ElQarar Journal for Peer-Reviewed Scientific Research | Issue 27, Vol 9, Year 3 | March 2026 | Ramadan 1447
ISSN 7294-3006

التحديات القانونية لمكافحة الجرائم الإلكترونية

إعداد: الباحث / أسامه صالح عبد المهدي | جمهورية العراق

طالب دكتوراه في الحقوق / القانون العام | الجامعة الإسلامية في لبنان

E-mail: wwww.2000.2004@gmail.com | https://orcid.org/0009-0008-7388-0578
https://doi.org/10.70758/elqarar/9.27.19

تاريخ الاستلام: 2026/2/28	تاريخ القبول: 2026/3/14	تاريخ النشر: 2026/3/15

للاقتباس: عبد المهدي، أسامة صالح، التحديات القانونية لمكافحة الجرائم الإلكترونية، مجلة القرار للبحوث العلمية المُحكّمة، المجلد التاسع، العدد 27، السنة 3، 2025، ص-ص: 449-471. https://doi.org/10.70758/elqarar/9.27.19

المُلخّص

يتناول هذا البحث التحديات القانونية المرتبطة بمكافحة الجرائم الإلكترونية في ظل التطور التكنولوجي السريع والانتشار الواسع لتقنيات المعلومات والاتصالات. فقد برزت الجرائم الإلكترونية كأحد أشكال النشاط الإجرامي الحديثة الناتجة عن التطور في أنظمة الحاسوب والشبكات الرقمية ونظم المعلومات، والتي أصبحت أدوات أساسية في مختلف القطاعات العامة والخاصة. وعلى الرغم من الفوائد الكبيرة للتقدم التكنولوجي، إلا أن هذه التطورات أوجدت في الوقت ذاته فرصاً جديدة لارتكاب أنشطة إجرامية يصعب اكتشافها أو تنظيمها في إطار القواعد القانونية التقليدية. يهدف البحث إلى توضيح مفهوم الجريمة الإلكترونية، وبيان أهم خصائصها، وتحليل أبرز التحديات القانونية التي تواجه مكافحتها. كما يركز بشكل خاص على الصعوبات الإجرائية المتعلقة بعمليات التحقيق وجمع الأدلة وتحديد الاختصاص القضائي، لا سيما عندما تتجاوز الجرائم الإلكترونية الحدود الوطنية. ويخلص البحث إلى أن مواجهة الجرائم الإلكترونية تتطلب تطويراً مستمراً للأنظمة القانونية وتحديث التشريعات الجزائية، إضافة إلى تعزيز التعاون الدولي في هذا المجال. كما أن تنمية القدرات القانونية والتقنية تعد أمراً أساسياً من أجل الوقاية من هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها بفعالية في البيئة الرقمية المتطورة.

الكلمات المفتاحية: الجريمة الإلكترونية؛ الأدلة الرقمية؛ الأمن السيبراني؛ القانون الجزائي؛ الجرائم العابرة للحدود.

مجلة القرار للبحوث العلمية المحكّمة | العدد 27، المجلد 9، السنة الثالثة | آذار (مارس) 2026 | رمضان 1447
ISSN 3006-7294

Legal Challenges in Combating Cybercrime

Author: Researcher / Osama Saleh Abdul-Mahdi | Iraq Republic
PhD student in law / Public Law | Islamic University of Lebanon
E-mail: wwww.2000.2004@gmail.com | https://orcid.org/0009-0008-7388-0578
https://doi.org/10.70758/elqarar/9.27.19

Received : 28/2/2026	**Accepted :** 14/3/2026	**Published :** 15/3/2026

Cite this article as: *Abdul-Mahdi, Osama Saleh, Legal Challenges in Combating Cybercrime, ElQarar Journal for Peer-Reviewed Scientific Research, vol 9, issue 27, Third year, 2026, pp. 449-471. https://doi.org/10.70758/elqarar/8.27.19*

Abstract

This research examines the legal challenges associated with combating cybercrime in the context of rapid technological development and the widespread use of information and communication technologies. Cybercrime has emerged as a modern form of criminal activity resulting from advancements in computer systems, digital networks, and information systems, which have become essential tools in both public and private sectors. Despite the benefits of technological progress, these developments have also created new opportunities for criminal activities that are difficult to detect and regulate using traditional legal frameworks.

The study aims to clarify the concept of cybercrime, identify its main characteristics, and analyze the most significant legal challenges that arise in addressing such crimes. Particular attention is given to procedural difficulties related to investigation, evidence collection, and the determination of jurisdiction, especially when cybercrimes cross national borders. The research also highlights the limitations of existing criminal legislation in effectively responding to technologically advanced forms of crime. The study concludes that addressing cybercrime requires the continuous development of legal systems, the modernization of criminal legislation, and enhanced international cooperation. Strengthening legal and technical capacities is essential to effectively prevent, investigate, and prosecute cybercrimes in the evolving digital environment.

Keywords: Cybercrime; Digital Evidence; Cybersecurity; Criminal Law; Transnational Crime.

المقدمة

تعتبر الجريمة الإلكترونية ثمرة من ثمار التقدم السريع الذى حدث مؤخرًا في تكنولوجيا المعلومات، وتعتبر من أهم وأخطر الصعوبات والتحديات الأمنية التي تواجه كافة المجتمعات البشرية في الوقت الحالي, وخاصة في مجال استخدامات تقنية المعلومات والاتصالات في مؤسسات القطاع العام والخاص والأفراد، فقد تميز القرن العشرين باختراعات هائلة على المستوى التقني لعل من اهمها ظهور الحاسبات الإلكترونية والذي تطور بالشكل الذي أفضى الى استحداث شبكات المعلومات ونظم المعلومات حتى بات يطلق على هذه التقنية بالنظام المعلوماتي.

ولما كانت جرائم الحاسبات الإلكترونية أو كما تسمى (جرائم المعلوماتية) لارتباطها بنظم المعالجة الآلية للمعلومات هي ظاهرة اجرامية حديثة النشأة لتعلقها بتكنولوجيا الحاسبات الآلية فقد اكتنفها الغموض بالشكل الذي دعا الكثيرين الى القول بأن الجريمة المعلوماتية هي أشبه بالخرافة، وانه لا يوجد أي تهديد حقيقي منبعه الحاسبات الإلكترونية، وان كانت هناك اشكال للسلوك غير المشروع التي ترتبط بالحاسبات الإلكترونية فهي جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها.

وتواجه الجرائم الإلكترونية العديد من التحديات القانونية، فهناك التحديات الإجرائية وهناك التحديات المتعلقة بسلطة العقاب والتحري وهناك التحديات المتعلقة بالقانون الواجب التطبيق على هذا النوع من الجرائم، ومنبت تلك الصعوبات يرجع إلى حداثة هذا النوع من الجرائم وعدم تطور التشريعات الجنائية لمواجهته.

إشكالية الدراسة

إن قدرة التشريعات الوطنية على مكافحة الجريمة تعد معيارا يقاس به درجة تقدم تلك التشريعات ومقدرتها على تحقيق أهدافها القانونية، فمما لا شك فيه أن التشريعات تهدف إلى حماية المواطنين من الجرائم، وهناك تحديات تواجه الجرائم الإلكترونية، تحتاج في معالجتها لمعرفة ماهية هذا النوع المستحدث من الجرائم، وهو ما يتطلب معرفة هذه التحديات وتحديد ماهيتها.

تساؤلات الدراسة

سيقوم الباحث من خلال الدراسة بالإجابة على التساؤلات الآتية:

ما المقصود بالجريمة الإلكترونية؟.

ما هي خصائص الجريمة الإلكترونية؟.

ما هي أهم مظاهر التحديات التى تواجه الجرائم الإلكترونية على المستوى القانوني؟.

أهداف الدارسة

تهدف الدراسة إلى الوقوف على عدة نقاط:

الوقوف على تعريف الجريمة الإلكترونية.

التعرف على أهم الخصائص التي تتمتع بها الجريمة الإلكترونية.

الوقوف على أهم التحديات الإجرائية التي تواجه مكافحة الجرائم الإلكترونية.

التعرف على أهم تحديات القانون الواجب التطبيق على الجرائم الإلكترونية.

منهج الدراسة

يتبع الباحث في معالجة الموضوع المنهج التحليلي والمنهج الاستنباطي

المنهج التحليلي: وذلك بتحليل نصوص القانون المرتبطة بمكافحة الجرائم الإلكترونية، مثل قوانين تقنية المعلومات، من أجل الوقوف على مناطق الضعف والقوة.

المنهج الاستنباطي: والقائم على استنباط الأفكار والحلول بعد تحليل النصوص.

خطة الدراسة

المبحث الأول: التعريف بالجرائم الإلكترونية

المبحث الثاني: أهم الإشكاليات التي تواجهه مكافحة الجرائم الإلكترونية

المبحث الأول

التعريف بالجرائم الإلكترونية

تمهيد وتقسيم

تعتبر الجريمة الإلكترونية موضوعا واسعا، فهي ظاهرة إجرامية تعاني منها المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية، ولقد تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم، سواء في التشريع المقارن أو في التشريع الأمريكي، حيث أثيرت العديد من التساؤلات حول تحديد تعريف جامع لهذه الجريمة العالمية.

فظهرت عدت تعريفات دارت كلها حول مفهوم أن الجريمة الإلكترونية هي جريمة مستخدمة بواسطة الوسائل الإلكترونية، وقد أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم حيث ظهرت عدة آراء فقهية في محاولة فهم المقصود بالجريمة الإلكترونية، وتحديد تعريف لها وبيان طبيعتها القانونية.

كما أن تعريف الجريمة الإلكترونية يستوجب الإلمام بالجانب الموضوعي والإجرائي لها، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة، والإحاطة بالأمور الفنية لها.

هذا ما نتناوله في هذا المبحث والذي قسمته إلى مطلبين على النحو الآتي:

المطلب الأول: تعريف الجريمة الإلكترونية

لم يتفق الفقه على تعريف جامع مانع للجرائم الإلكترونية، ويرجع ذلك لغياب تنظيمها تشريعيًا في مختلف دول العالم وحداثة نشأتها مقارنة بغيرها من الجرائم نظرًا لغياب تعريف قانوني لهذا النوع من الجرائم في أغلب التشريعات، بالإضافة إلى غياب مصطلح قانوني موحد للدلالة على ماهية الجرائم الناشئة عن استغلال غير القانوني لتقنية المعلومات واستخدامها.

وفي ظل هذا الفراغ القانوني حاول الفقه إيجاد تعريف للجرائم الإلكترونية، والملاحظ أن الفقة قد انقسم بدوره إلى اتجاهين رئيسيين وهذا بالنظر الى الزاوية التي ينظر من خلالها لهذا النوع من الجرائم، حيث أن الاتجاه الأول مضيّق لمفهوم الجريمة الإلكترونية، أما الاتجاه الثاني فقد حاول التوسع في تعريف الجريمة الإلكترونية.

أولاً: التعريف الضيق للجريمة الإلكترونية

من التعريفات التي وضعها أنصار هذا الاتجاه أيضا ما ذهب إليه الفقيه (Merwe)، حيث يرى أن الجريمة الإلكترونية: ماهي إلا الفعل غير المشروع الذي يدخل في ارتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في ارتكابه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات [1].

وعرفها جانب آخر من الفقة بأنها: « الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورًا هامًا، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية «[2].

كما عرفتها الدكتورة هدى قشقوش هي: « كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات»، كما عرفتها بأنها «أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات»[3].

ثانيًا: التعريف الواسع للجريمة الإلكترونية

تناول رأي آخر من الفقه تعريف الجريمة الإلكترونية بأنها: «عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابًا»[4].

كما عرفت الجريمة الإلكترونية في إطار المنظمة الأوروبية للتعاون والتنمية الاقتصادية بأنها: « كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية « [5].

وجاء تعريف الجريمة الإلكترونية في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا سنة 2000 بأنها «يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية

(1) د. طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص 153

(2) من أنصار هذا الجانب راجع د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص 25

(3) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 25

(4) د. طارق إبراهيم الدسوقي، الأمن المعلوماتي، مرجع سابق، ص 158

(5) د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، مرجع سابق، ص 26

المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية»[1].

وفي النهاية نقول أن هذا الاتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يسقط وصف الجريمة الإلكترونية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسوب الآلي في النشاط الإجرامي فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا فلا يمكن إعطاؤها وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محلا لفعل الاختلاس.

المطلب الثاني: خصائص الجريمة الإلكترونية

أدى ارتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الإنترنت إلى إضفاء مجموعة من الخصائص و السمات المميزة لهذه الجريمة عن الجرائم التقليدية ويمكن إجمالها في ما يلي:

أولا: الجريمة الإلكترونية جريمة عابرة للحدود

إن أول خاصية تميز بها الجريمة الإلكترونية، أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الإنترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، بسبب السرعة الهائلة في تنفيذها. يمكن أن تقع الجريمة من طرف الجاني في دولة والمجني عليه في دولة أخرى في وقت يسير جدّا.

في عصر الحاسب الآلي ومع انتشار شبكة الإنترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، بحيث يغدو أمر التنقل والاتصال فيما بينها أمرًا سهلا، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة في هذه البيئة، يمكن أن توصف جرائم التقنية بأنها جرائم عابرة لحدود الدول، إذ غالبًا ما يكون الجاني في بلد ومجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه، تتخذ الجرائم الإلكترونية شكلا جديدًا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية [2].

إن الخاصية التي تتميز بها الجريمة الإلكترونية أوجدت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق، بالإضافة إلى إشكالية تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة

(1) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011 ، ص 28

(2) أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان ، 2014 ، ص 93

للحدود بشكل عام [1].

ثانيًا: صعوبة الاكتشاف والإثبات

نظرًا للطبيعة الخاصة الذي تتميز بها الجريمة الإلكترونية فإن إثباتها يحيط به كثير من الصعوبات، والتي تتمثل في صعوبة اكتشاف هذه الجرائم، لأنها لا تترك أثرًا خارجيًا، فالجريمة الإلكترونية لا عنف فيها ولا أثر اقتحام لسرقة مثلا، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، وبمعنى آخر فإن الجريمة الإلكترونية هي جريمة فنية، وهي جريمة هادئة لا تتطلب العنف[2].

فبما أن تعتبر الجريمة الإلكترونية جريمة مستحدثة، فهي تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، على اعتبار هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء كان في تجميعها أو في إدخالها إلى الحاسوب المرتبط بشبكة المعلومات، ولغرض الحصول على معلومات معيّنة، وقد ترتكب هذه الجرائم في معالجة الكلمات أو النصوص، وتمكن المستخدم من تحرير الوثائق والنصوص على الحاسوب مع إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة [3].

ثالثًا: الجرائم الإلكترونية مغرية للمجرمين

وإذا كانت الجرائم التقليدية تحتاج إلى استخدام الأدوات والوسائل المادية والعنف غالبًا كما هو الحال في جرائم المخدرات والإرهاب، والسطو المسلح، إلا أن الجرائم المعلوماتية تمتاز بأنها جرائم ناعمة لا تتطلب العنف على الإطلاق، فكل ما يحتاجه المجرم المعلوماتي هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظفه في ارتكاب الأفعال غير المشروعة، ويحتاج كذلك إلى وجود شبكة المعلومات الدولية، بالإضافة إلى الإرادة في تحقيق الغرض الإجرامي وكل ذلك دون عنف [4].

(1) عنية باطلي الجريمة الإلكترونية «دراسة مقارنة»، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص49 و د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، 22010،ص 45

(2) د. جعفر حسن الطائي، جرائم تكنولوجياالمعلومات، رواية جديدة للجريمة الحديثة، ط 1، جامعة عمر المختار، 2007، ص 53

(3) د. عفيفي كامل، جرائم الكمبيوتر وحقوق المِؤلف والمصنفات الفنية و دور الشرطة و القانون «دراسة مقارنة»، منشورات الحلبي الحقوقية ، الإسكندرية، 2007 ، ص 270

(4) د. خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، ص 37

رابعًا: قلة الإبلاغ عن الجريمة الإلكترونية

تتميز الجرائم الإلكترونية بأن المجني عليه يحجم عن طلب مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها، حتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفًا مما يترتب عليه من دعاية مضرة، وضياع ثقة المساهمين، في الحالة التي يكون فيها المجني عليه عادة بنكًا أو مؤسسة مالية (شخصًا معنويًا) يهمه المحافظة على سمعته وثقة عملائه، أكثر من اهتمامه بالكشف عن الجريمة ومرتكبيها، لذلك يفضل المجني عليه تقديم ترضية سريعة لعميله، وينهي الأمر داخليًا.

كما أن للمجني عليه دور مثير للريبة، قد يشارك بطريقة غير مباشرة في ارتكاب السلوك الإجرامي، ذلك في الحالة التي يكون فيها مثلًا المجني عليها امرأة، تمّ التحرش بها وابتزازها عبر مواقع التواصل الاجتماعي (Facebook) فتضطر الضحية للرضوخ لطلبات المجني خشية من تشويه سمعتها[1]، لكن هناك حالات ضئيلة يتم الإبلاغ فيها عن الجرائم الإلكترونية نسبة إلى شخصية المجني التي تلعب دورا مهما في عملية الإبلاغ.

(1) شهدت دولة الجزائر في السنوات الأخيرة تضاعف مخيف للجرائم الإلكترونية، التي باتت تهدد كيان المجتمع، حيث تقول زهرة فاسي أستاذة في علم الاجتماع أن أكثر عرضة لهذا النوع من الجرائم هن النساء اللاتي لا يبلغن عن الفاعل خوفًا من الفضيحة، مشيرة أن العديد من الفتيات رضخن للابتزاز وسلمن مبالغ مالية ضخمة مقابل عدم نشر صورهن على سبيل المثال، ومنهن من هربت من بيوت الأهل خوفًا من الفضيحة. ينظر: إلى مقال صحفي، باسم خديجة بدوميس، الجزائر www.dw.com

المبحث الثاني

أهم الإشكاليات التي تواجه مكافحة الجرائم الإلكترونية

تمهيد وتقسيم

لقد كان لارتباط الجريمة الإلكترونية بجهاز الحاسب الآلي من جهة وشبكة الإنترنت من جهة أخرى أن نتج عن ذلك عدة صعوبات سواء في طابع الجريمة وأساليب مواجهتها أم أساليب التحقيق فيها.

فقد نتج عن الدمج بين وسائل الحوسبة وطرق الاتصال إلى ظهور مفهوم جديد يعرف بتقنية المعلومات، الذي يتيح التبادل الواسع لمختلف أنماط المعلومات والبيانات في بيئة رقمية، إلا أن الاستخدام السيئ لتقنية تكنولوجيا المعلومات نتج عنه ما يعرف بجرائم المعلوماتية، والتي أصبحت تشكل هاجسا وتحديًا كبيرًا للجهات التشريعية والقضائية وحتى الأمنية من أجل مواجهتها.

تعتبر جريمة المعلوماتية من جرائم العصر الرقمي التي تمس المعلومات بكافة أشكالها والتي تمخضت عن الاستغلال السيئ لتكنولوجيا المعلومات، فقد تسببت في انقلاب خطير في مفهوم النظرية التقليدية للجريمة والتي ترتكب من قبل المجرم المعلوماتي، وقد نتج عن هذا الأمر ضرورة استحداث أساليب خاصة للتحري و التحقيق فيها، وكذا آليات مسبقة للوقاية منها سواء على المستوى الوطني أو الدولي باعتبارها من الجرائم العابرة للحدود والتي لا تعترف بالحدود الجغرافية، بمعنى تتيح شبكة الإنترنت لأي مستخدم على مستوى أغلب دول العالم تحميل ونشر البيانات والمعلومات في غضون ثوان معدودة و بمجرد ضغطة زر على لوح المفاتيح.

هذا ما نتناوله في هذا المبحث والذي قسمته إلى ثلاثة مطالب على النحو الآتي:

المطلب الأول: مظاهر التحديات الإجرائية

المطلب الثاني: التحديات المتعلقة بسلطة التحري والعقاب

المطلب الثالث: التحديات المتعلقة بالقانون الواجب التطبيق

المطلب الأول: مظاهر التحديات الإجرائية

تتخذ الصعوبات الإجرائية عدة صور في مجال الجريمة الإلكترونية، وتنبع تلك الصعوبات من ذاتية الجريمة الإلكترونية وما تتمتع به من سمات تميزها عن غيرها من الجرائم التقليدية، وطبيعتها الخاصة.

أولا: التحديات المتعلقة بذاتية الجريمة الإلكترونية

تظهر التحديات من منبت الجريمة الإلكترونية، فتتنوع الجريمة الواقعة من جهاز واحد ونتج عن ذلك تعدد أنواع هذه الجرائم:

الجريمة المادية: هي تلك الجريمة التي ينتج عنها أضرار مادية على الضحية أو المستهدف من عملية النصب وتظهر في واحدة من الأشكال الثلاثة التالية [1]:

– عملية السرقة الإلكترونية مثل الاستيلاء على ماكينات الصرف الآلي، والبنوك كتلك المنتشرة في الكثير من الدول وبها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ثم استخدامها لصرف أموال حساب الضحية.

– إنشاء صفة إنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة.

– الرسائل البريدية الواردة من مصادر غير معروفة بخصوص طلب المساهمة في تحرير الأموال من الخارج من الوعد بنسبة من المبلغ أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب.

الجريمة الثقافية: هي تلك الجريمة التي يتنج عنها استيلاء المجرم على الحقوق الفكرية ونسبتها له دون موافقة الضحية وتكون على إحدى الصور الآتية [2]:

– قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل.

– التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الإنترنت من خلال تقنية « سوفت كوبي «.

– جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة.

الجريمة السياسية والاقتصادية: تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويل بعض الأموال في سبيل تحقيق أهدافهم، وتأخذ تلك الجريمة عدة صور منها.

(1) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص 96 وما بعدها

(2) د. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013 ، ص 31

– الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات.

– نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

الجريمة الجنسية: هذا النوع من الجريمة يمكن أن يتمثل في إحدى الصور الآتية:

– الابتزاز: من أشهر مظاهر الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وفيه مجموعة من صورها وإجبارها على الخروج معه أو فضحها بما يملكه من صورها.

– التغرير والاستدراج: في العادة هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر برامج المحادثة يكون مع علاقة معها ثم يستدرجها بالكلام ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها بما يملكه من صور وتسجيلات من صوتها إن لم تستجب لرغباته [1].

الجرائم الواقعة على الأفراد: هي تلك الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير شرعية، كحسابات البريد الإلكتروني وكلمات السر التي تخصهم وقد تصل إلى انتحال شخصياتهم وأخذ صور وملفات المهمة من أجهزتهم بهدف تهديدهم وينطوي تحت هذا القسم من الجرائم كل من [2]:

– جرائم التشهير بهدف تشويه سمعة الأفراد.

– جرائم السب والشتم والقذف.

– جرائم المطاردة الإلكترونية.

ثانيًا: صعوبات مكافحة الجريمة الناتجة عن طبيعتها الإلكترونية

ترتب على ظاهرة الجريمة الإلكترونية تحديات عدة: منها ظهور وتنامي الأنشطة الإجرامية الإلكترونية وتَوَسُّل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها، الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها، من حيث تستعصي بعض الأنشطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين

(1) د. نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الإلكترونية، جامعة المسيلة، 2018، ص 25
(2) د. بن سولة نور الدين، الجرائم الإلكترونية في ضوء التشريع الجزائري، المجلد التاسع، العدد 1، مارس 2018 ، ص 272

الجنائية الوطنية والأجنبية ؛ ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية.

من أهم التحديات التي تواجه الجريمة الإلكترونية تلك الصعوبة الناتجة عن طبيعتها الإلكترونية، فيعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية، وذلك للأسباب التالية [1]:

– يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.

– صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الإنترنت باستخدام اسم مستعار، وغالبا ما يقوم بالدخول للإنترنت عن طريق مقاهي الإنترنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.

– تنازع القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين سوف يخضع لها الجاني؟.

– صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الاتصال، أم مورد المنافذ، أم مورد المعلومات، أو غيرهم من العاملين في مجال الإنترنت.

المطلب الثاني: التحديات المتعلقة بسلطة التحري والعقاب

يتعرض التحقيق والبحث والتحري في الجرائم المعلوماتية للعديد من العراقيل والصعوبات التي تعيق الوصول للحقيقة وإثباتها نسبتها لمرتكبيها، مما يسجل عجز جهات التحقيق عن مواجهة الإجرام المعلوماتي والتصدي له، إما بسبب الطبيعة الخاصة للإجرام المعلوماتي والجهات المتضررة، أو معوقات خاصة بجهات التحقيق، وأخرى تشريعية:

أولاً: الصعوبات الخاصة بالجهات المتضررة

بالنسبة للصعوبات المتعلقة بالجهات المتضررة فتمثل في النقاط التالية:

1- عدم إدراك مسؤولي المؤسسات لخطورة الجرائم المعلوماتية التي تهدد كيانها كونها

(1) د. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة) ، دار البلدية، عمان الأردن، 2007، ط 1 ، ص220 وما بعدها

تستخدم النظام المعلوماتي لتقديم خدماتها لعملائها بشكل أسرع [1].

2- إحجام المتضررين من الجريمة المعلوماتية من أفراد ومؤسسات عن الإبلاغ عنها، إما لعدم علمهم بها أصلا أو خوفا من الفضيحة أو الظهور بمظهر مشين أمام الآخرين، ويعطي انطباعا بقمة خبرة هذه المؤسسات وعدم اتخاذها إجراءات الحماية الأمنية لأنظمتها المعلوماتية وتقرر تفضيل سمعة المؤسسة ومصداقيتها على الإبلاغ عنها [2].

فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدًا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ نظام الحاسوب الآلي أو الشبكة أو في الأجهزة.

و عدم إدراك خطورة جرائم الحاسوب والإنترنت من قبل المسؤولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالإنترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة وإذا تعلق الأمر بالمؤسسات المالية أو ما شابهها [3].

ثانيًا: صعوبات تتعلق بالجهات القائمة بالتحقيق

يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها.

1- قلة خبرة القائمين بالتحقيق في هذه الجرائم

لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارات في استخدام جهاز الحاسوب والإنترنت، وعدم توافر المعرفة بأساليب ارتكاب الجرائم الإلكترونية، وقلة الخبرة

(1) د. طارق عبدالله الشدي، آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، 1423 هـ، ص 210
(2) د. خالد عياد الحلبي، المرجع السابق، ص 225
(3) يوسف جفال، التحقيق في الجريمة الإلكترونية، بدون ناشر، 2016 ، ص 43

في مجال التحقيق في جرائم الحاسوب والإنترنت وقلة المعرفة باللغة الأجنبية لا سيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات [1].

2- الصعوبات التقنية لاستخدام بروتوكولTCP / IP في الإثبات [2]

هناك تحديات عند استخدام المحقق بروتوكولTCP / IP، كدليل إلكتروني للإثبات وهي [3]:

- بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصًا محددا أحدث الفعل غير المشروع، ومع ذلك يمكن أن يستخدم كقرينة قضائية ضد مالك الجهاز إلى أن يثبت العكس.

- الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الاتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا موزعا على عدة عناوين.

- تكون المعلومات المحملة لمصدر عنوان بحيث يظهر بأن المعلومات جاءت من حاسوب IP باستخدام مصدر زائف لمصدر عنوان محدد وفي الحقيقة جاءت من حاسوب آخر.

3- ارتفاع تكاليف جمع الأدلة

إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بتكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا.

4- عدم توفر الأجهزة والبرامج الحديثة للكشف عن الجرائم المعلوماتية وتتبع مرتكبيها وضرورة اللجوء لوحدات تحقيق متخصصة للتحقيق في الجرائم المعلوماتية تضم محققين قضائيين وخبراء فنيين مختصين في مجال تقنية المعلومات على دراية بكل مستجداتها[4].

(1) د. خالد ممدوح إبراهيم، المرجع السابق، ص 69

(2) هو اختصار لكلمة Transmission Control Protocol بروتوكول التحكم في نقل البيلنات وكلمة Inter-net protocol وبرتوكول TCP/IP
هو العصب المحرك للإنترنت يضم مجموعة بروتوكولات مطورة كطريق للتواصل بين مختلف أنواع الحواسيب

(3) د. خالد عياد الحلبي، المرجع السابق، ص 226

(4) د. حنان ريحان مبارك، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، لبنان، ط 1، 2014، ص 361

ثالثا: الصعوبات التشريعية

لقد أدى التطور العلمي في المجال المعلوماتي لظهور أنواع جديدة من الإجرام المعلوماتي وتطور أشكالها ويقابله جمود النصوص التشريعية عن مواجهتها وحصر أنواعها وأركان كل نوع منها ووضع العقوبة المناسبة لها، الأمر الذي أثار عدة إشكالات قانونية، فمن جهة القاضي الجنائي مقيد عند نظره في الدعوى بمبدأ شرعية الجرائم والعقوبات الشرعية الموضوعية أي أنه لا يستطيع تجريم أفعال لم ينص عليها المشرع صراحة حتى ولو كانت هذه الأفعال ضارة أو خطيرة وعلى مستوى عال من الخطورة الإجرامية [1] وكذا حصر القياس في النصوص الجزائية الموضوعية.

المطلب الثالث: التحديات المتعلقة بالقانون الواجب التطبيق

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية، فإننا نعتقد إن كان لهذا الرأي شيئا من الواقعية، وهي أن بعض النصوص القائمة تواجه بعض الأنشطة المجرمة التي ترتكب بطريق الإنترنت، فإنه ينبغي ألا ننكر أن هناك نصوصا أخر صادف تطبيقها بعض الصعوبات.

أولا: عدم وجود اتفاق حول طبيعة النشاط الإجرامي

لم تتفق الأنظمة القانونية في مختلف بلدان العالم على صورة موحدة ونموذج موحد بالاتفاق المشترك بين الدول حول الجريمة المعلوماتية خاصة وأن ما يكون مجرم منها في بعض الأنظمة قد لا يكون كذلك في دولة أخرى[2].

فعدم الاتفاق على صور الإجرام المعلوماتي جعل من البيئة الإلكترونية فضاءً لقراصنة الحاسب الآلي لارتكاب جرائمهم العابرة للحدود.

ثانيا: اختلاف النظم القانونية في تحديد مكان الجريمة الإلكترونية

بسبب هذا الاختلاف قد تكون هنالك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أو لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية، بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات تم جمعه بطرق ترى الدولة الأخرى أنها غير مشروعة أو أن فيها اعتداء على الحريات الخاصة.

غالبا ما يتحدد السريان المكاني للقانون الجنائي الوطني وفقا لأحد مبادئ أربعة: مبدأ الإقليمية ومبدأ الشخصية، ومبدأ العينية، ومبدأ العالمية، وتتفاوت أهمية هذه المبادئ فيما بينها، وتتدرج

(1) د. خالد عياد الحلبي، المرجع السابق، ص 220
(2) د. عبد الفتاح بيومي حجازي، المرجع السابق، ص 188

في أهميتها بحسب ترتيبها، وتأخذ معظم التشريعات الجنائية بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى.

وإعمال السريان المكاني للقانون الجنائي وفقا لأحد المبادئ الأربعة سالفة الذكر، لا يخلو من صعوبات، تفضي تارة إلى إثارة تنازع إيجابي في الاختصاص بين أكثر من تشريع وطني، وتارة أخرى يقوم تنازع سلبي في الاختصاص يخرج معه اختصاص أي من الدول بملاحقة الجاني، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد اختصاصها وفقا لمعايير الاختصاص المعروفة[1] ؛ أما في حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة يثور فيها التنازع كما في الجرائم عبر الوطنية التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، أو في حالة تجرد بعض عناصر هذا السلوك من خصيصتها المادية، كما هو الحال في القرصنة في مجال الحوسبة، وصور المساهمة الجنائية التي تتم باستخدام أجهزة الاتصالات الحديثة ؛ مثل هذه الظاهرة تفرض تنازعا في الاختصاص بل غموضا في تحديد معياره، تتطلب بطبيعة الحال حلولا مستحدثة وابتكارا لمفاهيم قانونية جديدة دون إخلال بمبادئ الشرعية الجنائية التي ترتكز عليها معظم النظم الجنائية الوطنية.

ثالثا: التجريم المزدوج

يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين، وقد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بخصوص الجريمة المعلوماتية، لا سيما وأن معظم الدول مازالت نصوصها العقابية خالية من هذا النمط الإجرامي.

وفي الحقيقة فإن المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب عن هذه الصعوبات وإيجاد تعاون دولي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتحقق من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية [2].

وقد أدركت الدول أهمية التعاون الدولي وأحست بأنه أمر محتِّمٌ لتجاوز تحديات الجرائم الإلكترونية،

(1) الأمر يدق بالنسبة لجريمة غسيل الأموال أو استخدام عائدات الأنشطة الإجرامية غير المشروعة في الدول التي تجرم تشريعاتها هذا النشاط على أساس أنه فعل من أفعال الاشتراك أو كصورة من صور الإخفاء وليس بوصفه جريمة مستقلة ، وفي الحالتين نكون بصدد جريمة تبعية يتبع الاختصاص بملاحقتها الجريمة الأصلية ، وبالتالي يخرج عن اختصاص إحدى تلك الدول ملاحقة مرتكب جريمة غسيل الأموال ، خاصة إذا كان المتهم لا يتمتع بجنسيتها؛ إذن للتغلب على هذا النوع من التنازع السلبي في الاختصاص يتعين تقرير مبدأ الاختصاص العالمي الذي يعطي لدولة القبض على المتهم الاختصاص بملاحقته إذ كان يحمل جنسيتها ، فإن لم يمكن كذلك ، وجب تسليمه في حالة المطالبة به من دولة أخرى وفقا لمبدأ الإقليمية أو الشخصية

(2) سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة للماجيستير، جامعة مولود معمري، الجزائر، 2018، ص 95

فعمد الكثير منها إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الكمبيوتر[1]، ففي عام 1983 أجرت منظمة التعاون و الإنماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية وسوء استخدامه، وفي عام 1985 أصدرت هذه المنظمة تقريراً عن تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب على الدول أن تجرمها و تفرض لها عقوبات في قوانينها ومن أمثلة هذه الأفعال: الغش أو التزوير في الحاسب الآلي، تغيير برامج الحاسب الآلي أو المعلومات المخزنة فيه، سرقة الأسرار المدعمة في قواعد الحاسب الآلي؛ تفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، كما عالجت اتفاقية فيينا لسنة 1988 الموضوع ذاته، وحثت الكثير من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم، وكذلك لفت اللقاء التمهيدي الإقليمي لآسيا و الباسفيك المنعقد 1989 الممهد للمؤتمر الثامن للأمم المتحدة المنعقد في كوريا 1990 النظر إلى نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة، والمؤتمر الأخير ناشد في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف إلى ضرورة تكثيف جهودها لمكافحة الجرائم الإلكترونية في عدة وجوه[2].

رابعًا: عدم الاعتراف في بعض الحالات بحجية التشريعات والأحكام الجنائية غير الوطنية:

القاعدة التقليدية هي تلازم السيادتين التشريعية والقضائية في المجال الجنائي، بما يعني أن كل دولة لا تعترف سوى بأحكام قانونها الجنائي الوطني، ولا تعتد ولا تنفذ على إقليمها سوى الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك سنده في أن تطبيق القانون الجنائي يعد تعبيرًا عن سيادة الدولة بوصفه يحمي المصالح الأساسية للمجتمع والدولة والحقوق الجوهرية لأفراده، إضافة إلى أن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهو ما يحول دون الخضوع لحكم قانون أجنبي وتطبيقه[3].

أما فيما يتعلق بحجية الأحكام الجنائية الأجنبية في شقها الإيجابي[4]، فإنه يجب أن يُفسَحَ لها مكانٌ بين أحكام المعاهدات الدولية ذات الصلة، وهكذا يمكن أن يؤخذ في الاعتبار بالآثار الجنائية

(1) د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة منن 1 – 3 مايو 2000 بكلية الشريعة والقانون بدولة الإمارات، ص1078.

(2) انظر في ذلك د. محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25 –28 أكتوبر، 1993، ص 362

(3) وإذا كان القاضي الوطني يمكنه تطبيق أحكام قانون أجنبي في مجال القانون الدولي الخاص، فإن ذلك راجع إلى أن قواعد القانون الأخير لا تتعلق بحسب الأصل بفكرة النظام العام؛ بل تحمي مصالح خاصة مدنية أو تجارية أو مسائل الأحوال الشخصية.

(4) في معنى الاعتراف بما يتضمنه الحكم من عقوبات وآثار جنائية أخرى.

غير المباشرة للأحكام الجنائية الأجنبية، لا سيّما في الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية، لا سيّما في مجال العود، ووقف التنفيذ وتقدير العقوبة في ضوء ما يثبت من الخطورة الإجرامية للجاني.

أما بالنسبة لحجية الأحكام الجنائية في شقها السلبي، فقد اعترف بها بعض المشرعين[1]؛ إذ يمتنع إقامة الدعوى الجنائية ضد من ارتكب جريمة في الخارج متى ثبت أن المحاكم الجنائية الأجنبية قد برأته أو أدانته نهائيًا، واستوفى عقوبته، فكأن هؤلاء المشرعين يعترفون بقوة الشيء المحكوم فيه، ولو تعلق الأمر بحكم أجنبي، تطبيقًا لقاعدة امتناع محاكمة الشخص عن ذات الفعل مرتين.

ونعتقد أنه حان الأوان لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادتين التشريعية والقضائية في المجال الجنائي، وذلك بالتوجه نحو الاعتراف في بعض الحالات، وعلى نحو ما بحجية لتشريع جنائي عبر وطني؛ بل وبحجية لحكم جنائي صادر عن محاكم دولة أخرى، وتتجلى أهمية ذلك على وجه الخصوص في مجال الجرائم التبعية التي تفترض ارتكاب جريمة أصلية على إقليم الدولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى، ومثال ذلك جريمة الاعتداء على الملكية الفكرية، وقد ظهرت أفكار تنادي بوجوب الاعتراف فيما بين الدول، بحجية الأحكام الجنائية الأجنبية على إقليم الدول الأخرى، وحجة ذلك استفحال ظاهرة الجرائم الإلكترونية، وضرورة تعاون دولي فيما بينها لمكافحتها حتى لا يفلت مرتكبوها من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة وصار ممكنًا الاعتراف بمثل هذه الحجية استنادًا إلى معاهدة دولية تبرم بين الدول.

خامسًا: عدم تطوير قواعد القانون الجنائي فيما يخص نظام المساهمة الجنائية والتقادم

جعل اكتمال البناء القانوني لبعض الأنشطة الإجرامية يستند إلى قيام جريمة أصلية سابقة عليها، كجريمة الاعتداء على الملكية الفكرية، وجريمة تسلم أو إخفاء أشياء مسروقة أو محصلة بأي وجه من الوجوه من جناية أو جنحة (أي المحصلة من مصدر غير مشروع الذي يشكل الجريمة الأصلية)؛ فثمة قوانين وطنية تعاقب على مثل هذه الأنشطة بوصفها من قبيل المساهمة التبعية في الجريمة الأصلية، بمعنى أن مصير ملاحقة مرتكبيها وعقابهم يكون متوقفًا على مصير ملاحقة وعقاب الفاعلين الأصليين للجريمة الأصلية، وقد تتعذر ملاحقتهم لعدم خضوعهم للاختصاص الإقليمي للدولة التي ارتكبت عليه الجريمة التبعية، وهو نهج يترتب عليه التقليل من الحماية الجنائية ويضعف من نظام الملاحقة، على عكس لو اعتبرت هذه الأنشطة جرائم مستقلة بذاتها وليست من الجرائم المساهمة التبعية[2]، والذي من شأنه التقليل من فرص الإفلات من الملاحقة

(1) نص عليها المشرع الليبي صراحة في المادة السابعة من قانون العقوبات.
(2) المادة 465/1 مكررة (أ) من قانون العقوبات الليبي.

والعقاب أمام مرتكبي مثل هذه الجرائم، إضافة إلى أن يكون لهذه الأنشطة مدة تقادم خاصة بها، تعطي مدة زمنية أطول للملاحقة، كما لا ينحصر الاختصاص القضائي بنظرها في الدائرة التي وقعت فيها الجريمة الأصلية؛ بل حسب القاعدة العامة في تحديد الاختصاص[1].

يمثل نظام تقادم الجرائم والعقوبات وسيلة لمرتكبي الجرائم والمحكومين للإفلات من الملاحقة أو تنفيذ الأحكام، وللحد من اختراق ثغرات هذا النظام ينبغي تجريم بعض الأنشطة كالجرائم التبعية باعتبارها جرائم ذات طبيعة مستقلة كما سبقت الإشارة، على الأقل فيما يتعلق بالقواعد المنظمة لتقادم الجرائم، وكذلك اعتبار الجريمة الإلكترونية مرتكبة في وقت اقتراف السلوك، أو وقت حدوث النتيجة الإجرامية؛ أي اعتبار تاريخ السلوك وكذلك تاريخ حدوث النتيجة الإجرامية كنقطة بداية لسريان مدة التقادم، أو باعتبار بعض الجريمة الإلكترونية من قبيل الجرائم المستمرة، بما يكفل مدة تقادم أطول، وأخيرًا رفع تباين التشريعات الوطنية فيما يخص تحديد مدة التقادم وتدقيق فكرة انقطاعه ووقفه.

(1) تنص المادة 190 من قانون الإجراءات الجنائية الليبي على أنه يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة، أو الذي يقيم فيه المتهم، أو الذي يقبض عليه فيه.

الخاتمة

تعتبر الجرائم الإلكترونية من الجرائم الحديثة نسبيا التي تستلزم دراسات مستقبلية بهدف وضع المبادئ العامة بكل ما يتعلق من جرائم ترتبط بالتطور الإلكتروني والمعلوماتي ووسائل الاتصال الحديثة، وهذا ما يتطلب تدخلا تشريعيا بغرض وضع حماية قانونية متكاملة وسد جميع الثغرات التي تعتري قوانين العقوبات النافذة والتي تعد صالحة لمسايرة ومواكبة هذا التطور الحالي في نظم المعلومات.

وأمام هذا التطور قد ارتبط به ظهور ما يعرف بالجريمة الإلكترونية، وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب، الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

وتواجه هذه الجرائم العديد من التحديات في سبيل مواجهتها، فهناك التحديات الإجرائية والتحديات المتعلقة بالتحري والعقاب والتحديات الخاصة بالقانون الواجب التطبيق.

النتائج

– إن مفهوم الجريمة الإلكترونية يعنى كل فعل إجرامي متعمّد أيًّا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.
– إن الجريمة الإلكترونية ذات طبيعة تقنية وفنية وكيفية معنوية غير ملموسة لا تدرك بالحواس العادية يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبة الآلية.
– إن عملية مكافحة الجريمة الإلكترونية تقابلها عدة صعوبات ترجع إلى حداثة مثل هذا النوع من الجرائم، والتى تتطلب مكافحتها تضافر الجهود الدولية وإجراء تعديلات تشريعية تتناسب مع طبيعتها.

التوصيات

– نوصي بتقنين قواعد جديدة لمكافحة الجرائم الإلكترونية؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولا سيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم؛ سواء في ذلك الدعاوى الجنائية والمدنية والتأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.
– نوصي بالتنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم الإلكترونية.
– نوصي بتخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية، وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت.
– نوصي بتدريب وتحديث رجال الادعاء العام أو النيابة لعامة والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت.

المراجع

الكتب

1. أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، 2014
2. د. جعفر حسن الطائي، جرائم تكنولوجيا المعلومات، رواية جديدة للجريمة الحديثة، ط 1، جامعة عمر المختار، 2007
3. د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014
4. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011
5. د. خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، ص
6. د. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013
7. د. طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009
8. د. طارق عبدالله الشدي، آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، 1423 هـ
9. د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة،الإسكندرية، 2010
10. د. عبد الفتاح بيومي حجازي، مكافحة جرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006
11. د. عفيفي كامل، جرائم الكمبيوتر وحقوق المِؤلف والمصنفات الفنية ودور الشرطة والقانون «دراسة مقارنة»، منشورات الحلبي الحقوقية ،الإسكندرية، 2007
12. عنية باطلي الجريمة الإلكترونية «دراسة مقارنة»، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015
13. د. نواوي سليمة، دور الدرك الوطنى في محاربة الجريمة الإلكترونية، جامعة المسيلة، 2018
14. د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر
15. يوسف جفال، التحقيق في الجريمة الإلكترونية، بدون ناشر، 2016

الرسائل

سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة للماجيستير، جامعة مولود معمري، الجزائر، 2018

الدوريات

د. بن سولة نور الدين، الجرائم الإلكترونية في ضوء التشريع الجزائري، مجلة الحوار المتوسطى، المجلد التاع، العدد 1، مارس 2018

المؤتمرات

1. د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة منن 1 – 3 مايو 2000 بكلية الشريعة والقانون بدولة الإمارات
2. د. محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25 –28 أكتوبر، 1993