

التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاتها وآليات التغلب عليها)

عزيزة لرقط

كلية الحقوق والعلوم السياسية، جامعة باجي مختار - عنابة، aziza.metatla@yahoo.com

تاريخ القبول: 2018/11/27

تاريخ المراجعة: 2018/11/04

تاريخ الإيداع: 2017/11/08

ملخص

إن الانتشار الواسع لاستخدام التقنية الحديثة، أظهر للوجود أنماطاً جديدة من الجرائم لاسيما المتعلقة بالانترنت، حيث إن الانترنت أو كما يسميه البعض - طريق البيانات السريع، قد أذاب الحدود الجغرافية بين الدول، مما جعل التعاون الدولي لمواجهة الجرائم المعلوماتية وردع مرتكبيها ضرورة وواقعا ملحا خصوصا بعد ثبوت عجز الجهود الداخلية في القضاء عليها أو حتى التقليص منها، إلا أن هذا التعاون الدولي تعترضه إشكالات وصعوبات تحول دون فعاليته، مما يستدعي خلق آليات جديدة وسبل مستحدثة تساعد في التغلب على هذه الإشكالات.

الكلمات المفتاحية: تعاون دولي، جرائم معلوماتية، إشكالات، آليات.

**International Cooperation in the Fight against Cyber Crimes
(Problems and Mechanisms to Overcome Them)**

Abstract

The widespread popularization of the use of new technologies has created new forms of crime, especially those related to the Internet, because the internet or the data highway - as some call it - has blurred the geographical boundaries between States. Hence, international cooperation in the fight against "cybercrimes" and the deterrence of its perpetrators has become a necessity and an urgent reality, especially after proving the inability of internal efforts to eliminate or even reduce them. However, this international cooperation faces certain problems and difficulties that hinder its effectiveness, which requires the creation of new mechanisms and innovative means that would help overcome these problems.

Key words: International cooperation, cybercrime, problems, mechanisms.

Coopération internationale dans la lutte contre la cybercriminalité (Problèmes et mécanismes pour les surmonter)

Résumé

La large diffusion de l'utilisation des technologies modernes, a créé de nouvelles formes de criminalité, surtout celles qui sont liées à l'usage d'internet car internet où l'autoroute des données- comme certains l'appellent-, a fait fondre les frontières géographiques entre les Etats, d'où une coopération internationale pour la lutte contre les « cyber crimes » et la dissuasion de ses auteurs, est devenue une nécessité et une réalité urgente, surtout après avoir prouvé l'incapacité des efforts internes pour les éliminer ou même les réduire. Cependant, cette coopération internationale affronte certains problèmes et difficultés qui entravent son efficacité, ce qui nécessite la création de nouveaux mécanismes et des moyens novateurs qui aideraient à surmonter ces problèmes.

Mots-clés: Coopération internationale, cybercriminalité, problèmes, mécanismes.

مقدمة

إن التدفق الهائل للمعلومات بكل سهولة وغازرة، وانتقالها بسرعة فائقة من مناطق متباعدة باستخدام التكنولوجيا الحديثة والقدرة على تخزينها واسترجاعها في وقت قصير جدا، جعلها عرضة للاعتداءات التي قد تلحقها إما بالحو أو التعديل أو إدخال معلومات غير صحيحة، وهو ما خلف آثارا سلبية تجلت في التحديات الماسة بأغلب القيم الأساسية، إذ إن هذه الاعتداءات طالت قيما جوهرية تخص الأفراد والمؤسسات والدول في كافة نواحي الحياة الاقتصادية، والأمنية، والثقافية، لأنه أصبح من السهل مزاولة الأنشطة الإجرامية عبر حدود الدول.

وترتبنا على ذلك كان لابد من تكاتف جهود الدول وتعاونها من أجل مواجهة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة وإنما أضرارها تلحق دولاً ومجتمعات متعددة، بعد أن عجزت الجهود الداخلية للدولة مهما بلغت درجة من القوة والحضارة في منع الجريمة أو التقليل من حجمها بسبب اتساع مسرح ارتكاب هذه الجرائم وسهولة حركة العناصر الإجرامية وتنقلها، أو إخفاء دليل ارتكابها، مع إمكانية ارتكابها عن بعد باستخدام التكنولوجيا.

وأمام هذه المميزات والخصائص للجرائم المعلوماتية تضافرت جهود الدول والمنظمات لأجل الحد من انتشارها وردع مرتكبيها باعتمادها على آليات متطورة تتماشى وتطور هذه الجرائم، وتتجسد صور التعاون الدولي لمكافحة الجرائم المعلوماتية الذي عرف بأنه: "تبادل العون والمساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة مشتركة سواء كانت هذه الخدمة أو النفع على مستوى عالمي أو على مستوى إقليمي أو على المستوى الوطني للدول التي يتم الاتفاق فيما بينها"⁽¹⁾ في التعاون الدولي بتسليم المجرمين وربط شبكات الاتصال والمعلومات حتى يتحقق التواصل بين سلطات التحقيق والملاحقة لمختلف الدول على وجه السرعة في تبادل المعلومات، بالإضافة إلى القيام ببعض العمليات الأمنية المشتركة لأجل ضبط الأدلة الرقمية، وما يحقق التعاون الدولي هو الجهود المبذولة من طرف المنظمة الدولية للشرطة الجنائية "الإنتربول" في مكافحة الجرائم المعلوماتية التي أصبح يخشاها المجرم المعلوماتي في الأعوام الأخيرة، وتعتبر المديرية العامة للأمن الوطني عضوا فعالا فيها لما تتيحه من تحقيق التبادل المعلوماتي، وتسهيل تنفيذ الإجراءات القضائية المتعلقة بتسليم المجرمين، وتنفيذ الإنابات القضائية الدولية، ونشر أوامر القبض للمبحوث عنهم دوليا⁽²⁾.

والجدير بالذكر في هذا المطاف أن المشرع الجزائري وإدراكا منه بخطورة الجرائم المعلوماتية وما ينتج عنها من خسائر معتبرة تمس الأفراد وكيان الدولة واقتصادها، تدخل بموجب القانون 04/09⁽³⁾ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وأكد على ضرورة التعاون القضائي والمساعدة القضائية الدولية في مكافحة الجرائم المعلوماتية بموجب نصوص خاصة، مما يفيد إقراره بعدم كفاية الأحكام الموضوعية والإجرائية في مواجهة هذا النوع المستحدث من الجرائم.

وعلى ضوء ما تقدم فإن التعاون الدولي الذي يرتبط غالبا بالثقافة الوطنية للدول ومدى تطورها، تعترضه إشكاليات وعوائق جدية ضد المواجهة والملاحقة، مما دعا إلى ضرورة تكاتف جهود الدول وحتمية التنسيق بينها وتوحيد جهودها لأجل زيادة فعاليتها وقدرتها على مواجهة تلك الإشكاليات والعمل على حلها والتغلب عليها لإرساء الاستقرار الدولي والأمن الداخلي للدول، وعليه تتمحور إشكالية الدراسة حول: ما هي الصعوبات التي تعترض التعاون الدولي في مكافحة الجرائم المعلوماتية؟ وما هي الحلول والآليات المقترحة للتغلب على هذه الإشكالات؟

وللإجابة على هذه الإشكالية قمنا بتقسيم الموضوع إلى مطلبين نتناول في المطلب الأول إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية، وفي المطلب الثاني نعرض إلى آليات التغلب على معوقات التعاون الدولي في مكافحة الجرائم المعلوماتية.

المطلب الأول: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية

سبق القول وأن التعاون الدولي في مجال مكافحة الجريمة غالبا ما يرتبط بالثقافة الوطنية للدول ومدى تطورها للإسهام إيجابيا في هذا التعاون، كما يشكل أحيانا صعوبات في التعاون، أما فيما يتعلق بالجريمة المعلوماتية فإمكانية ارتكابها في أماكن مختلفة من العالم باستخدام التقنية الحديثة تستدعي ضرورة تعاون دولي للقضاء عليها ومعاقبة مرتكبيها، إلا أن هذا التعاون تعثره بعض الصعوبات والإشكاليات سواء على المستوى الوطني أو الدولي مما يتعين التطرق لها، وعليه سوف نتناول هذه الصعوبات والإشكاليات على المستوى الوطني في فرع أول وعلى المستوى الدولي في فرع ثان.

الفرع الأول: إشكاليات التعاون في مكافحة الجرائم المعلوماتية على المستوى الوطني

تعترض التعاون الدولي في مجال مكافحة الجرائم المعلوماتية صعوبات على المستوى الوطني تتمثل أساسا في عدم كفاية وملائمة القوانين القائمة (أولا) وصعوبة إثبات الجرائم المعلوماتية والتحقيق فيها (ثانيا).

أولا: عدم كفاية وملائمة القوانين القائمة

إن اعتماد أفراد المجتمع بجميع فئاته على التقنية الحديثة، واستخدام الحاسوب في جميع مجالات الحياة اليومية، جعل الجناة يتفنون في ارتكاب جرائمهم، كما أن التطور السريع في مجال تكنولوجيا الحاسوب والانترنت لا يقابله في الحقيقة تطور بذات الدرجة في النصوص القانونية، وهو ما تؤكد التشريعات الوطنية الصادرة في فترات متباعدة، كما أن النصوص التي أصدرها المشرع الجزائري بخصوص الجرائم المعلوماتية لم تنظم كافة أشكال وصور الجريمة المعلوماتية مثل التزوير المعلوماتي الذي يبقى خاضعا للنصوص التقليدية التي لا تتلاءم والطبيعة المعنوية للمعلومات محل هذا النوع من الجرائم، على خلاف التشريع الفرنسي الذي عدل نص المادة 441 من قانون العقوبات المنظم لجريمة التزوير وقرر حماية ضد الاعتداء الواقع على المعلومات الموجودة على دعامة معلوماتية ومن أبرز صورها بطاقات الائتمان، وكذا المعلومات بصفة مستقلة عن هذه الدعامة⁽⁴⁾.

وترتبطا على ذلك فإن الطبيعة المعنوية لمحل الجرائم المعلوماتية جعل النصوص التقليدية غير قادرة على مواجهة هذا النوع المستحدث من الجرائم، كما أن مبدأ الشرعية والتفسير الضيق لنصوص قانون العقوبات حال دون مواجهة الجرائم المعلوماتية، إضافة إلى تقليل جهود الضبطية القضائية في حال الكشف عن هذه الأفعال المجرمة ومعرفة مرتكبيها كونهم اعتادوا التعامل مع جرائم ذي طبيعة مادية، وعليه فإن الاعتماد على النصوص التقليدية في مواجهة النوع المستحدث يصعب من مهمة الأجهزة الأمنية في ضبط هذه الجرائم وملاحقة مرتكبيها⁽⁵⁾.

ثانيا: صعوبة إثبات الجريمة المعلوماتية والتحقيق فيها

الأصل أن الجريمة تقع في نفس مكان تنفيذ النشاط الإجرامي، إلا أن الجريمة المعلوماتية في كثير من الأحيان تقع في مكان آخر غير مكان البث، مما يؤدي إلى تأخر الجهات المختصة في اتخاذ ما يلزم من إجراءات الاستدلال والتحقيق التي تلعب الدور الأساسي في كشف الجريمة لأن سلطات مكان البث لم يصل إلى

علمها بعد وقوع الجريمة⁽⁶⁾، كما أن السلوك الإجرامي في الجرائم المعلوماتية ليس له آثار مادية، فلا توجد أدلة مادية ملموسة يمكن إدراكها بالحواس لأن الدليل في هذه الجرائم عبارة عن نبضات الكترونية غير محسوسة، مما يتطلب قدرات ودراية كافية في مجال المعلوماتية بالنسبة للمحقق حتى يتسنى له التعامل مع الأدلة والمحافظة عليها⁽⁷⁾.

كما أن الفاعل في الجرائم المعلوماتية كثيرا ما يأخذ الاحتياطات التي تحول دون الوصول إلى كشف الجريمة ومعرفة الفاعل، إذ بإمكانه تدمير دليل الإدانة في ثوان بواسطة البرامج المتخصصة، أو القيام بتشفير التعليمات مما يصعب الوصول إلى دليل يدينه، أو وضع كلمات السر ورموز تحول دون الوصول إلى الدليل⁽⁸⁾. وترجع صعوبة إثبات الجرائم المعلوماتية بالإضافة إلى ما سبق بيانه إلى الأسباب الآتية⁽⁹⁾:

- 1- نقص الخبرة الكافية لدى رجال الضبطية الذين اعتادوا التعامل مع الجرائم التقليدية.
- 2- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- 3- صعوبة معرفة الفاعل أحيانا لاستخدامه أساليب التمويه بقصد إخفاء شخصيته، أو يستخدم موقع شخص آخر أو جهة أخرى للقيام بأفعاله الإجرامية.
- 4- إشكالية القانون الواجب التطبيق والمحكمة المختصة.
- 5- إجماع الكثير من المجنى عليهم في التبليغ عن هذه الجرائم، خاصة البنوك، والشركات والمؤسسات الادخارية حتى لا يكشف عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي الأموال التي تتعامل معها، وعليه تكفي في أغلب الأحيان باتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضت له السلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.

الفرع الثاني: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي

إن رغبة الكثيرين في التعاون الدولي لأجل مكافحة الجرائم المعلوماتية تعترضه العديد من الإشكاليات والمعوقات على المستوى الدولي التي تقف دون تحقيقه، ومن أهم هذه المعوقات القصور التشريعي للدول (أولاً)، وتنوع واختلاف النظم القانونية الإجرائية (ثانياً)، وتنازع الاختصاص القضائي الدولي (ثالثاً)، والإشكاليات الخاصة بالإنباء القضائية (رابعاً)، وأخيراً الإشكالات الخاصة بتسليم المجرمين (خامساً).

أولاً: القصور التشريعي للدول

إن اختلاف الدول في موروثها الثقافي والاجتماعي ومستواها السياسي أثر بشكل مباشر على السياسة التشريعية لكل دولة، وهذا ما جعل بعض الأنظمة القانونية تشكل عائقاً كبيراً أمام التعاون الدولي، إذ إن هناك من الدول من تستشعر خطورة بعض الأفعال فتجرمها في قوانينها الداخلية، في حين أن دولاً أخرى لم تجرم هذه الأفعال مما يجعلها أفعالاً مباحة تطبيقاً لمبدأ الشرعية⁽¹⁰⁾، وهو ما ينطبق على الجرائم المعلوماتية، إذ من الدول من تدرج نصوصاً قانونية لمواجهة الآثار السلبية على هذه التقنية الحديثة والناجئة عن الاعتداءات التي تلحق المعلومات خاصة المخزنة في النظام المعلوماتي، كما أن الاطلاع على الأنظمة القانونية القائمة في العديد من الدول لمكافحة الجرائم المعلوماتية يتضح عدم وجود اتفاق بين الدول على نماذج إساءة استخدام الأنظمة المعلوماتية وشبكة الأنترنت الواجب تجريمها، أو بعبارة أخرى عدم وجود نظام قانوني موحد بين الدول خاص بمكافحة الجرائم المعلوماتية، والعلة في ذلك هو كثرة التعاريف والمفاهيم القانونية المتعلقة بالجريمة المعلوماتية⁽¹¹⁾.

ثانيا: اختلاف الأنظمة القانونية الإجرائية

ويتجلى هذا العائق في اختلاف الأنظمة القانونية الإجرائية بين الدول، ذلك أن طرق التحري والتحقيق والمحاكمة قد تثبت فعاليتها في دولة ما إلا أنها تكون عكس ذلك في دولة أخرى، أولا يسمح بإجرائها لعدم مشروعيتها في هذه الدولة، كما أن الدليل المتحصل عليه بالطرق غير المشروعة حسب قانون دولة ما لا يمكنها اعتماده كدليل إثبات حتى وإن كان قد تم الحصول عليه في اختصاص قضائي وبشكل مشروع حسب قانون الدولة الأخرى، ونذكر على سبيل المثال في هذا المجال إجراء المراقبة الالكترونية⁽¹²⁾ الذي تعتد به بعض الدول، في حين أن دولاً أخرى ترى فيه مساساً بالحياة الخاصة مما يتعين استبعاده.

ثالثا: تنازع الاختصاص القضائي الدولي

يقصد بتنازع الاختصاص القضائي بين الدول تقديم دعوى عن ذات الجريمة أو عدة جرائم مرتبطة إلى جهتين أو أكثر من جهات التحقيق أو الحكم، وتمسك كل جهة باختصاصها بالنظر أو التحقيق في الدعوى وهو ما يعرف بتنازع الاختصاص الإيجابي، أو رفض كل دولة النظر في الدعوى على أساس عدم اختصاصها وهو ما يسمى بتنازع الاختصاص السلبي، وعليه يتحقق تنازع الاختصاص الدولي في الجريمة المعلوماتية في الحالة التي يقوم فيها مثلاً أجنبي بإرسال فيروس⁽¹³⁾ إلى نظام معلوماتي لأحد أجهزة دولة ما غير التي يقيم بها، فيقوم هذا الأخير (الفيروس) بتدمير وإتلاف المعلومات الموجودة به، وهنا يقوم الاختصاص للدولة التي ارتكب على إقليمها الجريمة اعتماداً على مبدأ الإقليمية، كما يقوم الاختصاص أيضاً للدولة التابع لها الأجنبي مرتكب الجريمة استناداً لمبدأ الشخصية، وفي الأخير يقوم الاختصاص أيضاً للدولة التي هدد أمنها وسلامتها مصالحها الجوهرية بغض النظر عن مكان ارتكاب الجريمة أو جنسية الجاني وهو ما يطلق عليه مبدأ العينية، وعليه يكون التساؤل عن الدولة المختصة هل هي الدولة التي ارتكب على إقليمها الفعل الإجرامي؟ أم الدولة التي حدثت نتيجة الفعل فيها؟ أو بعبارة أخرى الدولة التي لحق الضرر مصالحها الأساسية؟ أم الدولة التي يحمل المجرم المعلوماتي جنسيتها؟

وعالج المشرع الجزائري هذه المسألة من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذ أكد في المادة 15 منه على مبدأ العينية بالإضافة إلى مبدأ الإقليمية ومبدأ الشخصية، وعليه تنص المادة 15 على أنه "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

رابعاً: الإشكالات الخاصة بالإنباء القضائية

يشير التعاون القضائي الدولي لمكافحة الجرائم المعلوماتية عن طريق الإنابة القضائية إشكاليات تتمثل أساساً في فكرة السيادة وكذلك إشكالية البطء في الإجراءات.

أ- إشكالية فكرة السيادة:

يقصد بالسيادة: "استنثار جهة الحكم في الدولة بكافة اختصاصات السلطة ومظاهرها، دون أن تخضع في ذلك لأي جهة أعلى، ودون أن تشارك معها في ذلك سلطة أوجهة ماثلة"⁽¹⁴⁾.

وتثور إشكالية فكرة السيادة في الحالة التي يرتكب فيها الجاني جرماً على إقليم دولة ما وتجري محاكمته في دولة أخرى، فحتى تقام محاكمة عادلة لا بد من جمع الأدلة التي تثبت الجريمة ويتم نسبتها للجاني، وهذا لا يتحقق

إلا على إقليم الدولة التي كانت مسرحا للجريمة وهو ما يعرف بالتعاون القضائي الدولي، إلا أن هذا التعاون يصطدم مع فكرة السيادة التي تتمسك بها الدولة على إقليمها، ومن ثم لا تسمح لدولة أخرى القيام بالإجراءات على إقليمها، وإنما تقوم بها عن طريق أجهزتها القضائية باعتبارها صاحبة الاختصاص بالفصل في كافة الجرائم المرتكبة على إقليمها اعتمادا على فكرة السيادة.

ب- إشكالية البطء في إجراءات الإنابة القضائية:

إن إرسال طلبات الإنابة القضائية بالطريق الدبلوماسي يجعلها تتسم بالبطء والتعقيد الذي يتعارض مع طبيعة وخصائص الجريمة المعلوماتية التي تتميز بالسرعة، إذ يمكن تدمير أدلة الإثبات، وهو ما انعكس سلبا على فكرة التعاون الدولي في مكافحة هذا النوع المستحدث من الجرائم، كما أن التباطؤ في الرد بسبب نقص الموظفين، أو الصعوبات اللغوية، أو الاختلاف في الأنظمة الإجرائية يحول دون تفعيل التعاون الدولي.

خامسا: الإشكاليات الخاصة بتسليم المجرمين

من بين الإشكاليات التي يثيرها تسليم المجرمين نجد إشكاليتي ازدواجية التجريم والتزام في طلبات التسليم:

أ- ازدواجية التجريم:

إن التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، إلا أنه بالرغم من أهميته فإنه يشكل عقبة أمام التعاون القضائي في مجال تسليم المجرمين بشأن الجرائم المعلوماتية، خاصة وأن معظم التشريعات قد أغفلت النص على هذا النوع من الجرائم، بالإضافة إلى ثبوت عجز مواكبة النصوص التقليدية لهذا النوع المستحدث من التجريم، وهو الأمر الذي يشكل عائقا أمام تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، وبحول دون جمع الأدلة لإدانة مرتكبي الجرائم المعلوماتية⁽¹⁵⁾.

ثانيا: التزام في طلبات التسليم

يقصد بالتزام في طلبات التسليم قيام دولتين أو عدة دول بتقديم طلب تسليم عن نفس الشخص، سواء كان الطلب متعلقا بذات الجريمة أو بجرائم مختلفة، وتتحقق هذه الإشكالية في الجرائم المعلوماتية عندما يرتكب الجاني الفعل الإجرامي الذي يمس في ذات الوقت مصالح أساسية لأكثر من دولة، وعليه فكل دولة لحقها ضرر جراء النشاط الإجرامي الذي قام به الجاني يمكنها تقديم طلب التسليم إلى الدولة المطلوب منها.

والجدير بالذكر أن طلب التسليم لا بد أن يكون مبنيا على أدلة تثبت قيام الجاني بالأفعال المنسوبة إليه، وليس مجرد ادعاء من الدولة الطالبة، كما يشترط أن يكون إرسال الطلب بصورة فعلية وليس مجرد تصريحات شفوية، أو إبداء الرغبة في استلام الشخص⁽¹⁶⁾.

ولا يشترط أن تكون طلبات التسليم قد وردت إلى الدولة المطلوب منها في ذات الوقت، بل يكفي أن تكون طلبات التسليم قد وردت إلى الدولة المطلوب منها تسليم شخص في الوقت الذي مازال فيه المطلوب على إقليمها، ولم يتم تسليمه بعد لأي دولة من الدول التي تطالب به⁽¹⁷⁾.

المطلب الثاني: آليات التغلب على إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية

بعد التطرق لأهم العقبات والإشكاليات التي تعترض التعاون الدولي في مكافحة الجرائم المعلوماتية، لا بد من معرفة ما هي الحلول والآليات التي يتعين اتخاذها لأجل التغلب على هذه الإشكاليات، أو على الأقل التقليل منها، وهو ما نتطرق له في فرعين نتناول في الأول آليات التغلب على إشكاليات التعاون الدولي على المستوى

الوطني، أما الفرع الثاني فنعرض فيه لآليات أو تدابير التغلب على إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي.

الفرع الأول: آليات التغلب على صعوبات التعاون الدولي على المستوى الوطني

تتجلى أهم إجراءات وآليات التغلب على إشكالية التعاون الدولي لمكافحة الجرائم المعلوماتية على المستوى الوطني في ضرورة اتخاذ الدولة لتدابير موضوعية وأخرى إجرائية على النحو الآتي:

أولاً: التدابير الموضوعية

يتعين على كل دولة أن تتبنى في تشريعاتها الداخلية أحكاماً موضوعية تتلاءم مع الطبيعة الخاصة للجرائم المعلوماتية، واستبعاد تطبيق النصوص القانونية التقليدية التي ثبت عجزها في مواكبة أو مواجهة هذا النوع المستحدث من الجرائم، ذلك أن التطور التقني الذي نعيشه والذكاء الذي يتمتع به مرتكبو هذا النوع من الجرائم يؤكد بأننا نواجه العديد من الجرائم شديدة التعقيد والتطور لا تجد لها محلاً في النصوص القانونية التقليدية، كما أن التفسير الضيق لنصوص قانون العقوبات لا يجيز القياس.

والجدير بالذكر أن الأمر لا يتوقف عند استحداث نصوص قانونية قادرة على مواجهة الجرائم المعلوماتية فحسب، بل الأمر يتطلب ضرورة التدخل وتعديل النصوص القانونية المتعلقة بمحل الجرائم ذات الطابع المادي الذي لا يتلاءم ومحل الجرائم المعلوماتية ذي الطبيعة المعنوية غير الملموسة، ومن ثم استيعاب كل تطور يحدث في المستقبل لأجل القضاء على إشكاليات التعاون القضائي.

وبالرجوع للتدابير الموضوعية المتخذة من طرف المشرع الجزائري نجد أن هذا الأخير قد خطى خطوة إيجابية في هذا المجال، إذ إنه وبموجب تعديل قانون العقوبات بالقانون رقم 15/04⁽¹⁸⁾ قام بتنظيم مجموعة من الجرائم المستحدثة المتعلقة بسرقة المعلومات وسلامتها وكذلك مساءلة الأشخاص المعنوية، إلا أن ذلك لا يمنع من القول إن المشرع قد أغفل العديد من جرائم التقنية الحديثة، ومن أمثلتها جريمة الاعتراض غير القانوني للمعلومات، وكذلك جريمة التزوير المعلوماتي التي بقيت خاضعة للنصوص التقليدية التي لا تتلاءم مع الطبيعة الخاصة لهذه الجريمة بالرغم من تصديق الجزائر بموجب المرسوم الرئاسي رقم 252/14⁽¹⁹⁾ على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي نصت في مادتها العاشرة على التزوير المعلوماتي وحثت من خلال المادة الخامسة على ضرورة تناول الدول الأطراف للجرائم المنصوص عليها في قوانينها الداخلية.

ثانياً: التدابير الإجرائية

بالإضافة إلى التدابير الموضوعية ولأجل التغلب على إشكالات التعاون الدولي على المستوى الوطني لابد من اتخاذ تدابير إجرائية⁽²⁰⁾ ولذا عملت معظم الدول على تجسيد أغلبها في قوانينها الداخلية، ومنها المشرع الجزائري من خلال القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتتمثل هذه التدابير الإجرائية التي أقرها المشرع والتي يستوجب على باقي الدول إعمالها في قوانينها الداخلية فيما يأتي:

1- استحداث نصوص قانونية تسمح بتفتيش نظم وشبكات الحاسوب أو أجزائها، وفحص البيانات الموجودة بها والمخزنة على مختلف وسائط التخزين سواء كانت داخل الدولة أو خارجها طالما أنها تفيد التحقيق في الجريمة، وهو ما تناوله المشرع الجزائري من خلال المادة 5 من القانون رقم 04/09 التي تنص على أنه: "يجوز للسلطات

القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش، ولو كان عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك.

إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل".

2- استحداث نصوص إجرائية قانونية تخول للسلطات المختصة ضبط وإحضار الأشخاص مرتكبي الجرائم المعلوماتية، سواء كانوا متواجدين على إقليمها أو في مكان آخر، طالما أنه تقع تحت أيديهم بيانات مخزنة في أنظمة معلوماتية أوفي وسائط التخزين الأخرى، وعلى كل الدول أن تتعاون فيما بينها لأجل تسهيل كل ما يرتبط بتسليم المجرمين وتبادل المعلومات، وهو ما عمدت إليه الدولة الجزائرية في إبرام العديد من الاتفاقيات الثنائية المرتبطة بذلك.

3- ضرورة تدعيم وتفعيل التعاون بين أجهزة الشرطة ورجال العدالة في الدول المختلفة في مجال التدريب، وهو ما تسعى له الدولة الجزائرية بالنظر إلى التحاقها الجديد في استخدام التكنولوجيا الحديثة، ونقص كفاءة القائمين على التحري والتحقيق والمحاكمة في الجرائم المعلوماتية، إذ تعمل الدولة باستمرار على إرسال رجال العدالة للتكوين في مجال التحقيق والبحث والمحاكمة بشأن الجرائم المعلوماتية إلى دول مختلفة كفرنسا مثلاً، أو دعوة مختصين في مجال التحري والتحقيق بهذا النوع المستحدث من الجرائم لإجراء دورات تكوينية لرجال العدالة الجزائريين، وما يؤكد ضرورة هذا الإجراء هو إبرام الجزائر للاتفاقيات الثنائية منها الاتفاقية بين الجزائر والولايات المتحدة الأمريكية أثناء زيارة وزير العدل الأمريكي للجزائر في أبريل 2010 والتي تهدف إلى تحسين التعاون في مجال مكافحة الجرائم والتبادل الجيد للأدلة التي تمكن المسؤولين في كلا البلدين من استعمالها في سياق التحقيق ومحاكمة مرتكبيها⁽²¹⁾.

كما أن الاتفاقيات المبرمة في هذا المجال حثت الدول المشاركة على ضرورة إنشاء هيئة على مستوى الدولة تقوم بتلقي الشكاوى والبلاغات المتعلقة بالجرائم المعلوماتية، كما توكل لها مهمة اتخاذ التدابير الأمنية الوقائية لأجل الحد من تنامي هذه الظاهرة الإجرامية المرتبطة بالتقنية الحديثة، كما يتعين على المصالح المختصة لكل دولة تكتشف ارتكاب جريمة على شبكة الانترنت أضرت بدولة أخرى إعلام هذه الأخيرة بالجريمة، وهو ما تناوله المشرع الجزائري في المادة 13 وحدد مهام هذه الهيئة من خلال المادة 14 من القانون 04/09 إذ تنص المادة 13 على أنه "تتأسس هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته".

4- تحديد كل دولة لاختصاصها الإقليمي بالنسبة للجرائم المعلوماتية في قوانينها الداخلية، وهو ما أقره المشرع الجزائري من خلال المادة 16 من قانون الإجراءات الجزائية التي تنص على تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاقبة الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات إلى كامل التراب الوطني.

5- على كل دولة أن تتخذ التدابير الإجرائية التشريعية لتمكين الدولة من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد أنظمة الحاسوب بما يفيد التحقيق خاصة في الحالة التي تكون هذه البيانات معرضة للمحو والتعديل والإزالة، وهو الإجراء الذي نص عليه المشرع الجزائري بموجب المادتين 6 و 7 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وإن كانت هذه هي التدابير الإجرائية التي عمل المشرع الجزائري على النص عليها في القانون 04/09 إلا أنها لا تعد كافية في مواجهة الجرائم المعلوماتية التي تتطلب تدابير إجرائية أخرى يتعين على المشرع إعمالها حتى تكون أكثر فعالية ومنها إضفاء صفة الضبطية القضائية على العاملين في مجال المعلوماتية من غير رجال الشرطة، كمزودي خدمات الأنترنت استنادا لمهامهم المتمثلة في القيام بالرقابة عبر المزود على سير حركة العمل ومدى الالتزام والخضوع للقانون من طرف المتعاملين والعاملين في شبكة الأنترنت، لأندور همفي الأصل يقتصر في حالة اكتشاف الجريمة على حفظ أدلة إثبات الجريمة دون اتخاذ أي إجراء آخر إلى حين وصول رجال الضبطية القضائية الذين حددتهم المادة 4 من الأمر 02/15⁽²²⁾ المعدل والمتمم لقانون الإجراءات الجزائية والذين لا يملكون من المهارة والدراسة الكافية بالتقدم التكنولوجي الحاصل، وإن كان المشرع الجزائري قد أجاز الاستعانة بأصحاب الخبرة بإعداد مسودة بشأن تفتيش المنظومة المعلوماتية.

الفرع الثاني: آليات التغلب على إشكاليات التعاون الدولي على المستوى الدولي

لقد تعددت الإشكاليات التي تعترض التعاون الدولي على المستوى الدولي، إلا أن هناك من التدابير والآليات التي حاولت التخلص والقضاء على هذه الإشكاليات، وعليه سنتناولها على النحو الآتي:

أولاً: آلية التغلب على إشكالية القصور التشريعي للدول

إن اختلاف الأنظمة القانونية بين الدول جعل ضرورة التغلب عليه عن طريق توحيد الأنظمة القانونية المنظمة للأنشطة الإجرامية المتعلقة بالجرائم المعلوماتية، ويتحقق توحيد الأنظمة القانونية عن طريق تحديث التشريعات الوطنية الداخلية للدول المعنية بالجرائم المعلوماتية، وإبرام اتفاقيات خاصة في هذا النوع من الجرائم، لذا يجب على جميع الدول أن تعدل نصوصها القانونية وتجعلها تتلاءم مع الجرائم المستحدثة، أو استحداث نصوص قانونية لأجل تفعيل المواجهة القانونية لهذه الجرائم⁽²³⁾.

وترتيباً على ذلك يرى الخبراء في مجال الجرائم المعلوماتية أن الطابع الدولي لمتطلبات فضاء الأنترنت الذي أطلق عليه طريق البيانات السريع⁽²⁴⁾ يتطلب تطوير استراتيجيات جديدة من أجل مكافحة النشاط الإجرامي، ذلك أن الجريمة العابرة للحدود عبر الأنترنت تتطور وتتزايد بسرعة، والعلة في ذلك هو اختلاف النظم القانونية والقيم لكل دولة، والحل الأمثل هو تنظيم الجانب التشريعي للجرائم المعلوماتية في صورة اتفاقية دولية.

والجدير بالذكر أن التشريعات الغربية خطت خطوات هامة في مجال مكافحة الجريمة المعلوماتية عن طريق إنشاء منظمات دولية وإقليمية، خاصة المنظمات والهيئات الإقليمية الأوروبية، مع سعي الدول الغربية إلى استحداث نصوص خاصة على المستوى الداخلي أو العمل على تعديل القوانين الداخلية لأجل توفير حماية أكثر

فعالية، أما على المستوى العربي فإن معظم الدول العربية تعد متأخرة في مواكبة المستجدات التشريعية العالمية، والعلة في ذلك هو التأخر التقني في مجال المعلوماتية لهذه الدول⁽²⁵⁾.

وتتجسد أبرز الجهود العربية المبذولة في مكافحة الجريمة المعلوماتية - كآلية للتغلب على القصور التشريعي في مجال مكافحة الجرائم المعلوماتية- في القانون الجزائري العربي الموحد الذي اعتمده وزراء العدل العرب بموجب القرار رقم 225 لسنة 1996⁽²⁶⁾.

أما على المستوى الإفريقي وبجهود من الدولة الجزائرية في مكافحة الجرائم العابرة للحدود ومنها الجريمة المعلوماتية تم إنشاء هيئة جديدة أطلق عليها "الأفريبول" لأجل تفعيل التعاون بين مختلف أجهزة الشرطة على مستوى القارة الإفريقية في مكافحة الجريمة الدولية والتي يوجد مقرها بالجزائر العاصمة، كما حددت المادة 4 من النظام الأساسي مهام الأفريبول.

ثانياً: آلية التغلب على إشكالية اختلاف النظم القانونية الإجرائية

لقد شجعت المواثيق الدولية الصادرة عن الأمم المتحدة الدول الأطراف لأجل السماح باستخدام بعض تقنيات التحقيقات الخاصة، الشيء الذي يترتب عليه التخفيف من الاختلاف في الأنظمة القانونية الإجرائية ويفتح المجال أمام تعاون دولي فعال.

وترتبط لذلك فإن العديد من الاتفاقيات الدولية التي أبرمت في مجال التعاون الدولي قربت بين القوانين الجنائية الداخلية للدول لأجل مكافحة الجريمة العابرة للحدود، ويتجسد هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة والاعتراف بالأحكام الجنائية الأجنبية⁽²⁷⁾، أما الاتفاقية الأوربية للإجرام المعلوماتي (اتفاقية بودابست) فنصت في المادة 29 بالتحفظ العاجل على البيانات المعلوماتية المخزنة في نظام معلوماتي يوجد داخل أراضي طرف آخر حتى لا يتم تغيير هذه البيانات أو نقلها أو حذفها، خلال الفترة اللازمة لإعداد ونقل وتنفيذ المساعدة المتبادلة بخصوص الحصول على هذه البيانات بسهولة محوها وتدمير أدلة الإدانة، كما أكدت ذات المادة على إمكانية التفتيش أو الدخول بإحدى الطرق أو الوسائل الإلكترونية لأجل الوصول أو الكشف عن البيانات المشار إليها.

أما المادة 31 من هذه الاتفاقية فتضمنت إمكانية الولوج إلى البيانات والمعلومات المحفوظة في النظام المعلوماتي عن طريق السماح للدولة الطالبة للقيام بالتفتيش والدخول بطريقة مشابهة وضبط أو الحصول بطريقة مماثلة على البيانات والمعلومات المخزنة بواسطة شبكة المعلومات داخل النطاق المكاني للدولة المطلوب منها المساعدة، ويجب الاستجابة على وجه السرعة لهذا الطلب إذا ما كانت هناك أسباب تدعو للاعتقاد بأن المعلومات والبيانات المعنية عرضة لمخاطر المحو والفق أو التعديل، وكذلك الحالة التي توجد فيها اتفاقيات أو معاهدات تنص على التعاون الفوري.

وفي الأخير فإن المادة 35 تناولت إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة والتي يطلق عليها الشبكة 24/7 بمعنى تلك الشبكة التي تعمل على مدار 24 ساعة يوميا بمعدل سبع أيام في الأسبوع، بغرض التأكد من توفير المساعدة الفورية لإجراء التحقيقات المتعلقة بالجرائم المرتبطة بنظام وبيانات معلوماتية، أو لتجميع أدلة ذات شكل إلكتروني لجريمة ما، وهذه المساعدة يجب أن تكون مشتملة على تسهيل، وتعتبر هذه الوسائل من أفضل آليات التغلب على التحديات الكبيرة التي يفرضها عصر المعلوماتية على السلطات المناط بها تنفيذ القانون⁽²⁸⁾.

ثالثا: آلية التغلب على إشكالية تنازع الاختصاص القضائي الدولي

إن حل إشكالية تنازع الاختصاص يكمن في اعتبار الجرائم المعلوماتية من الجرائم العالمية، أين يرجع فيها الاختصاص القضائي لكل دولة تنص قوانينها الداخلية على هذه الجرائم اعتمادا على مبدأ العالمية، الذي مفاده سريان قانون عقوبات الدولة بغض النظر عن مكان ارتكاب الجريمة أو جنسية مرتكبها، ودون النظر فيما إذا كان القانون الأجنبي يعتد بها كجريمة أم لا.

ويهدف مبدأ العالمية إلى التصدي لتنامي الظاهرة الإجرامية ذات الأبعاد الدولية، من خلال تجاوز القيود التي يفرضها مبدأ الإقليمية، كما يؤسس هذا المبدأ لفكرة التضامن بين الدول في مكافحة الجرائم المعلوماتية لأن التدخل الدولي وفقا لهذا المبدأ يحقق معاقبة الجناة وعدم إفلاتهم وضمان محاكمتهم بغض النظر عن جنسيتهم أو جنسية ضحاياهم⁽²⁹⁾.

وترتبيا على ذلك فإن مبدأ العالمية أصبح ضروريا لأجل تفعيل مكافحة هذا النوع المستحدث من الجرائم مما يتعين على المشرع الجزائري تبنيه في النصوص القانونية الوطنية حتى يكون هناك تضيق الخناق على مرتكب الجرائم المعلوماتية، بالإضافة إلى مبدأ العينية الذي تبناه بموجب المادة 15 من القانون 04/09 مسايرة منه لما جاء به القانون العربي النموذجي بشأن مكافحة جرائم الكمبيوتر والانترنت، ومسألة تنازع الاختصاص القضائي الدولي إذ نصت المادة 22 من الباب الرابع على أنه "تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بنظر الدعوى المترتبة على تلك الجرائم، وعلى الدول العربية عقد اتفاقيات لتبني المعيار الأولى بالإتباع في حالة تنازع الاختصاص بين الدول.

كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات"⁽³⁰⁾.

واعتمادا على هذا النص فهناك مسألتان يمكن إثارتها وهما القانون الواجب التطبيق والمحكمة المختصة.

1- القانون الواجب التطبيق:

أخذ القانون النموذجي العربي بشأن مكافحة جرائم الكمبيوتر والانترنت من خلال الفقرة الأولى من المادة 22 بمبدأ الإقليمية الذي قرره المشرع الجزائري في المادة 03 من قانون العقوبات، والذي يجعل الاختصاص للقانون الوطني على كافة الجرائم المرتكبة على إقليم الدولة بغض النظر عن جنسية مرتكبها سواء كان وطنيا أو أجنبيا، وبغض النظر عن المصلحة التي تم الاعتداء عليها سواء كانت تخص الدولة ذاتها أو أي دولة أجنبية، وهذا المبدأ يعتبر مظهرا من مظاهر ممارسة الدولة لسيادتها على إقليمها، كما أن لهذا المبدأ فائدة للقضاة والمتهم، فالمتهم من مصلحته أن يحاكم وفقا لقانون الدولة التي ارتكبت على إقليمها الجريمة أين توجد أدلة الإثبات والشهود، كما أن القضاة في هذه الحالة يطبقون قانون دولتهم الذي هم على دراية كافية به.

ويعد مبدأ الإقليمية هو المبدأ الأصلي أو العام في حالة سكوت القانون الجنائي لدولة ما بالنص عليه، لأن باقي المبادئ الأخرى كمبدأ الشخصية ومبدأ العينية ومبدأ العالمية، ما هي إلا مبادئ استثنائية وقواعد احتياطية لا يؤخذ بها إلا في حالة النص عليها صراحة.

وترتيباً على ما سبق فإن القانون الوطني يطبق على الجرائم المعلوماتية إذا وقع عنصر من العناصر المكونة للجريمة، أو حتى وقوع النتيجة على الإقليم، وعليه فإن القانون الوطني يطبق على الرسائل ذات الطابع الإجرامي أو الصور الإباحية التي تنشر عبر شبكات الانترنت بصرف النظر عن الدولة التي صدرت منها الرسالة.

2- المحكمة المختصة:

وفقاً لنص المادة 22 من القانون النموذجي العربي فإن الاختصاص بالنظر في الجرائم المعلوماتية للمحاكم الوطنية أياً كان نوع هذه الجرائم قد وقع على شبكة معلوماتية داخلية أو عن طريق شبكة الانترنت، وسواء كان ذلك داخل الدولة أو خارجها شريطة أن يكون القانون الوطني صالحاً للتطبيق عليها، كما أن ذات المادة دعت إلى ضرورة عقد اتفاقيات لتبني معيار الإقليمية في حالة تنازع الاختصاص بين الدول.

رابعاً: آلية التغلب على الإشكاليات الخاصة بالإنباء القضائية الدولية

تمثل فكرة السيادة - كما سبق القول - إحدى العقبات التي تحول دون تجسيد فكرة التعاون الدولي مما تسهل في هروب المجرمين من العدالة، وتهريب الأموال المتحصل عليها من الجرائم، وهو ما يجعل الضرر الناتج يلحق بكافة الدول دون استثناء، وهو ما جعل الدول تتخلى عن التمسك بالسيادة المطلقة وقبلت بوضع قيود على سيادتها لتحقيق مصلحة المجتمع الدولي⁽³¹⁾.

وإذا كان إجراء الإنابة القضائية الدولية هو الوسيلة التي تتحقق بها مصالح المجتمع الدولي في ملاحقة المجرمين ومكافحة الجريمة دون الإخلال بسيادة الدول، كانت ضرورة حتمية لأجل التخلص من العقبات المادية والقانونية الناتجة عن عجز الدول عن اتخاذ أي إجراء من الإجراءات اللازمة لكشف الحقيقة خارج حدود إقليمها. وعليه فإن الإنابة القضائية الدولية تساعد في التغلب على تلك العقبات، إذ تقوم الدولة المطلوب منها اتخاذ الإجراء على إقليمها وعن طريق سلطاتها القضائية نيابة عن الدولة التي انعقد لها الاختصاص.

وإذا كانت الإنابة القضائية تخفف نوعاً ما من فكرة السيادة إلا أنها قد تقف عقبة أمام جدية التحقيق وكشف الجريمة، لأنه قد تكون التقنيات المستعملة من طرف الدولة المطلوب منها القيام بالإجراء غير مجدية في التحقيق، في حين أن الدولة الطالبة لها من التقنيات المتطورة التي تمكنها من الوصول إلى كشف الحقيقة، وللتغلب على هذا الإشكال فإن الاتفاقيات الدولية وكذلك القوانين الداخلية لبعض الدول أجازت ما يعرف بالتفتيش أو التحقيق عن بعد كما سبق بيانه، وهو ما فعله المشرع الجزائري من خلال المادة 05 من القانون 04/09.

أما العقبة الثانية التي سبقت الإشارة إليها والتي تحول دون تحقيق فعال للتعاون القضائي فتتمثل في بطء الإجراءات، والتي نصت الاتفاقيات الدولية على الاتصال المباشر بين السلطتين القضائيتين للدولتين الطالبة والمطلوب منها، ويعد هذا الطريق الأكثر اختصاراً وسرعة ومرونة والذي يتماشى وحالة الضرورة والاستعجال، لأن سلوك الطريق الدبلوماسي يترتب عنه كثرة الشكليات والعقبات التي تنسم بالبطء والتي قد تؤدي إلى فقدان الدليل وفوات الوقت وهو ما يتعارض مع الجرائم المعلوماتية التي تتميز بسرعة عبور وتبادل المعلومات من خلال الشبكة، كما أن الجرائم المرتبطة بالانترنت تقتضي وتتطلب ردوداً سريعة خشية التلاعب بالبيانات التي قد تشكل دليلاً ضد المتهم⁽³²⁾.

خامساً: آلية التغلب على الإشكاليات الخاصة بتسليم المجرمين

أسلفنا القول أن تسليم المجرمين يثير إشكاليتين تتمثل الأولى في ازدواجية التجريم، أما الإشكالية الثانية فتتعلق بالتزام في طلبات التسليم، وعليه ما هي الآليات المتخذة أو الواجب اتخاذها لأجل التغلب على هذه الإشكاليتين؟

1- آلية التغلب على ازدواجية التجريم:

لقد نصت المادة 24 فقرة الأولى من اتفاقية بودابست على تبادل المجرمين بالنسبة للجرائم المحددة في ذات المادة شريطة أن تكون معاقبا عليها في قانون الطرفين بعقوبة سالبة للحرية، وعليه فإن الاتفاقية نصت صراحة على شرط ازدواجية التجريم، وهو ما ترتب عنه العديد من الإشكاليات فيما يتعلق بالجرائم المعلوماتية لأن هناك من الدول من لم تستحدث نصوص قانونية تعمل على ردع مرتكب هذا النوع من الجرائم، كما أنها لم تقم بتعديل النصوص التقليدية، وبالتالي يستبعد تطبيق هذا النص بشأنها.

إلا أن هناك من الاتفاقيات التي حاولت إيجاد مخرج لهذا الإشكال بالقول إن انضمام وتصديق دولة ما لاتفاقية تنظم جرائم معينة يعتبر في حد ذاته تجريما من طرفها لهذه الأفعال حتى ولو لم تنص على ذلك في قوانينها الداخلية، ومن هذه الاتفاقيات اتفاقية الأمم المتحدة لمكافحة الفساد⁽³³⁾.

أما الاتجاهات التشريعية فمن الضروري أن تركز على تخفيف التطبيق الصارم لهذا الشرط وذلك من خلال تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية، وإبرام اتفاقات خاصة تراعي هذا النوع من الجرائم.

2- آلية التغلب على إشكالية التزام في طلبات التسليم:

إن إشكالية التزام طلبات التسليم لم يستقر بشأنها الاتجاه الدولي على ترتيب معين، فظهرت العديد من الاختلافات في ترتيب هذه الأولويات، بل إن هذا الاختلاف موجود على مستوى الدولة الواحدة في إبرامها للاتفاقيات مع مختلف الدول والعلّة في ذلك هو اختلاف مصالح الدولة مع باقي الدول.

ويظهر من خلال المادة 13 من اتفاقية الجامعة العربية الخاصة بالتسليم أن واضعي هذه الأخيرة أعطوا الأولوية لجسامة الفعل أو الجرم، إذ نصت المادة على أنه "إذا قدمت إلى الدولة المطلوب إليها عدة طلبات من دول مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية في التسليم للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أراضيها، ثم للدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم بجرائم مختلفة فتكون الأولوية للدولة التي طلبت التسليم قبل غيرها"، ويعتبر هذا الترتيب الذي جاءت به الاتفاقية ترتيبا منطقيا⁽³⁴⁾، وهو ما اتبعه المشرع الجزائري من خلال المادة 699 من قانون الإجراءات الجزائية⁽³⁵⁾.

وفي هذا المطاف يتعين إثارة الحالة التي سكتت عنها الاتفاقيات الدولية والمتمثلة في ارتكاب المطلوب تسليمه إحدى الجرائم المعلوماتية المضرة بالدولة طالبة، في حين أنه محل اتهام أو صدر حكم في حقه بالدولة المطلوب منها التسليم، وتزداد الأهمية في الحالة التي تكون فيها الجريمة الثانية أشد خطورة من الجريمة المعلوماتية المطلوب تسليمه لأجلها.

فالحل في هذه الحالة يرى البعض تطبيق مبدأ الإقليمية ومحاكمة الشخص المطلوب على الجريمة التي وقعت منه وتوقيع العقوبة عليه أولا، مع إخطار الدولة طالبة بذلك التي يمكنها إعادة تقديم طلب التسليم بعد تنفيذ العقوبة، أما إذا كانت الجريمة التي وقعت من الشخص المطلوب تسليمه من الجرائم البسيطة أو التافهة التي يكون الهدف منها إعاقة إجراء التسليم إلى الدولة طالبة، وجب على دولة المرور إجراء تسليم الشخص المطلوب إلى الدولة طالبة مع أخذ التعهد عليها بإعادته لأجل محاكمته على الجريمة المرتكبة على إقليمها، وعليه يستوجب على الاتفاقيات المبرمة بين الدول وضع حلول لمثل هذه الحالات⁽³⁶⁾.

خاتمة

إن الإيجابيات التي نتجت عن التكنولوجيا الحديثة والمتمثلة أساسا في تقريب المسافات بين الشعوب وسهولة الاطلاع على المعلومات بكل وفرة عن طريق وسائل الاتصال الالكترونية زادت من إقبال الأفراد والمؤسسات على شبكة الانترنت، إلا أنه في المقابل أنتجت العديد من السلبيات لعل أهمها صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل التقنية السهلة الاستعمال من طرف أشخاص يعرفون بقرصنة شبكة الانترنت، الذين لم تعد الحدود الجغرافية حاجزا أمامهم في ارتكاب أنشطتهم الإجرامية وهو ما أكد حتمية تضافر الجهود الدولية في مواجهة هذا النوع المستحدث من الجرائم الذي غير الكثير من المفاهيم التقليدية التي كانت تقوم عليها المسائل القانونية المسلم بها.

إلا أن خصوصية الجريمة المعلوماتية ومميزاتها جعلت منها خطرا يهدد الاستقرار الدولي والأمن الداخلي للدول، وعليه أصبحت محل اهتمام الهيئات الدولية والمجتمع الدولي لأن عالمية الإجرام تتطلب عالمية المواجهة، غير أن المواجهة الدولية للجريمة المعلوماتية اعترضتها صعوبات وعراقيل حالت دون تفعيل التعاون الدولي في مواجهتها، مما استوجب وضع واقتراح حلول تساعد في التغلب على هذه العراقيل سواء كانت على المستوى الوطني خاصة بالنسبة للدول التي كان استخدامها للتقنية الحديثة متأخرا دون وضع منظومة قانونية قادرة على مواجهة الجريمة المعلوماتية، أو على المستوى الدولي خاصة أمام التفاوت التكنولوجي والتقني بين الدول.

ويحاول المشرع الجزائري دوما مواكبة التطور التكنولوجي الحاصل وفي المقابل سن القوانين القادرة على مواجهة هذا النوع المستحدث من الجرائم، والعمل على تفعيل التعاون الدولي للحد من انتشار الجريمة بجميع أشكالها ومنها الجريمة المعلوماتية التي تأكدت خطورتها وجسامة أضرارها.

وبناء على ما تقدم تم التوصل في هذه الدراسة إلى النتائج والاقتراحات الآتية:

نتائج:

- إن التطور التكنولوجي والذي صاحبه التطور في ظاهرة الجريمة وأساليب ارتكابها أقم حتمية التعاون الدولي لأجل مكافحة الجريمة بكل أنواعها وصورها، خاصة وأن الجرائم المعلوماتية هي جرائم عابرة للحدود.
- تحتاج كل دولة مهما بلغت درجة تقدمها وقوتها الدخول في علاقات تعاون متبادلة مع غيرها من الدول، خاصة أن الوسائل والإمكانيات الداخلية لم تعد كافية في مكافحة الجرائم المعلوماتية، وملاحقة مرتكبها بسبب التقدم التكنولوجي.

- إن التعاون الدولي تعثره العديد من الإشكاليات والعقبات سواء على المستوى الوطني - أهمها عدم كفاية وملائمة القوانين القائمة، وصعوبة إثبات الجرائم المعلوماتية- أو المستوى الدولي - أهمها القصور التشريعي للدول، وتنوع الأنظمة القانونية الإجرائية، وتنازع الاختصاص القضائي الدولي، والإنابة القضائية وتسليم المجرمين التي تقوم على شرط ازدواجية التجريم - والتي يتعين التغلب والقضاء عليها ببذل المزيد من الجهد.

اقتراحات:

لأجل التغلب على الإشكاليات التي تعترض التعاون الدولي في مكافحة الجريمة المعلوماتية يتعين اتخاذ بعض التدابير سواء على المستوى الوطني أو على المستوى الدولي

على المستوى الداخلي:

- يجب على كل دولة أن تدرج في قوانينها كل ما يعتبر إتلافا للمعلومات عن طريق المحو أو التعديل أو الإدخال جرائم معاقب عليها قانونا.
- دعوة السلطات الجزائرية إلى إنشاء مواقع إلكترونية مخصصة للتبليغ عن جرائم تقنية المعلومات بصفة عامة وإرسالها للجهات المختصة وهو ما يصطلح "التبليغ الرقمي" وهو ما انتهجته الدولة الفرنسية مثلا، خاصة أمام إجماع الضحايا عن التبليغ.
- العمل على استخدام الاتصال المرئي المسموع في مباشرة إجراءات التحقيق للتغلب على إشكالية الإنابة القضائية وبطء إجراءاتها.

على المستوى الدولي:

- تفعيل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المنوط بها مكافحة الجرائم المعلوماتية باعتبارها من الوسائل التي تعمل على مكافحتها والإقلال منها، إذ يتعذر ويستحيل على الدولة وحدها القضاء على الجرائم العابرة للحدود، بسبب عدم إمكانية ملاحقة المجرمين على إقليم دولة أخرى.
- تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على اتفاقيات دولية، بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم المعلوماتية قد تم ممارستها عبر شبكة الانترنت من خلال موقع موجود في الخارج فإنها تقوم بالإبلاغ عن هذه الجريمة إلى السلطات المختصة بالدولة التي تم فيها البث.
- حبذا لو يوجد تنسيق وتصور شامل لمفهوم الجريمة المعلوماتية بين الدول من أجل تحديد الأفعال التي تشكل جريمة معلوماتية، ويتحقق ذلك بإنشاء معاهدة دولية ملزمة للدول.
- لأجل التغلب على إشكالية القصور التشريعي يتعين على الدول التي لم تنظم هذا النوع من الجرائم في قوانينها الانضمام إلى الاتفاقيات الدولية مع إدخال هذه الأخيرة حيز التنفيذ الفعلي.
- لأجل التغلب على إشكالية التنازع القضائي الدولي يتعين اعتبار الجرائم المعلوماتية تدخل ضمن الاختصاص القضائي العالمي والذي مفاده إعطاء الحق لكل دولة في ملاحقة مرتكبي الجرائم المعلوماتية بغض النظر عن جنسية مرتكبها أو مكان ارتكابها.
- إبرام اتفاقيات دولية تتضمن وضع ضوابط موضوعية ومجردة وبعيدة عن مصالح أي دولة لأجل تسليم المجرمين تغلب فيها مصلحة المجتمع الدولي كأن تكون الأولوية للدولة التي مست مصالحها الأساسية ثم تليها الدولة التي ارتكبت على إقليمها الجريمة المعلوماتية، وفي الأخير الدولة التي يحمل المجرم المعلوماتي جنسيتها.

الهوامش:

- 1- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة والوراقة الوطنية، المغرب، 2011، ص 229.
- 2- مصطفى عبد القادر، الشرطة الوطنية ومكافحة الجريمة الإلكترونية، مركز البحوث القانونية والقضائية، ملتقى دولي حول محاربة الجريمة المعلوماتية المنعقد بالجزائر العاصمة يومي 5، 6 ماي 2010، ص 128.
- 3- القانون رقم (04/09) المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 بتاريخ 16 غشت 2009.
- 4- أيمن عبد الله فكري، جرائم نظم المعلومات - دراسة مقارنة -، دار الجامعة الجديدة، مصر، 2007، ص 376.
- 5- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، 2007، ص 40. وما بعدها.

- 6- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، مصر، 2010، ص 221.
- 7- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية، وسبل التغلب عليها، دار الجامعة الجديدة، مصر، 2015، ص 54.
- 8- غنام محمد غنام، مرجع سابق، ص 220.
- 9- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 55.
- 10- غنام محمد غنام، مرجع سابق، ص 224.
- 11- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2008، ص 102.
- 12- يقصد بالمراقبة الالكترونية "العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا، أو شيئا طبيعته مرتبطة بالزمن لتحقيق غرض أمني أو لأي غرض آخر" انظر، نبيلة هبة هروال، مرجع سابق، ص 198.
- 13- يعرف الفيروس بأنه: "البرنامج أو التعليمات البرمجية الخبيثة التي تكون عادة مدرجة في ملف، وتستعمل وتخزن في نظام التشغيل دون علم المستخدم، وتنفذ ذاتيا في وقت محدد أو عند انطلاق البرمجيات، وتهدف إلى جعل النظام خارج الخدمة وتدمير ملفات أساسية أو شل موارد الجهاز"، انظر:
- (R) Boos, (La lutte contre la cybercriminalité au regard de l'action des états), Thèse de doctorat en droit privé et sciences criminelles, faculté de droit sciences économiques et gestion, université de Lorraine, soutenue le 09-12-2016, P.25 disponible sur le site: <https://tel.archives-ouvertes.fr/tel-01470150/document>, تاريخ الاطلاع: 2018/04/28 على الساعة: 17.30
- 14- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 62.
- 15- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، مصر، 2001، ص 72.
- 16- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 65.
- 17- عادل عبد العال إبراهيم خراشي، المرجع نفسه، ص 65.
- 18- القانون رقم (15/04) المؤرخ في 10 نوفمبر 2004 يعدل ويتم الأمر 156/66 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 المؤرخة في 10 نوفمبر 2010.
- 19- المرسوم الرئاسي رقم 252/14 مؤرخ في 13 ذي القعدة 1435 الموافق 8 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، جريدة رسمية رقم 57 بتاريخ 28 سبتمبر 2014.
- 20- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 70. وما بعدها.
- 21- ورشة حول الجريمة المعلوماتية وأمن المعلومات، الاستخبارات الأمريكية تدرب قضاة وضباط على محاربة جرائم الانترنت 2010/11/15 على الموقع www.algeriachannel.net تاريخ الاطلاع: 2017/09/25 على الساعة: 2130.
- 22- الأمر (02/15) المؤرخ في 7 شوال 1436 الموافق 23 يوليو 2015 يعدل ويتم الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 40 المؤرخة في 23 يوليو 2015.
- 23- حسن بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الانترنت، ص 47. منشور على الموقع www.minshawi.com تاريخ الاطلاع: 2017/09/27 على الساعة: 16 00.
- 24- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 86.
- 25- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية، الأردن، 2009، ص 158.
- 26- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، الأردن، 2005، ص 171.
- 27- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 79.
- 28- هلال عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليه، الطبعة الأولى، دار النهضة العربية، مصر، 2007، ص 385.

- 29- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 87.
- 30- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص 750.
- 31- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 94.
- 32- عادل عبد العال إبراهيم خراشي، المرجع نفسه، ص 98.
- 33- حسين بن سعيد الغافري، مرجع سابق، ص 58.
- 34- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 104، 103.
- 35- تنص المادة 699 من قانون الإجراءات الجزائية على أنه: "إذا طلب التسليم في وقت واحد من عدة دول عن جريمة واحدة فتكون الأفضلية في التسليم للدولة التي سببت الجريمة إضراراً بمصالحها أو للدولة التي ارتكبت في أراضيها. وإذا كانت طلبات التسليم المتعارضة متعلقة بجرائم مختلفة فإنه يؤخذ في الاعتبار عند تحديد الأفضلية بينها جميع الظروف الواقعة وعلى الأخص خطورتها النسبية ومكان ارتكاب الجرائم والتاريخ الخاص بكل طلب والتعهد الذي قد تلتزم به إحدى الدول الطالبة بإعادة التسليم".
- 36- عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 106.

المصادر والمراجع

المصادر:

أ- الاتفاقيات الدولية:

- اتفاقية بودابست 2001.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010/12/21.

ب- التشريعات:

- القانون رقم (15/04) المؤرخ في 10 نوفمبر 2004 يعدل ويتم الأمر 156/66 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 المؤرخة في 10 نوفمبر 2004.

- القانون رقم (04/09) المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 بتاريخ 16 غشت 2009.

- الأمر (02/15) المؤرخ في 7 شوال 1436 الموافق 23 يوليو 2015 يعدل ويتم الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 40 المؤرخة في 23 يوليو 2015.

ج- المراسيم:

- المرسوم الرئاسي رقم 252/14 مؤرخ في 13 ذي القعدة 1435 الموافق 8 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، جريدة رسمية رقم 57 بتاريخ 28 سبتمبر 2014.

المراجع:

أ- المؤلفات:

- 1- أيمن عبد الله فكري، جرائم نظم المعلومات- دراسة مقارنة-، دار الجامعة الجديدة، مصر، 2007.
- 2- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، مصر، 2001.
- 3- رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات حلبي الحقوقية، لبنان، 2012.
- 4- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة والوراقة الوطنية، المغرب، 2011.
- 5- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية، وسبل التغلب عليها، دار الجامعة الجديدة، مصر، 2015.
- 6- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.

- 7- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2008.
- 8- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية، الأردن، 2009.
- 9- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، مصر، 2010.
- 10- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، الأردن، 2005.
- 11- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، 2007.
- 12- هلالى عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليه، الطبعة الأولى، دار النهضة العربية، مصر، 2007.

ب- الرسائل العلمية:

1-(R)Boos, (La lutte contre la cybercriminalité au regard de l'action des états), Thèse de doctorat en droit privé et sciences criminelles, faculté de droit sciences économiques et gestion, université de Lorraine, soutenue le 09-12-2016.

ج- المقالات العلمية:

1- مصطفىاوي عبد القادر، الشرطة الوطنية ومكافحة الجريمة الالكترونية، مركز البحوث القانونية والقضائية، ملتقى دولي حول محاربة الجريمة المعلوماتية المنعقد بالجزائر العاصمة يومي 5، 6 ماي 2010.

2- حسن بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الانترنت، منشور على الموقع WWW.minshawi.com

د- المواقع الالكترونية:

-WWW.algeriachannel.net

-WWW.minshawi.com.

.<https://tel.archives-ouvertes.fr/tel-01470150/document>