جامعة القدس

عمادة الدراسات العليا

"التعاونُ الدَولـيُ في مواجهةِ الجريمةِ الالكترونية "

محمد مُنذر طه عمايره

رسالة ماجستير

القدس – فلسطين

1445 هـ / 2023 م

التعاون الدَولي في مواجهةِ الجريمةِ الالكترونية

إعداد:

محمد مُنذر طه عمايره

بكالوريوس القانون / جامعة الاستقلال- أريحا/ فلسطين

المشرف: الدكتورة جميلة زيد

قُدَّمت هذه الرسالة استكمالاً لمتطلباتِ الحصولِ على درجةِ الماجستير في

القانون العام–عمادة الدراسات العليا- جامعة القدس- فلسطين

القدس- فلسطين

1445 هـ / 2023 م

جامعة القدس

عمادةُ الدراساتِ العليا

إجازة الرسالة

التعاونُ الدَولي في مواجهةِ الجريمةِ الالكترونية

اسم الطالب: محمد منذر طه عمايره

الرقم الجامعي: 21911633

المشرف : د. جميلة زيد

نوقشت هذه الرسالة وأجيزت بتاريخ : 2023/8/22 من لجنة المناقشة المدرجة أسماؤهم وتواقيعهم:

1- الدكتورة جميلة زيد (مشرفاً ورئيس لجنة المناقشة) التوقيع:.....

2- الدكتور جهاد الكسواني ممتحناً داخلياً التوقيع:.....

3- الدكتور محمود صلاح الدين ممتحناً خارجياً التوقيع:.....

القدس – فلسطين

1445 هـ / 2023 م

الإهداء

إلى مَنْ كان دعاؤُها سرَّ نجاحي وحنانُها بلسمَ جراحي إلى أغلى الأحبَّهِ .. **أمي الغالية**

إلى مَنْ كلله الله بالهيبة والوقارِ إلى من أعطاني لأكونَ .. **والدي الغالي**

إلى مصدرِ فرحي وسبب بسمتي الى سندي وعوني.. **أخوتي وأختي**

الى رمزِ الثقةِ والأمانِ الذي رافقني في اتمامِ هذه الدراسةِ .. **مشرفتي**

إلى من قضينا معهم أجملَ أيامِ حياتنا، الى فرسانِ الحقِ والعدلِ .. **زملائي**

إلى كل من علّمني حرفاً

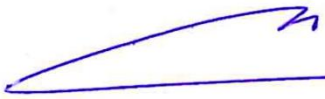
إلى كل من دفع حريتَه ثمناً لحبِّ وطنه .. **أسرانا البواسل**

إلى من هم أكرمُ منّا جميعاً .. **شهداؤنا الأبرار**

إقرار:

أقرُّ أنا معدُّ الرسالةَ بأنها قُدّمت لجامعةِ القدس، استكمالاً لنيلِ درجةِ الماجستير، وهي نتيجة أبحاثي الخاصة، باستثناءِ ما تمت الإشارة إليه حيثما ورد، وأنَّ هذه الرسالةَ، أو أيَّ جزءٍ منها، لم يُقّدمْ لنيلِ أيةِ درجةٍ عُليا لأيةِ جامعةٍ أو معهدٍ آخرَ.

التوقيع:



الاسم: محمد منذر عمايره

التاريخ: 2023/8/22

الشكر والتقدير

إلى العظيم مبدعِ الخلقِ وواهبِ العقولِ إلى اللهِ الكريمِ الحليمِ جلَّ جلالُه والحمُد للهِ ربِ العالمين

على توفيقهِ وكرمهِ وفضلهِ العظيم

الى منهلِ العلمِ ومنبعِ التعليمِ جامعِتنا التي نفتخر بها جامعةِ القدس

بكادرها التعليمي وجميعِ من فيها من الشامخينَ بعلمِهم وعطائِهم،

وأخصُّ بالشكرِ والتقديرِ الدكتورة جميلة زيد مشرفةَ الدراسة

وإلى كلِّ منْ ساهمَ في إنجاح هذه الدراسةِ

الملخص

تناولت الدراسة موضوع التعاون الدولي في مكافحة الجريمة الالكترونية، وذلك من خلال اتباع المنهج الوصفي التحليلي، بالنظر الى التشريعات الفلسطينية الناظمة لهذا الموضوع، اضافة الى التشريعات المقارنة والاتفاقيات الدولية، وقد تمحورت اشكالية الدراسة في التطرق الى أي مدى ساهمة التشريعات الوطنية والأنظمة السارية في دولة فلسطين في اتاحة الجوانب الموضوعية والاجرائية التعاون الدولي في مجال مواجهة الجريمة الالكترونية؟، وتهدف هذه الدراسة في المقام الأول الى تسليط الضوء حول الجهودِ الدوليةِ والاقليميةِ والعربيةِ لمواجهة الجريمة الالكترونية والهدف من هذا التعاون، والتعرف على ابرازِ أشكالِ التعاونِ الامنيٍ والقضائيٍ الدوليٍ في مواجهةِ الجريمةِ الالكترونية من خلالِ التطرقِ للصعوباتِ التي تعيقُ مبدأ مواجهتِها.

وذلك من خلال التعريف بالجريمة الالكترونية وخصائصها والتعريج على اليات التعاونِ الدوليٍ في مجالِ الجريمةِ الإلكترونية ما قبلَ المحاكمةِ وفي مرحلة المحاكمةِ أشكالِ وأوجه التعاونِ الدوليٍ وصعوباتهِ في مواجهةِ الجريمة الالكترونية،

ومن خلالِ الدراسةِ تمَّ التوصلُ إلى عددٍ من النتائج ومنها أنهُ تختص نيابة الجرائم الالكترونية في متابعة الطلبات المتعلقة بالجرائم الالكترونية في حين تعمل هذه النيابة بالتعاون مع وحدة مكافحة الجرائم الالكترونية من اجل الوصول الى الدليل الفني الالكتروني وربط الجناة فيه ، يعد التعاون الدولي في تنفيذ الأحكام الجزائية الأجنبية صورة خاصة من صور التعاون الدولي في مكافحة الجريمة الالكترونية، وذلك نظرا للدور الذي يلعبه في تحقيق مكافحة فعالة لهذه الجريمة ، تقوم منظمة الشرطة الدولية "الإنتربول" بدور مهم في مكافحة الجرائم الإلكترونية، ويظهر ذلك

في الأقسام والشُعب التي تتكون منها المنظمة، كشعبة الإجرام الاقتصادي والمالي، وشعبة التقصي الآلي وتحليل المعلومات.

وقد توصل الباحث في نهاية هذه الدراسة الى مجموعة من التوصياتِ أهمُّها: توحيدُ جهودِ الدُولِ من اجلِ التعاون والتصدي للجرائمِ الإلكترونيةِ ومكافحتها، من خلالِ هيئةِ الأممِ المتحدة والتعاونِ بين الهيئاتِ المختصةِ الوطنيةِ والدوليةِ بشأن ذلك، وحث المشرعُ الفلسطيني لتعديلِ قانونِ مكافحةِ الجرائمِ الالكترونية، بحيثُ تواكبُ كلَّ ما هو جديدٌ في هذا المجالِ، وبما يتوافقُ معَ الاتفاقياتِ الدوليةِ التي وقعْت عليها دولةُ فلسطين.

International cooperation in confronting cybercrime

Prepared by : Mohammad Monther Amayreh
Supervised by : Dr. Jamela Zaid

Abstract:

The study aimed to deal with the subject of international cooperation in combating cybercrime, by following the descriptive and analytical approach, in view of the Palestinian legislation regulating this subject, in addition to comparative legislation and international agreements. The problem of the study revolved around addressing the extent to which national legislation and regulations in force in the State of Palestine contribute. In providing the objective and procedural aspects of international cooperation in the field of confronting cybercrime? This study aims primarily to shed light on international, regional, and Arab efforts to confront cybercrime and the goal of this cooperation, and to identify the most prominent forms of international security and judicial cooperation in confronting cybercrime through addressing the difficulties that hinder the principle of confronting them.

This is done by defining cybercrime and its characteristics and highlighting the mechanisms of international cooperation in the field of cybercrime before the trial and during the trial stage, the forms and aspects of international cooperation and its difficulties in confronting cybercrime.

Through the study, several results were reached, including that the Cybercrimes Prosecution is specialized in following up on requests related to cybercrimes, while this prosecution works in cooperation with the Anti-Cybercrimes Unit to access the electronic technical evidence and link the perpetrators therein. International cooperation in the implementation of criminal rulings is considered Foreign Affairs is a special form of international cooperation in combating cybercrime, given the role it plays in achieving an effective fight against this crime. The International Police

Organization “Interpol” plays an important role in combating cybercrime, and this appears in the departments and divisions that make up the organization, such as the Crime Division. Economic and Financial Division, Automated Investigation and Information Analysis Division.

At the end of this study, the researcher reached a set of recommendations, the most important of which are: unifying the efforts of countries to cooperate and address and combat cybercrime, through the United Nations and cooperation between the competent national and international bodies regarding this, and urging the Palestinian legislator to amend the law on combating cybercrime, so that it keeps pace with all What is new in this field, and in accordance with the international agreements signed by the State of Palestine.

المقدمة

تعتبر الجريمة الالكترونية أحد الجرائم العابرة للحدود التي تستدعي تعاون مشترك على الصعيد الوطني والدولي للحد من اثارها والقضاء عليها، وذلك على اثر التطور التكنولوجي الكبير الذي تشهده العالم من تقنيات وأجهزة الكترونية، فمن الاستحالة قيام أي دولة بمواجهة الجرائم الالكترونية دونما اهتمام في التعاون والتنسيق الدولي في مجال مكافحة الجرائم الالكترونية، ومكافحة هذا الجريمة لا يقتصر على مستوى بلد او دولة ما بل على مستوى عموم بلدان العالم.

وتظهر الحاجة الملحة الناتجة عن الاثار السلبية المترتبة على الجرائم الالكترونية على الامن والنظام العام والاضرار المترتبة على سمعة المواطنين وحياتهم اليومية، اوجبت ضرورةَ التعاونِ المجتمعِ الدوليِ لمواجهةِ تلك الجرائم، من خلال الهيئاتِ الأمنيةِ والقضائيةِ الدوليةِ والسعي لاتخاذِ الإجراءاتِ والتدابيرِ من اجلِ الحدِّ من انتشارِ الجرائمِ ومكافحتِها والتحقيقِ فيها ومقاضاةِ مرتكبيها حتى لا يفلتوا من العقاب، فطبيعة الجريمة الالكترونية يمكن ان يجعل احد أطرافها خارج حدود الدولة الامر الذي يعيق القبض على مرتكبيها واحالتهم على القضاء لمقاضاتهم وتحقيق الردع العام والخاص، الامر الذي يتطلب تضافر الجهود واجراء تعاون لتحقيق هذه الغاية، وذلك من خلالِ الاتفاقياتِ الدولية والاقليميةِ والثنائيةِ المتعددة بحيثُ أصبح مرتكبو الجريمةِ الالكترونيةِ من خلال نفوذهم وقوتهم الالكترونية يبسطونَ نفوذَهم على معظمِ أرجاءِ العالمِ.

وتعددت مجالاتُ التعاونِ الدَولي في مواجهةِ هذه الجريمة فمنها المجالُ الأمني والقانوني والقضائي، فالغرضُ منها الحمايةُ والوقايةُ من الجرائم وتبادلِ المعلوماتِ وتقديمُ المساعداتِ القانونيةِ واستخدامُ أساليبِ التحري القضائية وليس معاقبةَ مرتكبيها أينما كانوا، وتتأكدُ حتميةُ التعاونِ في كلِّ بُلدانَ العالم مهما بلغت درجةُ الدولة من القوة، إذ لا يمكنُها الاستغناءُ عن العلاقاتِ التعاونيةِ المتبادلةِ معَ غيرهِا من الدُول، وذلك لإدراكِها بأنّ الصفاتِ التي تتمتعُ بها الجريمةُ الالكترونيةُ

مميزةٌ أي تمتدُ أثارها إلى دولٍ أخرى، وتكون المهمةُ شاقةً بحدِّ ذاتِها عندَ تحديدِ مكانِ الجاني عبر حدودِ العالمِ من أجل مكافحةِ النوعِ المستحدثِ من الجرائمِ والتي تُلحِقُ أضراراً بدولٍ ومجتمعاتٍ عدة، وذلك من خلالِ استغلالِ التطورِ الهائلِ للوسائلِ التقنيةِ الحديثةِ، مما يستدعي التدخُّلَ السريعَ منْ أجهزةِ الدولةِ والأجهزة الدوليةِ مثل الإنتربول للحدِ من انتشارِ هذه الجريمةِ والسيطرةِ عليها ومعاقبةِ مرتكبيها.

أهمية الدراسة

تتمثلُ الاهميةُ النظريةُ لما يشكله التعاون الدولي في مجال الجرائم الالكترونية وضروة وجود اطار قانونية ينظمه من خلال إيجاد اتفاقياتِ الدَولية والتشريعات الوطنية ذاتِ العلاقةِ في التعاون بالجرائمِ الالكترونية، والبحث في القوانينِ المحليةِ ذاتِ العلاقةِ والربطِ ما بين هذه القوانين والاتفاقياتِ الدَوليةِ وكيفَ حدّت هذه القوانينُ والاتفاقياتُ الدَوليةُ من الجرائمِ الالكترونية، بالإضافة الى ضرورة توضيح ما هي أليّاتِ التعاونِ الدولي في التغلبِ على الجرائمِ الإلكترونيةِ من أجل التسهيلِ على الباحثينَ لمعرفة أهم الطرقِ والسبلِ في التغلب على هذه الجرائم.

اما منَ الناحية العملية فتكمنُ أهميتُها في درجة خطورتها أساساً علاوةً على صعوبةِ التصدي لها في ظل الثورة التكنولوجية الكبيرة وتطور ادوات والوسائل الالكترونية التي يتم استغلالها من قبل المجرمين لتنفيذ جرائمهم بشكل يتعارض مع التشريعات والاتفاقيات الدولية، الامر الذي استدعى ضروة وجود تشريعات وطنية واتفاقيات دولية تتيح عملية التعاون الدولي في مجال مكافحة الجرائم الالكترونية، وذلك لكون ان الجريمة الالكترونية جريمة عابرة للحدود ومن الممكن ان يتم اثرها خارج حدود الدولة ذاتها وعدم وجود تعاون يعيق مكافحتها ويرتب فشل جهود مكافحتها الامر الذي استدعى النهوض باليات وأساليبِ التعاونِ الدُولي لمكافحتها لكونِها تتطلبُ مواجهةً عالميةً

مشتركة وصولا الى الحد منها او منعها، ونتيجة وجود قصور في التعاون الدولي الفعال لمواجهة هذه الجريمة ساهم ذلك في وجود ضعف بالتصدي لمكافحة هذه الجريمة.

أهداف الدراسة

تهدف الدراسة الى تحقيق الامور الاتية:

1- بيان وتوضيح المقصود بالجريمة الالكترونية واركانه.

2- - الوقوف على اركان الجريمة الالكترونية.

3- بيان اليات التعاون الدولي في مكافحة الجريمة الالكترونية.

4- توضيح الصعوبات التي تتعرض لها التعاون الدولي في مكافحة الجريمة الالكترونية.

5- البحث في حلول التغلب على الصعوبات التي تواجه التعاون الدولي.

إشكالية الدراسة

تختلف الجريمة الالكترونية عن الجرائمِ التقليديةِ الاخرى باعتبارها من الجرائم العابرةِ للحدودِ أي التي تقع في أكثرَ من دولة، وفي غالبِ الاحيانِ يكونُ الجاني مرتكبُ الجريمةِ الالكترونية مقيماً في بلدٍ ويكون المجنيُّ عليه مقيماً في بلدٍ أخرَ، مما يستدعي ذلك للتطرقِ للاتفاقياتِ الدوليةِ والاقليميةِ والثنائية من أجل أعمال الملاحقةِ القضائيةِ وتبادلِ المعلوماتِ والخبراتِ والمساعدةِ بعمليةِ تسليمِ المجرمينَ الهاربينَ وعدمِ تركهم دونَ ملاحقةٍ، وبعد ذلك نصل إلى أنَّ مشكلةَ الدراسةِ تتمثل بالتساؤل الاتي: الى أي مدى ساهمة التشريعات الوطنية والأنظمة السارية في دولة فلسطين في اتاحة الجوانب الموضوعية والاجرائية التعاون الدولي في مجال مواجهة الجريمة الالكترونية؟

ويتفرع عن هذا التساؤل الرئيسي عدد من التساؤلات الفرعية وهي:

- التعرف على أشكالُ التعاونِ الدَولي وصعوباتهُ في مواجهة الجريمةِ الالكترونية؟
- هل امكن التوفيق بين متطلبات التعاون الدولي وبين ضمان الحقوق والحريات ؟

- ما هي الاوجهُ والالياتُ المناسبةُ للتعاونِ الدَولي في مواجهة الجريمةِ الالكترونية؟
- الى أي مدىً استطاعت الاتفاقياتُ الدوليةُ والاقليميةُ والثنائيةُ أنْ تحدَّ من انتشارِ ظاهرةِ الجريمةِ الالكترونيةِ على الصعيدِ الدولي؟

منهجيةُ الدراسة

اتبع الباحثُ لأغراضِ الدراسةِ في هذا الموضوعِ المنهجَ الوصفيَ التحليليَ، في سبيلِ وصفِ وتحليلِ التعاونِ الدَولي واستعراضِ النُصوصِ القانونيةِ والاتفاقياتِ الدوليةِ المرتبطةِ بالتعاونِ الدولي في سبيلِ مواجهةِ الجريمةِ الالكترونية، وذلك من اجل التعرفِ والوقوف على القصورِ لمعالجتِه وازالةِ التناقضِ الذي يتعلق بهذا الشأنِ، خاصةً واننا لا نزال في فلسطينَ نعيشُ حالةً من التشتتِ التشريعيٍ عموماً وفي مجال التعاونِ الدَولي خصوصاً، وكذلك اتبع المنهجَ الاستنباطيَ في استنباطِ الاحكامِ القضائيةِ وتحليلِها واتباعِ المنهجِ المقارنِ في المقارنةِ معَ التشريعاتِ الأخرى.

مصطلحاتُ الدراسة

الجريمة " سلوك يتمثل بفعل او امتناع غير مشروع أخل بمصلحة اساسية صادرة عن ارادة جنائية يقرر به القانون عقوبة او تدبيراً احترازياً" [1].

الجريمة الالكترونية: يقصدُ بها أيَّ فعلٍ يرتكبُ متضمناً استخدامَ وسيلةٍ أو نظامٍ او شبكةٍ الكترونيةٍ بطريقةٍ غيرِ مشروعةٍ تخالفُ أَحكامَ القانونِ، والجريمةَ الالكترونية المكتملةُ الاركانِ فيها جانٍ ومجنيٌّ عليهِ وأداة للجريمة، وتتفقُ معَ أركانِ الجريمةِ التقليديةِ في الركنِ القانونيٍ والمعنويٍ والماديٍ[2].

[1] كامل السعيد، شرح الاحكام العامة من قانون العقوبات دراسة مقارنة، دار الثقافة ، عمان ، 2011 ، ص 38

[2] عبد الله عبد الكريم، الجرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، 2011م، ص 53.

التعاون الدولي: يعني العونَ المتبادلَ بينَ الدولَ، أي تبادلَ المساعدةِ والعونَ لتحقيقِ اهدافٍ معينةٍ أو خدماتٍ أو حل مشكلاتٍ مشتركةٍ لتحسينِ احوالِهم.[3]

الشرطة الجنائية الدولية (الانتربول): منظمة دولية محايدة تعنى بتسليم المجرمين والتعاون الدولي عن طريق التعاون الشرطي لمواجهة الجريمة المنظمة وتتخذ من مدينة ليوم الفرنسية مقراً لها.[4]

الدراسات السابقة:

- **نسرين زينة، الاحكام الموضوعية والاجرائية للجرائم الالكترونية بفلسطين دراسة تحليلية تاصيلية مقارنة، رسالة ماجستير، جامعة القدس، 2020.**

تناولت الدراسات الطبيعة الموضوعية للجريمة الالكترونية من خلال التعرف على ماهية الجريمة الالكترونية والمواجهة التشريعية للجريمة الالكترونية، وبيان الاحكام الاجرائية لمكافحة الجريمة الالكترونية في التشريع الفلسطيني والاجراءات التحقيقية في الجريمة الالكترونية ورمحلة المحاكمة في الجرائم الالكترونية.

- **عاصف النجاجرة، خصوصية التحقيق في الجرائم الالكترونية، رسالة ماجستير، جامعة القدس، فلسطين، 2019.**

تناولت الدراسة خصوصية اجراءات التحقيق في الجرائم الالكترونية خلال مرحلة الاستجواب والتفتيش والجهة المختصة بتنفيذها وتناولت الدراسة ايضا الخصوصية المتعلقة باجراءات التحقيق الاستثنائية الخاصة في ندب الخبراء والتنصت والمراقبة والتطرق الى معوقات اجراءات التحقيق

[3] د. احمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، الجزء الاول، دار النهضة العربية، القاهرة، 1981م، ص 139.

[4] مراد ناصري، المنظمة الدولية للشرطة الجنائية – الانتربول، ط1، المغرب، 2002، ص 13

في الجرائم الالكترونية سواء المتصلة باجراءات التحقيق في الجرائم الالكترونية والمعوقات المتصلة باثبات الجرائم الالكترونية.

التعليق على الدراسات السابقة:

وبالنظر الى الدراسات السابقة نرى بانها قد تناولت في اغلبها موضوع الاحكام الموضوعية والاجرائية للجرائم الالكترونية بفلسطين، وموضوع خصوصية التحقيق في الجرائم الالكترونية في حين ان الدراسة الحالية يرتكز موضوعها على التعاونُ الدَوليُ في مواجهةِ الجريمةِ الالكترونية حيث تتميز الدراسات الحالية في كونها تعالج مسالة التعاون الدولي الخاص بمواجهة الجريمة الالكترونية من حيث اشكال التعاون والصعوبات التي تواجهها، حيث تناولت الدراسات السابقة المواجهة الوطنية لجرائم الالكترونية وخلت من أي إشارة الى أوجه التعاون الدولي في مواجهة هذه الجريمة باعتباره امر مهم لمواجهة هذا النوع من الجرائم العابر للحدود.

مخطط الدراسة:

قسمت الدراسة الى فصلين في كل فصل مبحثين على النحو التالي:

الفصل الأول: ماهية التعاون الدولي في مجال مواجهة الجريمة الالكترونية:

المبحث الأول: المفهوم العام للجريمة الالكترونية في التشريع الفلسطيني

المطلب الأول: المقصود بالجريمة الالكترونية وصورها.

المطلب الثاني: خصائص وأركان الجريمة الالكترونية في التشريع الفلسطيني.

المبحث الثاني: المفهوم العام للتعاون الدولي في مجال الجريمة الالكترونية.

المطلب الأول: تعريف التعاون الدولي لمكافحة الجريمة الالكترونية.

المطلب الثاني: الإطار القانوني للتعاون الدولي في مجال مكافحة الجريمة الالكترونية.

الفصل الثاني: اشكال التعاون الدولي وصعوباته في مواجهة الجريمة الالكترونية.

المبحث الأول: أوجه التعاون الدولي وصعوباته في مواجهة الجريمة الالكترونية.

المطلب الأول: التعاون الأمني والقضائي الدولي في مواجهة الجريمة الالكترونية.

المطلب الثاني: التعاون الدولي لتسليم المجرمين في مواجهة الجريمة الالكترونية.

المبحث الثاني: الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الالكترونية وكيفية التغلب عليها.

المطلب الأول: الصعوبات التي تواجه التعاون الدولي.

المطلب الثاني: الحلول للتغلب على الصعوبات التي تواجه التعاون الدولي.

الفصل الاول

ماهية التعاون الدولي في مجال مواجهة الجريمة الالكترونية

تعد الجريمة الالكترونية احد الجرائم المستحدثة التي ظهرت عام 1934، والتي تنتج عن استخدام الحاسب الالي والشبكات الالكترونية التي تتميز بالدقة والسرعة، وذلك باستغلالها بطرق غير مشروعة من قبل مجرمين اذكياء يمتلكون أدوات المعرفة التقنية ويقومون بارتكاب العديد من الجرائم المحلية والإقليمية والدولية، والتي تضر بالأفراد والمجتمع والدول، وذلك من خلال استخدام العديد من التقنيات والادوات الحديثة والمتطورة التي تشهدها الحياة اليومية وذلك بالتطور المتسارع في مجال تكنولوجيا المعلومات كونها اصبحت من اساسيات الحياة، باعتبارها قوة لا يستهان بها في ايدي الافراد والدول في الوقت الراهن، والجريمة الالكترونية من الجرائم العابرة للحدود أي لا حدود جغرافية لها وهذا الامر يكسبها طابعاً دولياً،[5] واكتسابها الطابع الدولي رتب وجود تعاون دولي لمواجهة هذه الجريمة والحيلولة الى امتداد اثارها القانونية ترتب ضرر كبير لضحايا هذه الجريمة.

ويعد التعاون من الطبائع المهمة للبشر التي لا يستطيع البشر العيش دونها في مجالات الحياة المختلفة، بحيث يتعاون افراد المجتمع الواحد من أجل مواجهة الكوارث والحوادث ومعالجتها، وذلك من خلال تقديم العون والمساعدة لصاحب الحاجة، في حين اخذت العلاقات الدولية التعاونية طابعا اخر في الأعوام الأخيرة، كون دول العالم اصبحت تحتاج وبشكل ضروري لتعاون من اجل مصلحة شعوبها بحيث لن تستطيع اية دولة من دول العالم مواجهة الجريمة الالكترونية دون تنسيق وتوحيد الجهود التعاونية الدولية،[6] نظرا للتطور التقني والمعلوماتي في مستوى الجريمة.

[5] عبدالله عبد الكريم عبدالله، الجرائم الالكترونية دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الاولى، بيروت، 2007م، ص5.

[6] أشرف لبيب صادق، التعاون الدولي في مكافحة الجريمة المنظمة، اطروحة دكتوراه، جامعة أسيوط، مصر، 2011م، ص17.

حرصت دول العالم على التصدي للجريمة الالكترونية بكافة السبل والجهود، وذلك من خلال إيجاد تشريعات والسياسات والاستراتيجيات وعقد الاتفاقيات الثنائية والدولية للتصدي لمثل هذه الجريمة ومواجهتها، ويأتي هذا الاهتمام في ظل الانتشار الواسع لهذه الجرائم على الصعيدين الدولي والمحلي، وهو ما استدعى من المشرع الفلسطيني مواكبة التشريعات المقارنة والاتفاقيات الدولية ذات الصلة بمكافحة الجرائم الالكترونية وذلك باستصدار القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته[7]، من خلال الصلاحيات الاستثنائية الممنوحة لرئيس دولة فلسطين بموجب القانون الأساسي الفلسطيني[8]، ليكون احد السبل المهمة في تحقبق مواجهة تشريعية للجرائم الالكترونية.

وسنتناول في هذا الفصل المفهوم العام للجريمة الالكترونية في التشريع الفلسطيني، ثم ماهية التعاون الدولي في مجال الجريمة الالكترونية ما قبل المحاكمة وفي مرحلة المحاكمة في مبحثين على النحو الآتي:

المبحث الاول: المفهوم العام للجريمة الالكترونية في التشريع الفلسطيني.

المبحث الثاني: المفهوم العام التعاون الدولي في مجال الجريمة الالكترونية

7 شار الى ان هذا القرار بقانون تم تعديل اسمه بموجب قرار بقانون رقم 38 لسنة 2021 بتعديل قرار بقانون رقم 10 لسنة 2018 م بشان الجرائم الالكترونية وتعديلاته ليصبح (قرار بقانون بشان رقم 10 لسنة 2018 بشان الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات) والمنشور في العدد 186 من مجلة الوقائع الفلسطينية الصادرة بتاريخ 2021/12/23 ، ص 30.

8 المادة 43 من القانون الأساسي الفلسطيني المعدل لسنة 2003 تنص على انه " 1 – لرئيس السلطة الوطنية في حالات الضرورة التي لا تحتمل التأخير في غير أدوار انعقاد المجلس التشريعي، إصدار قرارات لها قوة القانون، ويجب عرضها على المجلس التشريعي في أول جلسة يعقدها بعد صدور هذه القرارات وإلا زال ما كان لها من قوة القانون، أما إذا عرضت على المجلس التشريعي على النحو السابق ولم يقرها زال ما يكون لها من قوة القانون."

المبحث الاول: المفهوم العام للجريمة الالكترونية في التشريع الفلسطيني

بفضل التطور الهائل في التقنيات وتكنولوجيا المعلومات اصبح العالم قرية صغيرة الامر الذي ادى الى اجتياح الجريمة الالكترونية للعالم بأكمله، بحيث اصبح هناك استغلال لهذا التطور والانجاز من اجل قضاء المصالح الشخصية وارتكاب الجرائم الالكترونية بشتى انواعها، مما ادى الى انتشارها على الصعيدين المحلي والدولي باعتبارها من الجرائم العابرة للحدود، مما جعل موضوع السيطرة عليها امراً ليس بسهل، اذ يحتاج هذا الامر الى تكثيف الجهود الدولية والإقليمية والمحلية وذلك من خلال عقد الاتفاقيات للحد من انتشار الجريمة الإلكترونية ومواجهتها ومعاقبة مرتكبيها، وستتمُّ دراسة هذا المبحث من خلال المقصود بالجريمة الالكترونية وصورها **(المطلب الاول)**، خصائص وأركان الجريمة الالكترونية في التشريع الفلسطيني **(المطلب الثاني)**.

المطلب الاول: المقصود بالجريمة الالكترونية وصورها.

تعتبر شبكة الانترنت مستودعا هاماً لعديد من الاسرار المرتبطة بالاشخاص والدول باعتبارها أحد البوابات العلمية التي تم اكتشافها عالميا حتى هذه اللحظة ، وهو ما رتب تنامي مساعي المجرمين في الوصول الى هذه الاسرار والكشف عنها من خلال الوسائل الالكترونية، الامر الذي استوجب بذل عناية للحيلولة دون ارتكابهم مثل هذه الجرائم واجراء أبحاث ودراسات عالمية مختصة لتحديد سبل مواجهتها،[9] وفضلا على ذلك وقبل الخوض في الحديث عن الجريمة الالكترونية لا بد لنا اولا بتعريف الجريمة الالكترونية **(الفرع الاول)**، ومعرفة صور الجريمة الالكترونية **(الفرع الثاني)**.

[9] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008م، ص13.

الفرع الاول: تعريف الجريمة الالكترونية

الجريمة الإلكترونية هي صنف جديد من الجرائم الحديثة، وبطبيعة الحال نجد بأَن هناك العديد من التعريفات التي تحدثت عنها، وذلك بسبب عدم وجود تعريف جامع ومحدد للجريمة الالكترونية باعتبارها من الجرائم المستحدثة التي تتميز بخصوصية عن الجرائم التقليدية، أي يتم ارتكابها بأساليب الكترونية قد يصعب التعامل معها بالاختلاف عن باقي الجرائم التقليدية.[10]

أولا: التعريفات الفقهية للجريمة الالكترونية

اختلفت وجهات النظر بين الفقهاء والقضاء والتشريع في تحديد مصطلحات الجريمة الإلكترونية، وذلك باختلاف النظم القانونية والثقافية بين دول العالم، حيث نجد بأن فقهاء القانون الجنائي في التشريع الفلسطيني والتشريع المصري والأردني لم يتفقوا على تعريف جامع يعرف الجريمة الإلكترونية بالوصف القانوني الدقيق والسليم، لوجود أكثر من تعريف متشابها ومتقارباً مشتقاً من تعريف الجريمة الالكترونية، الا انهم اعتبروا الجريمة الالكترونية جريمةً مستحدثة كونها مرتبطة ارتباطا بالتقدم والتطور التكنولوجي بصورة مستمرة، وذلك من خلال زيادة معدلات ارتكابها على الصعيد المحلي والدولي بأنماط مستحدثة وجديدة من خلال استخدام التقنيات الحديثة باستخدام الحاسب الالي والانترنت وليس بالطرق التقليدية، ولكن لا يفوتنا ان ننوه الى بعض التعريفات الفقهية التي تحدثت عن الجريمة الإلكترونية باعتبارها موضوع الجريمة والوسيلة لارتكابها، وذلك بالنحو الاتي:[11]

حيث قام جانب من فقهاء القانون الجنائي الأردني بتعريف الجريمة الالكترونية على انها، " نوع محدد من الجرائم تتطلب إلماماً خاصاً بتقنيات الحاسوب والتقنية المعلوماتية والانترنت، وذلك من اجل ارتكابها والتحقيق فيها ومعاقبة مرتكبها".[12]

---

[10] هشام محمد فريد، الاجرام المعلوماتي، دار النهضة العربية، مكتبة الآلات الحديثة، مصر، 1994م، ص 15.

[11] عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، الاسكندرية، 2008م، ص21.

[12] علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري للنشر والتوزيع، عمان، 2009م، ص33.

وفي هذا المقام قام تاديمان بتعريف الجريمة الالكترونية على انها، " كل شكل من اشكال السلوك غير المشروعة قانونا والتي تضر بمصلحة المجتمع الذي تحصلُ فيه الجريمة الالكترونية باستخدام الحاسوب الالي"، في حين قام الفقيه الجنائي توم فوريستر بتعريف الجريمة الكترونية بانها، "كل فعل اجرامي يتم ارتكابه باستخدام الحاسب الالي كأداة رئيسية"، وفي نفس الصدد قام فقيه القانون الجنائي ويدعى ديفيد تومبسون بتعريف الجريمة الالكترونية على انها، "اية جريمة يكون المتطلب لارتكابها ان تتوافر ادوات المعرفة بالتقنية المعلوماتية والحاسب الالي لدى مقترفها"، وعرفها ايضا الفقيه ستين سكيو لبييرج على انها، "اي فعل غير مشروع تكون المعرفة بالتقنية المعلوماتية المتطلب الاساسي لمقترف هذه الجريمة والتحقيق فيها وملاحقة مرتكبها قضائيا ومعاقبته".[13]

وجدير بالذكر بان الفقه المصري قد عرف الجريمة الالكترونية على انها، "نشاط اجرامي يستخدم فيه تقنيات الحاسوب وذلك باستخدام طرق مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الشخص لفعله الاجرامي المقصود"،[14] في حين جاء الفقه الاردني بتعريفها بانها، "هي الجرائم التي يستخدم فيها الحاسب الالي كوسيلة لاقتراف الجريمة الالكترونية غير المشروعة، او محل الفعل غير المشروع وذلك بالقيام بفعل او امتناع عن فعل من شأنه ان يؤدي الى ضرر معنويٍ أو ماديٍّ بالأموال، بحيث يكون مقترف هذه الجريمة على معرفة وخبرة بالتقنيات المعلوماتية واستعمال الحاسب الالي ولديه المعرفة في التعامل مع المعطيات والبيانات".[15]

---

[13] محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر، الطبعة الأولى، الاصدر الثاني، عمان، 2009م، ص15.

14 محمد العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2011م، ص 56.

[15] خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، 2011م، ص31.

ويلاحظ هنا بان التعريف الجامع للجريمة الالكترونية يكون بغض النظر عما اذا اختلفت الوسيلة التي يقوم الجاني باستخدامها في اتمام الجريمة وهو ما جاء به الفقه المصري والاردني باشتمال تعريفه لكل ما تحيط به الجريمة الالكترونية بان جعل التعريف الجامع مطلقاً ولم يقيده بوسيلة واحدة دون غيرها في ارتكاب الجريمة، وهو ذاته ما سار عليه المشرع الفلسطيني بعدم التطرق لتعريف موحد وشامل للجريمة الالكترونية وترك الامر للفقهاء والقضاء، وذلك لخطورة وحداثة الجريمة وازدياد ارتكابها بشكل مستمر وبطرق مختلفة[16].

ويتفق الباحث مع هذا الراي لشموله واتساعه مع تلك الجرائم فتطور ارتكاب الجرائم الالكترونية ووجود تعريف محدد قد يرتب فرار المجرمين من العقاب لعدم انطباق الوقائع والاركان على مرتكبها، في حين ان وضع تعريف عام وجامع يترك مجالا من المرونة يتيح شمول الجريمة وتغطيتها لسائر الجرائم الالكترونية والحيلولة دون فرار المتهم من العقاب.

ثانيا: التعريف القانوني للجريمة الالكترونية:

تعددت التعاريف القانونية والتشريعية بشأن الجريمة الإلكترونية مما ادى الى صعوبة ايجاد تعريف جامع وغير محدَّد لهذه الظاهرة، باعتبار ان الجريمة الالكترونية حديثة على الساحة القانونية، وفي نفس الصدد ادى ذلك الى عدم تطرق الاتفاقيات الدولية او الاقليمية ومنها اتفاقية مجلس اوروبا واتفاقية جامعة الدول العربية واتفاقية الرياض العربية واتفاقية الاتحاد الافريقي الى تعريف الجريمة الالكترونية بشكل صريح، في حين لم يقم المشرع الاردني بالتطرق لتعريف الجريمة

[16] احمد براك، عبد القادر جرادة، الجرائم الالكترونية في التشريع الفلسطيني: دراسة تحليله مقارنة، دار الشروق للنشر والتوزيع، فلسطين، 2019م، ص 32.

الالكترونية من خلال قانون العقوبات الاردني رقم (16) لسنة 1960 والمعمول به في الضفة الغربية.[17]

أما بخصوص قانون نظام مكافحة الجرائم الإلكترونية السعودي فقد اشتمل على تعريف الجريمة الإلكترونية من خلال المادة الاولى من نظام مكافحة جرائم المعلومات السعودي بأنها، " اي فعل يرتكب متضمنا استخدام الحاسب الالي او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[18]

وان قانون الجرائم الإلكترونية القطري جاء متناسقا مع ما جاء به المشرع الكويتي وذلك من حيث المفهوم ومحل الجريمة اي الركن المادي وليس هناك اي اختلاف يُذكر بينهما، بحيث تم تعريفها بانها، "أي فعل ينطوي على استعمال وسيلة تقنية المعلومات أو نظامٍ معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون"[19].

وعرف القانون الامريكي الجريمة الالكترونية (قانون الاحتيال والانتهاك الحاسوبي)[20] على انها، "الاستعمال الجائر لأنظمة الحاسوب المشفرة او الاستعمال المتعمد للبيانات والضار لأجهزة الحاسوب وتتراوح خطورة الجريمة الالكترونية ما بين جنحة من الدرجة الثانية الى جناية من الدرجة

---

[17] قانون العقوبات رقم 16 الصادر بتاريخ 10 نيسان/ ابريل 1960، الحكم الأردني، العدد 1487، 1 آيار/ مايو 1960، ص 374.

[18] المادة (1) من نظام مكافحة الجرائم الإلكترونية السعودي مرسوم ملكي رقم م/17 بتاريخ 8 / 3 / 1428 الصادر بتاريخ 08/03/1428 هـ الموافق : 2007/03/27 م، والمنشور بتاريخ: 08/03/1428 هـ الموافق : 2007/03/27م،

[19] المادة (1) من قانون الجرائم الإلكترونية القطري رقم 14 الصادر سنة 2014/9/15.

[20] تم تمرير قانون أمن الكمبيوتر في الولايات المتحدة كتعديل لقانون أضرار الكمبيوتر لعام 1986 ، والذي تضمن قانون منع الجريمة الشامل لعام 1984. يحظر هذا القانون الوصول غير المصرح به إلى أجهزة الكمبيوتر أو تجاوز أذونات الوصول. قبل القانون الجنائي للكمبيوتر، كانت جرائم الكمبيوتر تُعتبر جزءًا من الاحتيال عبر البريد والاتصالات السلكية ، لكن تطبيق القانون هذا لم يكن كافيًا.

الثالثة"[21]، أما بالنسبة الى المشرع الفلسطيني فانه لم يشر الى تعريف الجريمة الالكترونية في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وتعديلاته[22].

الفرع الثاني: صور الجريمة الالكترونية

تعتبر الجريمة الإلكترونية من الجرائم الحديثة والتي تتخذ عدة اشكال في تصنيفها لاختلاف طرق ارتكابها ومرتكبيها، ولها عدة انواع مختلفة بحسب الاساس القانوني الذي استند عليه، فنجد ان فقهاء القانون الجنائي قاموا بتقسيم الجرائم التقليدية الى عدة صور وهي : جرائم تقع على الاشخاص وعلى الاموال وجرائم تقع على نظام الامن العام، في حين يصعب إجمال صور الجريمة الالكترونية باعتبارها متغيرة ومتجددة بتطور التكنولوجيا وبظهور وسائل متطورة من الحواسيب والأنظمة المعلوماتية وشبكة الانترنت، مما يؤدي ذلك الى تطور وظهور صور جديدة من الجرائم، والتي يمكن حصرها في الصور التي سوف نتناولها في الاتي:

اولا: الجرائم الالكترونية التي تقع على الاشخاص

تعتبر هذه الجرائم الأكثر انتشارًا لأن لها أشكالًا وصوراً عديدة من بينها التهديدات عبر الإنترنت والتشهير حيث تتميز بحقيقة أنها في بعض الأحيان يصعب القبض أو كشف الجاني وذلك نظرًا لبعد المسافة بين الأشخاص،[23] فنصت المادة (1\15) من القرار بقانون رقم (10) لسنة (2018) على انه، "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو

---

[21] رامي متولي القاضي، مرجع سابق، ص 23.

[22] قرار بقانون بشأن الجرائم الإلكترونية رقم 10 الصادر بتاريخ، 2018/4/29، الوقائع الفلسطينية، العدد 0، 2018/5/3، ص 8.

[23] اسامة عبد الله كايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة، دار النهضة العربية، الطبعة الثالثة، القاهرة، 1999م، ص 48.

الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مئتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.[24]

وقد توصلت محكمة النقض في الدعوى الحقوقية رقم 113/ 2021الى قاعده من قواعد المحاكمة الجزائية بحيث يحظر على المحكمة معاقبه المتهم عن مواقع لم ترفع بها الدعوى ولو اثبتتها البينة، وذلك بأن البينة التي تصلح أساساً للإدانة هي تلك التي تنصب على الوقائع المرفوعة بها الدعوى والتي يتضمنها قرار الاتهام وأن العبارة التي أوردها المتهم لا تشكل عنصرا للتهديد حسب المادة 15 من القرار بقانون رقم 10 لسنه 2018.[25]

ومما سبق يرى الباحث بانه يمكن للجريمة الالكترونية ومن خلال الاعتداء على الاشخاص ان تؤدي الى جريمة القتل احيانا أي ازهاق ارواح البشر، كقيام شخص بالعبث في الانظمة الالكترونية والتي تكون موضوعة في احد الاماكن التي يقيم فيها المرضى كالمشفى مما يؤدي ذلك الى وفاة المريض بسبب هذه الجريمة،[26] في حين نصت معظم قوانين العالم ومنها القانون الاساسي الفلسطيني على حماية الحريات الشخصية والمقصود بها قيام الشخص بالاحتفاظ بأسراره الخاصة وبأسرار عائلته بعيدا عن العامة لحرمتها وذلك من اجل حمايتها من عبث الاخرين بها.

استنادا لذلك يمكن توضيحُ اركان جريمة الاعتداء على الاشخاص من خلال نشر الصور والافلام الاباحية والتي تكون مخله بالآداب والاخلاق العامة على مواقع الانترنت وهذا يتمثل بالركن المادي للجريمة الالكترونية، بينما الحالة النفسية التي يتمتع فيها مرتكب هذه الجريمة أي الجاني في نشر الصور والافلام الاباحية ويكون لديه العلم والارادة يتمثل ذلك بالركن المعنوي بالجريمة[27]

---

[24] المادة رقم (15) من القرار بقانون رقم (10) لسنة (2018م) ، مرجع سابق.

[25] الحكم الصادر عن محكمة النقض المنعقدة في رام الله المأذونة بإجراء المحاكمة وإصداره في الدعوى الحقوقية رقم 2021/113 الصادر بتاريخ 30 يونيو 2021.

[26] خالد ممدوح ابراهيم، الجريمة الالكترونية، دار الفكر الجامعي، الطبعة الاولى، الاسكندرية، 2009م، ص 410.

[27] مدحت رمضان، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2007م، ص 12.

ثانيا: الجرائم الالكترونية التي تقع على الاموال

تعتبر الجرائم التي تقع على الاموال من اخطر الجرائم الالكترونية كونها تؤدي الى الحاق الاضرار المادية الضخمة، والتي يتم ارتكابها من خلال قيام شخص باستخدام الحاسوب وشبكة الانترنت واستخدام اسهل الطرق دون ان يكون هناك تخطيط او تدبير مسبق ودون مجهود يقوم به الجاني وذلك لسهولة ارتكابها، في حين تؤدي هذه الجرائم الى الحاق الخسائر المادية الضخمة في وقت زمني قصير،[28] ومن الجرائم التي تقع على الاموال منها جريمة سرقة الاموال والمعلومات والبيانات والبرمجيات والخدمات الالكترونية، بحيث تقوم الجريمة على فعل الاختلاس التي يقوم به الجاني للأموال المنقولة والتي تكون مُلكاً للغير فهنا يقوم الركن المادي للجريمة، بينما يتمثل الركن المعنوي بالقصد الجنائي الخاص الصادر عن الجاني مرتكب جريمة الاعتداء على اموال الغير وذلك بنيته تملُّك الاموال المسروقة،[29] ونصت المادة (13) من القرار بقانون رقم (10) لسنة 2018 على أنها، "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

ولهذا يمكن للباحث طرح العديد من الامثلة التي تبين الجرائم الالكترونية التي تقع على الاموال ومنها قيام شخص بتزوير بطاقة ائتمان وقيامه بسحب اموال بها من احد البنوك وتكون هذه الاموال ملك لغيره، اذ تختلف هذه الجريمة عن غيرها بانها ترتكب بوسيلة الكترونية وان الجاني يكون بعيدا عن موقع العملية الجرمية، حيث نصت المادة (12) من القرار بقانون رقم (10) لسنة 2018 على انه، "يعاقب كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في

---

[28] سليمان بن مهيج العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، اكاديمية نايف العربية للعلوم الامنية، السعودية، 2003م، ص 113.

[29] خالد ممدوح ابراهيم، مرجع سابق، ص 297.

الوصول، دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها"[30]، وأيضاً من أخطر الجرائم الالكترونية والتي تقع على الأموال جريمة غسل الاموال بواسطة شبكة الانترنت وذلك من خلال استخدام الاسهم المالية في البورصات العالمية وقيام الجاني بشراء العقار بمختلف انواعه سواء الارض او الشقق وايضا قيامه بشراء التحف الثمينة وبمجالات لا يمكننا حصرها في هذا المجال،[31] وفي حين نصت المادة (18) من القرار بقانون رقم (10) لسنة (2018) على انه، "يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بقصد، القيام بارتكاب جريمة غسل الأموال بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".[32]

ثالثا: الجرائم الالكترونية التي تقع على انظمة المعلومات وشبكات الانترنت

ويقصد بها تلك الجرائم التي تلحق الضرر بمكونات الحاسوب الاساسية سواء بيانات مخزنه عليه او باختراقه عن طريق شبكة الانترنت للحصول على المعلومات، ومن هذا الجرائم جريمة اختراق الحاسوب وشبكة الانترنت وجريمة تخريب البيانات والانظمة، وجريمة انشاء برامج ضارة تعمل على تدمير واختراق المواقع واجهزة الحاسوب والبريد الالكتروني وذلك بهدف اغلاقها او الاستيلاء عليها واستخدامها لأغراض تؤدي الى الحاق الضرر بالمجني عليه يكون الهدف منها الاضرار بالحاسوب وشبكة الانترنت، في حين تقوم هذه الجريمة على سلوك مرتكب الجريمة وما ينتج من اضرار تلحق بالغير ويطلق عليه الركن المادي، بينما يقوم الركن المعنوي في هذه الجريمة على القصد الجنائي الخاص القائم على علم الجاني بالفعل المقترف وارادته بالنتيجة التي سوف

[30] المادة رقم (12) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية.

[31] يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، الطبعة الاولى، القاهرة، 2011م، ص 115.

[32] المادة رقم (18) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية.

تحصل من خلاله،[33]وهذا ما نصت عليه المادة (5) من القرار بقانون رقم (10) لسنة (2018) على انه، "كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مئتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".[34]

واستنادا لذلك، نجد أن الجرائم المتعلقة بأنظمة المعلومات وشبكة الانترنت تتم عن طريق دخول الجاني بطريقة غير مشروعة الى المواقع والاجهزة التابعة للمجني عليه، وهذا ما وضحه نص القرار بقانون من المادة (3\4) على انه، "إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغاؤه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"،[35] ومن خلال ما سبق نجد بانه قد تختلف الوسائل التي ترتكب فيها الجريمة الواقعة على أنظمة المعلومات وشبكات الانترنت وذلك من خلال التطور التكنولوجي الحديث.

---

[33] يوسف حسن يوسف، مرجع سابق، ص 116.

[34] المادة رقم (5) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية.

[35] المادة رقم (4) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية.

رابعا: الجرائم الالكترونية التي تقع على النظام والامن العام

تطورت في العصر الحديث الجرائم التي تقع على النظام والامن العام كنتيجة لتطور تكنولوجيا المعلومات وظهور الحاسوب وشبكة الانترنت بشكل واسع على الصعيد المحلي والدولي، كأن تقوم بعض دول العالم بالتجسس على مواقع للدول الاخرى من أجل الوصول الى معلومات لاختراقها، وتقوم أركان هذه الجريمة من خلال سلوك الجاني باستخدام النظام الالكتروني وذلك من اجل الدخول الى المواقع وحذفها او نسخها او مشاهدتها فهنا يقوم الركن المادي للجريمة التي تقع على النظام والامن العام، بينما يتمثل الركن المعنوي من خلال القصد الخاص للجاني الذي سوف يقوم بالحاق الضرر للدولة، وعليه يكون الهدف من هذه الجرائم التعرف على أسرار وأخبار وخطط الدولة المعنية، مما لا شك فيه بان هذا النوع من الجرائم يشمل قطاعاً واسعاً كونه يؤدي الى تعطيل أعمال الدولة وتعطيل قانونها ويعمل على تهديد الامن والسلامة العامة للدولة.[36]

ومن الجرائم التي تعمل على تهديد النظام والامن العام الجرائم التي تقوم العصابات بارتكابها من خلال انشاء المواقع الالكترونية الخاصة بهم من اجل مساعدتهم على ادارة نشاطاتهم والعمل على ارسال وتلقي البرقيات، في حين يكون الهدف من هذه الجرائم التي تعمل على تهديد السلم والنظام والامن العام هو بث الرعب والخوف في المجتمع من اجل القيام بتنفيذ العمليات الارهابية،[37] في حين نصت المادة (39) من القرار بقانون رقم (10) لسنة (2018) على انه، "لجهات التحري والضبط المختصة، إذا رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها، من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضراً بذلك على النائب العام

[36] يوسف حسن يوسف، مرجع سابق، ص 132.

[37] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت، الطبعة الاولى، دار العدالة، القاهرة، 2011م، ص 84.

أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض"

المطلب الثاني: خصائص وأركان الجريمة الالكترونية في التشريع الفلسطيني

تمتاز الجرائم الالكترونية بطبيعة خاصة عن الجرائم التقليدية سواء من حيث خصائصها او من حيث اركانها، فالجريمة الالكترونية حديثة لارتباطها بالتطور والتقدم التكنولوجي كونها تمتاز بأدوات واساليب خاصة تجعلها مختلفة تماما عن باقي الجرائم التقليدية، أي انها تستلزم عدة شروط ومكونات لارتكاب الجريمة وهي استخدام الحاسوب وشبكة الانترنت وتوفر المعرفة والقدرة العالية بتقنيات المعلومات لدى مستخدمها، باعتبار أنّ هذا النوع من الجرائم يتسم بالعالمية أي لا حدود جغرافية لها، الامر الذي نتج عنه ارتكاب الجرائم الالكترونية وذلك لارتباطها باستخدام الحاسب الالي، واستنادا لما سبق فان الجريمة الالكترونية لا تتوفر الا اذا توفرت جميع اركانها وفقا لما ورد في الاحكام العامة للقانون أي يجب ان تتم بتوافر الركن المادي والركن المعنوي والركن القانوني لارتكابها، أي ان الجريمة الالكترونية يجب ان تقوم على الركن المادي والمعنوي حتى يمكن اثباتها والعقاب عليها،[38] وهذا ما يتم البحث فيه من خلال خصائص الجريمة الالكترونية في التشريع الفلسطيني **(الفرع الاول)**، والاركان التي تقوم عليها الجريمة الالكترونية بحسب ما جاء في التشريع الفلسطيني **(الفرع الثاني)**.

[38] محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي: دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2018م، ص 163.

الفرع الاول: خصائص الجريمة الالكترونية في التشريع الفلسطيني

تتميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية بعدة خصائص سواء من حيث وسيلة ارتكابها او من حيث اكتشافها واثباتها، وتقوم الجريمة الالكترونية على هذه الخصائص التي تميزها عن باقي الجرائم وسنحاول حصرها بالتفصيل الآتي:

اولا: الجريمة الالكترونية عابرة للحدود

اصبحت الجريمة الإلكترونية ذات طابع عالمي كونها تتخطى في ارتكابها الحدود الجغرافية للدول، وذلك لاتصالها بشبكة الانترنت باعتبارها جعلت العالم قرية صغيرة ويستطيع الافراد التواصل بين مختلف قارات العالم بسهولة، ومن خلال ذلك اصبح مسرح الجريمة الالكترونية دوليا في حين يتمكن الجاني من ارتكاب الجريمة دون تواجده في مسرحها وذلك من خلال استخدام الحاسوب وشبكة الانترنت والقدرة على المعرفة بالتقنيات المعلوماتية لكي يتوصل الجاني الى تحقيق النتيجة الاجرامية المرغوب فيها، مما يصعب على الدول ملاحقتها دون اللجوء الى التعاون الدولي من اجل الحد منها، مما يستوجب اللجوء الى الاتفاقيات الدولية والاقليمية لمواجهتها،[39] الامر الذي دفع الدول للجوء الى التعاون في المجال الالكتروني والجرائم القائمة على الاستخدام التقني والالكتروني.

ويمكن القول بان مواجهة هذا النوع من الجرائم يحتاج للتعاون الدولي، باعتبارها عابرة للحدود أي ترتكب في دولة معينة وتقع على المجني عليه في دولة اخرى، بالرغم من بعد المسافات بين دول العالم، الامر الذي ادى الى تنازع القوانين المطبقة ما بين البلدين مما نتج عن ذلك لجوء الدول الى عقد الاتفاقيات الثنائية في مجال التنازع حول للجرائم الالكترونية وضبط وتسليم مرتكبيها،

[39] عبد الله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2002م، ص351.

وهنا يكمن دور الانتربول الدولي والذي له انجازات عدة بمجال ملاحقة المجرمين المرتكبين للجرائم الالكترونية والقاء القبض عليهم وتسليمهم الى الجهة صاحبة الاختصاص، ويكون ذلك من خلال الاتفاقيات الثنائية والدولية لمواجهة الجريمة الالكترونية والحد منها.

ثانيا: وقوع الجريمة الالكترونية أثناء المعالجة الآلية للبيانات

تعتبر مرحلة المعالجة الالية للبيانات من اهم المراحل الاساسية التي يجب ان تتوفر لقيام اركان الجريمة الإلكترونية سواء عند القيام بإدخال البيانات او مرحلة معالجتها او مرحلة اخراج المعلومات والمعطيات او بعد القيام بتخزينها، اذ لا تقع النتيجة الجرمية من دونها باعتبارها من الشروط الاساسية لتحقيق الجريمة الالكترونية، حيث قام الفقه الفرنسي بتعريف عملية المعالجة الالية للبيانات بانها، "مركب يشمل وحدة معالجة او اكثر ويتكون من ذاكرة وبرمجيات واجهزة ربط وادخال واخراج، ومن خلالها يتم ربط العلاقات بينها ويؤدي ذلك الى تحقيق النتيجة المرغوبة وهي معالجة المعطيات ويكون المركب خاضعاً لأنظمة الحماية الفنية".[40]

وتقوم المعالجة الالية للبيانات أثناء مرحلة ادخالها على ترجمتها الى لغة يسهل على المستخدم فهمها والتعامل معها من قبل الحاسوب، أي انه يكّون عناصر الجريمة الالكترونية في مرحلة ادخال البيانات، والمعطيات الجديدة اكبر منها في مرحلة المعالجة الالية للبيانات كونها تقوم هذه المرحلة بإدخال تعديلات على البرامج عن طريق التلاعب في برامج الحاسوب في حين تحتاج هذه المرحلة الى توفر المعرفة والقدرة التقنية العالية للجاني، وذلك من اجل تحقيق الهدف الاجرامي، كقيام الجاني بإضافة تعليمات غير صحيحة الى البرنامج الاصلي المطلوب، واما

[40] خالد ممدوح ابراهيم، مرجع سابق، ص 50.

بخصوص المرحلة الاخيرة من مراحل المعالجة الالية للبيانات فتكمن في إخراج النتائج بعد قيام الجاني بالتلاعب وتغييرها الى معلومات غير دقيقة.[41]

وقد جاء المشرع الفلسطيني بتعريف معالجة البيانات من خلال المادة الاولى من القرار بقانون رقم (10) لسنة (2018) على انها، "إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلاف ذلك، بما في ذلك جمع تلك البيانات، أو استلامها، أو تسجيلها، أو تخزينها، أو تعديلها، أو نقلها، أو استرجاعها، أو محوها، أو نشرها، أو إعادة نشر بيانات، أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها".[42]

ثالثا: الجريمة الالكترونية تتطلب وجود الحاسوب الالي ومعرفة بالتقنيات المعلوماتية

يعد الحاسوب الالي وشبكة الانترنت العالمية من الادوات الاساسية لارتكاب الجريمة الالكترونية وذلك لاختلافها عن باقي الجرائم التقليدية الاخرى، في حين يكون وجود الحاسب الالي أمراً مهماً لارتكابها فبغيره تنتفي عناصر واركان الجريمة الإلكترونية، ويتطلب الامر أيضا ان يكون لدى مرتكب الجريمة القدرة والكفاءة والخبرة العالية على استخدام الحاسوب وشبكة الانترنت، وان يتوفر لديه ايضا العلم والمعرفة سواء على المستوى الفني او المستوى التقني لاستخدامها، باعتبار ان العلاقة بين المعرفة والخبرة الفنية والتقنية والحاسوب الالي وشبكة الانترنت علاقة طردية، أي كلما زادت الخبرة لدى الجاني زادت قدرته على ارتكاب الجرائم الالكترونية،[43] وبدون توافر الحاسب الالي والخبرة الفنية المعلوماتية لدى الجاني مرتكب الجريمة لا تتوفر اركان الجريمة الالكترونية.

---

[41] محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية للصحافة، مصر، 2010م، ص 40.

[42] المادة رقم (1) من القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية.

[43] رامي متولي القاضي، مرجع سابق، ص 52.

رابعا: الجريمة الالكترونية تمتاز بصعوبة الاكتشاف والاثبات

تمتاز الجريمة الالكترونية بصعوبة اكتشافها كونها في أغلب الاحيان ترتكب خارج الدولة او الاقليم الذي يقيم فيه المجني عليه والمتضرر من هذه الجريمة في حين يتم اكتشافها عادة عن طريق الصدفة، باعتبارها من الجرائم التي ترتكب بشكل خفي ولا يترك لها اثار مادية لارتكابها،[44] وذلك بسبب القدرة الفنية والتقنية العالية التي يتمتع بها الجاني في استعمال الحاسوب الالي وشبكة الانترنت، بحيث يكون من الصعب تحديد مكان وقوع الجريمة وذلك لعدم ترك الجاني للأدلة الفنية التي تدل على الجريمة باعتبار الجاني يمكنه وبفترة قصيرة جدا ان يقوم بحذف او تغيير او اتلاف أَي بيانات تؤدي الى اكتشاف الجريمة الالكترونية، بحيث يعتمد بذلك على خبرته الفنية والتقنية والذكاء التي يتمتع بها مرتكب الجريمة.[45]

ومن خصائصها ايضا إنها جريمة تمتاز بصعوبة اثباتها وذلك باختلاف اسلوب الجاني في استخدام وسيلة تنفيذها، في حين تتم الجريمة الالكترونية بشكل منظم باستخدام شبكة الانترنت، بالإضافة الى الجاني الالكتروني وكما ذكرنا سابقا يمتاز بذكاء واحتراف كونه لا يترك أي اثار خارجية مما يصعب اكتشافها واثباتها، ومما لا شك فيه أنه في اغلب الاحيان يكون المجني عليه والمتضرر من هذه الجرائم الالكترونية هم المؤسسات العامة والخاصة في حين يتردّدون بتقديم البلاغات والشكاوي، وذلك من اجل تجنب السمعة والاساءة التي تكون قد وصلت له تلك المؤسسة.[46]

---

[44] محمد علي سكيكر، مرجع سابق، ص 43.

[45] خالد ممدوح ابراهيم، مرجع سابق، ص47.

[46] غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015م،ص 28.

خامسا: المساهمة الجنائية في الجريمة الالكترونية

عادة ما يتم ارتكاب الجريمة الالكترونية باشتراك أكثر من شخص، وفي اغلب الاحيان يكون أحدهم من متخصصين في مجال التقنيات المعلوماتية والحاسوب وشبكة الانترنت، ويكون الاخر من جانب المجني عليه المتضرر من اجل ان يقوم بتسهيل العمل لإتمام ارتكاب الجريمة الإلكترونية،[47] فيجب لتحقيق اركان الجريمة الالكترونية ان يكون هناك جانٍ او عدة جناة ومجني عليه ويتوافر لكل من الجناة القدرة الفنية والتي تساعدهم على ارتكاب الجريمة واستخدامها عبر وسيط الكتروني.

الفرع الثاني: أركان الجريمة الالكترونية في التشريع الفلسطيني

تتحقق الجريمة الإلكترونية باكتمال جميع اركانها الاساسية التي وردت في احكام القانون، في حين لا تقوم المسؤولية الجنائية للجريمة الالكترونية التي يرتكبها الجاني الا اذا توافرت جميع اركان الجريمة مجتمعة، وتتمثل هذه الاركان بالركن المادي للجريمة أي بالسلوك الذي يرتكبه الجاني ويكون له مظهر خارجي، بينما يتمثل الركن المعنوي للجريمة في ارادة الجاني من اجل مباشرة السلوك الاجرامي كونه يكمن في نفس الجاني مرتكب الجريمة الالكترونية، بينما يتمثل الركن الشرعي بوجود نص قانوني وفقا للمبدأ الشهير لا جريمة ولا عقوبة الا بنص قانوني.[48]

اولا: الركن الشرعي (القانوني)

يعتبر الركن الاول والاساسي للجريمة الالكترونية كونها تتطلب وجود نص قانوني يجرم الفعل المرتكب من قبل الشخص الجاني حتى تقوم المسؤولية الجنائية للجريمة، اذ لا جريمة ولا عقوبة الا بوجود نص قانوني يجرم الفعل، ولا يجوز القياس في النصوص القانونية ولا يمكن معاقبة

[47] نهلا عبد القادر المومني، مرجع سابق، ص 58.

[48] د. احمد فتحي سرور، مرجع سابق، ص 256.

الجاني على فعل أخر قام بارتكابه حتى ولو كان الفعل متشابهاً من حيث الدافع او من حيث نتائج وعناصر الجريمة والعمل على الاستعانة بنص مشابه من القانون، باعتبار ان النصوص القانونية وجدت من اجل منع ارتكاب الجرائم ومعاقبة مرتكبيها، في حين تكمن الغاية من وجود النصوص القانونية في الحفاظ على افراد المجتمع والحفاظ على الامن والسلم الاهلي، وايضا من اجل التزام القضاء بالنصوص القانونية الموضوعة.[49]

ثانيا: الركن المادي

يقوم الركن المادي للجريمة على المظهر الخارجي اي السلوك الاجرامي المتمثل بفعل يكون صادراً عن الشخص الجاني وهذا مما عمل القانون على تجريمه وتحديد العقوبة المناسبة لمرتكبها، في حين تمتاز الجريمة الالكترونية عن غيرها من الجرائم التقليدية بأن مرتكب الجريمة لديه الخبرة والمعرفة بتقنيات المعلومات والحاسب الالي ويتسم بصفة الذكاء والحيلة والخداع، بحيث يمكن ان ترتكب الجريمة الالكترونية من الشخص الجاني بالخطأ او من الجاني الذي يتمتع بمستوى عادي من الخبرة بالتقنيات المعلوماتية، وعليه يجب ان يقوم الركن المادي للجريمة الالكترونية على السلوك الاجرامي الذي يتمثل بالمظهر الخارجي للفعل، اما بخصوص النتيجة الاجرامية فإنها تقوم على اساس الضرر الذي وقع بسبب ارتكاب الجاني للفعل وذلك من المدلول المادي اي مظهر الفعل الخارجي او المدلول القانوني من خلال العقوبة التي حددها القانون بسبب ارتكاب الجاني للفعل وارتباطها بالعلاقة السببية.[50]

[49] د. كامل السعيد، مرجع سابق، ص 58.

[50] كامل السعيد، مرجع سابق، ص 183.

تتطلب الجريمة الالكترونية وجود الاعمال التحضيرية،[51]لاقترافها وذلك بوجود بيئة رقمية والحاسب الالي وشبكة انترنت، وايضا تتطلب وجود المعرفة لدى الشخص الجاني لممارسته للنشاط الاجرامي والشروع فيه وتحقيق نتيجته، ومما لا شك فيه بان بعض الجرائم الالكترونية لا تحتاج للأعمال التحضيرية لارتكابها، مثل قيام شخص بشراء برامج مخصصة لعملية الاختراق فهذا الامر بحد ذاته يشكل جريمة[52] تستلزم العقاب.[53]

ثالثا: الركن المعنوي

يعتبر الركن المعنوي النصف الاخر للجريمة في حين لا تقوم الجريمة من غيره كونه يتمثل في حالة الشخص الجاني النفسية وقت ارتكاب الفعل الاجرامي، اذ يمتلك الشخص الجاني الارادة نحو ارتكاب الفعل الاجرامي وتحقيق النتيجة ويكون فعله مخالفا للقانون، بحيث اعتبر القانون الركن المعنوي الطريق الذهني والنفسي للجاني وذلك من خلال توافر الارادة والقصد الجنائي، ومن صور الركن المعنوي للجريمة صورة القصد الجنائي الإهمال وقلة الاحتراز، وعليه يعرف الركن المعنوي للجريمة على انه، "العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني الذي قام بارتكابها، في حين تكون تلك العلاقة هي محل الذنب بمعنى استحقاق العقاب وفقا لما نص عليه القانون"، وعمل القانون على تعريف القصد الجنائي بانه، "العلم بعناصر الجريمة وارادة

---

[51] يشير العمل التحضيري إلى جميع الأفعال التي يكون من خلالها للمجرم وسيلة لارتكاب جريمة مثل شراء أسلحة وإعداد مواد سامة واستعارة أدوات لفتح خزنة وما إلى ذلك ويشمل أيضًا جميع الأعمال التي يضع فيها المجرم نفسه في وضع يمكنه من خلالها ارتكاب الجريمة والاستمرار في ارتكابها مثل شغل مقعد أحد الركاب في وسائل النقل العام أو محاولة ارتكاب جريمة قتل أو سرقة أو تدمير الضحية على الطريق ، وما إلى ذلك وفي الجرائم الالكترونية تكون الاعمال التحضيرية على سبيل المثال ان يقوم الجاني بالعمل على استدراج الضحية من اجل تهديها ولكن يرى الكثيرون ان القانون لا يعاقب على الاعمال التحضيرية.

[52] وتماشيا مع ما تم ذكره نجد بان اكثر انتشارا للجرائم الالكترونية هي جرائم القذف والذم، في حين يعتبر الركن المادي فيها من خلال ممارسة الجاني للسلوك الخادش للحياء والشرف والاعتبار من خلال استعمال الحاسوب وشبكة الانترنت، كقيام شخص بتوجيه رسالة نصية او صوتية او صورية تحمل عبارات مسيئة الى الشخص المجني عليه.

[53] عبد الفتاح حجازي، مرجع سابق، ص 113

متجهة الى تحقيق هذه العناصر او قبولها، وقد يتحقق الركن المعنوي في جريمة تحتوي بطاقة ائتمان واستخدامها وسحب نقود غير مملوكة للفاعل".[54]

يعد الركن المادي في الجريمة الالكترونية امراً مهماً وذلك من اجل تحديد طبيعة النشاط الذي يمارسه الشخص الجاني وايضا تحديد النصوص القانونية واجبة التطبيق، بحيث اذا كان الفاعل غير مدرك لخطورة الفعل الذي ارتكبه وانما كان مكره على ارتكابه او كان غير مميز، هنا لا نكون امام جريمة الكترونية كونها فقدت احد الاركان وهو الركن المعنوي للجريمة، بحيث يجب ان يكون الجاني مرتكب الجريمة يتمتع بالوعي والارادة الحرة، والقصد الجرمي فيها يلعب دورا هاما من اجل معرفة طبيعة السلوك الجرمي وهدفه وتكييفه القانوني وايضا معرفة النصوص القانونية الواجب تطبيقها.[55]

ومن خلال ما سبق يرى الباحث بان الجريمة الالكترونية تحتاج الى قصد اجرامي في الركن المعنوي كغيرها من الجرائم التقليدية باعتبار انه يلعب دورا هاما في معرفة مرتكب الجريمة والعمل على التكييف القانوني الصحيح لها واسناد النصوص واجبة التطبيق، باعتبارها في بعض الاحيان تقوم على علم الشخص الجاني بالجريمة، في حين لا يتم ارتكابها الا من خلال خبراء ومختصين يتمتعون بالخبرة بالتقنيات المعلوماتية والفنية.

المبحث الثاني: المفهوم العام التعاون الدولي في مجال الجريمة الالكترونية

تمتاز فكرة التعاون بقدمها عبر التاريخ كون جذورها تمتد لظهور الإنسان، وان هناك حاجة للتعاون بين الدول من اجل تنظيم العلاقات والجهود الدولية من اجل تحقيق المنافع والخير للجميع،

[54] د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، 1988م، ص 90.

[55] د. احمد فتحي سرور، مرجع سابق، ص 186.

بحيث ادركت جميع شعوب العالم عبر العصور على اهمية التعاون باعتباره الوسيلة الوحيدة التي تستخدم من اجل الامن والاستقرار بين الناس واشباع رغباتهم، في حين يعتبر التعاون الهدف الاساسي للعلاقات الدولية باعتباره من المبادئ الاخلاقية التي تهدف الى تحقيق الامن والخير والاستقرار للأفراد اذ يصعب عليهم الاستغناء عن التعاون كونه من سلوكيات الانسان منذ العصور الاولى، في حين يعتبر التعاون من احد المبادئ الاساسية التي تلجأ اليها العلاقات الدولية من اجل تحقيق وتعزيز واحترام الحقوق والحريات الاساسية للإنسان من اجل التعاون والمساهمة في حفظ الامن والسلم الدَولي وذلك لتحقيق الاستقرار والازدهار والتقدم الاقتصادي والثقافي والاجتماعي،[56] وسيتم دراسة هذا المبحث من خلال تعريف التعاون الدولي لمكافحة الجريمة الالكترونية **(المطلب الاول)**، الإطار القانوني للتعاون الدولي في مجال مكافحة الجريمة الالكترونية **(المطلب الثاني)**.

المطلب الاول: تعريف التعاون الدولي لمكافحة الجريمة الالكترونية

بالرغم من الاستخدام الهائل للتعاون الا ان العلماء لم يجدوا معنى واحداً يكون جامعاً لها، بحيث تطور مفهوم التعاون الدولي بتطور الجريمة على الصعيد المحلي والدولي، في حين تطورت اساليب مكافحة الجريمة الالكترونية كونها خرجت من النطاق المحلي الى النطاق العالمي، وذلك بإعطاء التعاون الدولي صيغة جديدة من خلال وجود العلاقات بين الدول، وقبل الخوض في الحديث عن هذا المطلب لا بد لنا اولا بتعريف التعاون الدولي لغةً **(الفرع الاول)**، وتعريف التعاون الدولي اصطلاحاً **(الفرع الثاني)**.

[56] خالد مبارك القحطاني، التعاون الامني الدولي ودوره في مواجهة الجريمة، اطروحة دكتوراه، جامعة نايف للعلوم الامنية، الرياض، 2006م، ص 30.

الفرع الاول: المقصود بالتعاون الدولي لغةً

تعريف التعاون لغةً هو العون المتبادل، ويتم ذلك من خلال تبادل الاعانة والمساعدة والمشاركة من اجل العمل على تحقيق هدف معين، فالعون والمعونة جميعها تدل على عمل طيب يقوم به شخص او جماعة لصالح الاخر، في حين يعتبر ذلك المعنى العام لكلمة التعاون، ويقال "تعاون القوم أي عاون بعضهم البعض"، ويقال ايضا استعان فلان بفلان، أي طلب منه ان يعاونه، بينما المعنى الدولي فانه يستعمل من خلال وصف الحاجة الحقيقية لتوضيح العلاقات بين دول العالم.[57]

في حين عرف التعاون بانه تبادل المساعدة بين شخصين او اكثر وذلك من اجل تحقيق اغراض وخدمات ومنافع معينة، كقول الله تعالى في محكم تنزيله، "وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان"،[58] وايضا كما قال رسول الله محمد صلى الله عليه وسلم، "الله في عون العبد ما دام العبد في عون أخيه".

الفرع الثاني: المقصود بالتعاون الدولي اصطلاحاً

بداية، يعتبر مصطلح التعاون اسماً مشتقاً من اشتراك طرفين في العون معاً، كونه يهدف الى المساعدة مقابل اجر من الله سبحانه وتعالى، في حين يكون المعنى الشامل للتعاون هو العمل المشترك، بينما يتمثل المعنى الخاص له من خلال المشاركة الاعتيادية في ممارسة نشاط شخصي لمساعدة شخص اخر، وبنفس الصدد يعد المصطلح الدولي من المصطلحات التي تختص بالعلاقات بين الدول، ويمكن أن يتم تطبيقه على مصادر القانون التي تكون غير صادرة عن دولة

---

[57] عادل محمد السيوي، التعاون الدولي في مواجهة جريمة غسيل الاموال، نهضة مصر للطباعة والنشر، الطبعة الاولى، مصر، 2008م، ص7.

[58] سورة المائدة الآية رقم (2).

او مجموعة من الدول، كونها تستهدف الاوضاع التي تشغل الكثير من الدول لأنها تطبق في عدة دول.[59]

ومن هذا المنطلق نجد بان هناك اختلاف واضح في هدف واهمية التعاون الدولي وذلك لتعدد انواعه والاطراف المشتركة به، باعتبار ان الامن والامان من احتياجات الناس الاساسية، الامر الذي ادى الى اعتبار التعاون الامني من اهم مجالات التعاون بين دول العالم بوجه عام، في حين عرفه البعض على انه المساعدة وتبادل العون المشترك بين دولتين او اكثر من اجل التنسيق والعمل على تحقيق المصالح والمنافع المشتركة من اجل الحد من ارتكاب الجرائم ومكافحتها.[60]

واستنادا الى ما سبق فانه يمكن تعريف التعاون الأمني الدولي على انه، "مجموعة من الإجراءات التي تقوم بها الدولة او المنظمات الدولية الحكومية وذلك بعد تقديم الطلب من الدولة الاخرى من اجل المساعدة الاجرائية في المجالات القضائية والامنية، استنادا إلى مجموعة من المصادر القانونية الدولية بمختلف انواعها من اجل تحقيق المساعدة الدولية لمواجهة الجريمة بصفة عامة والجرائم العابرة للحدود ذات الطابع الدولي بصفة خاصة.[61]

وبناءً على ما سبق يرى الباحث بان تعريف التعاون الدولي هو العمل المشترك بين دولتين او اكثر، من اجل تبادل العون والمساعدة لتحقيق الخدمات والمنافع المشتركة لمواجهة الجريمة التي ترتكب في الدولة، وذلك للتوصل الى نتائج مشتركة بما يكفل فرض الامن والعدالة للمجتمع وللدولة في اطار تنفيذ الاتفاقيات والمعاهدات المبرمة.

---

[59] جيرار كورنر، مرجع سابق، ص 496.

[60] احمد ابراهيم سليمان، الارهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع، بدون طبعة، القاهرة، 2006م، ص 294.

[61] خالد مبارك القحطاني، مرجع سابق، ص 38.

المطلب الثاني: الإطار القانوني للتعاون الدولي في مجال مكافحة الجريمة الالكترونية

تعتبر الجريمة الالكترونية كغيرها من الجرائم التقليدية، كونها تحتاج للقواعد الاجرائية التي لا يمكن الاستغناء عنها، ومن هذه الاجراءات مرحلة التحري وجمع الاستدلالات والتي يختص بها مأمور الضبط القضائي، ومرحلة التحقيق الابتدائي والتي تختص بها النيابة العامة، ومرحلة التحقيق النهائي أي المحاكمة،[62] وقبل الخوض في الحديث عن هذا المطلب لا بد لنا من توضيح التعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة ما قبل المحاكمة **(الفرع الاول)**، والتعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة المحاكمة وما بعدها **(الفرع الثاني)**.

الفرع الاول: التعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة ما قبل المحاكمة

تقوم مرحلة ما قبل المحاكمة على مجموعة من الاعمال التي يقوم بها مأمور الضبط القضائي من خلال التحري وجمع الاستدلالات على الجريمة الالكترونية، والتي تتطلب منه الالتزام بالقواعد والشروط الاجرائية وتتطلب ايضا الجهد والخبرة اثناء أعمال البحث على الادلة، وايضا من خلال مرحلة التحقيق الابتدائي التي تقوم بها النيابة العامة والتي يتم فيها جمع الادلة، وذلك لضمان سير التحقيق على أكمل وجه من اجل الوصول الى كشف الحقيقة، باعتبار مرحلة التحقيق الابتدائي المرحلة التحضيرية لمرحلة المحاكمة.[63]

---

[62] د. احمد فتحي سرور، مرجع سابق، ص 143.

[63] د. محمود نجيب حسني، شرح قانون الاجراءات الجرائية، الطبعة الثانية، دار النهضة العربية، مصر، 1998م، ص 614.

اولا: مرحلة التحري وجمع الاستدلالات في الجريمة الالكترونية:

والمقصود في التحري بالاصطلاح القانوني هو البحث والاستقصاء عن الحقائق، باعتباره عملاً من الاعمال الامنية والقانونية التي يقوم بها الشخص الذي يقوم بالتحري من اجل الوصول الى المعلومات والبيانات التي تقوم بتعريف وتوضيح الاشخاص والاماكن والاشياء، بهدف الحد من ارتكاب الجريمة وضبطها وذلك لتحقيق الامن والنظام العام في حين يمكن تعريف التحري الالكتروني والذي يكون باستخدام الحاسب الالي وتقنية المعلومات والانترنت بأنه عمل امني وقانوني يمارسه مأمور الضبط القضائي من خلال استخدام التقنيات الالكترونية والرقمية وذلك من اجل الوصول الى المعلومات عن الأشخاص أو الأماكن أو الأشياء، بهدف الاستقصاء عن الجرائم والحد من ارتكابها وضبطها وملاحقة مرتكبيها.[64]

في حين نص قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة (2001م)[65] ومن خلال المادة رقم (19\2) على انه: "يتولى مأمور الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم التحقيق في الدعوى"، ونجد بانه وفي هذه المرحلة يقوم مأمور الضبط القضائي بالإجراءات التي خوله القانون بها في مرحلة التحري وجمع الاستدلالات قبل احالتها الى النيابة العامة للتحقيق فيها، وعليه تتضح هذه الإجراءات من خلال نص المادة (22) من قانون الإجراءات الجزائية والتي جيء بها وفقا لأحكام القانون إلى مأموري الضبط القضائي للقيام بما يلي:

1. قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة.

---

[64] مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، الطبعة الاولى، القاهرة، 2005م، ص 23.

[65] قانون الإجراءات الجزائية الفلسطيني رقم (3) الصادر بتاريخ 12 أيار/ ماي 2001، الوقائع الفلسطينية، العدد 38، 5 أيلول/ سبتمبر 2001.

2. إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق، والاستعانة بالخبراء المختصين والشهود دون حلف يمين.
3. اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.
4. إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها.[66]

ومن هذا المنطلق نجد بان مأمور الضبط القضائي ذو الاختصاص العام او الخاص، بحيث يقتصر الاختصاص الخاص على جرائم معينة وتكون متعلقة بالأعمال الوظيفية التي يمارسها مأمور الضبط القضائي كونه يتمتع بكيان خاص.[67]

ومن خلال ما سبق نجد بان هذه الاجراءات التي فرضها القانون لعمل مأمور الضبط القضائي حالت دون ارتكاب الجريمة وجاءت لجميع الجرائم دون استثناء، وعليه فان الشرطة هي من تباشر عملها بالتحري وجمع الاستدلالات حال وقوع الجريمة الالكترونية، في حين يحق لهم استدعاء الخبراء المختصين بمجال التقنية المعلوماتية لكشف الحقيقة والحفاظ على الادلة من الضياع، وعليه يكون هناك رجال شرطة مختصين في وحدة الجرائم الالكترونية من اجل ملاحقة مرتكبي الجرائم الالكترونية ومعاقبتهم.[68]

وبطبيعة الحال يمكن القول بان المعاينة في الجرائم الالكترونية يمكن اعتبارها من الاجراءات التحقيقية والاستدلالية كونها تكون مرتبطة بخصوصية الافراد في حين جاء فقهاء القانون الجنائي بتعريفها بانها "رؤية بالعين لمكان او لشخص او لشيء وذلك من اجل إثبات حالته وضبط ما يلزم لكشف الحقيقة"، وفي واقع الامر يعتبر اجراء المعاينة من اهم الاجراءات التي

---

[66] المواد (19) و (22) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة (2001م).
[67] د. مصطفى عبد الباقي، شرح قانون الاجراءات الفلسطيني: دراسة مقارنة، جامعة بيرزيت، فلسطين، 2015م، ص 162.
[68] رامي متولي القاضي، مرجع سابق، ص 112.

تؤدي الى كشف الحقيقة في الجرائم التقليدية، اذ لا يمكن لمأمور الضبط القضائي من مباشرة اعمال المعاينة دون ان ينتقل الى مسرح الجريمة من اجل اثبات الجريمة وضبط ادوات ارتكابها، بينما اجراء المعاينة في الجرائم الالكترونية قد لا يؤدي الى نتيجة احيانا، وذلك بتعدد الاسباب بحيث لا يمكن اجراء المعاينة لمحتويات الحاسوب الالي من خلال المعالجة الالية للمعلومات غير المرئية بمجرد قيام مأمور الضبط القضائي من خلال الاطلاع عليها في فترة وجيزة بحيث تكون ما بين وقوع الجريمة واكتشافها.[69]

وجدير بالذكر بان اجراءات التفتيش في الجرائم الالكترونية تختلف اختلافاً واضحاً عن التفتيش بالجرائم التقليدية كونه يتم بالفضاء الخارجي، وعليه فان التفتيش في الجرائم الالكترونية يحتوي على الصفة المادية والصفة المعنوية من خلال البيانات الالية التي يلزم الحصول عليها وتجميعها بالإضافة الى وجود مهارات فنية عالية لدى مأمور الضبط القضائي، ووجود قانون خاص يتلاءم مع خطورة الجرائم الالكترونية بشكل مستمر لملاحقة مرتكبيها[70]

وتأسيسا على ذلك، نجد بان المشرع الفلسطيني لم يتطرق لتعريف التفتيش الإلكتروني في القرار بقانون رقم (10) لسنة (2018) بشان الجرائم الالكترونية، في حين نصت المادة (32) منه على أليات التفتيش سواء التي يتم اجراؤها من قبل مأمور الضبط القضائي على مسرح الجريمة او التي يتم اجراؤها على الحاسب الالي والمعدات والتقنيات المعلوماتية، وذلك من اجل البحث عن الادلة الرقمية والتي يتم ربطها بمقترف الجريمة من قبل المختبر الجنائي الالكتروني، وبناء على ذلك يكون القصد من التفتيش الالكتروني القيام بضبط الحاسب الألي والمعدات من قبل مأمور

---

[69] احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى،2010م،ص 135.

[70] عبدالله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف للعلوم الامنية، 2011م، ص47.

الضبط القضائي المختص والذي يقوم بتنظيم تقريره الفني وتقديمه الى النيابة العامة وذلك للأهمية ولاستكمال اجراءات التحقيق حسب الاصول والقانون واحالته الى المحكمة.[71]

يعتبر اجراء الضبط في الجرائم التقليدية من الاجراءات الاصيلة التي اجازها القانون لمأمور الضبط القضائي، بينما جاء القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية ليغير هذا الاجراء بحيث جعله من الاجراءات التحقيقية أي مكلف بها من قبل النيابة العامة، في حين نصت المادة (32\3) من القرار بقانون على انه " إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها".[72]

واستخلاصا لما سبق، يمكن ان يتم التفتيش في الجرائم الالكترونية التي يقوم الجاني بارتكابها خارج حدود الدولة باعتبارها من الجرائم العابرة للحدود، بحيث يقوم التفتيش على الحاسب الالي والتقنيات المعلوماتية والفنية التي تكون متصلة بالأنترنت، ولذلك ينبغي على الدول تعزيز التعاون الدولي من خلال بعض التشريعات والاتفاقيات الدولية والاقليمية والثنائية التي تطرّق لها الموضوع ومنها اتفاقية بودابست التي بموجبها عملت على قيام الاطراف الخاضعين لها بالالتزام بكافة الاجراءات التي تمكن الجهات المختصة من اجراءات المعاينة والتفتيش بالبيئة الرقمية

---

[71] المادة رقم (32) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية والتي تنص على:1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

[72] المادة رقم (32\3) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية.

والمعلومات التقنية المخزنة، من اجل إثبات الجريمة الإلكترونية ومعاقبة مرتكبيها بموجب الاجراءات القانونية والقضائية في مجال تعزيز التعاون الدولي مع مختلف البلدان بموجب الاتفاقيات المصادق عليها من قبل الدول، وذلك بهدف تبادل المعلومات وتقديم المساعدة القانونية المتبادلة من اجل السرعة في التحقيق في الجرائم الالكترونية وتتبع مقترفيها وملاحقتهم وطلب تسليمهم من اجل تقديمهم للعدالة.[73]

ثانيا: مرحلة التحقيق الابتدائي في الجريمة الالكترونية:

هناك العديد من التعريفات التي تطرقت لمفهوم التحقيق الالكتروني، اذ لا بد لنا اولا من التطرق لتعريف المحقق،" هو الشخص الذي يتولى ويكلّف بالتحقيق وبالبحث وجمع الادلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها او اكتشافها بعد وقوعها وضبط مرتكبيها والادوات التي استعملت فيها"، في حين يمكن تعريف التحقيق على انه،" مجموعة من الاجراءات التي يقوم بها المحقق وتؤدي الى اكتشاف الجريمة ومعرفة مرتكبها، تمهيدا لتقديمه الى المحكمة لينال عقابه وقد تكون هذه الاجراءات كالتحقيق والتفتيش ومضاهاة البصمات".[74]

يعرف التحقيق الالكتروني على انه،" هو عمل قانوني يقوم به مأمور الضبط القضائي المختص والمتخصص لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمهم لسلطات التحقيق القضائي التي يجب ان تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل".[75]

---

[73] انظر الى المواد رقم (28 و 42 و 43) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية.

[74] خالد عياد الحلبي، مرجع سابق، ص 191.

[75] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، الطبعة الاولى، القاهرة، 2009م، ص 166.

ان ما يميز مرحلة التحقيق عن مرحلة التحري وجمع الاستدلالات في الجريمة الالكترونية الذي تطرقت لها سابقا، هو ان المشرع وضع بعض القيود على الاجراءات التي يقوم بها مأمور الضبط القضائي بحيث اشترط عليهم الحصول على اذن من النيابة العامة في غير حالة التلبس كونها هي الجهة المختصة بالتحقيق الابتدائي، والتي تهدف الى الحفاظ على الامن والامان في المجتمع والعمل على مواجهة الجرائم التي ترتكب ومعاقبة مقترفيها، ويكون ذلك باتباع اجراءات التحقيق العادلة بمراعاة ضمانات المتهم اثناء التحقيق، بحيث تقوم النيابة العامة في مباشرة اعمال التحقيق من لحظة ارتكاب الجريمة واحالة ملفها من قبل مأمور الضبط القضائي بموجب الصلاحيات التي فرضها القانون إلى المحكمة، وعليه يكون الهدف من هذا المرحلة هو كشف الحقيقة من خلال اقامة الدعوى الجزائية واحالة الملف الى المحكمة المختصة.[76]

وتختص نيابة الجرائم الالكترونية في متابعة الطلبات المتعلقة بالجرائم الالكترونية في حين تعمل هذه النيابة بالتعاون مع وحدة مكافحة الجرائم الالكترونية من اجل الوصول الى الدليل الفني الالكتروني وربط الجناة به، وعليه فان نيابة الجرائم الإلكترونية تتولى التحقيق في الشكاوى الواردة إليها وفقا للمعايير التي تتناسب مع طبيعة وخصوصية تلك الجرائم وغالبا ما يكون الدور التي تقوم به نيابة الجرائم المعلوماتية هو دور وقائي وعقابي[77]

---

[76] اشرف رمضان، النيابة العامة ودورها في المرحلة السابقة على المحاكمة (دراسة مقارنة)، الطبعة الاولى، دار النهضة العربية، 2004م، ص61.

[77] يشير الدور الوقائي في قانون الإجراءات الجنائية إلى السلطة التي يمنحها القانون للقضاة لمنع حدوث أفعال كيدية من شأنها إلحاق الأذى بالآخرين، لذلك إذا كان الدور أو الوسيلة مدرجًا في النص القانوني ، فلا يعتبر دورًا وقائيًا ، لأن الدور الوقائي المقصود في قانون الإجراءات لا يعني منع ممارسة الحرية أو الحق أو الترخيص الذي يأذن به المشرع. بل إن الدور الوقائي يتحقق من خلال مراقبة وضبط استخدام حق إجرائي ، ومن ثم منع الاستخدام التعسفي لذلك الحق ، لأن منع التعسف أفضل مما يحدث ، ومن ثم المساءلة عنه.

ان مسالة التحقيق في الجرائم الالكترونية من المسائل المهمة والصعبة، باعتبارها من الجرائم الحديثة والتي تحتاج الى وجود ادوات وتقنيات معلوماتية عالية، في حين تطلّب هذا الامر اخضاع مأموري الضبط القضائي المختصين واعضاء النيابة العامة الى تدريبات من اجل اكتساب الخبرات الفنية اللازمة لممارسة اعمال التحقيق بشكل ملم، وفي واقع الامر فان الغرض من التحقيق في الجرائم الالكترونية يكون من اجل التأكد من وقوع الجريمة المعاقب عليها قانونا، والتعرف على نوعها وكيفية حدوثها وادوات ارتكابها والتعرف على الشخص المتضرر من هذه الجريمة، ايضا يجب معرفة السبب الذي دفع مرتكب هذه الجريمة لاقترافها ومعرفة الظروف التي رافقت ارتكاب الجريمة الإلكترونية، والعمل على تجميع الادلة التي تم الوصول اليها من خلال اعمال التحقيق واحالة المتهم الى المحكمة المختصة لإدانته وايقاع العقوبة الرادعة بحقه.[78]

تتميز مرحلة التحقيق الابتدائي في الجرائم الالكترونية بإخضاعها لإشراف اعضاء النيابة العامة، سواء من علم النيابة بوقوع هذه الجريمة او من لحظة اكتشافها او قيام المتضرر برفع شكوى لدى مأمور الضبط القضائي المختص بالجرائم الالكترونية، بحيث تباشر النيابة العامة إجراءاتها التحقيقية والعمل على تكليف مأمور الضبط القضائي المختص في الجرائم الالكترونية بإجراء التفتيش واجراء الضبط والتحفظ على الادلة التي تم ضبطها في الجريمة من اجل ارسالها الى الخبراء المتخصصين في وحدة الجرائم الالكترونية لإجراء اعمال الخبرة وتنظيم تقرير فني بالدليل الرقمي الذي تم التوصل اليه.[79]

[78] خالد عياد الحلبي، مرجع سابق، ص 191.

[79] نسرين جورج رشماوي، الاحكام الموضوعية والاجرائية للجرائم الالكترونية بفلسطين ، ص 101.

الفرع الثاني: التعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة المحاكمة وما بعدها

تعتبر مرحلة المحاكمة في الجرائم الالكترونية اهم مرحلة تمر بها الدعوى، كونها تقوم بالرقابة على اعمال يقوم بها مأمور الضبط القضائي المختص في متابعة وملاحقة الجرائم الالكترونية، وايضا بالرقابة على اعمال النيابة العامة من اجل الوصول الى الدليل الرقمي أي الدليل الوحيد في بناء ملف القضية التحقيقية كونه يقوم بربط المتهم بجريمته التي اقترفها، سواء كانت على الصعيد المحلي او الدولي او الإقليمي، في حين نصت المادة (207) من قانون الاجراءات الجزائية الفلسطيني على انه، "لا يبنى الحكم الا على الادلة التي قدمت اثناء المحاكمة والتي تمت مناقشتها في الجلسة بصورة علنية امام الخصوم"،[80] في حين يعد الدليل الرقمي أساس الدعوى بحيث ينبني عليه الحكم، ولكن قبل الخوض في مدى مشروعية الدليل الرقمي المبرز امام المحكمة المختصة في نظر الدعوى وحجيته في بناء الاحكام القضائية، وعليه نصت المادة (38) من القرار بقانون رقم (10) لسنة (2018) بشان الجرائم الالكترونية على انه،" تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي".[81] لكن لا يفوتنا بان ننوه الى مراحل المحاكمة وضمانات المتهم التي اجازها القانون.

ولا مناص من القول بان قانون الاجراءات الجزائية الفلسطيني بيّن من خلال نصوص مواده العديد من ضمانات المتهم في مرحلة المحاكمة، فهناك ضمانات تتعلق بالمبادئ العامة في محاكمة المتهم وذلك من خلال علانية الجلسة وتدوين جميع اجراءات المحاكمة والمرافعة الشفوية،

[80] المادة (207) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة (2011).

[81] المادة (38) من القرار بقانون رقم (10) لسنة (2018) بشان الجرائم الالكترونية.

وضمانات تتعلق بالمتهم ومنها قرينة البراءة وحق المتهم بالدفاع عن نفسه وحقه ايضا بتوكيل محام وغيرها من الضمانات، وفي نفس الصدد فرض القانون من خلال نصوصه على المحكمة المختصة بنظر الدعوى الالتزام بتطبيق القانون والعمل على تطبيق اجراءات ومنها حياد القاضي وعدم الحكم بعلمه الشخصي وصولا للمحاكمة العادلة.[82]

نصت المادة (3\2)[83] من ذات القرار على انه، "تتولى المحاكم النظامية والنيابة العامة وفقا لاختصاصاتهم النظر في دعاوي الجرائم الالكترونية".[84]

تبين للباحث بانه تم تحديد موقف القانون الدولي بشأن مسالة الاختصاص القضائي من خلال الاتفاقيات الدولية والاقليمية، في حين يمكن استخدام اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان، لتكون أساس التدابير اللازمة للحصول على الولاية القضائية بالنسبة للجرائم الالكترونية، بحيث نصت المادة (15) من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان على انه، يتعين على كل دولة طرف ان تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات التالية ومنها، عندما يُرتكب الجرمُ في اقليم تلك الدولة، وعندما يُرتكب الجرُم ضد احد مواطني تلك الدولة، وعندما يَرتكب الجرمَ أحدُ مواطني تلك

---

[82] المادة (205) من قانون الاجراءات الجرائية الفلسطيني رقم (3) لسنة (2011).

[83] ونصت المادة (2) من قرار بقانون رقم (10) لسنة (2018) بشان الجرائم الالكترونية على انه،" 1-تطبق احكام هذا القرار بقانون على اي من الجرائم المنصوص عليها فيه، اذا ارتكبت كليا او جزئيا داخل فلسطين او خارجها، او امتد اثرها داخل فلسطين، سواء كان الفاعل اصليا ام شريكا ام محرضا ام متدخلا، على ان تكون الجرائم معاقبا عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ، 2- يجوز ملاحقة كل من يرتكب، خارج فلسطين، احدى الجرائم المنصوص عليها في هذا القرار بقانون في احدى الحالات التالية: أ-اذا ارتكبت من مواطن فلسطيني. ب-اذا ارتكبت ضد اطراف او مصالح فلسطينية. ج-اذا ارتكبت ضد اطراف او مصالح اجنبية من قبل اجنبي او شخص عديم الجنسية وجد بالأراضي الفلسطينية ولم تتوافر في شانه شروط التسليم القانونية"

[84] المواد (2) و (3\2) من القرار بقانون رقم (10) لسنة (2018) بشان الجرائم الالكترونية.

الدولة، بحيث نصت المادة ايضا على انه اذا ابلغت الدولة التي تمارس ولايتها القضائية فعلى هذه الدول ان تتشاور فيما بينها للتنسيق.[85]

يعد التعاون الدولي في تنفيذ الأحكام الجزائية الأجنبية صورة خاصة من صور التعاون الدولي في مكافحة الجريمة الالكترونية، وذلك نظرا للدور الذي يلعبه في تحقيق مكافحة فعالة لهذه الجريمة، في حين تزداد أهمية التعاون الدولي في تنفيذ الاحكام الصادرة بحيث لا قيمة لهذا التعاون في مجال المساعدة القضائية اذا لم يقترن بتعاون يضمن تنفيذ الحكم القاضي بالإدانة، كون الهدف من تنفيذ العقوبة الصادرة التي تحقق الردع العام والخاص، فوجود نص يجرم الفعل وحكم يطبق العقاب غير كافيين في تحقيق هذا الهدف، ما لم يتوج الحكم بتنفيذه.[86]

[85] المادة (15) من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر 2000.

[86] علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2011م، ص 310.

الفصل الثاني

أشكال التعاون الدولي وصعوباته في مواجهة الجريمة الالكترونية

تُعتبر الجرائم الإلكترونية من الجرائم الحديثة، والتي تتميز بطبيعة خاصة، حيث تتجاوز حدود الفرد لتمس كيان الدولة والمجتمعات علاوة على أن هذه الجرائم تدخل في صميم الجرائم الاقتصادية، والتي لها مخاطر كبيرة على الاقتصاد القومي والعالمي، وذلك نظراً لما تمثله من تهديد على الدول،[87] وبناءً على ما سبق نتحدث في هذا الفصل عن أشكال التعاون الدولي وصعوباته في مواجهة الجريمة الالكترونية بالوقوف عند أوجه التعاون الدولي في مواجهة الجريمة الالكترونية **(المبحث الأول)**، وكذلك التعرف على أهم الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الالكترونية وكيفية التغلب عليها **(المبحث الثاني)**.

المبحث الأول: أوجه التعاون الدولي في مواجهة الجريمة الالكترونية

شاع خلال الأعوام السابقة انتشار العديد من الجرائم الإلكترونية، حيث انتشر الكثير من الفيروسات المختلفة ،[88] وبالتالي وجب على المجتمع الدولي اتخاذ موقف موحد إزاء هذه الجرائم، ويتمثل في التعاون الأمني والقضائي لمكافحة الجرائم الإلكترونية بشكل عام **(المطلب الأول)**، وكذلك بحث أوجه التعاون الدولي لتسليم المجرمين في مواجهة الجريمة الالكترونية **(المطلب الثاني)**.

[87] إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، مصر، 2077م، ص493.

[88] إيهاب فوزي، مرجع، سبق، ص 495.

المطلب الأول: التعاون الأمني والقضائي الدولي في مواجهة الجريمة الالكترونية

إن مسألة التنسيق بين الدول في مجال مكافحة الجرائم ذات الأهمية في المجال الدولي، فقد أوضحت المذكرات التفسيرية للأعمال التحضيرية لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان، أن أهمية التنسيق تتمثل في ضمان عدم فقدان الأدلة الحسيَّة زمنياً، تماماً كالدليل في الجرائم الالكترونية، والتي قد تكون الجريمة المنظمة واحدة منها.[89]

وإذا وقعت الجريمة الالكترونية، وفي سبيل كشف حقيقتها والبحث عن أدلتها التي قد تتوافر في حدود دولة أخرى، فإننا ولغايات التفتيش نلاحظ أن رجال الاستدلال والتحقيق قد يكونون بحاجة إلى الدخول إلى حدود الدول الأخرى، وهذا يعني أنهم قد يحتاجون إنابة رجال التحقيق والاستدلال في تلك الدولة للقيام بأعمال التفتيش.

وعليه نستعرض في هذا المطلب أوجه التعاون الأمني والقضائي الدولي في مواجهة الجريمة الالكترونية:

الفرع الأول: التعاون الأمني في مواجهة الجريمة الإلكترونية

قد ترتكب الجريمة الالكترونية في دولة معينة ويتحقق الفعل الإجرامي في دولة أخرى فهي تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكن بفعل طبيعة شبكة الانترنت يمتد الفعل الإجرامي خارج هذه الحدود ليطال دولة أخرى، مما جعله بحق جريمة عابرة للحدود، والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الجرائم الالكترونية وبشكل خاص الإجراءات

---

[89] الفقرة الخامسة من المادة العاشرة من الملحوظات التفسيرية للأعمال التحضيرية لعملية التفاوض حول اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها رقم (A/55/383/Add.1)، الدورة الخامسة والخمسون، 2000، على الرابط:
www.uncjin.org/Documents/Conventions/dcatoc/final_documents/383a1adoc، تاريخ الزيارة: 15 مايو/ أيار 2023.

الجنائية والاختصاص والقانون، مما شكل عاملاً رئيسياً لضرورة تعاون وجمع الجهود الدولية لمكافحة هذه الجرائم[90]، وفي هذا الفرع نتحدث عن أوجه التعاون الأمني في مواجهة الجريمة الإلكترونية، والمتمثلة في الآتي:

أولاً: ضرورة التعاون الأمني الدولي

إدراكا من الدول بضرورة أهمية التعاون الدولي وذلك لتجاوز تحديات الجرائم الإلكترونية، عمل الكثير منها لعقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الكمبيوتر عابرة للقارات،[91] ففي عام 1983 أجرت منظمة التعاون والإنماء الاقتصادي[92] دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الالكترونية وسوء استخدامها، وفي عام 1985 أصدرت هذه المنظمة تقريرا تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب على الدول أن تجرمها وتفرض عليها 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 لأسيا والباسفيك المنعقد 1989 الممهد للمؤتمر الثامن للأمم المتحدة المنعقد

---

[90] نبيله هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2007، ص38-39.

[91] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من 1-3 مايو 2000 بكلية الشريعة والقانون بدولة الإمارات، ص1078.

[92] المنظمة التعاون الاقتصادي والتنمية (The Organization for Economic Cooperation and Development – OECD) هي المنظمة الدولية التي تشمل من 34 دولة من بين الدول المتقدمة التي تتبنى مبادئ الديمقراطية التمثيلية واقتصاد السوق الحرّ والتي يصل نتاجها إلى ثلثي النتاج العالمي".

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.[93]

أن تحديث قانون الإجراءات وتبادل المساعدة في الأمور المتعلقة بالجرائم الإلكترونية وإبرام الاتفاقيات الدولية ، بما في ذلك النصوص المنظمة لإجراءات التفتيش والرقابة المباشرة عبر الحدود على نظم المعلومات. من ناحية أخرى، أنشأت الأمم المتحدة آليات جديدة نشطة في إطار المساعدة المادية والتقنية، وتبادل الخبرات وإنشاء قواعد البيانات، لتمكين الجميع من المساهمة بشكل فعال في مكافحة الجريمة السيبرانية، او الجريمة الالكترونية.[94]

وعلى الرغم من ضرورة التعاون الدولي وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها: عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، والنقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء.[95]

---

[93] 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– 28أكتوبر، 1993، ص362.

[94] وذلك في المواد 31، 25، 24، 20 من الاتفاقية.

[95] محمد بن أحمد بن علي المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا: التكامل الدولي المطلوب لمكافحتها، جامعة الإمام محمد بن سعود الإسلامية، السعودية، 2015م، ص 33.

وبالرغم من الغياب الواضح لأي تنسيق رسمي عربي ملموس في إطار اتفاقية أو تنظيم إقليمي فيما يخص مكافحة الجرائم الالكترونية إلا أن الجهود العلمية والأمنية بشكل خاص واضحة ومتوالية في مجال رصد هذه الجرائم، ومنها:[96]

- ندوة حول الجرائم الناجمة عن التطور التكنولوجي نظمتها الجمعية الوطنية للدفاع الاجتماعي بنادي ضباط الأمن – عمان الأردن خلال الفترة من 28-1998/10/29.
- ندوة المواجهة الأمنية للجرائم المعلوماتية سنة 1999، مركز البحوث والدراسات لشرطة دبي.
- مؤتمر جرائم الانترنت بأكاديمية اتصالات دبي في الفترة ما بين 22-2000/10/23.
- الندوة الإقليمية حول الجرائم المتصلة بالحاسوب بالدار البيضاء في المغرب في الفترة 19-2007/6/20.
- ندوة فلسطينية بخصوص التعاون الدولي في مواجهة الجرائم العبرة للحدود والجرائم والمنظمة، رام الله، النيابة العامة، 8 تموز/ يونيو 2023.

ثانياً: جهود المنظمة الدولية للشرطة الجنائية (الانتربول)

تقوم منظمة الشرطة الدولية "الإنتربول" بدور مهم في مكافحة الجرائم الإلكترونية، ويظهر ذلك في الأقسام والشُعب التي تتكون منها المنظمة، كشعبة الإجرام الاقتصادي والمالي، وشعبة التقصي الآلي وتحليل المعلومات، وغيرها،[97] وفي هذا الإطار نظمت السكرتارية العامة للمنظمة أولى مؤتمراتها الدولية بخصوص الاحتيال والغش في البطاقات البنكية في عام 1994، ونتج عن هذا المؤتمر توصيتين هامتين هما:[98]

---

[96] فائز بن عبد الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وضعية تأصيلية للظاهر الإجرامي على شبكة الانترنت، موقع الدليل الالكتروني، www. Arablawin fo com، تاريخ الزيارة: 12 مايو/ أيار 2023.

[97] فيصل بن حمدان الخاطري. أنظمة الدفع الالكتروني وفقاً للقانون العماني. رسالة ماجستير، جامعة السلطان قابوس، عمان، الأردن، 2018، ص52.

[98] محمد الكعبي، الحماية الجنائية للتجارة الإلكترونية. رسالة دكتوراه، جامعة القاهرة، مصر، 2009، ص276.

- على الدول الأعضاء مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الدفع بما يتضمن تجريم كل فعل يتضمن تصنيع وامتلاك أي معلومات غير قانونية تم الحصول عليها بطريق غير مشروع أو استعمالها في نظام بطاقات الدفع.[99]
- إنشاء مجموعات عمل بوليسية من خبراء متابعة جرائم الغِش والإحتيال على المستوى الدولي التابعين لبوليس (هونج كونج والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية النيوزلندية ومندوبين من منظمات الائتمان) لمكافحة هذا النوع من الأجرام ووضع الأسس الخاصة لتبادل المعلومات والحد منه.[100]

وفي هذا الصدد نُشير إلى أن المنظمة الدولية للشرطة الجنائية (الإنتربول) لها دور في دعم التعاون الأمني والمتمثل في تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف لمكافحة الجريمة حيث تقوم بتجميع البيانات والمعلومات المتعلقة بالجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية، كما أن المنظمة تقوم بدور الوسيط للدول المشتركة فيها للمعاونة في التصدي للجريمة بكافة أشكالها.[101]

تمثل النشرات الدولية للإنتربول واحدة من المهام الرئيسية التي تتيح إيجاد تعاون دولي ومساعدة لجهاز الشرطة في البُلدان البالغ عددها 195 دولة، من خلال تبادل المعلومات حول الجرائم الخطيرة والأشخاص المفقودين والتهديدات المحتملة والجريمة المنظمة التي تنطوي على أشخاص يريدون ارتكاب أعمال إجرامية، وهناك بيانات أساسية تتضمنها النشرات الدولية للإنتربول وهي هوية الشخص المطلوب وبصمته وصورته ومهنته ومواصفاته البدنية، بالإضافة الى بياناته القضائية كالتهمة المنسوبة اليه.

---

[99] محمد الكعبي، الحماية الجنائية للتجارة الإلكترونية. ص276.

[100] محمد الكعبي، المرجع السابق، ص276.

[101] فهد عبد الله العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016م، ص477-478.

وهناك انواع عديدة من النشرات الدولية للإنتربول ومنها: **النشرة الحمراء:** تحديد مكان الشخص المطلوب أو توقيفه مؤقتا او إلقاء القبض استعدادا لتسليمه، بناء على أمر بالقبض عليه لتقديمه للمحاكمة أو تنفيذ الحكم. **النشرة الزرقاء:** يتم من خلالها تحديد مكان الشخص المطلوب والغرض منها هو ادخال البيانات الاضافية حول هوية الأشخاص الطلوبين أو مكانهم أو أنشطتهم المتعلقة بالتحقيقات الجنائية. **النشرة الخضراء:** تقديم التنبيه لأولئك الذين يرتكبون جرائم جنائية والذين يشكلون خطرا على الامن والنظام والسلامة العامة، **النشرة الصفراء:** غالبا ما يتم استخدامها للمساعدة في العثور على الأشخاص المفقودين وخاصة القصر، أو للمساعدة في تحديد أولئك الذين لا يستطيعون تحديد هويتهم، **النشرة السوداء:** لطلب معلومات عن جثث مجهولة الهوية **النشرة البرتقالية:** للتحذير من حدث أو شخص أو شيء أو عملية تمثل تهديدًا وخطرًا وشيكًا على الأشخاص أو الممتلكا، **النشرة الأرجوانية:** لتوفير معلومات عن طريقة العمل أو الإجراءات أو الأشياء أو الأجهزة أو أماكن الاختباء التي يستخدمها المجرمين، النشرة **الخاصة بالإنتربول:** تصدر للجماعات والافراد الخاضعين لعقوبات من قبل مجلس الامن التابع للأمم المتحدة.[102]

أما بشأن انضمام فلسطين إلى المنظمة الدولية للشرطة الجنائية (الإنتربول)، فقد بدأ الفلسطينيون يسعون إلى عضوية كاملة في أعقاب سنوات من التحضير ومع ارتفاع ملحوظ في عدد بلدان العالم التي بدأت تعترف بفلسطين كدولة، ممّا يزيد من حظوظ تصويت الجمعية العامة للشرطة الدولية على عضويتها، وبحسب لوائح الانتربول تحتاج كلّ دولة للحصول على عضوية كاملة في المنظمة إلى ثلثي الاصوات زائد صوت واحد من أعضاء الجمعية العامة، ومع اعتراف 130 دولة بفلسطين، يبدو الحصول على أغلبية الأصوات مسألة في متناول اليد، وخلال اجتماع

[102] خالد مبارك القحطاني، التعاون الدولي ودوره في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، اكاديمية نايف للعلوم الامنية، الرياض ، 2006، 151.

عقدته الجمعية العامة في بكين في 2017/9/27 صوتت 75 دولة من أعضاء الجمعية على انضمام فلسطين.[103]

ثالثاً: القيام بالعمليات المشتركة الشرطية والأمنية

هذا يكون بتعقب مجرمي المعلوماتية، وشبكات الإنترنت، والبحث والتحري المشترك في مجال الأدلة الجنائية وضبطها، والقيام بعمليات التفتيش العابر للحدود لمكونات الكومبيوتر والأنظمة المعلوماتية، وشبكات الاتصال بحثا عن الأدلة التي تؤدي إلى وضع حد للأنشطة الإجرامية في المجال الإلكتروني، هذا كله يستدعي القيام بعمليات شرطية وأمنية مشتركة تؤدي كذلك إلى تبادل المعلومات والخبرات الفنية في هذا المجال.[104]

ونظراً لكون الجريمة الإلكترونية عابرة للحدود، فإن هذا ما يجعل قوات الشرطة والسلطات القضائية عاجزة عن القيام بدورها، خاصة أن أغلبية هذه الجرائم يتطلب التحقيق فيها الوصول الى شبكات أخرى تقع خارج الدولة مما يؤدي إلى إعاقة الإجراءات، ويلعب التعاون الأمني الدولي في هذا المجال دوراً كبيراً من خلال تبني آلية متطورة لإجراء التحريات والتحقيقات في مجال الجريمة المعلوماتية، وذلك باستخدام أساليب خاصة للتحري والمراقبة واستحداث قنوات الاتصال والتنسيق الأمني عن طريق الأقمار الصناعية وشبكة المعلومات بغية سرعة تبادل المعلومات ويتحقق ذلك من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتين والاتفاق على معايير موحدة تحكم هذه المسائل.[105]

---

[103] المؤسسة الفلسطينية لحقوق الإنسان (شاهد)، تقرير بعنوان: ماذا يعني قانونياً انضمام فلسطين إلى الشرطة الدولية (الانتربول)؟، منشور على موقع المؤسسة على الانترنت، تاريخ النشر: 27 سبتمبر/ أيلول 2017، تاريخ الزيارة: 22 مايو/ أيار 2023، على الرابط: pahrw.org/portal/ar-LB.

[104] محمد بن حاج الطاهر وشكيرين دليمي، سبل الحماية الدولية من الجريمة الإلكترونية، مجلة الناقد للدراسات السياسية، جامعة محمد خيضر بسكرة – كلية الحقوق والعلوم السياسية، المجلد السادس، العدد الأول، الجزائر، 2022، ص713.

[105] فهد عبد الله العازمي، مرجع سابق، ص470-471.

وأثبت الواقع العملي بأنه لا تستطيع أي دولة بمفردها القضاء على الجرائم الدولية العابرة للحدود، ذلك أن جهاز الشرطة في هذه الدول أو تلك غير قادر على تعقب المجرمين وملاحقتهم إلا في حدود الدولة، فيقف الجهاز الشرطي عاجزاً، لذلك من الضروري وجود كيان دولي يهدف إلى تعاون الأجهزة الشرطية في الدول المختلفة لا سيما في مجال تبادل المعلومات المتعلقة بالجريمة والمجرمين،[106] كما أن التعاون الأمني الدولي له عدة صور وهي ربط شبكات الاتصال والمعلومات، تبادل المعونة الدولية لمواجهة الكوارث والأزمات والمواقف الحرجة، القيام ببعض العمليات الشرطية والأمنية المشتركة.[107]

الفرع الثاني: التعاون القضائي في مواجهة الجريمة الالكترونية

ان شبكة الانترنت تعتبر من الشبكات العالمية التي تمتاز بأنها عابرة للحدود ولا تعرف للحدود الجغرافية معنى، وبالتالي فإن الجرائم المتصلة بها تعتبر هي الأخرى عالمية وذات طابع دولي وأثرها يمتد لأكثر من دولة، ففي واقعة تتلخص وقائعها في قيام شخصين مقيمين في ملبورن بأستراليا بإرسال ما بين ستة إلى سبعة ملايين رسالة إلكترونية على عناوين في أستراليا والولايات المتحدة الأمريكية بالإضافة إلى قيامهما بوضع عدة رسائل على لوحات الرسائل لدى الشركات الرئيسية المقدمة لخدمات الإنترنت، وتعّرف المساعدة القضائية الدولية بأنَّها " كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم".[108]

وقد نص المشرع الفلسطيني في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية على التعاون الدولي في مجال مكافحة الجرائم الالكترونية، حيث نصت المادة 42 من هذا القرار

---

[106] غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها وخصائصها وكيفية التصدي لها قانونا، دار الثقافة للنشر والتوزيع، عمان، 2016م، ص 96.

[107] فهد عبد الله العازمي، مرجع سابق، ص474.

[108] سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية. رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 1997، ص425.

بقانون على أن "1–تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل[109]، بقصد الاسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. 2– يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون".

ومن هنا نجد بأنه يمكن للسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، وتتخذ المساعدة القضائية الدولية عدة صور، أهمها:

أولاً: تبادل المعلومات [110]

أن السلطات القضائية الأجنبية تستند إلى توفير البيانات اللازمة لوجود اتهامات بارتكاب جرائم ضد الرعايا الأجانب والإشارة إلى التدابير المتخذة ضدهم، ومن ناحية أخرى، هناك شكل

[109] التعريف القانوني لمبدأ المعاملة بالمثل: بأن تنص اتفاقية دولية أو تشريع داخلي، على أن يتعهد كل طرف بتوفير ذات المعاملة للطرف الآخر، وهو ينحصر ضمن نطاق معين أو محدد من المجالات كالمعاملة بالمثل في مركز الأجانب أو المعاملة بالمثل في العلاقات الدبلوماسية، كما يمكن أن يتقرر هذا المبدأ بموجب العرف والممارسات الدولية، وفي هذه الحالة يكون أعمال المبدأ أكثر مرونة ولاسيما في الدول التي يحتل القانون العرفي فيها مكانة مهمة، انظر عز الدين فودة، النظم الدبلوماسية، مكتبة الآداب، القاهرة، 1989، ص129.

[110] يعرف تبادل المعلومات بأنه: "تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، حيث تتسلم المنظمة الدولية للشرطة الجنائي من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء تلك البيانات والمعلومات، وتقوم بتجميعها وتنظيمها، ومن هذه البيانات تتكون وثائق ذات أهمية كبرى في مكافحة الجرائم على المستوى الدولي"، ددوش، نسيمة، التعاون الدولي الجنائي لتبادل المعلومات مع المحكمة الجنائية الدولية، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، العدد (35)، المجلد (1)، 2019، ص146

آخر من أشكال تبادل المعلومات، والمتمثل بالسوابق القضائية للأشخاص المطلوبين، حيث تحدد السلطات القضائية بدقة أولئك الذين أشاروا إليهم، وبالتالي تحديد العقوبة ووقف تنفيذ العقوبة.[111]

لا يمكن إنكار أهمية تبادل المعلومات في مكافحة أي جريمة كانت سواء تقليدية أو من الجرائم الحديثة، تبرز الأهمية خصوصاً في جرائم الحاسب الآلي والإنترنت، نظراً لحداثتها وعدم كشف كل طرق ارتكابها، ولكونها جرائم متطورة تختلف مواصفاتها من مكان لآخر.[112]

إن الصعوبة والمشكلة التي تواجه التعاون الدولي في مكافحة جرائم الحاسب الآلي والانترنت، تتركز في عدم وجود آليات واضحة وشاملة لمعظم دول العالم، لتبادل المعلومات حول جرائم الحاسب الآلي والانترنت، وهذا ما أكدته الجمعية المصرية للقانون الجنائي في مؤتمرها الخامس المنعقد عام 1993 حول جرائم الحاسب الآلي والانترنت، إذ أكدت أن هذه الطائفة من الجرائم التي تعد من الجرائم العالمية، وأنه يجب أن تتكاتف الجهود لمكافحتها لأنها تمثل وجهاً سلبياً للتقدم الحضاري، كما يجب تعديل النصوص التقليدية في قوانين العقوبات أو إضافة نصوص جديدة، لعدم كفاية النصوص الحالية، وإحاطتها بالأنشطة المراد تجريمها، كما أكد المؤتمر على ضرورة التعاون الدولي في مكافحتها، وتحقيق التعاون الدولي في مجال الإنابة القضائية وتسليم المجرمين وتنفيذ الأحكام.[113]

وقد لقي هذا الشكل من المساعدة القانونية صدى كبيراً في عدد من الاتفاقات ولا سيما الفقرة 2 من المادة 1 من معاهدة الأمم المتحدة النموذجية بشأن المساعدة المتبادلة في المسائل

---

[111] احمد سعد الحسيني، الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، حقوق عين شمس، القاهرة، 2012، ص 295.

[112] يحيى محمود محمد عيشان، دراسة مقارنة بين التشريع الأمريكي والتشريع الأردني للصعوبات التي تواجه التنسيق والتعاون الدولي في مكافحة جرائم الحاسب الآلي والانترنت، رسالة ماجستير، جامعة عمان العربية، الأردن، 2008، ص92.

[113] سلطان محيا الديحاني، الجرائم المعلوماتية، جامعة الكويت، 2007م، ص5؛ د. مصطفى محمد موسى، الاساليب الاجرامية بالتقنية الرقمية ومكافحتها، مطابع الشرطة للنشر والتوزيع، الطبعة الاولى، القاهرة، 2003م، ص 531.

الجنائية والفقرات 3 و4 و5 من المادة 8 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان التي تلزم الدول الأطراف بتسهيل تبادل المعلومات المتعلقة بجوانب مختلفة من النشاط الإجرامي.[114]

ونصت المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، وفي هذا الإطار أيضاً صاغ اتفاق شنجن للاتحاد الأوروبي نظاماً متكاملاً لتبادل المعلومات.[115]

وبناءً على ما سبق، نجد بأنه في مجال التعاون الدولي من الناحية القضائية في الجرائم الإلكترونية ومكافحتها، يجد الباحث بأن التعاون لا يرقى أيضاً إلى المستوى المطلوب والسبب في ذلك يعود إلى عدم وجود الاتفاقيات الدولية المنظمة لهذا النوع من الجرائم، رغم وجود بعض الاتفاقيات في المجال القضائي والتي تساعد في بعض الأحيان في مكافحة الجرائم الالكترونية.

ثانياً: نقل الإجراءات

ويقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في الجريمة الكترونية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوبة، ونقل الاجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها.[116]

---

[114] جدير بالذكر أن هذه المعاهدة صدرت في 14 ديسمبر/كانون أول 1990 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات او إجراءات المحكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلاً في اختصاص السلطة القضائية للدولة الطالبة المساعدة.

[115] Michel quellie: strategies en france par la police la criminalite organisee, 1996, p:96.

[116] سالم محمد سليمان، مرجع سابق، ص427-428.

في حين تكون هذه الاجراءات مقررة في قانون الدولة المطلوب منها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شأنها أن تؤدي دوراً مهماً في الوصول إلى الحقيقة، والذي بدورهُ يحق لأي من الاطراف المتعاقدة ان يطلب من الاخر باتخاذ الاجراءات وفق الحالات التالية:

- إذا كان المتهم خاضعا لحكم يقيد حريته في الدولة الطالبة.
- إذا كانت التدابير التي يتعين اتخاذها منصوص عليها في تشريعات الولاية المطلوبة لنفس الجريمة.
- إذا أدى الإجراء الذي يجب اتخاذه إلى الوصول إلى الحقيقة، فيجب أن يكون هناك دليل على الجريمة في البلد المطلوب فيها.
- إذا كان تنفيذ الحكم في الدولة متلقية الطلب قد حقق إعادة دمج الشخص المحكوم عليه.
- إذا كان حضور المتهم في الجلسة لا يمكن ضمانه في الدولة المطلوب منها، مع التأكد من أن وجوده في الدولة المطلوب منها سيتحقق.

ولا مناص من القول بانه يحق للدولة المطلوب اليها ان ترفض نقل الاجراءات بحال عدم وجود تبرير واضح بالطلب، وايضا كان القصد من الطلب سياسياً او دينياً او عنصرياً، وايضا اذا كانت الدولة متلقية الطلب قد طبقت قانونها على الجريمة قبل استلامها من الدولة متلقية الطلب، وكانت الإجراءات المتخذة سابقا متوافقة مع القانون، وإذا كانت الإجراءات التي طلبتها الدولة تتعارض مع الالتزامات التي ارتكبتها الدولة متلقية الطلب ومخالفة للقانون.[117]

[117] شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، جامعة الشارقة، الامارات العربية المتحدة، 2019، ص 11.

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية منها معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية،[118] وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية.[119]

ثالثاً: الإنابة القضائية الدولية

أقرت العديد من الاتفاقيات الدولية الانابة القضائية الدولية كإحدى صور المساعدة القضائية وذلك مثل معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان لعام 2000، حيث ان المادة 21 منها.

فبطبيعة الحال نجد بأن عامل السرعة هو الأساس فهو يعتبر من العوامل الرئيسية والهامة في مكافحة الجرائم المتعلقة بالإنترنت، ولكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الإنترنت قد ظهرت، أو كانت موجودة ولكنها محدودة، فإن تعديل هذه الاتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة خاصة مع التطور الكبير في تكنولوجيا المعلومات والاتصالات.

ويمكن تعريف الانابة القضائية الدولية بأنها "هي آلية تعتمد الدولة من خلالها على طلب إجراءات قضائية معينة من دول أخرى في إقليمها، سواء لمصلحتها الخاصة أو نيابة عنها، مقابل أن ترد الدولة الطالبة المعاملة بالمثل، مع احترام النتائج القانونية التي تحققت من خلال الدعم القضائي للدولة متلقية الطلب"، وتتناول الانابة عددا من القضايا، بما في ذلك القضايا الجنائية

---

[118] المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدت بقرار الجمعية العامة للأمم المتحدة رقم 45/118 المؤرخ في 14 ديسمبر/ كانون أول 1990.

[119] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 للدورة الخامسة والخمسون في 15 نوفمبر 2000.

المدنية والتجارية وغيرها، والذي يتثمل دورها في اجراء التحقيقات التي تنفذها السلطة القضائية بالدولة بشأن جرائم محددة للسلطة القضائية الأجنبية، مع التأكيد على أهمية الولاية القضائية الدولية في القضايا الجنائية، وهذا يمثل طريقة استثنائية للمحكمة لدراسة الدعوى المرفوعة اليها والتحقيق فيها واتخاذ جميع الإجراءات ذات الصلة حتى صدور الحكم، ولكن قد تكون هناك عقبات تمنع المحكمة من إجراء التحقيقات اللازمة للأدلة فيما يتعلق بهذا النزاع.[120]

ويرى بعض فقهاء القانون الدولي أنه يُسمح للمحاكم بحرية رفض تطبيق القانون الأجنبي، وإضفاء الطابع الوطني على عواقب العبودية، ولا تطبق المحكمة الوطنية القانون الأجنبي إلا عند إرادتها استيعاب قانون دولة أخرى، لأن المجاملة الدولية رضائية وليست واجبة، وبمرور الزمن، فإن نمط سلوك الدول التي تطبق قوانين بعضها طواعية، من شأنه أن يشجع المعاملة بالمثل وزيادة الثقة، وربما يقلل من مخاطر نشوب نزاعات عدائية بين الدول[121]

تعد الإنابة القضائية الدولية هي أحد الموضوعات المهمة جدا في العالم الحديث، وهي شكل من أشكال التواصل من خلال الطلبات المقدمة من السلطات القضائية الأجنبية إلى السلطات القضائية للدول الأخرى بالوسائل الدبلوماسية، فالإنابة القضائية تسهل الإجراءات الجنائية بين الدول وبها يُتغلب على العقبات الإقليمية التي تمنع الدول الأجنبية من القيام ببعض الأعمال القضائية داخل أراضي الدول الأخرى، من أجل ضمان إجراء التحقيق اللازم لتقديم المتهم إلى العدالة.[122]

---

[120] شريهان ممدوح احمد، الإنابة القضائية الدولية في المسائل الجنائية في ضوء اتفاقية الرياض العربية للتعاون القضائي لسنة 1983م، مجلة الدراسات القانونية، المجلد 51، العدد 1، جمهورية مصر العربية، 2021، ص 203.

[121] عسكر، محمد، قواعد المجاملات الدولية في سياق التطبيق القضائي، مجلة البحوث القانونية والاقتصادية، العدد (81)، جامعة المنصورة، 2022، ص150.

[122] متعب بن عبدالله السند، التعاون الدولي في تنفيذ الاحكام الجنائية واثره في تحقيق العدالة، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2011، ص 108.

وبرأي الباحث فإنَّ المساعدة القضائية الدولية في الجرائم الإلكترونية تمثل أي إجراء قضائي تقوم به الدولة بهدف تسهيل محاكمة المجرمين في دولة أخرى، وتأخذ صوراً عديدة، أهمها تبادل المعلومات، وقيام الدولة باتخاذ إجراءات جنائية بصدد جريمة بطاقة دفع الكتروني ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط المساعدة القضائية الدولية، وكذلك تعتبر الإنابة القضائية الدولية من أهم صور المساعدة القضائية، بهدف تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراءات التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية بداخل أقاليم دولة أخرى.

وبالنظر إلى الواقع العملي نجد بأن أسلوب المساعدة القضائية الدولية ما زال يحتاج إلى مزيد من العمل والجهود فيما يخص الجرائم الالكترونية.

المطلب الثاني: التعاون الدولي لتسليم المجرمين في مواجهة الجريمة الالكترونية

يعد نظام تسليم المجرمين احد الانظمة التي ظهرت كاستجابة لضرورة ملحة تطلبتها مقتضيات العدالة الدولية، ومن الجهود الدولية التي اهتمت بنظام تسليم المجرمين اتفاقية الرياض العربية للتعاون القضائي والتي مثلت صورة من صور التعاون الدولي لمنع الجريمة وحماية المجتمع الدولي من آثارها، ولما كان مفهوم تسليم المجرمين يقتضي تسليم شخص لدولة أخرى لارتكابه احد الافعال الجرمية المنصوص عليها والمعاقب عليها ويجري تسليمه الى الدولة التي طلبت تسلمه من اجل محاكمته او لتنفيذ العقوبة المقررة بحقه، ويتسم نظام تسليم المجرمين بالطابع الاجرامي والطابع السيادي والطابع القضائي.

ان مبدأ قانون تسليم المجرمين يقوم على اساس ان الدولة التي يتواجد على اقليمها المتهم خاصة لارتكابه احدى الجرائم العابرة للحدود كالجريمة الالكترونية،[123] وجب على الدولة التي وقعت الجريمة على اراضيها تقديمه للعدالة، والا قامت بتسليمه للدولة التي ينتمي اليها المتهم، من هنا ظهرت حاجة الدول الماسة لتوقيع اتفاقيات التعاون وتبادل المجرمين تسهيلا على تلك الدول في تقديم المتهمين للعدالة، كما تعتبر هذه المهمة احدى مظاهر التعاون في مكافحة الجريمة، ولهذا نادى العديد من الدول لإبرام الاتفاقيات والمعاهدات الدولية بما يخص تسليم المجرمين، ومثال على ذلك المؤتمر الاول للشرطة القضائية في موناكو عام 1924م، والمؤتمر الدولي للعقاب في لندن عام 1945م، وقد تناولت اتفاقية الرياض العربية للتعاون القضائي لعام 1983م نظام تسليم المجرمين وتناولت احكامه من حيث شروط تسليم المجرمين التي تتعلق بالشخص المطلوب

[123] ندوة فلسطينية بخصوص التعاون الدولي في مواجهة الجرائم العبرة للحدود والجرائم والمنظمة، رام الله، النيابة العامة، 8 تموز/ يونيو 2023، تاريخ الزيارة: 20 تموز 2023.

تسليمه وشروط التسليم المتعلقة بالجريمة ذاتها، كما وتناولت موانع التسليم المتعلقة بنوع الجريمة والمتعلقة بالمواطنين،[124] وغير ذلك من الأحكام التي سيتم بيانها في هذا المطلب.

الفرع الاول: ماهية تسليم المجرمين

يعد تسليم المجرمين واحداً من اهم مجالات التعاون الدولي كونه يتعلق بسيادة الدولة ويعتبر محلا للجدل السياسي،[125] بحيث عرف فقهاء القانون الجنائي نظام تسليم المجرمين على أنه: إجراء بموجبه تقوم دولة ما بتسليم أحد المجرمين الموجود على أرضها الى دولة أخرى طالبت بتسليمه إليها، وذلك إما بتأجيل محاكمته على جريمة كان قد ارتكبها، أو لتوقيع العقوبة المقررة بحقه[126].

ومن التعريفات الواردة في نظام تسليم المجرمين، التعريف الذي ذهبت إليه المحكمة العليا الأمريكية والتي قالت فيه بأنه" إجراء قانوني مبني في أساسه على وجود معاهدة أو معاملة بالمثل أو قانون داخلي، تلزم بموجبه دولة ما بتسليم مجرم موجود على أرضها كان قد خالف القوانين الخاصة الوطنية، او ارتكب مخالفة للقانون الجنائي الدولي، حيث يتم ايقاع العقوبة بحق المجرم في الدولة التي طالبت بتسليمه"[127].

وقد عرفت المحكمة الجنائية الدولية نظام تسليم المجرمين في نظامها الأساسي وذلك في المادة (102) والتي تنص على أن "التسليم يعني نقل دولة ما شخصا إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني...".[128]

---

[124] فهد عبدالله العازمي، مرجع سابق، ص 562.

[125] احمد ابراهيم سليمان، الارهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع، بدون طبعة، القاهرة، 2006م، ص 332.

[126] جهاد محمد البريزات، الجريمة المنظمة: دراسة تحليلية، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2008م، ص 177؛ جميل عبد الباقي الصغير، مرجع سابق، ص 130.

[127] عبد الكافي، ورياشي، " نظام تسليم المجرمين"، منشورات مجلة الحقوق– سلسلة المعارف القانونية، الإصدار 16، بلا مكان نشر، 2013م، ص225–226.

128 المادة (102) من نظام روما الاساسي للمحكمة الجنائية الدولية.

ويعد نظام تسليم المجرمين من اجراءات التعاون الدولي، وقد أكد على ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية، والتي نصت على :" ضرورة تسليم المجرمين، وذلك في الجرائم المشمولة بهذه الاتفاقية، أو في الحالات التي تنطوي على ضلوع جماعة إجرامية منظمة في ارتكاب جريمة مع وجود الشخص وموضوع طلب التسليم في إقليم الدولة الطرف متلقية الطلب، شريطة أن يكون الجرم الذي يلتمس بشأنه التسليم معاقبًا عليه بمقتضى القانون الداخلي لكل من الدولة الطالبة والدولة متلقية الطلب"[129].

الفرع الثاني: شروط واجراءات تسليم المجرمين

يتبين من نص المادة (16) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية أن المعاهدات والاتفاقيات الدولية قد اكدت على ضرورة هذا الإجراء، في سبيل تحقيق التعاون الدولي ومنعًا لفرار المجرمين، واشترطت في هذا الإجراء أن يكون الجرم المرتكب من قبل الشخص مجرماً ومعاقباً عليه في قانون كلتا الدولتين طالبة التسليم ومتلقية الطلب.

ومن الشروط الواجب توافرها في الجرائم التي يجوز فيها التسليم ما يلي:[130]

1- أن تكون الجريمة من الجرائم الهامة.

2- أن تكون الجريمة من الجرائم المعاقب عليها في القانون الداخلي لكل من الدولتين.

3- ألا يكون الحكم قد اكتسب الدرجة القطعية سواء بالإدانة أو البراءة.

4- ألا تكون العقوبة قد سقطت بالتقادم أو بالدعوى العامة.

5- ان لا تدخل الجريمة ضمن ما لا يجيز العرف فيها التسليم.

---

[129] المادة (16) فقرة 1 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية والصادرة بتاريخ 2000/11/15م

[130] محاسن، الباشا، " تسليم المجرمين في القانون الدولي والفقه الإسلامي"، رسالة ماجستير، جامعة أم درمان الاسلامية، السودان، 1999م، ص42-46.

يتشابه نظام تسليم المجرمين مع غيره من الأنظمة، كنظام الطرد والإبعاد، ونظام التسليم المراقب، فنظام الطرد والإبعاد هو إجراء مقابل للهجرة تقوم فيه الدولة بتكليف شخص أجنبي بمغادرة إقليمها وإجباره على مغادرته، وحق الدولة في اتخاذ هذا الإجراء يعود الى مسؤوليتها في حفظ النفس الإنسانية وضمان بقائها، وقد يتخذ هذا النظام صورة من نظام تسليم المجرمين في حال قيام الدولة بطرد الشخص وسحبه الى النقطة التي تمكن الدولة التي تبحث عنه من القبض عليه في تلك النقطة وهنا يتم الوصول الى ذات النتيجة التي يؤدي اليها نظام تسليم المجرمين، كما ويتشابه نظام تسليم المجرمين مع نظام التسليم المراقب والذي يتم فيه فتح المجال لتهريب المخدرات والمؤثرات العقلية والسماح بمرورها الى دولة أخرى وذلك تحت إشراف السلطة المختصة بهدف الكشف عن المتورطين بهذه الجرائم، ويتشابه النظامان من حيث وجود مصطلح التسليم، ولاعتبار ان كلّاً منهما يعتبر اجراء من اجراءات التعاون الدولي، الا أن نظام التسليم المراقب يقتصر على تسليم المخدرات والمؤثرات العقلية أي ان نطاقه ضيق بخلاف نظام تسليم المجرمين الذي يعد اوسع وأشمل ويعمل على سد النقص الموجود في نظام التسليم المراقب.[131]

كما يتشابه هذا النظام مع نظام البدائل المستترة والتي تظهر في شكل ارهاب دولي تقوم فيه الدولة بخرق السيادة الدولية السياسية والقضائية في الدول التي يتواجد فيها مطلوبون، اذْ تعمل هذه الدول على خطفهم بواسطة قواتها الخاصة، ومن الأنظمة المشابهة أيضًا نظام رفض اللجوء والذي يقره القانون الدولي لحماية الأشخاص الذين يعانون من اضطهاد عرقي أو سياسي أو ديني فيطلب اللجوء الى دولة أخرى.[132]

---

[131] لحمر فافة، " إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، رسالة ماجستير، جامعة وهران، 2013-2014م، ص13-15.

[132] عبد الكافي، ورياشي، مرجع سابق، ص233.

يجد الباحث أن تسليم المجرمين أحد الإجراءات الدولية المهمة التي تحول من فرار المجرمين، والتي تشكل اجراء رادعًا لمن يعزم على مخالفة القانون الجنائي الدولي، والقوانين الوطنية، ولمن يحارب ويقف عائقًا أمام مسؤولية الدولة في حفظ البقاء والنفس الإنسانية.

الفرع الثالث: مظاهر التعاون الدولي في مجال تسليم المجرمين

يعد الاختصاص التشريعي الوطني للدولة هو المعيار الأساسي لتحديد الطبيعة القانونية لنظام تسليم المجرمين، فالمشرع هو الذي يقوم بدور تحديد ما اذا كان النظام ذا طبيعة قضائية، أو طبيعة ادارية، وغالبًا فان الاتفاقيات الدولية الثنائية او متعددة الأطراف لا تختص بتحديد الجهة المختصة في البت بطلب تسليم المجرمين، وانما يُرجع في ذلك الى الجهات ذات الاختصاص والمحددة بموجب القوانين الداخلية للدولة، ويعود الاختلاف في ذلك الى حقيقة اختلاف النظم التي تتبناها الدول، فمنها من يعهد بذلك الى الحكومة على اعتبار ان الاختصاص في نظره طلب التسليم والبت فيه عمل اداري، ودول أخرى تعهد في النظر في طلب التسليم والبت فيه الى الجهات القضائية المختصة في الدولة وذلك على اعتبار ان العمل عملًا قضائيًا، كما وقد تعهد بعض الدول في مهمة الفصل في الطلب الى الدولة والجهات القضائية المختصة على حد سواء، وذلك على اعتبار ان العمل ذو طبيعة قضائية وادارية معًا أي أنه ذو طبيعة مختلطة.[133]

ومن هنا يتبين للباحث أن المعاهدات الدولية الثنائية ومتعددة الأطراف والقوانين الدولية لا تحدد الجهة المختصة في البت في طلب تسليم المجرمين، وانما يرجع تحديد الاختصاص في ذلك الى القوانين الوطنية لكل دولة من الدول.

[133] زياد، جفال، " تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 16، العددى1، الامارات، 2019، ص 516.

وقد يحصل أن تتعدد الاختصاصات نظراً لتعدد الدول التي تطلب التسليم لنفس الجريمة، فما هي الدولة صاحبة الاختصاص في هذه الحالة؟

في هذه الحالة يتم إعطاء الاسبقية إلى الدولة التي حدث بها موقع الجريمة، وفقاً للاختصاص الإقليمي، وهذا ما جاء في قانون التسليم الفرنسي والذي منح الأرجحية للدولة التي استهدفت مصالحها ثم للدولة التي وقعت الجريمة على أرضها، وعلى كل حال يجب أن يكون الحل دائما في مقتضيات حسن سيرة العدالة علما أن المشروع الذي وضعته المنظمة الدولية للشرطة الجنائية يعطي الأسبقية للدولة التي وقعت الجريمة فوق أرضها.[134]

ويكيف التسليم على انه عمل من اعمال السيادة التي تمارسه الدولة والتي تخول صلاحيات النظر في طلب التسليم والبت فيه الى السلطة التنفيذية، دون التطرق الى القواعد القانونية او حتى منح الشخص المطلوب تسليمه أي حق للدفاع عن نفسه، مما سبب ذلك في ضياع الحقوق واهدارها، وحرمان الشخص من ضماناته الحقوقية، وتعد فرنسا من أول الدول التي تبنت هذا الاتجاه في العام 1927م، ويتميز هذا النظام بسهولة الاجراءات، وحيث ان مثل هذه الطبيعة القانونية لإجراء التسليم لم تعد تواكب وتخدم التعاون الدولي، لذلك لا يتم التعامل معها في الوقت الحاضر.[135]

وهذا يعني ان اجراء التسليم يعد عملًا قانونيًا يرجع في الفصل والبت فيه الى الجهات القضائية المختصة في الدولة والمحددة بموجب قوانينها الداخلية، غير انه لا يعول على ذلك بأن يكون القرار الصادر في طلب التسليم قراراً قضائياً محضاً، اذ ان البت في هذا الطلب من قبل

---

[134] نسرين الرحالي، "الإطار القانوني الدولي لمسطرة تسليم المجرمين"، مسارات في الأبحاث والدراسات القانونية، عدد 5، المغرب، 2018، ص 390.

[135] عبد الكافي، ورياشي، مرجع سابق، ص52.

الجهات القضائية لا يعتبر محاكمة بمفهومها القانوني، بالإضافة الى ان القرار الصادر قد يجري تحقيقه من قبل الجهات الحكومية في الدولة، وقد ترفض التسليم إذا وجدت مبررات تقتضي ذلك.[136]

وبالرغم من مزايا هذا النظام حيث يسمح للشخص المطلوب تسليمه من الدفاع عن نفسه لمواجهة القرار الدولي الصادر بحقه، الا انه قد شابهُ بعضُ الانتقادات، اذ ينطوي على بعض التعقيدات فهو يتطلب من الاطراف إدلاء كافة الحجج وادلة الاثبات، مما يؤثر في القرار الصادر في الطلب.[137]

أما عن موقف المشرع الفلسطيني من نظام تسليم المجرمين، فقد وضحته المادة (8) من قانون تسليم المجرمين رقم 56 لسنة 1926م، النافذ في الضفة الغربية، والذي ينص على:" في الحالات التي ينطبق فيها هذا القانون على طلبات التسليم المقدمة من أية دولة أجنبية، كل مجرم فار من بلاد تلك الدولة موجود في أي قسم من فلسطين أو يشتبه بوجوده في أي قسم منها يعرض نفسه للقبض عليه وتسليمه بالصورة المنصوص عليها في هذا القانون سواء ارتكب الجريمة المطلوب تسليمه من أجلها قبل العمل بهذا القانون أم بعده وسواء أكانت لأية محكمة في فلسطين صلاحية مشتركة للنظر في تلك الجريمة أم لم تكن".[138]

ومن نص هذه المادة يجد الباحث أن المشرع الفلسطيني قد أخذ بنظام تسليم المجرمين وفق نصوص مواد قانون تسليم المجرمين ساري النفاذ في فلسطين، وقد اكد على الأثر الرجعي الفوري لهذا القانون بقوله ان هذا القانون ينطبق على أي طلب تسليم بغض النظر عما اذا كان الشخص قد ارتكب الجريمة قبل نفاذ هذا القانون أو بعده.

---

[136] فريدة، شبري، " تحديد نظام تسليم المجرمين"، رسالة ماجستير، جامعة محمد بوقرة بومرداس ، 2007-2008م، ص14-15.

[137] عبد الكافي، ورياشي، مرجع سابق، ص53.

[138] قانون تسليم المجرمين رقم 56 الصادر بتاريخ 1/تشرين اول/1926، قوانين فلسطين (مجموعة درايتون- الانتداب البريطاني)، العدد 56، 22/تشرين الثاني/ 1926، ص20.

وعليه فإن تحديد الطبيعة القانونية لنظام تسليم المجرمين اختلف بين أكثر من اتجاه، بين من يرى بأنه اتجاه ذو طبيعة قانونية متمثل في كونه عملاً سيادياً، واتجاه اخر اعتبره عملاً من أعمال القضاء، واتجاه ثالث اعتبره ذا طبيعة مختلطة يضم كلاً من أعمال السيادة وأعمال القضاء في ذات الوقت.[139]

وفي رأي الباحث فإن تحديد الطبيعة القانونية لتسليم المجرمين يتحقق بواسطة معرفة الجهة المختصة بمباشرة إجراءات طلب التسليم والبت فيه، ولا يخرج عن أن يكون نظاماً من أعمال السيادة أو نظاماً قضائياً أو نظاماً مزدوجاً يجمع بين كليهما.

وقد اكدت الاتفاقيات الدولية والتشريعات الوطنية على ضرورة احترام مبدأ الخصوصية، وكذلك فان اتفاقية الرياض العربية للتعاون القضائي اكدت على ذلك صراحة من خلال ما نصت عليه في الفقرة الثانية من المادة 52 منها، والتي تضمنت عدم جواز توجيه اتهام للشخص الذي تم تسليمه او محاكمته على فعل ارتكبه قبل تاريخ التسليم، غير الفعل الجرمي الذي سُلّم لأجله.[140]

كما أنها تهدف إلى حماية الأشخاص المطلوب تسليمهم من لمحاكمتهم عن جرائم غير التي سُلّموا لأجلها، بحيث تكون المحاكمة العادلة فيها غير متوفرة، والمثال التطبيقي واضح على هذه القاعدة، مثل منع الدولة طالبة التسليم من عدم الالتزام بشروط التسليم بهدف القصاص من الشخص المطلوب حالة ارتكابه جريمة سياسية على سبيل المثال، وذلك على اعتبار الجرائم السياسية لا يجوز تطبيق نظام تسليم المجرمين فيها، وقد يحدث ذلك أن تطلب الدولة تسليم شخص معين عن جريمة عادية وفي الحقيقة ترغب بمحاكمته عن جريمة سياسية لا تذكرها في الطلب،

---

[139] لطفي أمين بلفراد، "التعاون الدولي في مجال تسليم المجرمين"، مجلة الشرطة المصرية، العدد الأول، مصر، أكتوبر/ تشرين أول 2009، ص15.

[140] زياد، جفال، " تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 16، العدد1، الامارات، 2019، ص518.

وعليه ظهرت هذه القاعدة كضمان حقيقي للشخص المطلوب تسليمه،[141] ومما تقدم يتبين ان قاعدة التخصيص تنطوي على جانب من الأهمية اذ انها تحمي الشخص المراد تسليمه من توجيه أي اتهام له غير ما وجه اليه بفعل الجريمة التي ارتكبها والتي تم تقديم طلب التسليم من أجلها.

كذلك من الشروط الخاصة بالأشخاص الواجب تسليمهم هو عدم تمتعهم بالحصانة، بحيث أنه من الجدير ذكره بأن هناك فئة من الأشخاص تتمتع بالحصانة داخل الدولة لا يجوز تسليمهم، من بينهم رؤساء الدول والمبعوثين الدبلوماسيين، فإذا ارتكب أحد يحمل الحصانة جريمة داخل إقليم دولة معينة ثم لجأ لدولة أخرى، فلا يجوز في هذه الحالة تسليمه إلى الدولة التي ارتكب الجريمة فيها، وذلك نظراً لتمتعه بالإعفاء من قضائها الإقليمي بما يمنع من محاكمته فيها، ولا يجوز تسليمه إلا في حالة واحدة، وهي زوال صفة الحصانة عنه، مثل الرئيس الذي تنتهي ولايته أو المبعوث الدبلوماسي الذي تنتهي مدة عمله، أو الذي عُزل من شغله، وهذا ما جرى عليه العرف الدولي بموجب مجموعة من المعاهدات بين الدول.[142]

لقد وضعت الدول بما لها من حق السيادة على إقليمها شروطًا وقواعد معينة من الواجب مراعاتها حين ممارستها للتسليم، وذلك من خلال الاتفاقيات سواء كانت ثنائية أو جماعية أو بناء على مبدأ المعاملة بالمثل.[143]

وفي مثل هذه الحالة، فإن مبدأ المعاملة بالمثل يتمثل في أن تتعهد الدولة طالبة التسليم بمساعدة الدولة المطلوب منها التسليم، وتفحص طلبات التسليم التي تتقدم بها الأخيرة في المستقبل وفقا لقانونها الداخلي؛ بمعنى أن الدولة طالبة التسليم تطلب من الدولة المطلوب منها التسليم أن

---

[141] محمد الفاضل، محاضرة في تسليم المجرمين، منشورات معهد الدراسات العربية التابع لجامعة الدول العربية، المطبعة القنية الحديثة، القاهرة، 1967، ص193.

[142] الهام محمد العاقل، مبدأ عدم تسليم المجرمين في الجرائم السياسية: دراسة مقارنة، مركز دراسات العالم الإسلامي، سلسلة الدراسات القانونية، الطبعة الأولى، الأردن، 1993، ص179.

[143] الهام محمد العاقل، مرجع سابق، ص168.

تطبق قانونها الداخلي بشأن تسليم المجرمين على حالة فعلية نص عليها في الطلب، وعلى نحو مماثل فإن الدولة المطالبة تلزم نفسها بأن تفعل نفس الشيء كلما طلبت منها ذلك الدولة المطلوب منها التسليم، ويتم ذلك دون أن يكون هناك أي شروط استثنائية معينة، كاستثناء مواطني الدولة المطلوب منها التسليم، أو وضع قائمة بالجرائم التي يمكن التسليم بالنسبة لمرتكبيها، فإن وجدت أي شروط استثنائية فإن العرض لم يعد في نطاق نظام المعاملة بالمثل وأصبح يحتوي حينئذ على عناصر المعاهدة لأن التشريع الداخلي للدولة المطلوب منها التسليم لم يعد كافياً، إذ أن هذه المعاملة بالمثل المقيدة بالشرط أصبحت مماثلة تماما لمعاهدة ثنائية على الرغم من أنها أكثر اقتصادا في نصوصها [144]

وتلجأ الدول لمبدأ المعاملة بالمثل لتسليم الأشخاص المطلوبين في الحالات الآتية:

في حالة عدم وجود معاهدة: تختلف الدول في الأخذ بقاعدة تسليم المجرمين في حالة عدم وجود معاهدة، فالدول الأوربية وبعض الدول الأخرى لا تمانع في التسليم على أساس المعاملة بالمثل، باعتبار أن شرط المعاملة بالمثل هو مسألة سياسية يرجع الأمر فيها لمطلق تقدير الحكومة، وليس من متطلبات العدالة ، وهو ما أقره مجمع القانون الدولي في اجتماعه بأكسفورد عام 1880م، وما دام التسليم منشأه السلطة التقديرية ، فإنه يمكن أن يتم التسليم بين عدد من الدول دون أن تكون بينها معاهدة لتسليم المجرمين، أو عرض رسمي للمعاملة بالمثل.[145]

ومن ناحية أخرى فإن بعض الدول مثل الولايات المتحدة الأمريكية؛ تخالف ما تسير عليه الدول الأوربية وبعض الدول الأخرى، إذ لا تطبق مبدأ المعاملة بالمثل في حالة عدم وجود معاهدة، غير أن هذا لا ينفي إمكانية اعتمادها على مبدأ المعاملة بالمثل إذا لم تكن هناك معاهدة واقتضت

[144] عبد الغني، محمود، تسليم المجرمين على أساس المعاملة بالمثل، دار النهضة العربية، القاهرة، 1991، ص11

[145] المرجع نفسه، ص6

المصلحة المشتركة بين الدولتين تسليم الشخص المطلوب وكانت إنجلترا في بادئ الأمر تأخذ بقاعدة التسليم بدون وجود معاهدة، ثم عدلت عن ذلك وأصبح التسليم بدون معاهدة غير جائز لمخالقته أحكام الدستور.[146]

ومن الأمثلة على إجابة طلب التسليم في غياب معاهدة تسليم المجرمين سابقة المواطن الهندي نيرانجان شاه المقيم بدولة الإمارات العربية المتحدة، الذي اتهمته سلطات بلاده القضائية بارتكاب جرائم خيانة الأمانة، والخداع، والرشوة والتزوير، وتدليس الحسابات، وطلبت الحكومة الهندية من حكومة دولة الإمارات تسليمها مواطنها لمحاكمته عما نسب إليه من جرائم فإجابتها حكومة الإمارات لطلبها وسلمتها مواطنها رغم عدم وجود اتفاق لتبادل المجرمين بين الحكومتين.[147]

اللجوء إلى المعاملة بالمثل بشأن موضوع معين: في معاهدات تسليم المجرمين الموقعة بين بعض الدول تنص المعاهدة على الجرائم التي يمكن التسليم لأجلها، ولهذا تستند الكثير من الدول الموقعة لهذه المعاهدات إلى مبدأ المعاملة بالمثل لجعل التسليم ممكنا بالنسبة لجريمة لم تشتمل عليها قائمة الجرائم المنصوص عليها في معاهدة التسليم الموقعة بين هذه الدول.[148]

إن تسليم المواطنين يعتبر مبدأ المعاملة بالمثل حلا لمشكلة معقدة من مشاكل تسليم المجرمين، وهي الخاصة بتسليم المواطنين إلى الدول الأجنبية، اما بالنسبة الى الانتربول في فلسطين فهنالك العديد من الجهود التي يقوم بها الانتربول من اجل تسليم المجرمين الذين يقومون بالجرائم الالكترونية، ففلسطين عضو في الانتربول (الشرطة الدولية) وقد قام الانتربول باستلام

146 عبد الفتاح، محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة 2003، ص160
147 الوهاب، عبدول، تسليم المجرمين في دولة الامارات، ورقة عمل منشورة في التعاون القضائي الدولي، دار العلم، ص77.
148 المرجع نفسه، ص76.

العديد من المجرمين المطلوبين لدى السلطة الفلسطينية في الجرائم الالكترونية الهاربين الى الدول الأجنبية وخصوصاً في الأردن وغيرها من الدول.

وهو يتفق مع ما نصت عليه المادة (28) من القانون الأساسي الفلسطيني: " لا يجوز إبعاد أي فلسطيني عن أرض الوطن أو حرمانه من العودة إليه أو منعه من المغادرة أو تجريده من الجنسية أو تسليمه لأية جهة أجنبية"

فهذه المادة تعطي الحصانة للمواطن الفلسطيني للحفاظ على حرياته وضمان سلامته من خلال منع تسليمه لدول أو جهات أجنبية، وبالتالي فإن هذه المادة تمنح الحق في حال ارتكاب المجرم لجرائم في دول أجنبية، محاكمته داخل الدولة الفلسطينية، ومن جانب آخر فإن هذه المادة تتناول إبعاد المواطن الفلسطيني كشكل من أشكال العقاب، وهي لا تتعارض مع تسليم المجرمين الأجنبيين التي تنص عليها المعاهدات الدولية.

وبالنظر في اتفاقية الرياض العربية للتعاون القضائي لعام 1983م، والتي اشارت الى الشروط الخاصة بالشخص المطلوب تسليمه في المادة (40) منها والتي نصت على:" يجب التسليم بحق:

أ- من يوجه إليه الاتهام عن أفعال معاقب عليها بمقتضى قوانين كل من الطرفين المتعاقدين طالب التسليم والمطلوب إليه التسليم- بعقوبة سالبة للحرية مدتا سنة أو بعقوبة أشد في قانون أي من الطرفين- أيا كان الحدان الأقصى والأدنى في تدرج العقوبة المنصوص عليها .

ب- من وجه إليه الاتهام عن أفعال غير معاقب عليها في قوانين الطرف المتعاقد المطلوب إليه التسليم أو كانت العقوبة المقررة للأفعال لدى الطرف المتعاقد طالب التسليم لا نظير لها لدى

الطرف المتعاقد المطلوب إليه التسليم. إذا كان الأشخاص المطلوبون من مواطني الطرف المتعاقد طالب التسليم أو من مواطني طرف متعاقد آخر يقرر نفس العقوبة .

ج- من حكم عليهم حضوريا أو غيابيا من محاكم الطرف المتعاقد الطالب بعقوبة سالبة للحرية لمدة سنة أو بعقوبة اشد عن أفعال معاقب عليها بمقتضى قانون الطرف المتعاقد المطلوب إليه التسليم.

د- من حكم عليه حضوريا أو غيابيا من محاكم الطرف المتعاقد الطالب عن فعل غير معاقب عليه في قوانين الطرف المتعاقد المطلوب إليه التسليم أو بعقوبة لا نظير لها في قوانينه، إذا كان من مواطني الطرف المتعاقد طالب التسليم أو من مواطني طرف متعاقد آخر يقرر نفس العقوبة".

الفرع الرابع: التعاون الدولي في مجال التدريب على مواجهة الجريمة الالكترونية

يفرض التقدم المتواصل في تكنولوجيا الحاسب الآلي والإنترنت على جهات إنفاذ القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية، لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها، حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلي وشبكة الإنترنت قد ارتكبت على مرأًى ومسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل، أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون. مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل

جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة لذلك أتلف ما كان قد سلم من الملفات والبرامج.[149]

وإتلاف الأدلة قد يقع كذلك عن خطأ مشترك بين الخبراء وبين الجهة المجني عليها، فمثلا في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول طلب أحد الأشخاص من إحدى الشركات زعم أنه وضع قنبلة منطقية بنظام حاسبها الآلي، تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة ذلك وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة على وجودها.[150]

وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئاً ثقيلاً على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها وهذا ما أثبته الواقع العملي، سيما وأن متطلبات العدالة وكما أسلفنا تقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم، لأجل ذلك كان لا بد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيتين، وهذا لن يتحقق إلا بالتدريب، فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها لا بد وأن ترتكز على كيفية تطوير العملية التدريبية، والارتقاء بها والنهوض بأساليب تحقيقها لأهدافها، من هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين

---

[149] محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، دبي، الإمارات العربية المتحدة، 2003، ص24.

[150] رستم، هشام محمد فريد، الجرائم المعلوماتية "أصول التحقيق الجنائي الفني". بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3م المجلد الثاني، الطبعة الثالثة، الإمارات العربية المتحدة، 2000، ص439-440.

على هذه الأجهزة، وحيث أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول وكانت الدعوة إلى ضرورة وجود تعاون دولي في مجال التدريب.[151]

واستنادا الى ما سبق، يرى الباحث بان الجريمة الالكترونية من الجرائم الحديثة كونها تتطور بشكل سريع ومستمر، بحيث يجب على اجهزة الدولة المتخصصة بمكافحة هذه الجرائم الاستعانة بالأفراد المتخصصين واصحاب الخبرات العلمية والفنية الكافية في مجال الحاسب الالي وتكنولوجيا المعلومات وشبكات الانترنت، مما يستدعي ذلك العملَ على تشجيع دور التدريب لمكافحة الجرائم الالكترونية من خلال قيام الكليات العسكرية الشرطية والامنية لقبول الاشخاص ذوي الخبرة التقنية والعلمية والفنية وخريجي كليات تكنولوجيا المعلومات لتخرجهم ضباطاً اصحاب قدرة وخبرة ومؤهلين بالثقافة التقنية المعلوماتية وايضا بالثقافة القانونية.[152]

[151]صالح محمد النويجم، تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها. رسالة ماجستير في العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2005، ص7.

152 عادل عبد العال خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الطبعة الاولى، الاسكندرية، 2015م، ص 23.

المبحث الثاني: الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الالكترونية وكيفية التغلب عليها

من خلال التطبيق العملي للتشريعات الوطنية المرتبطة بالجرائم الالكترونية يلاحظ وجود الكثير من الثغرات في القوانين الموجودة في فلسطين التي تحتاج الى التعديل بشكل كبير من اجل مبادئ العدالة والانصاف، وكذلك هناك وسائل كثيرة تظهر لم ينظمها القانون وعليه يجب ان ينظمها، فالجرائم الالكترونية يجب ان يكون التعامل معها ادق وبشكل حساس من الجرائم التقليدية لخطورتها على المجتمع، وبالتالي فالتنظيم القانوني لمسألة الجرائم الالكترونية في فلسطين ضعيف للغاية، وفي هذا المبحث سوف يقوم الباحث بتقسيم هذا المبحث الى مطلبين على النحو الاتي: حيث ان المطلب الأول يتحدث عن الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الإلكترونية، اما بالنسبة الى المطلب الثاني فهو يتحدث عن الحلول للتغلب على الصعوبات التي تواجه التعاون الدولي.

المطلب الأول: الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الإلكترونية

إن التطور الهائل في شبكة المعلومات أنتج مجموعة معقدة ومتنوعة من الاستخدامات في مختلف المجالات الثقافية والاقتصادية والسياحية والأمنية، وأصبحت أداة لتنفيذ الجرائم الإلكترونية عن طريق شبكة الانترنت، مما يؤدي إلى تهديد الأمن والاعتداء على سرية المعلومات بقصد التجسس أو السرقة أو القرصنة أو التخريب، وزيادة الصعوبات والتحديات في مواجهة هذه الجرائم على المستوى الدولي والوطني، لذلك تم تقسيم هذا المطلب إلى فرعين، يتناول الفرع الأول

الصعوبات الدولية في مواجهة الجرائم الإلكترونية، والفرع الثاني يتحدث عن الصعوبات الوطنية في مواجهة الجرائم الإلكترونية.

الفرع الأول: الصعوبات الدولية التي تواجه التعاون الدولي.

إن التعاون الدولي يقوم بدور فعال في سبيل مكافحة الجرائم الإلكترونية إلا أنه يحيط بهذا الدور تحديات متعددة على الصعيد الدولي تتمثل هذه التحديات في:

أولاً: القصور التشريعي للدول والتعارض بين مصالحها

يعد التحدي الأكبر الذي يواجه مكافحة الجرائم المعلوماتية ويؤدي إلى إشكالات في تطبيق القانون من الناحية العملية، إن عدم توفر نظام قانوني محدد وخاص في مكافحة الجرائم الإلكترونية يؤدي إلى جعل ما هو مباح في نظام معين مُجرَّماً في نظام آخر؛ لعل من أسباب ذلك اختلاف العادات والبيئات والثقافات والديانات من مجتمع لآخر، وتعد المفاهيم القانونية التي تتعلق بالجرائم الإلكترونية، وجميع هذه الأسباب بأنها انعكست سلباً على التعاون الدولي، فالقصور التشريعي يؤدي إلى إفلات المجرمين من العقاب.[153]

ثانياً: تنازع الاختصاص القضائي الدولي

وهو "مجموعة من القواعد التي تبين حدود ولاية المحاكم فيما يخص العلاقات القانونية ذات العنصر الأجنبي إزاء محاكم الدول الأجنبية التي تنازع هذا الاختصاص".[154] تكمن الإشكالية في اختلاف النظم القانونية والتشريعات من دولة إلى أخرى؛ مما يؤدي إلى تنازع الاختصاص بين الدول فيما يتعلق بالجرائم الالكترونية التي تتميز بأنها عابرة للحدود، استناداً لمبدأ الإقليمية فإن الاختصاص

---

[153] بوربابة صورية، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد الأول، جويلية 2019، ص98 ص99.

[154] عكاشة محمد عبد العال، القانون الدولي الخاص، دار الجامعة الجديدة، الإسكندرية، 1999، ص 402.

يكون للدولة الأولى، واستناداً لمبدأ الاختصاص الشخصي ينعقد الاختصاص للدولة الثانية، وإذا كانت الجريمة تهدد سلامة وأمن دولة أخرى فإن الاختصاص يكون لهذه الدولة وفقاً لمبدأ العينية.[155]

ثالثاً: تنوع واختلاف النظم القانونية الإجرائية

تتنوع وتختلف النظم القانونية الإجرائية من دولة إلى أخرى، وتتمثل هذه الإجراءات في التحقيق والتحري والمحاكمة التي قد تكون فعالة في دولة ما وقد تكون عديمة الفائدة في دولة أخرى، وقد تعتبر طريقة معينة من طرق التحقيق أو جمع الاستدلالات القانونية في دولة ما وغير مشروعة في دولة أخرى، مما يؤدي إلى شعور الدولة الأولى بخيبة أمل كبيرة لعدم قيام الدولة الثانية باستخدام ما تراه أداة فعالة، كما أن السلطة القضائية في الدولة الثانية لا تعتد بأي دليل تم الحصول عليه بصورة غير مشروعة بنظر هذه الدولة إلا أنها مشروعة بنظر الدولة الأخرى، يتبين من ذلك غياب التنسيق الاجرائي بين الدول فيما يتعلق بالجرائم الإلكترونية لعدم وجود قنوات اتصال بين مختلف الدول.[156]

رابعاً: التحديات الخاصة بالتدريب في مجال مكافحة الجرائم الإلكترونية

وهي المتمثلة في الرغبة لدى البعض من القيادات الإدارية في بعض الدول فيما يتعلق بالتدريب لاعتقادهم بما له من دور سلبي يتمثل في تطوير العمل عن طريق التطبيق العملي لما يتعلمه المتدربون في الدورات التدريبية والخبرات المكتسبة، والفوارق الفردية ما بين المتدربين و تأثيرها بقوة تامة ومتكافئة على المهارات المستهدفة لمختلف المتدربين تحديداً في مجال شبكات

[155] غانم مرضي الشمري، الجرائم المعلوماتية، ط1، دار الثقافة، عمان، 2016، ص58.

[156] غانم مرضي الشمري، مرجع سابق، ص126.

الاتصال وتكنولوجيا المعلومات، حيث يوجد أشخاص على ثقافة ومعرفة بدرجة كبيرة في هذا المجال وأناس لا يعلمون شيئاً في هذا المجال.[157]

خامساً: التحديات الخاصة بالإنابة القضائية

وهي التي تظهر في جانبين: **الجانب الأول** التحديات المرتبطة بفكرة السيادة ويقصد بها "السلطة العليا للدولة على رعاياها وإقليمها، وغير المقيدة بأية تبعية أو تأثير يأتي من خارج الدولة، وتستأثر بمباشرة جميع الاختصاصات داخل حدود الإقليم في مواجهة الرعايا، وتتصرف في الخارج على قدم المساواة مع غيرها من السيادات المماثلة".[158]

عندما يقوم شخص بارتكاب جريمة تصنف من ضمن الجرائم الإلكترونية في دولة ما ويتم محاكمته في دولة أخرى يتم البحث عن كافة الأدلة التي تثبت أو تنفي وجود هذه الجريمة وفق قانون الدولة التي كانت مسرحاً للجريمة وهذا ما يعرف "بالتعاون القضائي" ما بين الدول؛ على الرغم من أهمية التعاون القضائي إلا أنه يمكن أن يصطدم مع سيادة الدولة على إقليمها، على اعتبار أن الدولة من خلال جهازها القضائي بالفصل في كافة المنازعات على أراضيها كونها تتعلق بفكرة السيادة وهذا يعيق التعاون القضائي ما بين الدول في مكافحة الجرائم.[159]

والجانب الثاني: المتمثل في التحديات المرتبطة بإجراءات الإنابة، وهي من أهم المساعدات القضائية في الأمور الجنائية، الأصل في طلبات الإنابة القضائية الدولية أن تسلم بالطرق

---

[157] صالح منير محمد، الجرائم المعلوماتية (وطرق مواجهتها)، بحث منشور بمركز بحوث الشرطة، بالقاهرة، العدد الثالث، يوليو 2005، ص 179.

[158] نسيب أزرقي، مستقبل السيادة والنظام العالمي الجديد، المجلة الجزائرية للحقوق والعلوم الإدارية والقانونية، ج 36، 1998، ص 86.

[159] نسيب أزرقي، مرجع سابق، ص 88.

الدبلوماسية، وبهذا تكون متسمة بالتعقيد والبطء الأمر الذي يتعارض مع طبيعة الإنترنت الذي يمتاز بالسرعة وانعكس ذلك على الجرائم التي تتعلق بالإنترنت.[160]

ومن ضمن الصعوبات أيضاَ التباطؤ في الرد، غالباً ما تكون الدولة التي تتلقى الطلب بطيئة في الرد نتيجة للصعوبات اللغوية أو نقص الموظفين المدربين أو الفرق في الإجراءات مما يؤدي إلى تعقد وإعاقة الاستجابة.[161]

سادساً: التحديات الخاصة بتسليم المجرمين

وتظهر من خلال جانبين: **الجانب الأول** وهو التجريم المزدوج الذي يعتبر من أهم الشروط المتعلقة بنظام تسليم المجرمين ومنصوص عليه في أغلب الصكوك الدولية المعنية بتسليم المجرمين والتشريعات الوطنية التي يقوم أساسها الفلسفي على أن التسليم يعتبر مساساً بالحرية الشخصية ويستند إلى قضاء أجنبي، يحتاج هذا الإجراء إلى ضرورة وجود ما يبرره في القوانين الوطنية أي أن يكون الفعل مُجرّماً في القانون الوطني.[162]

على الرغم من الأهمية البالغة لهذا الشرط إلا أنه في الغالب يكون عقبة أمام التعاون الدولي في تسليم المجرمين فيما يتعلق بالجرائم الالكترونية، لكون معظم الدول لا تجرم هذه الأفعال، كما أن الدولة المطلوب منها التسليم يصعب عليها تحديد هل النصوص التقليدية يمكن لها أن تنطبق على الجرائم التي تتعلق بالشبكة العنكبوتية أم لا.[163]

---

[160] عادل إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، ط1، دار الجامعة الجديدة، الإسكندرية، 2015، ص63.

[161] عادل إبراهيم خراشي، المرجع السابق، ص64.

[162] عادل إبراهيم خراشي، مرجع سابق، ص66.

[163] عكاشة عبد العال، القانون الدولي الخاص، دار الجامعة الجديدة، الإسكندرية، 1999، ص 402.

الجانب الثاني يتمثل في التزاحم في طلبات التسليم ويقصد به "تلك الحالة التي يصل فيها إلى الدول المطلوب منها التسليم أكثرُ من طلب تسليم من عدة دول تطلب ذات الشخص، سواء كان الطلب متعلقاً بنفس الجريمة أو بجرائم أخرى".[164]

من الممكن أن يكون الشخص المطلوب تسليمه قد ارتكب جريمة أو أكثر من الجرائم الإلكترونية تمس مصالح أكثر من دولة في آنٍ واحد، ففي مثل هذه الحالة تتزاحم طلبات التسليم من الدول التي مسها الضرر إلى الدولة المطلوب إليها. حتى يكون هناك تزاحم في طلبات التسليم يجب أن تقوم كل من الدول الطالبة بتقديم الأدلة التي تثبت قيام الشخص المطلوب بارتكابه الجريمة الالكترونية وليس مجرد شك أو ادعاء، ولا يكفي أن تبدي تصريحاً شفوياً أو رغبة في استلام الشخص بل يجب أن يتم تقديم الطلب بشكل فعلي، ولا يشترط وصول الطلبات جميعها في أوقات متقاربة إلى الدولة المطلوب إليها، بل يكفي أن يكون هناك عدة طلبات توالت إلى الدولة المطلوب إليها، طالما أن الشخص المطلوب تسليمه متواجد على إقليمها ولم يغادر ولم يتم تسليمه إلى أي دولة من الدول التي تطالب بتسليمه.[165]

الفرع الثاني: الصعوبات الوطنية

تواجه الجريمة الالكترونية العديد من التحديات التي تهدد وجودها ولا تقتصر هذه التحديات على المستوى الدولي فقط، بل تمتد لتشمل التحديات الوطنية، والتي تتمثل في عدد من الصور ابرزها:

---

[164] أحمد السيد عبدالله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراه، كلية حقوق المنصورة، 2009، ص 394.

[165] أحمد السيد عبدالله، مرجع سابق، ص63.

أولاً: عدم كفاية وملاءمة القوانين القائمة

نظراً للتطور التكنولوجي في مختلف جوانب الحياة الذي استغلتْهُ التقنيات التكنولوجية لارتكاب الجرائم المعلوماتية؛ لكن لم يتم إيجاد نصوص قانونية تتناسب مع هذا التطور، فمعظم القوانين الجنائية في بعض الدول لا تواجه الصور المستحدثة من الجرائم الالكترونية، بعض النصوص القانونية تتطلب الصفة المادية في محل الجريمة الأمر الذي يتنافى مع الطبيعة الخاصة بالجرائم الالكترونية وبالتالي فإن هذه الصور تخرج من إطار التجريم والعقاب.[166]

ثانياً: إحجام الكثير من الجهات عن الإبلاغ عن تلك الجرائم

معظم الجهات والمؤسسات الادخارية والبنوك تحرص على عدم الكشف عما تعرضت له من عجزها عن تحقيق الأمان للمعلومات وأصول الأموال التي تتعامل معها بصورة كافية، فتقوم هذه الجهة بالاكتفاء باتخاذ الإجراءات الإدارية الداخلية دون أن يتم إبلاغ السلطات المختصة عما تعرضت له، محاولة في ذلك تجنب الإضرار لمكانتها وسمعتها وزعزعة الثقة في كفاءتها، وبالتالي يجب العمل على تحديث الأساليب الإجرائية لمواجهة الجرائم المعلوماتية واستكمالها على نحو يضمن استجابتها بالشكل الكافي.[167]

ثالثاً: صعوبة إثبات الجرائم المعلوماتية والتحقيق

فالتحقيق فيها يعود إلى عدة أسباب تتمثل في طبيعة الدليل الخاصة في الجرائم الالكترونية، فهو ليس دليلاً مرئياً يتم فهمه بمجرد قراءته، وإنما يتمثل وفق ما تعتبره النظم من الادلة على الجرائم التي تتم بواسطتها أو تقع عليها، فهي بيانات غير مرئية لا تقوم بالإفصاح عن شخصية

---

[166] غانم مرضي الشمري، مرجع سابق، ص128.

[167] صالح منير محمد، الجرائم المعلوماتية (وطرق مواجهتها)، بحث منشور بمركز بحوث الشرطة، القاهرة، العدد 3، يوليو 2005، ص 179.

محددة ويزداد الأمر صعوبة في الجرائم الإلكترونية التي تقوم باستخدام البريد الإلكتروني لأنه يصعب على جهات الاختصاص تحديد مصدر الإرسال.[168]

وتتميز الجريمة الالكترونية أيضا بسهولة إزالة الدليل، حيث يستطيع الجاني أن يتوجه إلى متجر خاص بالإعلام الآلي وقيامه بالدخول إلى أحد المواقع وإرسال رسالة على إيميل أحد من الناس تحتوي على قذف وسب، ثم يشرع بإزالة الدليل ومغادرة المتجر وكأن شيئاً لم يكن، كما أن مرتكبي الجرائم الالكترونية يعتمدون على التخفي والخداع عن طريق تغيير قناع الشبكة العنكبوتية؛ نتيجة لما يمتلكونه من خبرة عالية في الأمن البرمجي والمعلوماتي.[169]

من ضمن الصعوبات أيضاً صعوبة الحصول على الدليل كنتيجة لقيام المواقع العالمية على الشبكة العنكبوتية بتوفير حماية أمنية على البيانات المخزنة على خوادمها كوسيلة لمنع التسلل غير المشروع للوصول إليها لتبديلها أو تدميرها أو نسخها أو الاطلاع عليها، ومن جهة أخرى إن الجاني إذا كان لديه خبرة بمجال الأمن المعلوماتي فبذلك تزداد صعوبة عملية الحصول على أي دليل.[170]

ومن ذلك أيضاً اختراق خطوط الطول ودوائر العرض عبر العالم، مع إمكانية تنفيذ ارتكاب الجريمة عن بعد واختلاف النظم القانونية بين الدول؛ فالقانون واجب التطبيق يلعب دوراً كبيراً في التنسيق الدولي والتحري لتعقب مثل هذه الجرائم.[171]

---

[168] مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الانترنت، دراسة مقارنة، دار الكتب، القاهرة، 2003، ص3.

[169] رستم فريد هاشم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، اسيوط،1994 ، ص 25.

[170] سامي علي عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص 103.

[171] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2007، ص 60.

رابعا: تناقض القوانين المطبقة في فلسطين

من الصعوبات التي تواجه الجرائم الإلكترونية هو تناقض القوانين مع بعضها البعض في فلسطين ونذكر مثالاً على توضيح الفكرة المطروحة جيداً.

جريمة تسجيل المكالمات الصوتية ويمكن تعريفها بأنها هي اعتداء على حرمة الحياة الخاصة للمواطن، وذلك بأن يقوم الجاني باستراق السمع أو أن يقوم بالتسجيل أو ينقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثاتٍ جرت في مكان خاص أو عن طريق جهاز الهاتف. ولكن هناك استثناءات لهذه الجريمة عندما يتعلق الأمر بالمصلحة العامة. وفي هذا المطلب سأقوم بالمقارنة بين قانون الإجراءات والقرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية فيما يتعلق بالمواد المتعلقة بتسجيل المكالمات:

مواد القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية: تحدثت فيه المواد 8 و 22 و34 و36 من هذا القرار والتي تتعلق بتسجيل المكالمات:

حيث تشير المادة (1/8) منذ ذات القرار بقانون الى فك بيانات مشفرة في غير الأحوال المصرح بها قانونا أي أنه كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مئتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.[172] وبالنسبة إلى المادة (22) تتحدث عن التدخل التعسفي أو غير القانوني في خصوصيات الأشخاص وبمنتهى الصراحة والوضوح يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته[173]

[172] قرار بقانون بشأن الجرائم الإلكترونية رقم 10 الصادر بتاريخ، 2018/4/29، الوقائع الفلسطينية، العدد 0، 2018/5/3، ص 8.

[173] قرار بقانون بشأن الجرائم الإلكترونية رقم 10، مرجع سابق.

اما بالنسبة الى المادة (34) تتحدث عن مراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها أي "انه يمكن لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توفر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة، 2. وللنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بمزودي الخدمات، حسب نوع الخدمة التي يقدمها."[174]

وهنا المادة 2/34 قالت انه الاستعانة بمزودي الخدمات عند الضرورة والمادة التي تحدثت عن ذلك هي المادة 33 من القرار بقانون، "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي: 1. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة. وهنا يجب أن تقوم الجهة المشرعة في فلسطين بتعديل المادة بما يتفق على أن تكون المحكمة هي المختصة فقط دون غيرها".[175]

اما بالنسبة الى المادة (36) "تتحدث عن الاذن للمحكمة المختصة بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة

[174] قرار بقانون بشأن الجرائم الإلكترونية رقم 10.

[175] ورقة موقف صادرة عن مؤسسة حق بشأن قرار بقانون الجرائم الالكترونية وحجب المواقع الإلكترونية، مؤسسة حق، رام الله، 2019/10/23، ص3.

أشهر من بداية تاريخ الشروع الفعلي في إنجازه، وقابلة للتمديد مرة واحدة فقط. ويتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها".[176]

أما قانون الإجراءات الجزائية فقد تطرق الى ذلك في المادة 51: "للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة و شخص مرتكبها. كما يجوز له بمراقبة المحادثات السلكية واللاسلكية، أو إجراء تسجيلات لأحاديث في مكان خاص بناء على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة. ويجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسبباً، ولمدة لا تتجاوز خمسة عشر يوما قابلة للتجديد لمرة واحدة".[177]

<u>أوجه المقارنة:</u>

لقد جاء نص المادة (34/1) من القرار بقانون، والتي تنظم حالات مراقبة الاتصالات والمحادثات الإلكترونية، منسجمة مع نص المادة (51) من قانون الإجراءات الجزائية ساري المفعول.

الفقرة الثانية من المادة 34 من القرار بقانون، جاءت مخالفة لنص المادة (51) المذكور أعلاه، ومنقصة بشكل واضح من ضمانات مراقبة الاتصالات، بإسقاطها لشرط الحصول على إذن قاضي الصلح بالجمع والتزويد الفوري للبيانات بما فيها بيانات المرور. وإسقاطها لشرط جسامة الجريمة، بأن تكون جناية أو جنحة لا تقل عقوبتها عن الحبس مدة سنة.[178]

---

[176] قرار بقانون بشأن الجرائم الإلكترونية رقم 10، مرجع سابق.

[177] قانون الإجراءات الجزائية رقم 3 الصادر بتاريخ 2001/5/12، الوقائع الفلسطينية، العدد 38، 2001/9/5، ص 94.

[178] مذكرة قانونية حول القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، الهيئة المستقلة لحقوق الإنسان، رام الله، 2018/5/20، ص4.

ويرى الباحث هنا بانه يوجد تناقض بين القوانين المطبقة في فلسطين بخصوص الجرائم الالكترونية ويظهر وجود حاجة الى اجراء تعديلات قانونية حتى تستطيع التشريعات الوطنية المتعلقة بمكافحة الجرائم الالكترونية من تحقيق الغاية من وجودها ومكافحة الجرائم الالكترونية بفعالية وكفاءة عالية.

المطلب الثاني: الحلول للتغلب على الصعوبات التي تواجه التعاون الدولي

على الرغم من كون التعاون الدولي هو حجر الأساس في مكافحة الجرائم الإلكترونية إلا أنه يواجه العديد من التحديات على الصعيد الوطني والدولي، فمن التحديات على المستوى الدولي في تعارض مصالح أشخاص القانون الدولي وتنازع الاختصاص القضائي، أما على المستوى الوطني فتتمثل في التباين والاختلاف في التشريعات الوطنية لطبيعة هذه الجرائم وصعوبة التحقيق فيها، وسيتم الحديث في هذا المطلب حول الحلول للتغلب على هذه التحديات من خلال فرعين يتناول الفرع الأول الحديث حول الحلول للتغلب على التحديات على المستوى الدولي، أما الفرع الثاني يتناول الحلول للتغلب على التحديات التي على المستوى الوطني.[179]

الفرع الأول: الحلول للتغلب على الصعوبات على المستوى الدولي

آلية التغلب على تحدي القصور التشريعي للدول والتعارض بين مصالحها تتمثل في العمل على إيجاد نظام قانوني محدد وموحد خاص بالجرائم الإلكترونية، وتحديث الأنظمة القانونية على المستوى الوطني التي تنظم الجرائم، وإبرام معاهدات دولية ذات طبيعة خاصة بالجرائم الإلكترونية؛ لذلك يتوجب على الدول التفاوض مع بعضها البعض لإبرام اتفاقيات ومعاهدات إقليمية ودولية تتناسب مع التشريعات الوطنية كمحاولة لوضع تشريع موحد لمكافحة الجرائم الإلكترونية تلتزم به الدول عند

[179] يونس عرب، دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والإنترنت، ط1، اتحاد المصارف العربية، 2002، ص 99.

تعديل قوانينها أو إصدار قوانين جديدة لمواجهة هذه الجريمة وتنظيم التعاون الدولي في مجال مكافحة الجرائم الالكترونية.[180]

إن التعاون الدولي في مكافحة الجرائم الالكترونية يقتضي التخفيف من الفوارق التي تكون بين القوانين الوطنية، والعمل على تقليل الفجوة ما بين الدول النامية والدول المتقدمة، لأن معظم قوانين الدول النامية متأخرة عن مواكبة مستجدات القوانين العالمية التي تتعلق بالجرائم الالكترونية.[181]

تواجه الأمم المتحدة تحدياً بتنوع واختلاف النظم القانونية الإجرائية عن طريق قيامها بتشجيع الدول الأطراف فيها على السماح باستخدام بعض التقنيات الخاصة مما يقلل الاختلاف في القواعد القانونية والاجرائية ويفتح المجال للتعاون الدولي بشكل فعال. فمثلاً تشير المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للأوطان لعام 2000 إلى التسليم المراقب والمراقبة الالكترونية والتسليم المراقب التي تعتبر من أهم التقنيات التي تستخدم لمواجهة الجماعات الإجرامية المنظمة.[182]

يمكن التغلب على التحدي الخاص في مجال التدريب من خلال إجراء الكثير من الحملات التوعوية التي تهدف إلى التنبيه حول مخاطر الجرائم الإلكترونية والأضرار التي تنتج عنها وأهمية تدريب رجال العدالة الجزائية في سبيل مواجهتها، كذلك التنسيق ما بين الأجهزة التي تُعنى بتدريب رجال تنفيذ القانون والعمل على إيجاد برامج تدريبية مشتركة تناسب مختلف الفئات، والقيام

---

[180] حسين صالح عبيد، القضاء الجنائي الدولي، ط1، دار النهضة العربية، 1977، ص 30.

[181] وليد الزبيدي، القرصنة على الانترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة، عمان، 2003، ص 128.

[182] علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار الشاخوري العلمية، عمان، 2009، ص 158.

بالعمليات المشتركة التي تهدف إلى صقل مهارات القائمين على مواجهة الجرائم الالكترونية وتقريب وجهات النظر فيما يتعلق بها.[183]

أما فيما يتعلق بالتحديات المتعلقة بالإنابة القضائية يمكن التغلب على التحدي المتعلق بفكرة السيادة من خلال التخلي عن فكرة السيادة المطلقة للدولة لكونها عائقاً أمام التعاون والتضامن الدولي في مواجهة التحديات التي تواجه المجتمع الدولي. [184]

أما فيما يتعلق بالبطء في الإجراءات التي من خلالها يتم الاتصال بشكل مباشر ما بين السلطة القضائية الطالبة والسلطة القضائية المطلوب إليها، فالاتصال يُعتبر أكثر اختصاراً ومرونة وسرعة ويتلائم مع حالات الاستعجال والضرورة التي تتطلب سرعة في اتخاذ إجراءات التحقيق، ولهذا نجد أن أغلب التشريعات الوطنية والمعاهدات والاتفاقيات الدولية التي تُعنى بتنظيم الإنابة القضائية الخارجية على إجازة اتباع هذه الطريق في حالات الضرورة والاستعجال.[185]

ويمكن التغلب على التحديات الخاصة بتسليم المجرمين في مكافحة الجرائم المعلوماتية التي سبق ذكرها وأن هذا التحدي يتمثل في جانبين أولاً ازدواجية التجريم الذي يمكن التغلب عليه من خلال التزام الدول بتجريم الأفعال التي تم ذكرها في الاتفاقيات المبرمة فيما بينها فقد نصت المادة 2/23 من اتفاقية الأمم المتحدة لمكافحة الفساد على ما يلي: "في مسائل التعاون الدولي كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفياً، بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة، أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة،

---

[183] فائزة يونس الباشا، الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، رسالة دكتوراه، حقوق القاهرة، 2001، ص 372.

[184] علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دار النهضة العربية، القاهرة، 2000، ص230_231.

[185] عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2001، ص 177.

وكان السلوك الذي يقوم عليه الجرم الذي تلتمس بشأنه المساعدة يعتبر فعلا إجراميا في قوانين كلا الطرفين".[186] ويمكن التغلب عليه أيضاً من خلال التخفيف من التطبيق الصارم والحازم لهذا الشرط من خلال رد الأفعال التي تتطلب التجريم كأفعال أو جرائم مخلة بمقتضى قوانين الدولتين معاً أو بمجرد السماح بالتسليم يخضع بدوره إلى مستوى معين من العقوبة حسب كل دولة.[187]

أما الجانب الآخر وهو تحدي التزاحم في طلبات التسليم مما يجدر ذكره في هذا الشأن أن الفقه الدولي لم يستقر على ترتيب وتحديد التسليم في حالة تزاحم طلبات التسليم، ويوجد العديد من الاختلافات حول ترتيب هذه الأولويات الذي هو أيضاً موجود على مستوى نطاق الدولة الواحدة في كل اتفاقية؛ والذي يعود إلى اختلاف أولويات ومصالح الدول ومصالحها مع الأطراف المتعاقدة،[188] إن الاتفاقية العربية الخاصة بالتسليم اعتمدت على معيار جسامة الفعل الإجرامي فقد نصت في المادة 13 منها على "إذا قدمت إلى الدولة المطلوب إليها عدة طلبات مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أرضها، ثم للدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة، فتكون الأولوية إلى الدولة التي طلبت التسليم قبل غيرها".[189]

---

[186] اتفاقية الأمم المتحدة لمكافحة الفساد لعام 2016.

[187] غانم مرضي الشمري، مرجع سابق، ص130.

[188] أحمد السيد عبدالله، التعاون الدولي في الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراه، حقوق، المنصورة، 2009، ص 394.395-

[189] الاتفاقية العربية الخاصة بالتسليم.

في حالة كون الشخص متعدد الجنسيات[190] تزداد صعوبة هذا التحدي وتجعله أكثر تعقيداً، تتعدد الأسباب التي تؤدي إلى تعدد الجنسية، فمنها ما يكون لاحقاً لتاريخ الميلاد ومنها ما يتحقق وقت الميلاد ومنها ما يكون معاصراً للميلاد وهذه الحالة هي أكثر الحالات شيوعاً. تختلف مشكلة تنازع الجنسيات وفقاً للمبدأ الذي تتبناه الدولة سواء كان بحظر تسليم الرعايا أو تسليمهم ولم تقم التشريعات بمعالجة هذا الأمر بل تركته لقواعد المجاملات الدولية ومبدأ المعاملة بالمثل، وفي حالة أنْ كان الشخص المطلوب تسليمه يتمتع بجنسية الدولة الطالبة إلى جانب دولة أخرى فإنها تتمسك بتطبيق القواعد العامة التي تطبقها في هذا الأمر، ومن الممكن أن ترفض تسليمه إلى الدولة الثانية ولو كان يحمل جنسيتها، وقد توافق على تسليمه وفقاً للمعاير والضوابط التي تحددها. وتزداد هذه الإشكالية في حال أنْ كان الشخص المطلوب تسليمه يحمل جنسية الدولة المطلوب إليها فهنا يخضع الأمر إلى العلاقات الدبلوماسية.[191]

الفرع الثاني: الحلول للتغلب على الصعوبات على المستوى الوطني

يمكن التغلب على الصعوبات على المستوى الوطني من خلال مجموعة من التدابير الموضوعية والتدابير الإجرائية على النحو التالي:

أولا: التدابير الموضوعية للتغلب على الصعوبات على المستوى الوطني

يجب على كل دولة أن تقوم باتباع سياسة تشريعية تهدف إلى التعاون مع الدول الأخرى من أجل حماية المجتمعات من تداعيات ومخاطر الجرائم الإلكترونية، من خلال تبنيها تشريعات تتناسب وتتلاءم مع الطبيعة الخاصة لهذه الجرائم؛ حتى تتمكن من مواجهة المخاطر الناجمة عن استخدام الإنترنت في ارتكاب أفعال إجرامية، لذلك على كل دولة أن تقوم باتخاذ التدابير التشريعية

---

[190] ويقصد بالجنسيات المتعددة او كما تسمى الجنسيات المزدوجة هي حالة مواطنة لشخص، وهو فيها يكون الشخص يمتلك اكثر من جنسية لدولة مثلا شخص حامل لجنسية فلسطينية وجنسية أمريكية في نفس الوقت.

[191] فؤاد رياض، الوسيط في الجنسية ومركز الأجانب، ط1، دار النهضة العربية، القاهرة، ص 80.

لمعرفة أي استيلاء غير مشروع قانونياً وجعله جريمة جنائية وفقاً لأحكام القانون الوطني وغيرها من التدابير التي تساعد في الكشف المبكر عن هذه الجرائم.[192]

على كل دولة أن تقوم في قوانينها بإدخال جميع أعمال الإتلاف أو الإضرار أو الإعاقة أو المحو أو التعديل التي تستهدف بيانات الحاسوب كجريمة يعاقب عليها القانون، إضافة إلى الأعمال التي تعيق وظائف الشبكة العنكبوتية والأجهزة المتصلة بها من نقل أو إدخال أو محو أو تعديل أو إعاقة لبيانات أجهزة الحاسوب المتصلة بالإنترنت سواء كانت الحواسيب المستضيفة أو المضيفة.[193]

يجب على كل دولة أن تقوم بوضع إجراءات تشريعية يتم من خلالها المساءلة المعنوية للاشخاص جنائياً عما ينشأ من الجرائم التي تتعلق بالإنترنت والحاسوب، وذلك في حالات قصور الرقابة والإشراف من الشخص الطبيعي الذي يتسبب بحدوث هذه الجرائم أو تسهيل حدوثها.[194]

من المهم القيام بإجراء تعديل البعض من النصوص الموضوعية في قانون العقوبات ليتم النص فيه صراحة على تجريم الجرائم الالكترونية بدلاً من كونه يطلق عليها الجرائم التقليدية القديمة تندرج ضمن النصوص القانونية القديمة. ويوجد حاجة ملحة إلى إضافة نصوص قانونية جديدة تنص على تجريم الجرائم الالكترونية المستحدثة وما ينتج عنها من جرائم أخرى وتطور في الأدوات وارتكاب الجرائم.[195]

---

[192] أحمد فتحي سرور، الوسيط في شرح قانون العقوبات القسم العام، ط6، دار النهضة العربية، القاهرة، 1996، ص 220.

[193] جميل الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 2002، ص 40.

[194] المرجع السابق، ص44.

[195] أحمد فتحي سرور، مرجع سابق، ص 225.

ثانيا: التدابير الإجرائية للتغلب على الصعوبات على المستوى الوطني

تتمثل التدابير الإجرائية التي يجب على الدول أن تتخذها للتغلب على التحديات التي تواجه التعاون الدولي في سبيل مكافحة الجرائم الإلكترونية في:

على الدول أن تقوم بوضع تدابير إجرائية تشريعية تسمح لها بتفتيش شبكات ونظم الحاسوب وأجزائها، وفحص البيانات التي تم تخزينها بها، سواء كانت هذه الأجزاء المراد تفتيشها تقع داخل الدولة أو خارجها طالما أن هذا الإجراء يفيد التحقيق في الجريمة. وعلى الدول أن تقوم باتخاذ التدابير التشريعية لمنح سلطاتها المعنية صلاحيات ضبط وإحضار الأشخاص الذين هم متورطين في الجريمة سواء كانوا على إقليم الدولة أو لا.[196]

إضافة إلى إضفاء صفة الضبطية القضائية على الذين يعملون في مجال المعلومات من غير رجال الشرطة مثل مُزوّدي خدمات الإنترنت والدخول، فيقومون بالرقابة من خلال المزود عن سير حركة العمل ومدى الخضوع وتطبيق القانون والنظام من قبل المتعاملين والعاملين مع شبكة الإنترنت، فإذا تم اكتشاف جريمة ما بهذا الأسلوب فليس عليهم سوى أن يقوموا بالتحفظ على أدلة الجريمة حتى حضور رجال الضبط القضائي.[197]

على أجهزة الشرطة داخل كل دولة أن تقوم بعمل دوريات لمراقبة المؤسسات التي تنتج الحواسيب، كوسيلة للوقاية من مختلف صور الجرائم التي تتعلق بالإنترنت والكمبيوتر كتقليد برنامج من برامج الحاسب الآلي بطريقة غير قانونية.[198]

---

[196] محمد فتحي أنور، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف، دراسة مقارنة، رسالة دكتوراه، كلية حقوق عين شمس، 2010، ص545.

[197] المرجع السابق.

[198] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط1، دار النهضة العربية، القاهرة، 1999، ص 59.

ضرورة دعم التعاون ما بين أجهزة الشرطة في مختلف الدول من خلال معاهدات واتفاقيات دولية، فإذا اكتشفت الشرطة الوطنية أن جريمة ما تمت بدولة أخرى عن طريق شبكة الانترنت بواسطة موقع موجود بالخارج فتقوم بإبلاغ سلطات الشرطة في الدولة التي تم فيها البث عن هذه الجريمة، كما تعمل الدول على تشكيل الإدارة الأمنية بمكافحة هذه الجرائم، ويوكل لهذه الإدارة تلّقي البلاغات التي تتمحور الجريمة الكترونية، ويحق لها اتخاذ كافة الإجراءات القانونية وفقاً لما يقتضيه القانون الوطني.[199]

على كل دولة أن تتخذ تدابير تشريعية تمكن السلطات المعنية من الحصول على نسخة سريعة ومحفوظة من البيانات المخزنة على أنظمة الحواسيب وفق مصلحة التحقيق، تحديداً إذا اتضح أن هذه البيانات معرضة للتعديل أو التلف أو المحو.[200]

كذلك اتخاذ التدابير التشريعية لمد اختصاصها القضائي في أي جريمة من الجرائم الإلكترونية إذا وقعت بشكل جزئي أو كامل على أراضيها أو على متن طائرة أو باخرة أو قمر صناعي مسجل لديها أو يحمل علمها، ومن أحد مواطني الدولة في حال أنْ كانت الجريمة تعتبر من الجرائم المعاقب عليها وفقاً لقانون العقوبات ساري النفاذ حين وقوع الجريمة.[201]

ففي نهاية المطاف وفي ضوء خصوصية الجريمة الإلكترونية، وكيفية تحديد طبيعة وخصائص الجرائم العابرة للحدود وعبر الوطنية وخصائص المجرمين وكيفية التحقيق في مسؤولياتهم الجنائية والمدنية من المهم جداً مكافحة الجريمة السيبرانية او الجريمة الالكترونية ولمكافحة هذه الجريمة يجب أن يعتمد التعاون الأمني والقضائي الدولي على آلياتٍ متطورةٍ تتوافق

---

[199] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت.

[200] المرجع السابق.

[201] أحمد فتحي سرور، مرجع سابق، ص43.

مع تطور وطبيعة هذه الجرائم ويجب أن يتم هذا الشكل من التعاون الدولي على أساسٍ مساعد لضمان مكافحة هذه الجرائم بشكل فعال. لذلك من الضروري أن تتمتع هذه الوكالات الوطنية والدولية بجميع أنواعها بقدرات عالية الكفاءة والمعرفة والقدرة على كشف هذه الألغاز الإجرامية التي تم ظهورها حديثًا.

الخاتمة

تناول الباحث في هذه الدراسة موضوع " التعاون الدولي في مجال مكافحة الجريمة الالكترونية، وذلك من خلال تسليط الضوء على مفهوم الجريمة الالكترونية واركانها والتطرف ايضا الى المقصود بالتعاون الدولي وسبله والجهات المنوطة بها التعاون الدولي والمعياقات التي تتعرض لها اثناء تنفيذ التعاون الدولي واليات مواجهة هذه المعيقات ، وقد اعتمدت الدراسة بصورة عامة على القوانين الفلسطينية والمتمثلة بقرار بقانون رقم 10 لسنة 2018 بشان الجرائم الالكترونية وتقنية المعلومات وتعديلاته، كذلك للدراسات السابقة المتهلقة بجزئيات معينة في هذا البحث وقد توصل الباحث في نهاية هذه الدراسة لمجموعة من النتائج والتوصيات وذلك على النحو التالي :

النتائج

1. أورد المشرع الفلسطيني تشريعا خاصا لمواجهة الجريمة الالكترونية وهو القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات ويعطي خصوصية لهذه الجريمة خلال مرحلة جمع الاستدلالات والمحاكمة والعقوبة.
2. تعتبر الجريمة الالكترونية من الجرائم المستحدثة العابرة للحدود والتي لا يقتصر مداها الى الدولة ذاتها بل يمتد الى باقي دول العالم، الامر الذي يرتب صعوبه بتتبعها والوصول الى مرتكبيها ويستدعي تعاون دولي لاجراء ملاحقة قضائية ومعاقبة مرتكبي هذه الجرائم.
3. يتطلب تحقق الجريمة الالكترونية توافر ثلاث اركان رئيسية في الفعل الجرمي وهي الركن المادي بوجد فعل او امتناع على فعل مجرم بالقانون، وركن معنوي بوجود إرادة وحرية لمرتكب الجريمة بارتكاب الفعل، وركن شرعي بوجود نص قانوني يجرم السلوك الإيجابي والسلبي المجرم في القرار بقانون الوطني بشان الجرائم الالكترونية.

4. يعد التعاون الدولي في تنفيذ الأحكام الجزائية الأجنبية صورة خاصة من صور التعاون الدولي في مكافحة الجريمة الالكترونية، وذلك نظرا للدور الذي يلعبه في تحقيق مكافحة فعالة لهذه الجريمة.
5. تقوم منظمة الشرطة الدولية "الإنتربول" بدور مهم في مكافحة الجرائم الإلكترونية، ويظهر ذلك في الأقسام والشُعب التي تتكون منها المنظمة، كشعبة الإجرام الاقتصادي والمالي، وشعبة التقصي الآلي وتحليل المعلومات.
6. تختص نيابة الجرائم الالكترونية في متابعة الطلبات المتعلقة بالجرائم الالكترونية في حين تعمل هذه النيابة بالتعاون مع وحدة مكافحة الجرائم الالكترونية من اجل الوصول الى الدليل الفني الالكتروني وربط الجناة فيه.
7. يعد تسليم المجرمين واحداً من اهم مجالات التعاون الدولي كونه يتعلق بسيادة الدولة.
8. يعد الاختصاص التشريعي الوطني للدولة هو المعيار الأساسي لتحديد الطبيعة القانونية لنظام تسليم المجرمين، فالمشرع هو الذي يقوم بدور تحديد ما اذا كان النظام ذا طبيعة قضائية، أو طبيعة إدارية.

التوصيات

توصل الباحث للعديد من التوصيات وهي كالاتي.

1. توحيد جهود الدول من اجل التصدي للجرائم الإلكترونية ومكافحتها والتعاون، من خلال هيئة الأمم المتحدة، والتعاون بين الهيئات المختصة الوطنية والدولية بشأن ذلك، وتعزيز التعاون الرسمي وغير الرسمي في مكافحة الجرائم الالكترونية.
2. الاستفادة من التكنولوجيا ووسائل التواصل الحديثة، في مواجهة الجرائم الالكترونية والتصدي لها.

3. حث المشرع الفلسطيني لتعديل قانون مكافحة الجرائم الالكترونية، بحيث تواكب كل ما هو جديد في هذا المجال، وبما يتوافق مع الاتفاقيات الدولية التي وقعت عليها دولة فلسطين.
4. تعديل قانون الإجراءات الجزائية بما يضمن اشتماله على قواعد للتحقيق في الجرائم الإلكترونية، والتفتيش في أجهزة الكمبيوتر وأجهزة الاتصال الذكية بما يضمن فعالية ضبط والاحتراز على الأدلة الرقمية.
5. تعزيز الاتصال المباشر بين السلطات القضائية الدولية الطالبة والمطلوب إليها؛ للتغلب على إشكالية البطء في إجراءات الإنابة القضائية الدولية في مكافحة الجرائم المعلوماتية.
6. العمل على تدريب وتأهيل العديد من المختصين من أجل التحري والتحقيق في الجرائم الإلكترونية، وتدريبهم على كيفية البحث في الأدلة من أجل اثبات تلك الجرائم وضبط الأدلة.
7. العمل على مواءمة التشريعات الوطنية التي تتعلق بالجرائم الالكترونية مع الاتفاقيات الدولية ذات الاختصاص في الجرائم الالكترونية التي انضمت فلسطين اليها.

المصادر والمراجع:

المصادر:

القرآن الكريم

1. القانون الأساسي الفلسطيني لسنة 2003.
2. القرار بقانون رقم (10) لسنة (2018م) بشأن الجرائم الالكترونية
3. اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001م
4. اتفاقية الرياض العربية للتعاون القضائي
5. القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية.
6. قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة (2001).
7. المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدت بقرار الجمعية العامة للأمم المتحدة رقم 45/118 المؤرخ في 14 ديسمبر/ كانون أول 1990.
8. من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر 2000.
9. نظام روما الاساسي للمحكمة الجنائية الدولية.
10. نظام مكافحة الجرائم الإلكترونية السعودي رقم (17) لسنة 2007م.
11. قانون الجرائم الإلكترونية القطري.
12. القانون الجزائري رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

13. ندوة فلسطينية بخصوص التعاون الدولي في مواجهة الجرائم العابرة للحدود والجرائم المنظمة، رام الله، النيابة العامة، 8 تموز/ يونيو 2023، تاريخ الزيارة: 20 تموز 2023.
14. قانون تسليم المجرمين رقم 56 الصادر بتاريخ 1/تشرين اول/1926، قوانين فلسطين (مجموعة درايتون– الانتداب البريطاني)، العدد 56، 22/تشرين الثاني/ 1926.
15. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 للدورة الخامسة والخمسين في 15 نوفمبر 2000.

الكتب القانونية

1. احمد ابراهيم سليمان، الارهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع، بدون طبعة، القاهرة، 2006م.
2. احمد براك، عبد القادر جرادة، الجرائم الالكترونية في التشريع الفلسطيني، دار الشروق للنشر، رام الله، 2019م.
3. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، الجزء الاول، دار النهضة العربية، القاهرة، 1981م.
4. احمد محمد رفعت، القانون الدولي العام، دار النهضة العربية للطبع والنشر والتوزيع، القاهرة، 2006م.
5. احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، 2010م.
6. أسامة عبد الله كايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة، دار النهضة العربية، الطبعة الثالثة، القاهرة، 1999م.

7. اشرف رمضان، النيابة العامة ودورها في المرحلة السابقة على المحاكمة (دراسة مقارنة)، الطبعة الاولى، دار النهضة العربية، 2004م.

8. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008.

9. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، مصر، 2007م.

10. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 1998

11. جهاد محمد البريزات، الجريمة المنظمة: دراسة تحليلية، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2008م.

12. جيرار كورنو، ترجمة منصور القاضي، معجم المصطلحات القانونية، بيروت، المؤسسة الجامعية للدراسات والنشر والتوزيع، 1998م.

13. خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، 2011م.

14. خالد مبارك القحطاني، التعاون الدولي ودوره في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، اكاديمية نايف للعلوم الامنية، الرياض، 2006.

15. خالد ممدوح ابراهيم، الجريمة الالكترونية، دار الفكر الجامعي، الطبعة الاولى، الاسكندرية، 2009م.

16. د. مصطفى محمد موسى، الاساليب الاجرامية بالتقنية الرقمية ومكافحتها، مطابع الشرطة للنشر والتوزيع، الطبعة الاولى، القاهرة، 2003م.

17. رامي متولي القاضي، مكافحة الجريمة الالكترونية في التشريعات المقارنة وفي ضوء الاتفاقيات الدولية، الطبعة الاولى، دار النهضة العربية، القاهرة، 2001م.

18. رستم، هشام محمد فريد، الجرائم المعلوماتية "أصول التحقيق الجنائي الفني". بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3م المجلد الثاني، الطبعة الثالثة، الإمارات العربية المتحدة، 2000.

19. سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية. رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 1997.

20. ساهر إبراهيم الوليد، شرح قانون الإجراءات الجزائية الفلسطيني، الجزء الأول، مكتبة غزة المركزية، فلسطين، 2009م.

21. شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، جامعة الشارقة، الامارات العربية المتحدة، 2019.

22. عادل عبد العال خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الطبعة الاولى، الاسكندرية، 2015م.

23. عادل محمد السيوي، التعاون الدولي في مواجهة جريمة غسيل الاموال، نهضة مصر للطباعة والنشر، الطبعة الاولى، مصر، 2008م.

24. عبد الرحمن بن محمد بن خلدون، مقدمة ابن خلدون، ترجمة علي عبد الواحد وافي، ج 1، دار نهضة مصر للطباعة والنشر، القاهرة، 2006م.

25. عبد الرحمن فتحي سمعان، تسليم المجرمين في ظل قواعد القانون الدولي، دار النهضة العربية، القاهرة، 2012م.

26. عبد الغني محمود، تسليم المجرمين على أساس المعاملة بالمثل، دار النهضة العربية، القاهرة، 1991.

27. عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، الاسكندرية، 2008م.

28. عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة 2003.

29. عبد الله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2002م.

30. عبد الله عبد الكريم، الجرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، 2011م.

31. عبدالله عبد الكريم عبدالله، الجرائم الالكترونية دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الاولى، بيروت، 2007م.

32. عز الدين فودة، النظم الدبلوماسية، مكتبة الآداب، القاهرة، 1989.

33. عفيفي كامل، فتوح الشاذلي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

34. علاء الدين شحاته، التعاون الدولي في مكافحة الجريمة، إيتراك للنشر والتوزيع، الطبعة الاولى، القاهرة، 2000م.

35. علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري للنشر والتوزيع، عمان، 2009م.

36. علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2011م.

37. عمر سعد الله، معجم في القانون الدولي المعاصر، ديوان المطبوعات الجامعية، الطبعة الاولى، الجزائر، 2005.

38. غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها وخصائصها وكيفية التصدي لها قانونا، دار الثقافة للنشر والتوزيع، عمان، 2016م.

39. غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015م.

40. فريدة، شبري، " تحديد نظام تسليم المجرمين"، رسالة ماجستير، جامعة محمد بوقرة بومرداس، 2007-2008م،.

41. فهد عبد الله العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016م.

42. كامل السعيد، شرح الاحكام العامة من قانون العقوبات، دراسة مقارنة، عمان، دار الثقافة، 2011م.

43. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، دبي، الإمارات العربية المتحدة، 2003.

44. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من 1-3 مايو 2000 بكلية الشريعة والقانون بدولة الإمارات.

45. محمد العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2011م.

46. محمد الفاضل، محاضرة في تسليم المجرمين، منشورات معهد الدراسات العربية التابع لجامعة الدول العربية، المطبعة الفنية الحديثة، القاهرة، 1967.

47. محمد بن أحمد بن علي المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا: التكامل الدولي المطلوب لمكافحتها، جامعة الإمام محمد بن سعود الإسلامية، السعودية، 2015م.

48. محمد بن منظور، لسان العرب، دار صادر، الطبعة الثالثة، بيروت، 1994م.

49. محمد صبحي نجم، قانون العقوبات (القسم العام) النظرية العامة للجريمة، دار الثقافة للنشر، 2012.

50. محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية للصحافة، مصر، 2010م.

51. محمد فواز المطالقة، النظام القانوني لعقود اعداد برامج الحاسوب الالي، دار الثقافة للنشر والتزويع، عمان، 2004م.

52. محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي: دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2018م.

53. 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- 28أكتوبر، 1993.

54. محمود صالح العادلي، الجريمة الدولية، دراسة مقارنة، دار الفكر الجامعي، بدون طبعة، الاسكندرية، 2002م.

55. محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر، الطبعة الأولى، الاصدار الثاني، عمان، 2009م.

56. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، 1988م.

57. محمود نجيب حسني، شرح قانون الاجراءات الجزائية، الطبعة الثانية، دار النهضة العربية، مصر، 1998م.

58. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، النظرية العامة للجريمة والعقوبة والتدبير الاحترازي، الطبعة الخامسة، دار النهضة العربية للنشر والتوزيع، القاهرة، 1982م.

59. مدحت رمضان، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2007م.

60. مصطفى عبد الباقي، شرح قانون الاجراءات الفلسطيني: دراسة مقارنة، جامعة بيرزيت، فلسطين، 2015م.

61. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، الطبعة الاولى، القاهرة، 2009م.

62. مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، الطبعة الاولى، القاهرة، 2005م.

63. نبيل صقر، قمراوي عز الدين، الجريمة المنظمة في التشريع الجزائري، دار الهدى، موسوعة الفكر القانوني، بدون طبعة، الجزائر، 2008م.

64. نبيله هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2007.

65. نسرين الرحالي، "الإطار القانوني الدولي لمسطرة تسليم المجرمين"، مسارات في الأبحاث والدراسات القانونية، عدد 5، المغرب، 2018.

66. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008م.

67. الهام محمد العاقل، مبدأ عدم تسليم المجرمين في الجرائم السياسية: دراسة مقارنة، مركز دراسات العالم الإسلامي، سلسلة الدراسات القانونية، الطبعة الأولى، الأردن، 1993.

68. هشام محمد فريد، الاجرام المعلوماتي، دار النهضة العربية، مكتبة الآلات الحديثة، مصر، 1994م.

69. الوهابعبدول، تسليم المجرمين في دولة الإمارات العربية المتحدة، ورقة عمل منشورة في كتاب التعاون القضائي الدولي في المجال الجنائي في العالم العربي، دار العلم للملايين.

70. يحيى محمود محمد عيشان، دراسة مقارنة بين التشريع الأمريكي والتشريع الأردني للصعوبات التي تواجه التنسيق والتعاون الدولي في مكافحة جرائم الحاسب الآلي والانترنت، رسالة ماجستير، جامعة عمان العربية، الأردن، 2008.

71. يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت، الطبعة الاولى، دار العدالة، القاهرة، 2011م.

72. يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، الطبعة الاولى، القاهرة، 2011م.

الرسائل العلمية:

1. احمد سعد الحسيني، الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، حقوق عين شمس، القاهرة، 2012.

2. أشرف لبيب صادق، التعاون الدولي في مكافحة الجريمة المنظمة، اطروحة دكتوراه، جامعة أسيوط، مصر، 2011م

3. خالد مبارك القحطاني، التعاون الامني الدولي ودوره في مواجهة الجريمة، اطروحة دكتوراه، جامعة نايف للعلوم الامنية، الرياض، 2006م.

4. سليمان بن مهيج العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، اكاديمية نايف العربية للعلوم الامنية، السعودية، 2003م.

5. صالح محمد النويجم، تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها. رسالة ماجستير في العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2005.

6. عبدالله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف للعلوم الامنية، 2011م.

7. فيصل بن حمدان الخاطري. أنظمة الدفع الالكتروني وفقاً للقانون العماني. رسالة ماجستير، جامعة السلطان قابوس، عمان، الأردن، 2018.

8. لحمر فافة، " إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، رسالة ماجستير، جامعة وهران، 2013-2014م.

9. متعب بن عبدالله السند، التعاون الدولي في تنفيذ الاحكام الجنائية واثره في تحقيق العدالة، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، الرياض، 2011.

10. محاسن، الباشا، " تسليم المجرمين في القانون الدولي والفقه الإسلامي"، رسالة ماجستير، جامعة أم درمان الاسلامية، السودان، 1999م.

11. محمد الكعبي، الحماية الجنائية للتجارة الإلكترونية. رسالة دكتوراه، جامعة القاهرة، مصر، 2009.

12. نسرين جورج رشماوي، الاحكام الموضوعية والاجرائية للجرائم الالكترونية بفلسطين، رسالة ماجستير، جامعة القدس، فلسطين، 2020م.

المجلات المحكمة:

1. زياد، جفال، " تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 16، العددى1، الامارات، 2019.

2. سهاد خليلي، خصوصية المجرم الالكتروني، مجلة الفكر للنشر والتوزيع، العدد 15، جامعة محمد خضير بسكرة، الجزائر، 2016م.

3. شريهان ممدوح احمد، الإنابة القضائية الدولية في المسائل الجنائية في ضوء اتفاقية الرياض العربية للتعاون القضائي لسنة 1983م، مجلة الدراسات القانونية، المجلد 51، العدد 1، جمهورية مصر العربية، 2021.

4. عبد الكافي، ورياشي، " نظام تسليم المجرمين"، منشورات مجلة الحقوق– سلسلة المعارف القانونية، الإصدار 16، بلا مكان نشر، 2013م.

5. عسكر محمد، قواعد المجاملات الدولية في سياق التطبيق القضائي، مجلة البحوث القانونية والاقتصادية، العدد (81)، جامعة المنصورة، 2022.

6. لطفي أمين بلفراد، "التعاون الدولي في مجال تسليم المجرمين"، مجلة الشرطة المصرية، العدد الأول، مصر، أكتوبر/ تشرين أول 2009.

7. محمد بن حاج الطاهر وشكيرين دليمي، سبل الحماية الدولية من الجريمة الإلكترونية، مجلة الناقد للدراسات السياسية، جامعة محمد خيضر بسكرة – كلية الحقوق والعلوم السياسية، المجلد السادس، العدد الأول، الجزائر، 2022.
8. مصطفى عبد الباقي، التحقيق في الجريمة الالكترونية واثباتها في فلسطين: دراسة مقارنة، مجلة علوم الشريعة والقانون، الجامعة الاردنية، 2018م.

المراجع الأجنبية:

1. Michel quellie: strategies en france par la police la criminalite organisee, 1996, p:96.

المراجع الالكترونية:

1. فائز بن عبد الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وضعية تأصيلية للظاهر الإجرامي على شبكة الانترنت، موقع الدليل الالكتروني، www. Arablawin fo com، تاريخ الزيارة: 12 مايو/ أيار 2023.
2. الملحوظات التفسيرية للأعمال التحضيرية لعملية التفاوض حول اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها رقم (A/55/383/Add.1)، الدورة الخامسة والخمسون، 2000، على الرابط: www.uncjin.org/Documents/Conventions/dcatoc/final_documents/38 3a1adoc، تاريخ الزيارة: 15 مايو/ أيار 2023.
3. المؤسسة الفلسطينية لحقوق الإنسان (شاهد)، تقرير بعنوان: ماذا يعني قانونياً انضمام فلسطين إلى الشرطة الدولية (الانتربول)، منشور على موقع المؤسسة على الانترنت، تاريخ النشر: 27 سبتمبر/ أيلول 2017، تاريخ الزيارة: 22 مايو/ أيار 2023، على الرابط: .pahrw.org/portal/ar-LB

المحتويات

إقرار: .....أ

الشكر والتقدير .....ب

الملخص .....ج

Abstract: ..... هـ

المقدمة 1

أهمية الدراسة 2

أهداف الدراسة 3

إشكالية الدراسة 3

منهجيةُ الدراسة 4

مصطلحاتُ الدراسة 4

الفصل الاول 8

ماهية التعاون الدولي في مجال مواجهة الجريمة الالكترونية 8

المبحث الاول: المفهوم العام للجريمة الالكترونية في التشريع الفلسطيني 10

المطلب الاول: المقصود الجريمة الالكترونية وصورها. 10

الفرع الاول: تعريف الجريمة الالكترونية 11

الفرع الثاني: صور الجريمة الالكترونية 15

المطلب الثاني: خصائص وأركان الجريمة الالكترونية في التشريع الفلسطيني 21

الفرع الاول: خصائص الجريمة الالكترونية في التشريع الفلسطيني 22

الفرع الثاني: أركان الجريمة الالكترونية في التشريع الفلسطيني 26

المبحث الثاني: المفهوم العام التعاون الدولي في مجال الجريمة الالكترونية 29

المطلب الاول: تعريف التعاون الدولي لمكافحة الجريمة الالكترونية 30

الفرع الاول: المقصود بالتعاون الدولي لغةً 31

الفرع الثاني: المقصود بالتعاون الدولي اصطلاحاً 31

المطلب الثاني: الإطار القانوني للتعاون الدولي في مجال مكافحة الجريمة الالكترونية 33
الفرع الاول: التعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة ما قبل المحاكمة 33
الفرع الثاني: التعاون الدولي لمكافحة الجريمة الالكترونية في مرحلة المحاكمة وما بعدها 41
الفصل الثاني 44
أشكال التعاون الدولي وصعوباته في مواجهة الجريمة الالكترونية 44
المبحث الأول: أوجه التعاون الدولي في مواجهة الجريمة الالكترونية 44
المطلب الأول: التعاون الأمني والقضائي الدولي في مواجهة الجريمة الالكترونية 45
الفرع الأول: التعاون الأمني في مواجهة الجريمة الإلكترونية 45
الفرع الثاني: التعاون القضائي في مواجهة الجريمة الالكترونية 52
المطلب الثاني: التعاون الدولي لتسليم المجرمين في مواجهة الجريمة الالكترونية 60
الفرع الاول: ماهية تسليم المجرمين 61
الفرع الثاني: شروط واجراءات تسليم المجرمين 62
الفرع الثالث: مظاهر التعاون الدولي في مجال تسليم المجرمين 64
الفرع الرابع: التعاون الدولي في مجال التدريب على مواجهة الجريمة الالكترونية 72
المبحث الثاني: الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الالكترونية وكيفية التغلب عليها 75
المطلب الأول: الصعوبات التي تواجه التعاون الدولي في مواجهة الجريمة الإلكترونية 75
الفرع الأول: الصعوبات الدولية التي تواجه التعاون الدولي. 76
الفرع الثاني: الصعوبات الوطنية 80
المطلب الثاني: الحلول للتغلب على الصعوبات التي تواجه التعاون الدولي 86
الفرع الأول: الحلول للتغلب على الصعوبات على المستوى الدولي 86
الفرع الثاني: الحلول للتغلب على الصعوبات على المستوى الوطني 90
الخاتمة 95

النتائج 95

التوصيات 96

المصادر والمراجع: 98