوماتية؛ باتخاذ الدول الأطراف الإجراءات اللازمة التي تؤدي إلى توقيع الجزاءات على كل من يرتكب أيًّا من الجرائم المعلوماتية مثل جريمة اختراق النظم المعلوماتية[1].

وقد عملت الاتفاقية في المادة (2) على ضرورة تجريم الدول الأطراف في تشريعاتها الوطنية الدخول إلى النظم المعلوماتية – سواء للوصول إلى كل النظام المعلوماتي أو جزءٍ منه – دون وجه حقٍّ. فضلًا عن تجريم اعتراض النظم المعلوماتية أو نقل البيانات إلى العامة دون وجه حقٍّ؛ وفقًا للمادة (3). وكذلك تجريم حذف النظم المعلوماتية أو تغييرها أو إلغائها أو إتلافها دون وجه حقٍّ؛ طبقًا للمادتيْن (4 و5) من الاتفاقية[2].

---

[1] أ. ناير نبيل عمر: الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012م، ص192.

[2] Conention on cybercrime, Budapest, 23Xl.2001, Details of Treaty no. 185, Council of Europe, p3-4. Date of entry: 15/1/2023

وقد فتحت الاتفاقية في المادة (13) المجال للدول الأطراف لتطبيق نصوصٍ أو موادَّ جنائيةٍ تحدُّ من الجرائم المعلوماتية، حيث نصت على أن: "كل طرف يتولى التشريع والمعايير الأخرى التي قد تكون ضرورية للتأكد على أن الجرائم المقررة وفق نص المواد من 2-11 معاقب عليها بعقوبات فعالة ومتناسبة ورادعة ومتضمنة الحرمان من الحرية، والتأكيد على أن الأفراد المعرضين للمساءلة يتم تطبيق مختلف الجزاءات السابقة عليهم والمتضمنة الحبس والجزاءات النقدية"[1].

ونخلص إلى القول، إن الاتفاقية الأوروبية "بوادبست" لمكافحة الجريمة الإلكترونية لعام 2001م تهدف إلى تحقيق الحماية الإجرائية والعقابية للنظم المعلوماتية، وذلك من خلال إلزام الدول الأطراف اتخاذ التدابير التشريعية الإجرائية والعقابية لكل من تُسَوِّل له نفسه ارتكاب جرائم معلوماتية على النظم المعلوماتية؛ بهدف حذف تقنية المعلومات أو تغييرها أو إلغائها أو إتلافها دون وجه حق؛ وفقًا للمواد (2-5) من الاتفاقية.

وفي هذا الجانب عملت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على مكافحة الجرائم الإلكترونية، رغبة من الدول العربية الموقعة عليها في تعزيز التعاون فيما بينها، وتم توقيع دولة الإمارات العربية المتحدة عليها في 2010/12/21م، وجمهورية مصر العربية في 2010/12/21م، وتضم 22 دولة عربية وإسلامية، وتهدف الاتفاقية إلى حماية الدول العربية من الجرائم الإلكترونية، وقد ألزمت الاتفاقية

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[1] أ. ناير نبيل عمر: الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، مرجع سابق، ص192-193.

الدول العربية المنضمة إليها بتجريم الجرائم الإلكترونية[1]، ويمكن بيان صور التعاون الأمني في الاتفاقية على النحو التالي:

1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين.
2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص في إقليمها لتسليم معلومات معينة في حيازة الشخص مخزنة على تقنية معلومات أو وسيط تخزين معلومات، وأي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم المعلومات المشترط المتعلقة بتلك الخدمات التي في حوزة مزود الخدمة أو تحت سيطرته.
3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات أو جزء منها، والمعلومات المخزنة فيها أو المخزنة عليها، وبيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.
4. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها، إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م.

5. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها، وتلتزم كل دولة بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات، من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات.
6. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من جمع أو تسجيل معلومات بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف، وإلزام مزود الخدمة ضمن اختصاصه الفني بأن يجمع ويسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف، أو يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها، والتي تثبت بواسطة تقنية المعلومات.
7. تلتزم كل دولة طرف بتبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.
8. وإذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطاً بوجود معاهدة، وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة

تسليم، فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بنوعية هذه الجرائم [1].

وتجدر الإشارة إلى أن الاتفاقية الأوروبية بوادبست لمكافحة الجرائم المعلوماتية لعام 2001م هي الوحيدة التي عملت على تحقيق الحماية الإجرائية والعقابية للنظم المعلوماتية، ولا توجد أيُّ اتفاقياتٍ غيرها على مستوى العالم، وتستطيع جميع دول العالم الانضمام إليها. أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م فهي على مستوى الدول العربية والإقليمي فقط، ومن الأجدر أن تنضم هذه الدول إلى اتفاقية بوادبست، أو أن تصدر الولايات المتحدة الأمريكية اتفاقيةً دوليةً تختص بالحماية الإجرائية والعقابية للنظم المعلوماتية، وتضم معظم الدول على المستوى العالم لتكون أكثر فعالية.

ويرى الباحث، أنه يجب مواجهة المشكلات التي تواجه التعاون الدولي في الجرائم الإلكترونية، وتفعيل التعاون الدولي؛ من خلال توحيد النظم القانونية الإجرائية والعقابية. ونظرًا إلى استحالة هذا الأمر فإنه لا مناص من البحث عن وسيلةٍ أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذه الجرائم المستحدثة، ويخفف من غُلُوِّ الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم الإلكترونية، وتفعيل كلٍّ من: الاتفاقيات الإقليمية والدولية، ونظام تسليم مجرمي المعلوماتية، والتعاون الدولي والإقليمي في المجال الأمني والاستخباراتي

[1] المواد من (24-31) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م.

والمعلوماتي، بالإضافة إلى التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية.

وإذا كان التعاونُ الدولي هو السبيل الفعَّال لمكافحة الجرائم الإلكترونية؛ فإن التعاون يقتضي التخفيفَ من غلو الفوارق بين الأنظمة العقابية الداخلية؛ لأن التباعد بين هذه الأنظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة القانونية الأكثر تسامحًا، ولذلك أُبرِمت اتفاقياتٌ دوليةٌ عديدةٌ في مجال التعاون الدولي؛ بهدف التقريب بين القوانين الإجرائية والعقابية الوطنية من أجل مكافحة الجرائم الإلكترونية، وتظهر معالم هذا التقارب في: قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق، وجمع الأدلة، وتسليم المجرمين، والاعتراف بالأحكام الجنائية الأجنبية. وهذا التعاون القانوني الدولي لا ينال من سيادة الدولة؛ بل على العكس فإن انعدامه يُزيد من التباعد بين الأنظمة العقابية؛ مما يساعد على تزايد الجرائم الإلكترونية، ويعد التعاونُ الأمني الدولي والمساعدةُ القضائية في قضايا الجرائم الإلكترونية أهمَّ صور التعاون الدولي القضائي في مجال الجرائم التي تقع على النظم المعلوماتية، وانتهاك أمن المعلومات[1]؛ لذا فلا بد من تفعيل التعاون الأمني الدولي والإقليمي والقضائي والاستخباراتي والمعلوماتي. وللتغلب على المشكلات التي تواجه التعاون الدولي في الجرائم الإلكترونية؛ يجب العمل من المختصين على الآتي:

[1] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص591-593.

- يجب عدم إغفال أهمية التدابير الوقائية عند النظر في المسائل المتعلقة بالتعاون الدولي؛ حيث يمكن لهذا التعاون أن يساعد الدول في: زيادة مناعة الأجهزة الإدارية وأجهزة تنفيذ القوانين إزاء الفساد، وحماية المؤسسات المالية والتجارية ضد تصرف المنظمات الإجرامية لديها، والسيطرة عليها في نهاية المطاف[1].
- حتمية التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية، وبخاصةٍ في المجال الأمني، وأدلة إثبات الجريمة على مرتكبيها؛ حيث تتسم هذه الجرائم بحداثة الأسلوب، وسرعة التنفيذ، وسهولة إخفائها، والمقدرة على محو آثارها. حيث إن استخدام مجرمي المعلوماتية الشبكة المعلوماتية ووسائلها في ارتكاب الجرائم عن طريقها يشكل عبئًا ثقيلًا على عاتق جميع أجهزة العدالة الجنائية: سواء أكانوا رجال الضبط القضائي، أم رجال التحقيق، أم المحاكم بمختلف درجاتها. لا سيما وأن متطلبات العدالة تقتضي أن تتحمل الأجهزةُ الأمنية المسئوليةَ كاملةً تجاه اكتشاف كل الجرائم الإلكترونية، وضبط مرتكبيها؛ لتحقيق العدالة. لأجل ذلك كان لا بد أن تكون تلك الأجهزة الأمنيةُ – بمختلف أنواعها – على درجةٍ كبيرةٍ من الكفاءة والمعرفة والمقدرة على كشف غموض تلك الجرائم، ومعرفة مرتكبيها بسرعةٍ ودقةٍ متناهيتيْن، وهذا لن يتحقق إلا بالتدريب؛ فكفاءة رجال العدالة – لمواجهة هذه الظواهر المستحدثة

[1] أ.د. محمد سامي الشوا: التعاون الأوربي في مجال مكافحة الجريمة المنظمة، مرجع سابق، ص16.

– ومقدرتهم على التصدي لها؛ لا بد أن ترتكز على كيفية تطوير العملية التدريبية والارتقاء بها، والنهوض بأساليب تحقيقها لأهدافها، ومن هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين على هذه الأجهزة[1].

- تفعيل المعاهدات والاتفاقيات الدولية في مجال مكافحة الجرائم الإلكترونية؛ إذ لا توجد سوى اتفاقية دولية وحيدة، ولم يتم التصديق الكامل عليها؛ نظرًا إلى تباين مواقف الدول منها؛ بحجة تعارضها مع اعتبارات السيادة، والمصلحة القومية[2]. ويجب تعزيز هذه الاتفاقية من خلال توضيح الإجراءات المتخذة في حالة التعددية والاستمرارية للجرائم الإلكترونية؛ حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية عن معاقبتهم من ناحية، وغياب النظم الإجرائية والاتفاقيات الدولية التي تنظم سُبُلَ مواجهتهم من ناحية أخرى[3].
- يمكن أن يرتكز التعاون الدولي إلى عددٍ من المستويات، وبطرقٍ عديدةٍ مختلفةٍ، وقد يكون: ذا طبيعةٍ رسميةٍ أو غير رسميةٍ، وثنائيًّا أو متعدد الأطراف. وعادة ما تتمخض أشكال التعاون الثنائية – التي تقوم بها بنى دول ذات اهتمامات ونظم متشابهة – عن نتائجَ مقبولةٍ للغاية. ومع ذلك توجد ثمة حالات – لا سيما المتعلقة بالتعاون الثنائي الواسع النطاق بين قوتين غير

---

(1) د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، مرجع سابق، ص410-412.

(2) المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، مرجع سابق، ص810-811.

(3) د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص605.

متعادلتين – ربما لا تحظى بهذه الشعبية في الدول الضعيفة، وفي مثل هذه الظروف يكون من المفيد اختبار النهج المتعدد الأطراف، ويجب أن يستند التعاون الدولي إلى تدابيرَ تشريعيةٍ وتنظيميةٍ يمكن تطبيقُها على كل جانب من جوانب الجرائم الإلكترونية[1].

- يستلزم التعاونُ الدولي الفعَّالُ تبادلاتٍ سريعةً بين الدول، واستجابةً عاجلةً لطلبات المعلومات أو المساعدة. ومن الأمور المهمة – في هذا المجال – الاعتماد على أعمال المنظمات القائمة مثل المنظمة الدولية للشرطة الجنائية "الإنتربول"[2]، وتفعيل نظام تسليم مجرمي المعلوماتية، ويستهدف هذا النظامُ الحدَّ من إفلاتهم من محاكمة جنائية عادلة، ويرجع ذلك إلى أن معظم الاتفاقيات التي أُبرمت في هذا الشأن هي اتفاقياتٌ ثنائيةٌ أو إقليميةٌ؛ حيث لم تبرمْ – حتى الآن – معاهدةٌ دوليةٌ تنظم آلية تسليم مجرمي المعلوماتية[3]، مع الاسترشاد بالمعاهدة النموذجية للأمم المتحدة الخاصة بتسليم المجرمين لسنة 1990م سواء أثناء تعديلات قانون التعاون القضائي الدولي في المسائل

---

[1] أ.د. محمد سامي الشوا: التعاون الأوربي في مجال مكافحة الجريمة المنظمة، مرجع سابق، ص16.

[2] المرجع السابق نفسه، ص17.

[3] المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، مرجع سابق، ص811–812.

الجنائية لدولة الإمارات العربية المتحدة أو جمهورية مصر العربية، أو عند توقيع الاتفاقيات الدولية الثنائية التي تبرمها الدولتان[1].

- تكامل القانون الوطني مع الدولي؛ إذ يجب على المشرع الوطني تحديث النصوص الإجرائية والعقابية التي تشملها التشريعاتُ الداخلية، بحيث تتواءم مع الجرائم المستحدثة ومنها الجرائم الإلكترونية[2]، مع محاولة توحيد النظم القانونية المنظمة للأنشطة الإجرامية المتعلقة بالجرائم المعلوماتية، من خلال: التفاوض، والوصول إلى معاهدات واتفاقيات دولية أو إقليمية؛ تضع إطارًا حاكمًا لمكافحة كل أشكال الجرائم المستحدثة ومنها بطبيعة الحال الجرائم الإلكترونية[3].
- تفعيل المساعدة القانونية، والإنابة القضائية الدولية؛ من خلال التعاون الدولي في تنفيذ الأحكام الجنائية، فضلًا عن تفعيل أحكام الاتفاقيات الإقليمية، وتطويرها؛ لمكافحة الجرائم المعلوماتية[4].

---

[1] أ. طارق أحمد صالح الخطيبي الفلاسي: أحكام تسليم المجرمين في قانون التعاون القضائي الدولي في المسائل الجنائية في ضوء الاتفاقيات الدولية، أكاديمية شرطة دبي، دبي، 2016م، ص178.

[2] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص605.

[3] د. عادل عبد العال ابراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مرجع سابق، ص74-75.

[4] المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، مرجع سابق، ص814-818.

- اتخاذ التدابير الملائمة لحل مشكلات الاختصاص القانوني والقضائي التي تثيرها الجرائمُ الإلكترونية العابرة للحدود الوطنية، وتنظيم إجراءات التفتيش وضبط المعلومات التي تَعْبُرُ الشبكةَ المعلوماتية، مع كفالة الحماية – في الوقت نفسه – لحقوق الأفراد، وحرياتهم، وسيادة الدول، وتطوير أدلة الإثبات بما يتلاءم مع هذا الشكل الجديد والمُعَقَّد من النشاط الإجرامي المعلوماتي[1]. ولعل حلَّ هذه الإشكالية يكون من خلال اعتبار جميع الجرائم الإلكترونية جرائمَ دوليةً، وتدخل في الاختصاص القضائي العالمي أو ما يُعرَف بالولاية القضائية العالمية، ويعنى مبدأ العالمية أن كل دولة بإمكانها أن تُخْضِع لسلطتها كلَّ جريمةٍ ينص عليها قانونها العقابي؛ بغض النظر عن مكان ارتكابها أو شخص مرتكبها، أو المجني عليه، أو جنسيته، وعما إذا كان القانون الأجنبي يعتبرها جريمة من عدمه. وبمعنًى آخرَ فإن هذا المبدأ يعني وجوب تطبيق القانون الجنائي الوطني على مرتكب أيّ جريمةٍ يتم القبض عليه في أراضيها الوطنية؛ بغض النظر عن مكان ارتكابها، أو أيًّا كانت جنسيةُ فاعليها[2].

---

[1] د. طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، مرجع سابق، ص616.

[2] د. عادل عبد العال ابراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مرجع سابق، ص85-86.

- تعزيز التعاون الدولي والإقليمي بين مؤسسات المجتمع المدني، والاهتمام بحقوق الإنسان والحريات العامة[1].
- الوقوف على الأسباب الحقيقية، ومعالجة الموضوع بحكمةٍ وموضوعيةٍ، والقيام بالبدائل الديمقراطية التي ترتكز إلى رفع المستوى الاقتصادي والاجتماعي والثقافي، والتقليل من الفوارق الطبيعية، وبذلك يتم التعايش والسلام بين البشر[2].

وبعد أن استعرضنا مشكلات التعاون الدولي في الجرائم الإلكترونية، ومظاهر مواجهتها، وسبل تفعيلها؛ يجب أن يؤخذ في الاعتبار ما يأتي:

1- تعاون جميع الدول – على المستويْن العربي والدولي – في تسليم المطلوبين أمنيًّا إلى الدول التي تطالب بهم لارتكابهم الجرائم الإلكترونية[3]، وإلزامهم بذلك، وإذا امتنعوا تُفرَض عليهم عقوباتٌ اقتصاديةٌ.

2- العمل على تطوير أنماط وصياغة الاتفاقيات التي تم عقدها؛ لتتواءم مع الأنماط الإجرامية المستحدثة في الجرائم الإلكترونية، وتستوعبها؛ دون أن يفلت مرتكبوها من الملاحقة الإجرائية والعقابية.

---

[1] د. محمد المتولي: التخطيط الاستراتيجي في مكافحة جرائم الإرهاب الدولي، مرجع سابق، ص418.

[2] أ. عبد الرزاق قايد صالح: الأزمات الأمنية الناشئة عن الإرهاب، كظاهرة إجرامية، رسالة ماجستير، أكاديمية شرطة دبي، أكاديمية شرطة دبي، 2010م ، ص231.

[3] د. محمد محمود المكاوي: الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتبة العصرية، المنصورة، 2010م، ص421.

3- على كل دولة أن تحدَّ – قدر المستطاع – من الجهل والبطالة؛ فهما يشكلان التربةَ الخصبة لنمو ظاهرة الجرائم الإلكترونية، وتكاثرها. كما يلزم توعية الأفراد بنشر التعاليم الدينية؛ فالدين يساعد على نشر الفضائل، وتغليبها على الرذائل.

4- ضرورة إنشاء مركزٍ دولي لمكافحة الجرائم الإلكترونية، ويكون من اختصاصه العمل على تنمية تبادل الخبرات والمعلومات بين الدول في شأنها.

وتعد هذه القواعدُ مكملةً لما قد يتضمنه التشريع الوطني للدولة الطرف من أحكامٍ تتعلق بالتعاون الإجرائي الدولي، وتسد أيَّ فراغٍ محتملٍ في النظام القانوني الذي يحكم هذا التعاون[1]. ويجد التعاونُ الدولي – في مكافحة الجرائم الإلكترونية – تبريرَه في بعض الاعتبارات، ومنها:

1- يعد خطوةً على طريق تدويل القانون الجنائي، ذلك أن ثمة قواعدَ موضوعيةً وإجرائيةً تهيمن على أذهان العديد من مشرعي القرن العشرين، ومن شأن تشابه هذه القواعد أن يخلق نوعًا من التقارب بين التشريعات الحالية؛ مما يجعل الحديثَ – عن توحيد القانون الجنائي أو تدويله – أمرًا قابلًا للتحقيق، وبذلك نقف على أعتاب قانونٍ جنائيٍّ دوليٍّ في سبيل مكافحة الجرائم الإلكترونية العابرة للحدود الوطنية.

2- يعد من قبيل التدابير المانعة من ارتكاب الجرائم الإلكترونية؛ لأن المجرم سيجد نفسه محاطًا بسياجٍ مانعةٍ من إفلاته من المسئولية عن الجريمة التي

[1] المستشار د. سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، مرجع سابق، ص828-827.

ارتكبها، أو من العقوبة التي حُكِم بها عليه؛ فإذا ارتكب جريمته في دولةٍ ما، وتمكن من الهرب إلى دولة أخرى؛ فإنه سيكون عُرضةً للقبض عليه فيها، أو ترحيله إلى البلد الأول، ومن شأن ذلك كله أن يجعله يعزف عن سلوك سبيل الجريمة؛ مما يحقق الردعَ الخاصَّ للمجرم المعلوماتي، وعلى المستوى الأعم يتحقق الردع العام عندما تجد العقوبةُ سبيلَها للتطبيق على الجريمة الإلكترونية المرتكبة.

3- التعاون أو التنسيق بين التشريعات المختلفة – من أجل مكافحة الجرائم الإلكترونية التي تتم عن طريق الشبكة المعلوماتية ووسائلها – يقتضي من كل دولةٍ أن تطبق قوانينَها على ما يرتكب فوق إقليميها من جرائمَ، وذلك بالنسبة للأفعال التي تتفق التشريعات المختلفة على العقاب عليها[1].

4- تطوير وتحديث النظام المعلوماتي واللوجيستي للأجهزة الأمنية؛ مما يمكِّنُها من إحداث الضرر بمجرمي المعلوماتية، عن طريق إجهاض الكثير من عملياتهم التخريبية؛ باستخدام تقنية المعلومات، ووسائلها[2].

وعليه؛ فلا بد – لتحقيق الوقاية من الجرائم الإلكترونية – أن يعمل الأفرادُ والمؤسساتُ والدولُ على تعزيز أمن المعلومات في مواجهتها، وقد حددت هيئةُ تنظيم الاتصالات TRA بدولة الإمارات العربية المتحدة معاييرَ أمن وحماية المعلومات؛ حيث

---

[1] د. طارق الدسوقي: الموسوعة الأمنية، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، مرجع سابق، ص563-564.

[2] د. غادة نصار: الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017م، ص131.

إنه من الضروري أن تقوم الجهة الحكومية بالإجراءات اللازمة من أجل ضمان أمن الموقع الإلكتروني، وما يتضمنه من معلومات، وتوجد عدة أسئلةٍ توفر المساعدة الأساسية للجهات للقيام بهذه المهمة، وتتمثل في الآتي:

- هل لدى الجهة الحكومية خطة احتياطية أو خطة طوارئ لموقعها الإلكتروني؟
- هل لدى الجهة الحكومية سياسية لإدارة التحديثات الأمنية للبرمجيات؟
- هل تقوم الجهة الحكومية – بصفةٍ دوريةٍ – بتقييم نقاط الضعف؟ وإجراء اختبار كشف الثغرات الأمنية على موقعها الإلكتروني؟
- هل لدى الجهة سياسة واضحة لإدارة سجلات الموقع الإلكتروني؟
- هل لدى الجهة الحكومة سياسة أو إجراء لتصنيف درجة سرية المعلومات؟
- هل لدى الجهة الحكومية سياسة أو إجراء لمراجعة تصنيف سرية المعلومات المنشورة على موقعها الإلكتروني؟
- هل تطبق الجهة الحكومية الضوابط الأمنية اللازمة عند التعامل مع الجهات الخارجية، مثل اتفاقية سرية المعلومات؟
- هل لدى الجهة الحكومية سياسة أو إجراء للاستجابة للحوادث الأمنية الخاصة بموقعها الإلكتروني؟
- هل تطبق الجهة الحكومية ضوابط أمنية للحد من البرمجيات الخبيثة؟

- هل تطبق الجهة الحكومية نظام دخولٍ للموقع يعتمد على أمانٍ متعدد التحقق؟
- هل تطبق الجهة الحكومية آلية حماية لتبادل المعلومات الحساسة، مثل استخدم بروتوكولات SSL, TLS, SSH, SFTP وغيرها؟
- هل تطبق الجهة الحكومية آلية حماية للوصول وتخزين المعلومات الحساسة مثل استخدام التشفير؟[1].

وقد صدر قرارُ مجلس الوزراء رقم (21) لسنة 2013م بشأن لائحة أمن المعلومات في الجهات الاتحادية، ويهدف إلى تعزيز أمن المعلومات لدى الجهات الاتحادية والمستخدمين، وتحديد معايير الاستخدام الأمثل للأصول المعلوماتية، وتشجيع التطبيق الفعَّال للأمن المعلوماتي؛ عن طريق تعزيزه باعتباره جهدًا جماعيًّا يتطلب مشاركة كافة المستخدمين ودعمهم، والتأكد من أن المستخدمين على علم بالتزاماتهم فيما يتعلق باستخدام الأصول المعلوماتية، وبيان الإجراءات التي يتعين على الجهات الاتحادية اتباعها لحماية المستخدمين من الأعمال غير القانونية أو الضارة التي قد تؤدي إلى تلف الأصول المعلوماتية، وتوفير إطارٍ قانونيٍّ للجهات الاتحادية؛ لضمان أمن الأصول المعلوماتية، وإيجاد بيئةٍ آمنةٍ في الجهات الاتحادية لحفظ المعلومات، من خلال ضمان سرية المعلومات والبنية التحتية للشبكة، وحمايتها بمنع الدخول أو التعديل أو التغيير غير المصرح به لتلك المعلومات، وحمايتها كذلك من

[1] الموجهات الإرشادية للمواقع الإلكترونية الاتحادية، هيئة تنظيم الاتصالات TRA، الإمارات العربية المتحدة، 2016م، ص38-40.

الفقدان أو التسرب أو التلف أو الإضرار بها بأي وسيلة كانت، ومواجهة المخاطر المتصلة بأمن المعلومات، وتحديد المخاطر المحتملة، وكيفية مواجهتها؛ لضمان استمرارية سير العمل في الجهة الاتحادية عند التعرض لأي حادثٍ أو هجومٍ[1].

وهناك المعايير الوطنية لضمان أمن المعلومات، حيث تضاف المعايير الوطنية على المعايير المطبقة من قبل الجهات بغية الارتقاء بمستوى ضوابط وقدرات ضمان أمن المعلومات داخل جميع الجهات إلى الحد العام المطلوب، وتعمل المعايير على إيجاد الممكنات والعناصر المطلوبة لربط تلك الجهات الفاعلة بعضها ببعض داخل القطاع الواحد وعلى مستوى الدولة، ونستعرض فيما يلي المستويات الثلاثة للمعايير الوطنية لدولة الإمارات العربية المتحدة:

- المعايير العامة: هي تلك المعايير التي تسري على جميع الجهات وفي القطاع المختلفة.
- المعايير الخاصة بقطاع محدد: هي معايير ضمان أمن المعلومات التي تغطي النواحي والخصائص والمتطلبات المميزة لكل قطاع على حدة.
- المعايير الخاصة بالخدمات والمنتجات: هي المعايير المصممة خصيصاً لتلبية احتياجات منتجات وخدمات محددة[2].

---

[1] قرار مجلس الوزراء رقم 21 لسنة 2013 بشأن لائحة أمن المعلومات في الجهات الاتحادية، مجلس الوزراء، الإمارات العربية المتحدة.

[2] جاسم بوعتابة الزعابي: الاطار الوطني لضمان أمن المعلومات، الهيئة الوطنية للأمن الإلكتروني، المجلس الأعلى للأمن الوطني، ص47. الموقع الرسمي لدولة الإمارات العربية المتحدة، تاريخ الدخول: 2023/12/1م.

وتعزز الهيئة الوطنية للأمن الإلكتروني من بيئة العمل التعاوني مع الجهات المنظمة للقطاعات والجهات المشغلة للبنية التحتية للمعلومات الحيوية وغيرها من الجهات المعنية ذات الصلة من أجل تسهيل التطبيق الناجح لبرنامج الحماية وسينصبّ تركيز المنهج التعاوني المذكور على التحسينات الملموسة في إطار الحماية خلال فترة زمنية مناسبة، وستطلب الهيئة اتخاذ تدابير محددة عند الاقتضاء، سعياً للوصول على مستويات أكثر تقدماً من الأمن الإلكتروني للبنية التحتية للمعلومات الحيوية في دولة الإمارات العربية المتحدة، وستقوم الهيئة من خلال نموذج حوكمة حماية البنية التحتية للمعلومات الحيوية بوضع الآلية التي ستتفاعل في إطارها جميع الجهات المعنية بحماية البنية التحتية للمعلومات الحيوية عبر فرق عمل وطنية وأخرى خاصة بالقطاعات تعني بحماية البنية التحتية، وتعمل فرق العمل على مساعدة الهيئة الوطنية للأمن الإلكتروني والجهات المعنية ذات الصلة على مباشر ما يلي:

- وضع أنشطة التخطيط الخاصة بحماية البنية التحتية للمعلومات الحيوية الخاصة بالقطاع.
- تنفيذ الأنشطة الواردة ضمن مراحل عملية حماية البنية التحتية للمعلومات الحيوية.

https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation

- مراقبة تنفيذ عملية حماية البنية التحتية للمعلومات الحيوية داخل القطاعات الرئيسية، واقتراح إجراءات تصحيحية كلما دعت الحاجة[1].

ثم في إطار حماية أمن المعلومات صدر قرار مجلس الوزراء رقم (13) لسنة 2023 بشأن لجنة مكافحة التهديدات السيبرانية والبرامجيات الخبيثة، حيث تختص اللجنة بما يأتي:

1- دراسة واقتراح التشريعات المتعلقة بمكافحة التهديدات السيبرانية والبرمجيات الخبيثة، واقتراح الآليات المناسبة للتعامل مع المخاطر والتهديدات والجرائم المرتبطة بها.

2- التنسيق مع السلطات المختصة والجهات المعنية لتأمين الحماية ودعم المتضررين من التهديدات السيبرانية والبرمجيات الخبيثة.

3- إعداد ودراسة التقارير الخاصة بالإجراءات المتبعة لمكافحة التهديدات السيبرانية والبرمجيات الخبيثة بالتنسيق مع الأجهزة المعنية في الدولة، ورفعها إلى الجهات المختصة لاتخاذ اللازم.

4- إنشاء سجل بيانات خاص وموحد معني بالتهديدات السيبرانية والبرمجيات الخبيثة ومكافحة الجرائم المرتبطة بها.

---

[1] جاسم بوعتابة الزعابي: سياسة حماية البنية التحتية للمعلومات الحيوية، الهيئة الوطنية للأمن الإلكتروني، المجلس الأعلى للأمن الوطني، ص31. الموقع الرسمي لدولة الإمارات العربية المتحدة، تاريخ الدخول: 2023/12/1م.
https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation

5- تلقي الشكاوي والبلاغات من كافة الجهات الاتحادية والمحلية في حال تعرض أي منها لهجمات مرتبطة بالتهديدات السيبرانية والبرمجيات الخبيثة.

6- المتابعة مع الأجهزة والجهات المعنية بشأن مكافحة التهديدات السيبرانية والبرمجيات الخبيثة ومنعها أو الحد من آثارها وسبل التعامل معها، ومشاركة النتائج على الصعيد الوطني والدولي مع الجهات الذات العلاقة، وفقاً لما يقرره الوزير.

7- المساهمة في نشر الثقافة والوعي حول مكافحة التهديدات السيبرانية والبرمجيات الخبيثة.

8- إقامة المؤتمرات والندوات والتدريبات الخاصة بالتهديدات السيبرانية والبرمجيات الخبيثة، وإصدار النشرات والتعاميم بالتعاون والتنسيق مع الجهات ذات العلاقة.

9- أي اختصاصات أو مهام أخرى تُكلف بها من مجلس الوزراء أو الوزير[1].

وعلى ذلك؛ يجب الاستفادة من معايير المجموعة الدولية الخاصة بإدارة أمن المعلومات في تعزيز الأمن المعلوماتي في مؤسسات الدولة، مثل معيار ISO 27001 الذي يعد أحد معايير المجموعة الدولية المتكاملة الخاصة بإدارة أمن المعلومات، وهو معترَفٌ به دوليًّا في مجال أمن المعلومات، ويعمل على تقييم إجراءات أمن المعلومات في تقنية المعلومات والاتصالات؛ فهو يصف الحاجةَ إلى إنشاء نظام

[1] المادة (3) من قرار مجلس الوزراء رقم (13) لسنة 2023 بشأن لجنة مكافحة التهديدات السيبرانية والبرامجيات الخبيثة.

إدارة أمن المعلومات، وتشغيله، ومراقبته، ومراجعته، وصيانته، وتطويره. كما يأخذ في الاعتبار جميع الأخطار المحتملة التي قد تتعرض لها المؤسسةُ الحكومية، ويضع هذا المعيارُ الشروطَ اللازمة لتطبيق نقاط التحكم الأمنية التي تلبي احتياجات المؤسسة الحكومية[1].

ويعمل هذا المعيار على أربعِ مراحلَ متتابعةٍ: تتمثل الأولى في تأسيس نظامٍ لإدارة أمن المعلومات. والثانية في التنفيذ؛ من خلال البدء في تنفيذ الخطط وتشغيلها. والثالثة في التحقق؛ من خلال مراجعة النظام بعد تنفيذه. والرابعة في العمل؛ من خلال صيانة نظام إدارة أمن المعلومات وتطويره [2]، وفي مرحلة التطوير يجب على جهاز أمن المعلومات العمل على الآتي:

1- تنفيذ نظام إدارة أمن المعلومات في المؤسسات، وتطويره.

2- اتخاذ الإجراءات الوقائية والتصحيحية المناسبة، واستخلاص الدروس وتطبيقها من الأجهزة المختصة، والمؤسسات الأخرى التي تعمل على حماية أمن المعلومات.

---

[1] زكي أحمد الجبلي: تأمين المعلومات في الأزمات الأمنية، مرجع سابق، مرجع سابق، ص230-233.

[2] د. سعيدي سليمة: أمن المعلومات وأنظمتها في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017م، ص131.

3- التعاون مع الجهات المعنية بإجراء صيانة نظام إدارة أمن المعلومات وتطويره، والاتفاق على كيفية تطويره، مع ضمان تحقيق التطويرات على النظام؛ طبقًا للأهداف المنتظرة[1].

كما أصدرتْ المجموعةُ الدولية المتكاملة الخاصة بإدارة أمن المعلومات معيارَ ISO 27002، ويهدف إلى إنشاء نظام إدارة أمن المعلومات[2] فهو يتطابق في هيكلته مع ISO 27001، ولكنه أكثر تفصيلًا من حيث المضمون؛ فهو يشرح كيفية تطبيق الضوابط الأمنية عند اختيارها، ويتضمن بعض السياسات والتوجيهات المتعلقة بإدارة أمن المعلومات، ومنها: السياسة الأمنية، وتنظيم أمن المعلومات، وأمن الموارد البشرية، وإدارة الأصول، والتحكم في الوصول، والتشفير، والأمن البيئي والمادي، وأمن الاتصالات وإدارة العمليات، وإدارة استمرارية الأعمال، وإدارة الامتثال أو التوافق، وإدارة الحوادث الأمنية للمعلومات، واقتناء نظم المعلومات وتطويرها وصيانتها[3].

وفي مرحلة التطوير يجب على الجهاز الشرطي - المختص بمكافحة الجرائم الإلكترونية - العمل على تطوير نظام إدارة أمن المعلومات وصيانته، من خلال توفر معايير اقتناء نظم المعلومات وتطويرها وصيانتها، وهي: المعيار الأول يتعلق بالشروط الأمنية لنظم المعلومات المتمثلة في تحليل الشروط الأمنية، وتوصيفها. والثاني خاصٌّ

---

[1] زكي أحمد الجبلي: تأمين المعلومات في الأزمات الأمنية، مرجع سابق، ص241-244.

[2] د. أحمد عبادة العربي: معيار المنظمة الدولية للتوحيد القياسي آيزو 27002 لسياسة أمن المعلومات، دراسة وصفية تحليلية لمواقع الجامعات العربية، مجلة جامعة طيبة، العدد 7، السنة 4، المدينة المنورة، 2015م، ص679.

[3] د. سعيدي سليمة: أمن المعلومات وأنظمتها في العصر الرقمي، مرجع سابق، ص132-133.

بالمعالجة داخل التطبيقات المتمثلة في التحقق من: صحة البيانات المدخلة، وصحة البيانات المخرجة، وصحة الرسائل، ورقابة المعالجات الداخلية. أما الثالث فلضوابط التشفير التي تمثل السياسة العامة في استخدامه، وإدارة المفاتيح المستخدمة بالتشفير. ويتمثل الرابع في ملفات النظام التي تتحكم في برامج التشغيل، وحماية بيانات نظم الاختبار، والوصول إلى شيفرة المصدر. ويتمثل الخامس في الأمن في تطوير ودعم العمليات، من إجراءات ضبط التغير، ومراجعة تقنيات التطبيقات بعد التغييرات لنظام التشغيل، والقيود المفروضة على التغييرات في أحزمة البرمجيات، وتسرب المعلومات، والاستعانة بمصادرَ خارجيةٍ لتطوير البرمجيات. ويتمثل السادس في إدارة الثغرات الأمنية التي تتمثل في التحكم في الثغرات الأمنية[1].

[1] د. أحمد عبادة العربي: معيار المنظمة الدولية للتوحيد القياسي آيزو 27002 لسياسة أمن المعلومات، مرجع سابق، ص728-729.

الخاتمة

قد تم تسليط الضوء في هذه الدراسة على "التعاون الوطني والدولي في الجرائم الإلكترونية، المشكلات والحلول"، حيث لا يمكن مواجهة الجرائم الإلكترونية بدون تعاونٍ دوليٍّ؛ لكونها عابرةً للحدود الوطنية، ولا تستطيع دولة بمفردها مواجهتها، ولكن هناك معوقاتٌ تواجه التعاون الوطني والدولي تحد من فعالية مكافحة الجرائم الإلكترونية. ومن خلال معطيات هذه الدراسة؛ استطاع الباحثُ التوصلَ إلى العديد من النتائج والتوصيات الآتية:

أولًا- النتائج:

1. تتمثل المشكلات المتعلقة بسلطات الاستدلال والتحقيق في الجرائم الإلكترونية في نقص خبرة سلطات الاستدلال والتحقيق، والمشكلات التي تتعلق بالدليل التقني وصعوبة إثبات الجرائم الإلكترونية، وأنها جريمةٌ عابرةٌ للحدود الوطنية، وإخفاؤها، وإعاقة الوصول إلى الدليل بالوسائل الفنية من قبل الجاني، وإحجام المجني عليهم عن الإبلاغ عن تلك الجرائم.
2. من الأجهزة المختصة في التعاون الأمني في مكافحة الجرائم الإلكترونية بدولة الإمارات العربية المتحدة: المباحث الإلكترونية بشرطة دبي، وإدارة الأدلة الجنائية الإلكترونية بشرطة دبي، ويتعاون معهما مركز دبي للأمن الإلكتروني. وعلى المستوى الاتحادي: الهيئة الوطنية للأمن الإلكتروني، والهيئة العامة لتنظيم قطاع الاتصالات. وتعمل الأجهزة المختصة بالدولة على التعاون الأمني فيما بينهم للحد من الجرائم الإلكترونية، وذلك من خلال جمع البيانات

والمعلومات الخاصة بالجريمة عن طريق مأموري الضبط القضائي، وقيامهم بالبحث والتحري والمراقبة عن الجرائم ومرتكبيها، وجمع الأدلة التي تؤدي إلى كشف الحقيقة؛ لتقديمها إلى جهة التحقيق.

3. تعد الاتفاقية الأوروبية بودابست لمكافحة الجرائم الإلكترونية لعام 2001م هي الاتفاقية الوحيدة على مستوى العالم التي عملت على تحقيق الحماية الإجرائية والعقابية للنظم الإلكترونية، ولا توجد أيُّ اتفاقياتٍ أخري على مستوى العالم سواها، وتستطيع جميعُ دول العالم الانضمامَ إليها. وعلى مستوى الدول العربية والإقليمية؛ فلا توجد إلا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م.
4. هناك معوِّقاتٌ تواجه التعاونَ الدولي في الجرائم الإلكترونية، ومن أهمها: اختلال التشريعات الوطنية وتطبيق القواعد التقليدية في الجرائم الإلكترونية، واختلاف النظم القانونية الإجرائية الجنائية، وتنازع الاختصاص القضائي الدولي وهاجس المساس بالسيادة الإقليمية والقومية، فضلًا عن الصعوبات المتعلقة بالمساعدات القضائية الدولية، وعدم وجود قنوات الاتصال المرجوة من التعاون الدولي في مجال الجريمة الإلكترونية.
5. تواجه التعاون الوطني في الجرائم الإلكترونية معوِّقاتٌ، وتتمثل في: أنها تُرتكب في بيئة النظم الإلكترونية التي تعد هدف المجرم المعلوماتي، وأنها جريمةٌ عابرةٌ للحدود الوطنية، وعدم وجود اتفاقياتٍ ومعاهداتٍ دوليةٍ كافيةٍ للتعاون الدولي في مجال مكافحتها.

ثانيًا– التوصيات:

استنادًا إلى معطيات الدراسة الحالية، وإلى النتائج التي توصلنا إليها؛ فإننا نقدم مجموعةً من التوصيات، على النحو الآتي:

1. ينبغي رصد تحركات المجرمين على الشبكة المعلوماتية من خلال الأجهزة المختصة بعمليات البحث والتحري والانتقال والمعاينة في الجرائم الإلكترونية، وتحليل طبيعية الرسائل والملفات المتبادلة وتتبعها، ورصد بيانات حركة المرور التي أُنشئت أثناء استخدام الإنترنت، وتحديد عنوان IP للخادم، وتحديد موقع الجاني وهُوِيَّته سواء عن: طريق مزود الخدمة، والرسائل المرسلة والملفات، وبروتوكول الإنترنت، ونظام الـ PROXY، ومراقبة عمل الموظفين على الشبكة المعلوماتية.
2. يوصي الباحث بضرورة تأهيل المحققين وتدريبهم في استجواب المتهم في الجرائم الإلكترونية، على أن يشمل: مفردات الحاسوب الآلي، وتطبيقاته، والتقنية المعلوماتية ووسائلها، ومعرفته بالجرائم الإلكترونية المختلفة وطرق ارتكابها، وأسس أمن المعلومات؛ بهدف التواصل الجيد مع الشهود والخبير والمتهم والمجني عليه، والحصول على الأدلة الإلكترونية، وإثباتها جنائيًّا على الجاني.
3. يوصي الباحث بتشجيع المجني عليهم بالإبلاغ عن جرائم تقنية المعلومات، أو إفراد مادة في قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي، والمقارن تلزمهم بذلك.

4. يقترح الباحث أن تنضم الدول إلى اتفاقية بودابست، أو أن تصدر الولايات المتحدة الأمريكية اتفاقية دولية تختص بالحماية الإجرائية والعقابية للنظم المعلوماتية، وتضم إليها معظم الدول على المستوى العالم لتكون أكثر فعالية. فضلًا عن ذلك يجب دخول الدول في اتفاقياتٍ ثنائيةٍ ومتعددة الأطراف؛ لتحقيق التعاون الأمني الدولي والمساعدة القضائية لمكافحة الجرائم الإلكترونية؛ بوصفها جريمةً عبر وطنية.
5. ينبغي مواجهة تفعيل التعاون الدولي، ومواجهة معوقاته في سبيل مكافحة الجرائم الإلكترونية، من خلال توحيد النظم القانونية الإجرائية والعقابية، ونظرًا إلى استحالة هذا الأمر؛ فإنه لا مناص من البحث عن وسيلةٍ أخرى تساعد على إيجاد تعاونٍ دوليٍّ يتفق مع طبيعة هذا النوع المستحدث من الجرائم، ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في: تحديث التشريعات الوطنية المعنية بالجرائم الإلكترونية، وتفعيل الاتفاقيات الإقليمية والدولية، وتفعيل نظام تسليم مجرمي المعلوماتية، وتفعيل التعاون الدولي والإقليمي في المجال الأمني والاستخباراتي والمعلوماتي، بالإضافة إلى التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية.
6. يوصي الباحث بالعمل على تطوير أنماط وصياغة الاتفاقيات؛ لتستوعب أنواع الجرائم الإلكترونية، وتكامل القانون الوطني مع هذه الاتفاقيات بما يتعلق بالتعاون الإجرائي الدولي، وسد أي فراغ محتمل في النظام القانوني الذي يحكم هذا التعاون، وبما يسمح بالتبادل السريع بين الدول والاستجابة السريعة لطلبات

المعلومات والمساعدة الإجرائية، مع ضرورة إنشاء مركز دولي لمكافحة الجرائم الإلكترونية، لتبادل الخبرات والمعلومات بين الدول من أجل مكافحتها.

7. لا بد أن يعمل الأفراد والمؤسسات والدول على تعزيز أمن المعلومات في مواجهة الجرائم الإلكترونية، وذلك من خلال الاستفادة من معايير المجموعة الدولية الخاصة بإدارة أمن المعلومات، مثل معيار **ISO27001** و**ISO27002**، وهذه هي المعايير المعترف به دوليًا في مجال أمن المعلومات.

قائمة المصادر والمراجع

أولًا- المراجع العربية:

1- الكتب:

1- أحمد محمود خليل: الجريمة المنظمة، الإرهاب وغسل الأموال، المكتب الجامعي الحديث، الإسكندرية، 2009م.

2- أيمن عبد الحفيظ: مكافحة الجرائم المستحدثة، أكاديمية شرطة دبي، دبي، الطبعة الأولى، 2006م.

3- حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، الكتاب الثالث، أكاديمية العلوم الشرطية، الشارقة، الطبعة الأولى، 2009م.

4- خالد خلفان أحمد المنصوري: إطلالة معرفية على شبكات التواصل الإجتماعي "الفيسبوك – التويتر – اليوتيوب"، أكاديمية شرطة دبي، دبي، 2013م.

5- خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009م.

6- زكي أحمد محمد الجبلي: تأمين المعلومات في الأزمات الأمنية، دراسة تطبيقية لتأمين المعلومات بشرطة دبي، أكاديمية شرطة دبي، دبي، 2013م.

7- سعيد علي بحبوح النقبي: المواجهة الجنائية للإرهاب، في ضوء الأحكام الموضوعية والإجرائية للقانون الدولي والداخلي، "دراسة مقارنة"، دار النهضة العربية، القاهرة، الطبعة الأولى،2011م.

8- سعيدي سليمة: أمن المعلومات وأنظمتها في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017م.

9- السيد أحمد محمد مرجان: دور الإدارة العامة الإليكترونية والإدارة المحلية في الارتقاء بالخدمات الجماهيرية، دراسة مقارنة، بين الإدارة المحلية في مصر وبلدية دبي في دولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة، الطبعة الثانية، 2010م.

10- السيد عبد الفتاح على: مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2017م.

11- طارق إبراهيم الدسوقي: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009م.

12- طارق أحمد صالح الخطيبي الفلاسي: أحكام تسليم المجرمين في قانون التعاون القضائي الدولي في المسائل الجنائية في ضوء الاتفاقيات الدولية، أكاديمية شرطة دبي، دبي، 2016م.

13- عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، 2009م.

14- عزيزة علي عبد العزيز جمعدار: الجرائم المنظمة بين التقدم العلمي والمكافحة الأمنية، مطبعة رأس الخيمة الوطنية، رأس الخيمة، الطبعة الأولى، 2012م.

15- عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، جامعة الإسكندرية، كلية الحقوق، 2000م.

16- علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، جرائم الحاسوب والإنترنت، 2009م.

17- غادة نصار: الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017م.

18- فخري محمود خليل: جرائم البلطجة الإلكترونية، تتحدى التشريعات والقضاء وتدعم المجرم والجريمة المستحدثة، دراسة مقارنة، الناشر "المؤلف"، القاهرة، الجزء الأول، 2019م.

19- فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2016م.

20- لينا محمد الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، دار الحامد للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2015.

21- ليندا بن طالب: غسل الأموال وعلاقته بمكافحة الإرهاب "دراسة مقارنة"، دار الجامعة الجديدة، الإسكندرية، 2011م.

22- محمد سامي الشوا: التعاون الأوروبي في مجال مكافحة الجريمة المنظمة، أكاديمية العلوم الشرطية، الشارقة، 2017م.

23- محمد عبيد الكعبي: الحماية الجنائية للتجارية الإلكترونية، دار النهضة العربية، القاهرة، 2010م.

24- محمد كمال شاهين: الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2018م.

25- محمد محمود المكاوي: الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتبة العصرية، المنصورة، 2010م.

26- ناير نبيل عمر: الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012م.

2- البحوث العلمية:

27- أحمد عبادة العربي: معيار المنظمة الدولية للتوحيد القياسي آيزو 27002 لسياسة أمن المعلومات، دراسة وصفية تحليلية لمواقع الجامعات العربية، مجلة جامعة طيبة، العدد 7، السنة 4، المدينة المنورة، 2015م.

28- جميل عبد الباقي الصغير: مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الإنترنت، مجلة الأمن والحياة، العدد 329، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009م.

29- حمد عبد الرحمن حمد المظلوم: المواجهة الأمنية للجرائم العابرة للحدود، أكاديمية شرطة دبي، كلية الدراسات العليا، 2013م.

30- الراشد سالم عبيد سالمين ولد راحة: عرض التجارب والخبرات الأمنية المختلفة في التعامل مع جرائم تقنية المعلومات والاتصالات الخاصة بالأطفال، مركز بحوث الشرطة، أكاديمية شرطة دبي، دبي، الطبعة الأولى، 2010م.

31- شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة، المجلد 17، العدد1، الشارقة، يونيو 2020م.

32- صالح شنين: الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراة، جامعة أبوبكر بلقايد تلمسان، كلية الحقوق، غير منشورة، الجزائر، 2013م.

33- عادل عبد العال ابراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015م.

34- عبد الرزاق قايد صالح: الأزمات الأمنية الناشئة عن الإرهاب، كظاهرة إجرامية، رسالة ماجستير، أكاديمية شرطة دبي، أكاديمية شرطة دبي، 2010م.

35- عبد العزيز الزدجال: التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، رسالة ماجستير، أكاديمية شرطة دبي، دبي، 2014م.

36- عبد العزيز حسن الحمادي: نشاط المنظمة الدولية للشرطة الجنائية (الانتربول) وأنشطتها في ضوء القانون الدولي، مركز بحوث الشرطة، شرطة الشارقة، الطبعة الأولى، 2013م.

37- عبد العزيز خنفوسي: الآليات المستحدثة من طرف منظمة الإنتربول بغية التصدي للإجرام الدولي المنظم، الفكر الشرطي، مركز بحوث شرطة الشارقة، القيادة العامة لشرطة الشارقة، الشارقة، المجلد (21) العدد (83)، أكتوبر 2012م.

38- عبد الله علي سعيد بن ساحوه، ومحمد الأمين البشري: العدالة الجنائية مفهومها نظمها وتطبيقات دولة الإمارات العربية المتحدة، مركز بحوث الشرطة، شرطة الشارقة، الشارقة، الطبعة الأولى، 2013م.

39- عمر عباس خضير العبيدي: مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الوقائي، مركز الدراسات العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2020م.

40- محمد المتولي: التخطيط الاستراتيجي في مكافحة جرائم الإرهاب الدولي، دراسة مقارنة، مجلس النشر العلمي، جامعة الكويت، الطبعة الأولى، 2006م.

41- مروان جمعة بن بيات الفلاسي: انعكاسات الأزمات الإقليمية والعالمية الراهنة على الأمن والاستقرار الداخلي في دولة الإمارات العربية المتحدة، دراسات

شرطية، سلسة الرسائل العلمية، أكاديمية شرطة دبي، كلية القانون وعلوم الشرطة، 2011م.

42- مريم عثمان عبد القادر: الحماية الجنائية للطفل من الجرائم الإلكترونية، في ضوء القانون الإماراتي، دراسات قانونية، رسالة ماجستير، أكاديمية شرطة دبي، كلية الدراسات العليا، دبي، 2104م.

ثانياً- القوانين والقرارات والاتفاقيات:

43- الموجهات الإرشادية للمواقع الإلكترونية الاتحادية، هيئة تنظيم الاتصالات TRA، الإمارات العربية المتحدة، 2016م.

44- قانون رقم 17 لسنة 2023 بشأن قانون الجرائم الإلكترونية، والمنشور بالجريدة الرسمية، رقم 5874، الصادر بتاريخ 2023/8/13م.

45- القانون الاتحادي (3) لسنة 2012م بشأن إنشاء الهيئة الوطنية للأمن الإلكترونية.

46- القانون الاتحادي رقم (39) لسنة 2006م في شأن التعاون القضائي الدولي في المسائل الجنائية.

47- القانون الاتحادي رقم (3) لسنة 2003م في شأن تنظيم قطاع الاتصالات الإماراتي، والمنشور بالجريدة الرسمية العدد 421، السنة 34، أبريل 2004م.

48- القانون رقم (11) لسنة 2014م في شأن مركز دبي للأمن الإلكتروني، والمنشور في الجريدة الرسمية، حكومة دبي، العدد 379، السنة 48، يوليو 2014م.

49- القانون رقم (175) لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات المصري، والمنشور بالجريدة الرسمية، العدد 32 مكرر (ج) في 14 أغسطس سنة 2018م.

50- قرار مجلس الوزراء رقم (21) لسنة 2013م بشأن لائحة أمن المعلومات في الجهات الاتحادية، مجلس الوزراء، الإمارات العربية المتحدة.

51- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لعام 2010م.

52- قرار مجلس الوزراء رقم (13) لسنة 2023 بشأن لجنة مكافحة التهديدات السيبرانية والبرامجيات الخبيثة.

ثالثاً- المواقع الإلكترونية العربية:

53- جاسم بوعتابة الزعابي: الاطار الوطني لضمان أمن المعلومات، الهيئة الوطنية للأمن الإلكتروني، المجلس الأعلى للأمن الوطني، ص47. الموقع الرسمي لدولة الإمارات العربية المتحدة، تاريخ الدخول: 2023/12/1م.
https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation

رابعاً– المواقع الإلكترونية الأجنبية:

54- Conention on cybercrime, Budapest, 23Xl.2001, Details of Treaty no. 185, Council of Europe, P1, Date of entry: 15/1/2023
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

خامساً– المراجع الاجنبية:

55- Neil Robinson and Luke Gribbon, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime, Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders, European Network and Information Security Agency (ENISA), 2012.

56- Prof. Dr. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, The ITU publication Understanding cybercrime: phenomena, challenges and legal response has been, September 2012.

57- Stein Schjolberg, The History of Global Harmonization on Cybercrime, Legislation - The Road to Geneva, December, 2008.