مجلة الناقد للدراسات السياسية | المجلد: 06/ العـدد: 01 (2022)، ص 710– 720

سبل الحماية الدولية من الجريمة الإلكترونية

International protection against cybercrime

بن حاج الطاهر محمد [1]،شكيرين ديلمي[2]

[1] جامعة خميس مليانة (الجزائر)، mohttaher@gmail.com

[2] جامعة خميس مليانة (الجزائر)، d.chekirine@univ-dbkm.dz

تاريخ الاستلام: 2022/01/08 تاريخ القبول: 2022/02/10 تاريخ النشر: 2022/04/18

ملخص:

لقد عرفت نهاية القرن العشرين تسارعًا كبيرًا وتقدما هائلا في المجال التكنولوجي، وظهور الفضاء الإلكتروني، ووسائل اتصال حديثة بتطور الوسائل المستعملة لذلك، فقد كان للأقمار الصناعية دور هام في تسهيل الاتصال والتواصل. وقد ظهر ما يسمى بفضاء الإنترنت الذي من جهة سهل عمليات التواصل ومن جهة ثانية صار أداة لنوع مستحدث من الجرائم ألا وهي الجرائم الإلكترونية التي تستعمل الحاسوب والهاتف كأدوات لهذه الجريمة العابرة للحدود. وقد صعب للقوانين والتشريعات الوطنية والدولية التقليدية والإجراءات التي تتضمنها مواكبة هذه الجرائم المستخدمة، لذا وجب تحديث كل النظم الإجرائية الوطنية والدولية لمواجهة جيل من الجرائم.

كلمات مفتاحية: تكنولوجيا، جريمة الكترونية، مكافحة الجريمة، تعاون دولي.

ABSTRACT :

The end of the twentieth century witnessed a great acceleration and tremendous progress in the field of technology, the emergence of cyberspace, and modern means of communication with the development of the means used for that, as satellites had an important role in facilitating communication and communication. The so-called Internet space has emerged, which on the one hand facilitated communication operations, and on the other hand, it became a tool for a new type of crime, namely electronic crimes that use computers and telephones as tools for this cross-border crime. It has been difficult for traditional national and international laws and legislations and the procedures involved to cope with these used crimes, so all national and international procedural systems must be modernized to confront a generation of crimes.

Keywords: technology, cybercrime, crime fighting, international cooperation

المؤلف المرسل: شكيرين ديلمي ، **الإيميل**: d.chekirine@univ-dbkm.dz

مقدمة:

مع تسارع إيقاع التقدم الذي عرفته الإنسانية خاصة في المجال التكنولوجيا المعلوماتية، ووسائل الاتصال الحديثة ومنها الإنترنت، لم تعد الجريمة تعرف بمفهومها التقليدي، بل ظهرت الجريمة الإلكترونية، ولم يعد يقتصر تنفيذ هذا النوع الجديد من الجرائم على إقليم لدولة الواحدة بل تعرف ذلك وصارت جرائم عابرة للقارات والأوطان.

وتتميز به الجريمة الإلكترونية هي حداثة أسلوبها وبسرعة في تنفيذها وسهولة طمس معالمها وإخفاء أثرها، وتعدد صورها وأشكالها. كما لم تعد الحدود بين الدول والمراقبة الحدودية تشكل حاجزًا أمام مرتكبي هذا النوع المستحدث من الجرائم، فالأثر الإجرامي يتخطى حدود الدولة ليشمل دولا أخرى، حيث صار بالإدمان التخطيط للجريمة الإلكترونية في بلد ثم يمكن للمجرم تنفيذ جريمته في بلد آخر.

ولمواجهة هذا النوع الخطير من الجرائم صار لزامًا على الدول أن تكثف من جهودها لمواجهة آثارها الدولية، فهي لا تتمركز في دولة واحدة ولا يمكن تفادي آثرها على بقية الدولة في ظل التطور الهائل التي تعرفه تكنولوجيا المعلومات وسهولة تداولها، لذا لا بد من تضافر الجهود الدولية واتخاذ التدابير الفعالة للحد منها ومعاقبة مرتكبيها.

أهمية الدراسة: تعتبر الجريمة الالكترونية من الجرائم المستحدثة و التي تعد خطورتها و آثارها كبيرة على الصعيدين الدولي و الوطني، مما يجعل من مكافحتها و سبل الوقاية منها ضرورة حتمية.

إشكالية الدراسة : كيف يمكن للتعاون الدولي أن يحد من خطورة الجريمة الالكترونية؟

المناهج المستعملة: المنهج الغالب في دراستنا هذه هو المنهج التحليلي الذي يسمح بتحليل النصوص القانوني و المعطيات بشكل جيد.

خطة الدراسة: تشتمل الدراسة على مبحثين، كل محث يندرج تحته مطلبان، المبحث الأول: التعاون الدولي لمواجهة الجريمة الإلكترونية و يندرج تحته مطلبان، المطلب الأول: التعاون القضائي الدولي في مكافحة الجريمة الإلكترونية. والمطلب الثاني: التعاون الدولي في مجال تسليم المجرمين. ومبحث ثاني: الصعوبات التي تواجه التعاون الدولي لمكافحة الجريمة الإلكترونية يندرج تحته مطلبان هو كذلك مطلب أول: تعدد نماذج النشاط الإجرامي و المطلب الثاني: الاختصاص القضائي.

المبحث الأول: التعاون الدولي لمواجهة الجريمة الإلكترونية

تعددت الآراء في شأن تعريف الجريمة الالكترونية فهناك من عرفها من جانبها الفني، وهناك من عرفها من زاوية قانونية، وهناك من عرفها استنادا إلى معايير أخرى حسب توافر التقنيات لدى مرتكبيها [1] ، وهذا ما جعل الأمم المتحدة في مدونتها بشأن الجريمة المعلوماتية إلى عدم التوصل إلى تعريف متفق عليه دوليا، وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية على أنها "الجرائم التي تقع على برامج الحاسب الآلي وأنها كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ويهدف هذا الاعتداء إلى المساس بمصلحة مشروعة مادية كانت أو معنوية".[2]

المطلب الأول: التعاون القضائي الدولي في مكافحة الجريمة الإلكترونية

تعتبر التعاون القضائي الدولية هو الآلية الدولية الأهم في مجال مكافحة الجريمة بكل صورها، والجريمة الإلكترونية جزء مهم من الجريمة الدولية، ويقصد به ما تقدمه سلطات الدولة إلى سلطات دولة أخرى والذي يكون الهدف منه خلق تعاون دولي يسهل عملية مكافحة الجرائم الدولية، وتوقيع العقاب على مرتكبي هذه الجرائم، كما يهدف إلى إعطاء وتبادل المعلومات والأدلة، كما يهدف التعاون الدولي إلى اتخاذ التدابير الوقائية لنفادي وقوع تلك الجرائم. كما يهدف التعاون القضائي الدولي في هذا المجال إلى نزع الصفة الوطنية لهذه الجرائم وتضافر الجهود الدولية للحد من الجرائم الدولية خاصة في مجال الجريمة الإلكترونية.

ولعل من أهم صور التعاون الدولي هو التعاون الأمني الدولي، و المساعدة القضائية الدولية:

الفرع الأول: التعاون الأمني الدولي لمواجهة الجريمة الإلكترونية

كثيرًا ما تقف الحدود الدولية عائقا أمام محاولة وضع حد للنشاط الإجرامي عمومًا وفي مجال الجريمة الإلكترونية بوجه خاص، فالمتابعة الأمنية تتوقف على الحدود الجغرافية للدولة على عكس النشاط الإجرامي التي يعترف بالحدود الدولية، ويعتبر الربط الإلكتروني في مجال تبادل المعلومات بين الدول في هذا المجال من الحلول الفعالة التي تسهل من عمليات الملاحقة.

عمليا فإن الدولة لا تستطيع الوقوف لوحدها في وجه العصابات الإجرامية المتخصصة في مجال المعلوماتية، فهذا المجال يستغله المجرمون في التبادل السريع للمعلومات عبر الإنترنت وهي الجرائم التي وصلت إلى حد اختراق نظم المعلومات السرية والأمنية للدولة ذاته [3] ولا يمكن أن يتحقق هدف مكافحة هذه

الجرائم إلا من خلال تعاون دولي على مستوى الإجراءات الجزائية بحيث يسهل الاتصال بين مختلف أجهزة الشرطة عبر كل دول العالم، وذلك باستثناء مكاتب متخصصة بجمع المعلومات حول مرتكبي الجرائم المعلوماتية، وتعميم هذه المعلومات على كافة الدول [4]

تعد الحدود الجغرافية، والولاية القضائية من أهم العقبات التي تواجه مكافحة الجريمة الإلكترونية، لذا صارت مسألة التعاون الدولي حتمية لا مفر منها، وتقديم المساعدة القضائية، وتبادل المعلومات بين الدول خاصة في النقاط التالية:

1. القيام بعمليات شرطية مشتركة:

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

2. تفعيل التعاون الدولي ودور المعاهدات في مجال المعلوماتية:

أدركت الدول أهمية التعاون الدولي للتغلب على تحديات الجرائم الإلكترونية، وقد عقدت كثير من الدول اتفاقيات ثنائية لتسهيل التحقيق في جرائم الكمبيوتر [5] ففي عام 1973، أجرت منظمة التعاون والإنماء الاقتصادي دراسة حول تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية، وفي 1975، أصدرت هذه المنظمة تقريرًا تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب على الدول تجرينها وفرض عقوبات عليها ومن تلك الأفعال:

- الغش والتزوير في الحاسب الآلي.
- تغيير برامج الحاسب الآلي المخزنة فيه.
- سرقة الأسرار المدعمة في قواعد الحاسب الآلي.
- تفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية.

وقد عالجت اتفاقية فينا لعام 1988 ذات الموضوع، وحثت الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم، كما ناشد مؤتمر الأمم المتحدة لعام 1990 بكوريا الجنوبية الدول الأطراف تكثيف جهودها لمكافحة الجرائم الإلكترونية، ومنها:

- تحديث قوانين الدول لتواكب التعاون الدولي في مجال الجريمة الإلكترونية.
- تبادل المساعدة القضاء في مجال مكافحة هذه الجرائم.
- عقد اتفاقيات تنظيم إجراءات التفتيش والضبط.

وقد وضع المجلس الأوروبي عام 2001 اتفاقية "بودابست" والتي تشكل نصوصها منظومة تعاون دولي تتسم بالمرونة والفعالية، وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم، وتكفل استخدام الوسائل الفعالية في التحقيق وملاحقة مرتكبيها. (6)

3. جهود منظمة الأنتربول:

أسست المنظمة الشرطية الأنتربول عام 1923، ومقرها في باريس، تقوم هذه المنظمة لمحاربة الجريمة عبر العالم، وتعطي الأولوية لجرائم الفساد والمخدرات، والجريمة المنظمة، والإجرام المالي المرتبط بالتكنولوجيا، المجرمون الفارون، والإرهاب، والاتجار بالبشر.

تعد هذه المنظمة من أهم المنظمات التابعة لمنظمة الأمم المتحدة، وتوجد لديها مكاتب في كل الدول الأعضاء، تعمل على تبادل المعلومات في مجال الجرائم المذكورة، وأهمها الجريمة الإلكترونية، فهي تقوم بدور الوسيط بين الدول ونعمل على التصدي لكل أنواع الجرائم.

تجدر الإشارة إلى أن الجزائر انضمت إلى هذه المنظمة عام 1963، وقد أقام المشرع الجزائري علاقة قانونية بين أعمال المنظمة وما يتطلبه تحويل المتهمين عبر نقاط الحدود والسفارات، وقد جاء في قانون الإجراءات الجزائية النص على إجراءات التسليم وآثاره وحركة العبور وفق الطرق الدبلوماسية واتفاقيات دولية في شكل استثمارات من الأنتربول. (7)

الفرع الثاني: المساعدة القضائية الدولية

هي كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المكافحة في دولة أخرى بصدد جريمة من الجرائم. وقد نص عليه المشرع الجزائري في القانون 09-04- في المادة 16، وأعتبر أنه إطار التحريات

والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية بجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني وللمساعدة القضائية صور عديدة منها:

1. تبادل المعلومات: تبادل المعلومات بين الدول في مسألة الجريمة الإلكترونية، ومصادر الأموال لذلك أوصت منظمة الأمم المتحدة بضرورة تبادل المعلومات في مجال مكافحة الجريمة. ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية. وقد أقرته معاهدة الأمم المتحدة لتبادل المساعدة في المسائل الجنائية. (8)

2. نقل الإجراءات: هو قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية في جريمة ارتكبت في دولة أخرى ولمصلحة هذه الدولة بناء على شروط منها التجريم المزدوج، وشرعية الإجراءات المطلوبة في قانون الدولتين الداخليين. (9) وهي صورة أقرتها العديد من الاتفاقيات الدولية والإقليمية.

3. الإنابة القضائية الدولية: هي طلب اتخاذ إجراءات قضائية في الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، وهذا للفصل في قضية معروضة على السلطة القضائية للدولة الطالبة ويتعذر عليها القيام به بنفسها. (10) وهذا يُعد من قبيل تسهيل الإجراءات الجزائية بين الدول للمساعدة على مكافحة المجرمين وتخطي مشكلة السيادة التي تطرح في المتابعات الجنائية، وهي من أهم صور التعاون الدولي في مجال محاربة الجريمة الإلكترونية.

نصت المادة 28 من اتفاقية "بودابست" على الإجراءات المتعلقة بطلبات المساعدة القضائية المتبادلة بين الأطراف، وينجر على الإنابات القضائية ما يلي:

- الدولة التي توجه إنابة قضائية لا تتخلى عن اختصاصها للقاضي الأجنبي
- تكون الإنابة وفقا لإجراءات الدولة التي تقوم بالتنفيذ وليس قانون الدولة التي طلبت الإنابة
- كفالة أحسن الشروط الموضوعية لتنفيذ الإنابة، وأن تأمر الدولة المطلوب إليها التنفيذ من الأشخاص المقيمين لديها بالمثول أمام محاكم الدولة طالبة الإنابة.

4. الاعتراف بالمحاكم الأجنبية: مع استفحال ظاهرة الجريمة الإلكترونية ومن أجل تحقيق التعاون الدولي لمحاربة الجرائم الدولية، لا بد أن تعترف الدولة بحجية الأحكام الجنائية الصادرة عن المحاكم لدولة أخرى كي يتم معاقبة المجرمين المرتكبين لجرائم دولية وخاصة الجرائم الإلكترونية ومن مظاهر التعاون الدولي في مجال محاربة

الجريمة الإلكترونية هو ضرورة تجاوز فكرة أن الأحكام الصادرة عن المحاكم الأجنبية ليست لها حجية أمام القضاء الوطني.

المطلب الثاني: التعاون الدولي في مجال تسليم المجرمين

يعتبر هذا النوع من التعاون ضرورة حتمية توصلت عليها قناعات الدول بعد التطور الهائل الذي وصلت إليها تأثيرات الجرائم الدولية العابرة للأوطان، والتي طالت كل الدول أضرت بمصالحتها الإستراتيجية يقوم نظام تسليم المجرمين على أن الدولة التي يوجد على أراضيها المتهمون بإركاب جرائم دولية عابرة للحدود، خاصة تلك المتعلقة بالجرائم المعلوماتية، فعليها إما محاكمتهم وإما القيام بتسليمهم إلى الدولة التي تطلبهم عدالتها، وعملية التسليم تحقق مصلحة الدولة الطالبة لأنها تعاقب المرتكب للجريمة، ومصلحة الدولة المطلوب إليها التسليم كونها تطهر إقليمها من المجرمين.

الفرع الأول: مبررات نظام تسليم المجرمين

يعتبر تسليم المجرمين حق تمارسه الدولة وفقا لما يمثله الإجراء من أهمية في تحقيق مصالحها مع الدول الأخرى، ويقوم التسليم على أساس العلاقات الدبلوماسية الدولية أيا كانت طبيعة الجرائم المطلوب فيها التسليم. لا يوجد أي نظام دولي أو وطني يلزم أية دولة بالقيام بعملية التسليم يكون فيه مساس بمقتضيات السيادة الممارسة على الإقليم، فنظام التسليم ليس فيه مساس بسيادة الدولة .

كما يعتبر التسليم نظاما يحقق مبدأ الإقليمية للدولة طالبة التسليم في شقيه الموضوعي والإجرائي، وهو المبرر الأساسي للتسليم والذي يمكن من معاقبة المجرمين وضمان إفلاتهم من العقاب لمجرد وجودهم فوق إقليم دولة أخرى. كما يعتبر من أهم صور التعاون الدولي في مجال محاربة الجريمة الدولية.

الفرع الثاني: القانون الواجب التطبيق على التسليم

تخضع عملية تسليم المجرمين إلى الاتفاقية الثنائية بين الدولة طالبة التسليم والدولة المطلوب إليها التسليم في مجال التعاون القضائي أما في حالة عدم وجود اتفاقية بين الدولتين، يمكن اللجوء إلى تطبيق الاتفاقيات المتعددة والتي تجد أساسها القانوني في المادة 16 فقرة 4 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة. وتشير الإتفاقيات الدولية إلى أن مسألة التسليم يخضع لإجراءات القانون الداخلي لكل دولة.

وتبعا لذلك تنص المادة 694 من قانون الإجراءات الجزائية على شروط تسليم المجرمين وإجراءاته وآثاره تحدد وفقا لقانون الإجراءات الجزائية ما لم تنص المعاهدات والاتفاقيات السياسية على خلاف ذلك. لذلك فإن المعاهدة والاتفاقية الثنائية المصادق عليها هي التي تطبق في عملية تسليم المجرمين.

إذا كانت بنود الاتفاقية أو المعاهدة واضحة في مجال تطبيق مسألة تسليم المجرمين فإن القاضي يطبقها مباشرة، أما إذا كانت غامضة فإنه يطبقها بعد إدماجها في القانون الداخلي. وتطبيقا لنص المادة 695 من قانون الإجراءات الجزائية فإنه لا يمكن للدولة الجزائرية تسليم المجرم الأجنبي ما لم يكن قد اتخذت في حقه إجراءات متابعة عن جريمة منصوص عليها في المادة 697 من نفس القانون.

المبحث الثاني: الصعوبات التي تواجه التعاون الدولي لمكافحة الجريمة الإلكترونية

رغم وجود اتفاقيات دولية، ومعاهدات تحث على ضرورة التعاون الدولي في مجال محاربة الجريمة الإلكترونية وهذا لخطورتها ومساسها حتى بالأمن القومي للدول، إلا أن ذلك التعاون يواجه صعوبات وعراقيل كثيرة تحول دون تحقيق الهدف منه وهو القضاء على الجريمة الدولية أو حتى الحد منها. فاختلاف الأنظمة القضائية لمختلف الدول و كذا نقص الاتفاقيات الدولية الثنائية و الجماعية لتبادل المعلومات فيما يتعلق بالجريمة الالكترونية يحول دون الوصول إلى القضاء أو الحد من تلك الجرائم.

المطلب الأول: تعدد نماذج النشاط الإجرامي

كما سبقت الإشارة إليه فإن الدول لم توحد الأعمال التي تعتبر من قبيل الجرائم الإلكترونية، وما هي الأفعال التي إن هي اقترفت اعتبرت جريمة الإلكترونية يعاقب عليها القانون. فعدم وجود نموذج واحد متفق عليه من طرف كل التشريعات الوطنية فيما يخص النشاط الإجرامي المعلوماتي، يجعل من التعاون الدولي في مجال مكافحة الجريمة المعلوماتية أمرًا صعبًا، وهذا يعد قصورًا لا بد من تداركه في التشريعات الوطنية.

إن التشريعات الوطنية وإن أدركت خطورة أثار الجريمة الإلكترونية، إلا أن المشرع الوطني عبر العالم لم يخص هذه الجريمة بقانون خاص يبين بالتفصيل تعريف أنواعها والعقوبات المقررة لها، كل ما في الأمر أنه تناولها باحتشام في قانون العقوبات ولم يفرد لها قانونا خاصا لأهميتها وجدية خطورتها.

كما أن تنوع واختلاف النظم القانونية والإجرائية تعني اختلاف طرق التحقيق والتحري، والمكافحة، والتي إن كانت فعالة في دولة ما ربما لم تكن كذلك في دولة أخرى. فقد تكون أعمالا تشكل جريمة إلكترونية في

دولة قد تكون غير ذلك في دولة أخرى، واختلاف طرق البحث والتحري والتفتيش والإذن به يؤدي إلى صعوبة كبيرة في تطور العمل المشترك في إطار التعاون الدولي في مجال مكافحة الجريمة الإلكترونية.

لذلك فتوحيد مفهوم الجريمة الإلكترونية في التشريعات الوطنية يساعد في رفع الصعوبات التي تواجه العمل الموحد والجدّي لمحاربة هذه الجريمة الخطيرة، ولا تكفي الاتفاقيات الثنائية والمعاهدات وحدها في بيان أهمية التصدي لهذه الجريمة، بل لا بد من العمل على إعطاء تعريف جامع مانع للجريمة الإلكترونية كي يتم الاتفاق على الركن المادي والمعنوي والشرعي خاصة لهذه الجريمة.

ولا بد من توحيد إجراءات البحث والتحري والتفتيش في الجريمة الإلكترونية مع اختلاف النظم القانونية، الأمر الذي يجعل عملية البحث في هذه الجريمة موحد الإجراءات التشكيلية، وعدم تصادم وتعارض الإجراءات التشكيلية المختلفة في الدول والذي يؤدي إلى إفلات مرتكبي هذا النوع الخطير من الجرائم من العقوبة.

المطلب الثاني: الاختصاص القضائي

يطرح مشكل مدى خضوع الجرائم المعلوماتية التي ترتكب خارج الدولة للقانون الوطني وبالتالي لقضاء تلك الدولة، ويعرف كذلك بانعقاد الاختصاص المكاني أو الاختصاص المحلي للمحاكم، فالقاعدة أن الاختصاص المحلي ينعقد لمحكمة مكان وقوع الجريمة أو لمحكمة مكان إلقاء القبض على المجرم مرتكب الفعل مجرم أو أحد شركائه، أو لمحكمة موطن إقامة المجرم.

إذا أصرت الدول على تطبيق هذه القواعد في تحديد الاختصاص سوف يعرقل التعاون الدولي لمحاربة ظاهرة الجريمة الإلكترونية، كون هذه الجريمة عابرة للأوطان ويصعب تحديد موطنها، ومكان وقوع الفعل المجرم، الأمر الذي يجعل تطبيق هذه القواعد التقليدية صعب جدًا على الجرائم الإلكترونية التي تتم بالحداثة والسرعة في التنفيذ وطمس معالم الجريمة.

إن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، ولا بسياسات الدولة ولا تعرف للسيادة معنى، لذا وجب التعامل معها بهذا المنظور كي يتم التغلب عليها والحد منها، فلا يمكن أعمال قواعد الاختصاص المكاني على مثل هذه الجرائم، ولا بد من تضافر الجهود لإيجاد آليات إجرائية تختص بهذه الجرائم الخطيرة مما يتناسب مع طبيعتها. (1)

إن الجريمة الإلكترونية لها خصوصية أنها لا تحدها حدود جغرافية مثل الجرائم العادية المعروفة والتي تخضع للقواعد الإجرائية العامة، لذا فهي لا يمكن إخضاعها لهذه القواعد أو تصنيفها مع الجرائم العادية، إن ذلك يحتم على الدول العمل على توحيد تشريعاتها الداخلية وإيجاد آليات إجرائية موحدة لمواجهة هذه الجرائم المستحدثة لكي لا يستفيد مرتكبوها من غياب التعاون والتنسيق ويفلتون من العقاب يمكن إبرام اتفاقيات ثنائية ومتعددة، وإبرام معاهدات يكون موضوعها توحيد الإختصاص القضائي في الجرائم الإلكترونية، ومع التزام مع تحديث منظومة القوانين الوطنية بما يتلاءم وهذا الطرح ويتلاءم مع التطور الكبير الذي يشهده العالم في المجال المعلوماتي والبرمجيات وقد قام المشرع الجزائري كغيره عبر العالم بتخطي مسألة امتداد التفتيش إلى خارج الوطن بموجب القانون 09-04، كما عدّل المادة 329 من قانون الإجراءات الجزائية، وتم تمديد الإختصاص الإقليمي لبعض المحاكم ووكلاء الجمهورية بموجب المادة الأولى من المرسوم رقم 348/06 المؤرخ في 2005/10/05.

خاتمة:

لم يواكب التعاون الدولي في مجال مكافحة الجريمة الإلكترونية سرعة التطور التكنولوجي، الحاصل في مجال المعلوماتية، فنهاية العشرين شكلت طفرة في مجال الإلكترونيك وشبكة الإنترنت. حقيقة سعت الدول إلى التعاون للقضاء على ظاهرة الجرائم الإلكترونية من خلال الاتفاقيات الدولية الثنائية والمتعددة الأطراف، كما سعت منظمة الأمم المتحدة إلى عقد مؤتمرات دولية أفضت إلى إبرام معاهدات أهمها معاهدة الأمم المتحدة لمكافحة الجريمة الإلكترونية، لكن هذا كلّه يبقى غير كافي للتصدي لهذه الجريمة الخطيرة.

إن الجريمة الإلكترونية لا تعترف بالأوطان أو الحدود الجغرافية أو حتى السيادة الدولية، هي تتميز بسرعتها، وبتخطيطها الحدود وبسهولة اختراق أنظمة الحماية المتطورة التي طالت فضلا عن الأشخاص، البنوك وحتى مؤسسات عسكرية أو ذات تأثير على الأمن القومي للدول.

لذا فإننا نتقدم في نهاية بحثنا هذا بمجموعة اقتراحات لمحاولة الحد من هذه الجريمة الخطيرة:

- تكثيف التعاون الدولي في مجال مكافحة الجريمة الإلكترونية.
- تعديل التشريعات الوطنية الجنائية بما يتواكب مع تطور وسرعة هذه الجريمة.
- تمديد الإختصاص القضائي المحلي، وتوزيع الإنابة القضائية للتصنيف على المجرمين المرتكبين للجرائم الإلكترونية.
- العمل على تكوين شرطة مختصة، وتعطي لها صلاحية واسعة تمد إلى خارج إقليم الدولة.

الهوامش:

(1) عبد الفتاح بيومي، الدليل الجنائي في جرائم الانترنت، بدون دار النشر، القاهرة، 2009، ص 114.

(2) نفس المرجع، ص 7.

(3) حسين الفاطري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة، القاهرة، 2009، ص 636.

(4) نفس المرجع، ص 75.

(5) محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم بجامعة الشريعة والقانون ، الإمارات العربية المتحدة، 2000، ص 1078.

(6) محمد محي الدين عوضي، مشكلات السياسة الجنائية المعاصرة في جرائم المعلومات، المؤتمر السياسي للقانون الجنائي، القاهرة 256-28 أكتوبر 1993، ص 362.

(7) المواد 20، 24، 25 من إتفاقية الأمم المتحدة لمكافحة الجريمة الإلكترونية، كوريا الجنوبية، 1990.

(8)قادري عمر، أطر التحقيق، دار هومة، الجزائر، 2013، ص 302.

(9)راجع نص المعاهدة الصادرة في 1990/12/14 عن الجلسة 68 للجمعية العامة للأمم المتحدة.

(10)حسين الفاطري، مرجع سابق، ص 646.

(11) عبد الرؤوف مهدي، القواعد العامة للإجراءات الجزائية، دار النهضة، القاهرة، 2000، ص102 .