الآليات الدولية لمكافحة الجريمة الالكترونية

International mechanisms to confront cybercrime

قزران مصطفى[1]، زرقين عبد القادر[2]
[1] المركز الجامعي أفلو، kezmus@yahoo.fr
[2] المركز الجامعي تيسمسيلت، zerguinekada@yahoo.fr

تاريخ الإرسال: 2020/04/21 تاريخ القبول: 2020/06/09 تاريخ النشر: 2022/06/16

ملخص:
لـم يعـد يوجـد مجـال اقتصـادي أو اجتمـاعي أو صـناعي أو إداري إلا وتلعـب تكنولوجيـا المعلومات دورا رئيسيا في أدائه وتطويره . ونتيجة لهذا التطور في عالم المعلوماتية نشأت ونمت أنماط جديدة من الجرائم ،وبرز الاهتمام الدولي بمكافحتها لما تنطوي عليه هذه الجرائم من آثار سلبية بالغة الخطورة ، الأمر الذي استوجب التصدي لهذه الجرائم ، وقد أصدرت العديد من الدول قوانين تجرم مثل تلك الأفعال وتعاقب عليها لكن تلك الجهود المنفردة للدول أفصحت عن فراغ تشريعي وقصور عملي في آليات مكافحة الجرائم . هذا الأمر يبدو طبيعيا بالنظر لخصوصية جرائم المعلومات وتخطيها الحدود الجغرافية من جهة ومن جهة أخرى تميزها بالتطور المتسارع تقنيا والانتشار الكبير في جميع جوانب الحياة، وبالتالي فإن التطورات التي حدثت في مجالات المعلوماتية أملت ضرورة وجود تعاون دولي لمواجهة الجرائم الالكترونية ولم يعد هذا خيارا بل ضرورة حتمية في ظل غياب بدائل أخرى
كلمات مفتاحية: التعاون الدولي، الانترنت ، جرائم.

Abstract:
There is no longer any economic, social, industrial or administrative field could be an exception from that main role of information technology to improve its performance and development.
As a result of this development in informatics world ,a new types of crimes have showed up becuase of that

The emergence of that criminality information phenomenon in increasebly way it naturally led to more illegal acts, which necessitated to stop such crimes and their gravity, forthat many countries issued laws that criminalize and punish such dengerous acts, but those individual efforts of states revealed a legislative vacuum and a practical deficiency in crime-fighting mechanisms.
as a result , the developments that have occurred in the fields of informatics dictated the need for international cooperation to confront cybercrime, and this is no longer an option, but it becomes really an imperative necessity in the absence of other alternatives.
Keywords: *Coopération internationale, Internet, crimes.*

1- المؤلف المرسل: قزران مصطفى، أستاذ محاضر أ **الإيميل:** kezmus@yahoo.fr

مقدمة :

يشهد العالم حاليا عصرا جديدا أبرز سماته التقدم العلمي المتطور باستمرار و بوتيرة متسارعة و لعل أبرز جوانب هذا التقدم تتمثل بشكل أساسي بظهور أجهزة الإعلام الآلي و ما صاحبه من قفزة هائلة في تقنيات الاتصال لاسيما شبكة المعلومات الدولية و بحدوث هذه الطفرة التكنولوجية تحول العالم إلى مدينة صغيرة يمكن رصد الأحداث بها في أي منطقة جغرافية بالصوت و الصورة و ساعة وقوعها كما أصبح تدفق المعلومات و المعارف غزيرا بالشكل الذي يسمح بالحصول عليها بسهولة و سرعة وقد تجاوز استخدام وسائل الاتصال الحديثة الحدود التقنية الضيقة للاستعمال ليشمل أبعاد أكثر اتساعا في كل ما يتعلق بحياة المرء اليومية من أبسط الجزئيات إلى اعقدها كما أصبح من غير الممكن تقريبا الاستغناء عن خدمات تكنولوجيا المعلومات لا من طرف الأفراد ولا الدول بالنظر إلى القدرة الهائلة لهذه التكنولوجيا على حفظ المعلومات وتخزينها ومعالجتها بسرعة خيالية وما رافقه من إمكانية الاتصال بسرعة فائقة هذه التقنيات أتاحت للأفراد القدرة على القيام بجميع معاملاتهم بما في ذلك القضايا التجارية والمصرفية في وقت قصير وبجهد أقل وتكلفة أرخص

كما وفرت هذه التقنيات للدول أداءا أفضل بسرعة أكبر في جميع القطاعات بما في ذلك البنى التحتية الأساسية ولم يعد يوجد مجال اقتصادي أو اجتماعي أو صناعي أو إداري إلا وتلعب تكنولوجيا المعلومات دورا رئيسيا في أدائه وتطويره .

ونتيجة لهذا التطور في عالم المعلوماتية نشأت ونمت أنماط جديدة من الجرائم ما كانت لترى النور لو لا التقدم المذهل لأجهزة الكمبيوتر والإنتشار السريع لشبكة الإنترنت وقد تنوعت هذه الجرائم واتخذت مظاهر مختلفة إلى الدرجة التي أصبحت مكافحتها هاجسا يؤرق الدول المتقدمة والنامية على حد سواء ولقد تنبه العالم إلى خطورة الجرائم التي تتم باستخدام الكمبيوتر وشبكة الإنترنت وبرز الاهتمام الدولي بمكافحتها لما تنطوي عليه هذه الجرائم من آثار سلبية بالغة الخطورة . فبزوغ ظاهرة الإجرام المعلوماتي بصورة متنامية أدت إلى تزايد الأفعال اللامشروعة ، الأمر الذي استوجب التصدي لهذه الجرائم وخطورتها، وأصدرت العديد من الدول قوانين تجرم مثل تلك الأفعال وتعاقب عليها لكن تلك الجهود المنفردة للدول أفصحت عن فراغ تشريعي وقصور عملي في آليات مكافحة الجرائم . هذا الأمر يبدو طبيعيا بالنظر لخصوصية جرائم المعلومات وتخطيها الحدود الجغرافية من جهة ومن جهة أخرى تميزها بالتطور المتسارع تقنيا والانتشار الكبير في جميع جوانب الحياة .

وبالتالي فإن التطورات التي حدثت في مجالات المعلوماتية أملت ضرورة وجود تعاون دولي لمواجهة الجرائم الالكترونية ولم يعد هذا خيارا بل ضرورة حتمية في ظل غياب بدائل أخرى.

لكن الإشكالية التي تتداعى منطقيا : ما هي الآليات الدولية لمكافحة الجريمة الإلكترونية ؟ وما هي صور التعاون المفترضة للحد من آثارها ؟

للإجابة عن هاته الإشكالية اعتمدنا الخطة الآتية المكونة من مبحثين، حيث يستعرض المبحث الأول أوجه التعاون الدولي في مجال مكافحة جرائم المعلوماتية، في حين يستعرض المبحث لثاني الصعوبات التي تواجه التعاون

الدولي وتحول دون تفعيل مكافحة الجرائم الالكترونية، وكذلك سبل التغلب على هذه الصعوبات.

1. الأطر العامة للتعاون الدولي في مجال مكافحة الجرائم الالكترونية.

إن تسارع نسق التقدم التكنولوجي وظهور الفضاء الالكتروني، قد أحدث ثورة الكترونية تشمل جميع المجالات وأضحى من الصعوبة الاستغناء عن هذه الخدمات اللامتناهية، ولكن هاته التقنيات المستحدثة كانت في نفس الوقت محلا وفرصة يستغلها البعض لممارسة أنشطة غير مشروعة، ولما كانت هذه الثورة الالكترونية لا تخضع لأي حدود ولا تعترف بسيادة الدول أصبح من العسير إخضاعها لنظام قانوني تتكفل دولة ما وبمفردها بالتصدي لهذه الجرائم غير التقليدية ، مما يستوجب تطوير البنية التشريعية الدولية ، وفي نفس الوقت استحداث مسارات للتعاون الدولي مماثلة لإيقاع التطور المتنامي الذي تشهده هذه الجرائم سواء بترقية الآليات التقليدية أو إنشاء آليات جديدة من اجل التصدي لهاته الجرائم ومكافحتها.

1.1. التعاون القضائي.

إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تقتضي تتبع النشاط الإجرامي الأمر الذي يستوجب تقصي آثار الجريمة من مصدرها إلى غاية تنفيذها وتحديد مواقع الأضرار التي مستها ، وبما أن هذه العناصر قد تقع في بلدان مختلفة فإنه يتعين لملاحقة مرتكبي هذه الجريمة وجود نوع من التعاون بين السلطات القضائية لهذه البلدان قصد تمديد الولاية القضائية ولذا سنتعرض إلى أهم صورتين في مجال التعاون القضائي وهما : التعاون الأمني كصورة أولى ثم إلى المساعدة القضائية كصورة ثانية.

1.1.1. التعاون الأمني.

إنه من البديهي أن تقف الحدود الجغرافية ومشكلة الاختصاص الإقليمي حجر عثرة أمام الإجراءات الجنائية لملاحقة مرتكبي الجرائم لا سيما في جريمة الإنترنت التي تتميز بكونها جريمة عابرة للحدود فقد يكون مرتكب الهجوم

يحمل جنسية دولة ما وينفذ جريمته من أجهزة دولة أخرى وتقع آثار هذه الجريمة في دولة ثالثة ولهذا تبرز الحاجة الملحة لتوحيد الجهود فيما يتعلق بتبادل المعطيات المتعلقة بالجريمة والمعلومات التي تسمح بكشف هوية المجرمين ما دام أنه يستحيل على الدولة بمفردها القضاء على هذه الجريمة، فأجهزة الشرطة لا يمكنها تعقب مرتكبي الجرائم وملاحقتهم إلا من نطاق حدودها أي أنه متى فرّ المجرم خارج حدود الدولة فإنه يبقى في مأمن من المتابعة.

ونجد في هذا الإطار أن هناك ثلاثة أوجه لإقامة هذا التعاون:

أولا: إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الإنترنت ونشرها: وتهدف هذه المكاتب إلى تنمية التعاون بين سلطات الدول القضائية في مجال مكافحة الجريمة وملاحقة المجرمين (بتتبع المعلومات وتعميمها) بالإضافة إلى تقديم المعونة وتبادل الخبرات عند الاقتضاء[1].

ثانيا: التعاون في إطار المنظمة الدولية للشرطة الجنائية "الإنتربول": وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها وتتبادلها فيما بينها بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في دول الأطراف[2].

ثالثا : القيام بعمليات أمنية مشتركة: حيث يتم تعقب جريمة الانترنت وتتبع الأدلة الرقمية وضبطها والقيام بعمليات التفتيش العابر للحدود مكونات أجهزة الإعلام الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تتضمنه من أدلة وبراهين وهذه الإجراءات تستدعي كلها تعاونا دوليا مكثفا لا سيما العمليات الفنية والأمنية كما من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم[3] .

1.1.2.المساعدات القضائية الدولية

تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم.
ويمكن إستنباط المبادئ العامة التي تحكم الالتزام بالمساعدة القضائية المتبادلة في الفقرة 1 من المادة 25 من إتفاقية بوادبست للإجرام الالكتروني والالتزام بالمساعدة يجب أن يتوفر لأقصى حد ممكن، وأن تكون المساعدة شاملة وممتدة كما يجب تقليل المعوقات[4].
وتتخذ المساعدة القضائية صورا عدة منها :
أولا : تبادل المعلومات: ويتم بواسطة تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، حركت الدعوى فيها ضد أحد رعاياها أو رعايا دولة أخرى مما يتضمن تبادل السوابق القضائية للمتابعين لمثل هذه الجرائم ونجد لهذه الصورة تطبيقات عدة منها ما ورد في الفقرتين 6و7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[5] وكذلك الفقرات 3و4 من المادة الثامنة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.
ثانيا: نقل الإجراءات:
ويقصد به قيام دولة ما بموجب اتفاقية أو معاهدة باتخاذ جملة من الإجراءات الجنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك بناءا على توفر جملة من الشروط من أهمها التجريم المزدوج ويقصد به أن يكون الفعل مجرم في كل من الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالاضافة إلى مشروعية الإجراءات المطلوب إتخاذها أي أن توافق قانون الدولة المطلوب منها اتخاذ الإجراءات فضلا أن تكون الإجراءات المطلوب إتخاذها جدية أي أن تكون ذات أهمية بالقدر الذي يمكن أن يسهم في الوصول إلى حقائق فاصلة في ملابسات الجريمة ، ولقد أقرت العديد من الاتفاقيات والمعاهدات الدولية هذه الصورة مثلما هو الحال عليه في معاهدة الأمم المتحدة النموذجية بشأن نقل الاجرءات في المسائل الجنائية[6] واتفاقية الأمم

المتحدة في مكافحة الجريمة المنظمة عبر الوطنية في مادتها 21، وكذلك المادة 23 من اتفاقية بودابست للإجرام المعلوماتي.

وفي كل الحالات ينبغي مراعاة أنه في القضايا التي يتم فيها تطبيق شرط التجريم المزدوج، أن يكون بطريقة مرنة d'une façon souple تضمن تسهيل عملية المساعدة القضائية[7].

ثالثا : الإنابة القضائية الدولية:

ويقصد بها اتخاذ اجراء قضائي من اجراءات الدعوى الجنائية لأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية تعذر على الدولة التي تقدمت بطلب الإنابة القيام به بنفسها وتهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن اجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة تجاوزا لعقبة السيادة الإقليمية التي تحظر على الدول الأجنبية ممارسة الأعمال القضائية داخل أقاليم الدول الأخرى بإجراءات التحقيق والمعاينة والتفتيش أو سماع الشهود .

وتجدر الإشارة إلى أن طلب الإنابة عادة ما يتم عبر القنوات الدبلوماسية إلا أنه تفاديا لتعقيد الإجراءات وبطئها وبغية التعجيل والتبسيط منها درجت الدول على تعيين سلطة مركزية عادة ما تكون وزارة العدل توجه الطلبات إليها مباشرة.

وفيما يتعلق بمجال التعاون القضائي يمكن أن نخلص إلى نتيجة مفادها أن التعاون القضائي وإن كان يشكل أحد أهم آليات لمكافحة جرائم الأنترنت إلا أن الملاحظ إن غالبية الاتفاقيات في مجال التعاون القضائي قد تناولت جريمة الإنترنت بدون تعمق وبشكل سطحي ومنه باتت الحاجة ملحة لعقد اتفاقيات تواكب التطور السريع لتكنولوجيا المعلومات والاتصالات لاسيما أن عامل السرعة يعتبر عاملا أساسيا لمواجهة جريمة الإنترنت وهذا التوجه يمكن أن نرصد إرهاصات على تبنيه مؤخرا من خلال جملة الاتفاقيات التي تم إبرامها على المستويين الدولي والإقليمي والتي عالجت جريمة الإنترنت بشكل رئيسي وحصري.

1.2. تسليم المجرمين كآلية دولية في مجال مكافحة الجرائم الالكترونية.

لقد أتت هذه الصورة من صور التعاون الدولي كنتيجة حتمية للتطور الهائل الذي شهدته كافة المجالات وبوجه أخص مجال الاتصالات والمعلوماتية حيث لم تعد الحدود الإقليمية تشكل حاجزا أمام مرتكبي جرائم الإنترنت حيث أضحى في إمكان المجرم أن يشرع في التحضير لجريمته في بلد معين ويبدأ بالتنفيذ في بلد آخر ويمتد نشاطه الإجرامي إلى بلدان أخرى فجريمة الإنترنت أصبح لها طابع دولي وحيث أن أجهزة العدالة لا تستطيع تجاوز الحدود الإقليمية لممارسة الأعمال القضائي على المجرمين الفارين كان لابد من إيجاد آية للتعاون بين الدول تكفل ملاحقة المجرمين الفارين وإتخاذ كافة الإجراءات القضائية في مواجهتهم وبالتمعن في نظام تسليم المجرمين لوجدنا أنه يحقق مصالح الدول بدرجة أولى فالدولة التي يتواجد على إقليمها المتهم بإرتكاب أحد الجرائم العابرة للحدود لا سيما جريمة الإنترنت عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا يستوجب عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة. فهو إذا يحقق مصالح الدول الأطراف في عملية التسليم فهو من جهة يحقق مصلحة الدولة الأولى في كونه يشمل معاقبة الفرد الذي أخل بقوانينها ويكفل في ذات الوقت مصلحة الدول الثانية المطلوب منها التسليم كونه يضمن التخلص من فرد أو عنصر مجرم يهدد أمنها واستقرارها فضلا عن ذلك فإنه يمكن الدولة من الإيفاء بالالتزامات المترتبة عليها بصفتها عضوا في المجتمع الدولي.

1.2.1.صور تسليم المجرمين.

لقد درجت الممارسة الدولية على وجود ثلاثة أنظمة من الأنظمة المتبعة في تسليم المجرمين.

أولا: <u>التسليم القضائي</u>:

ويقصد به ذلك النوع من التسليم الذي تكون فيه المحاكم الجهة المختصة الوحيدة والمخول لها إصدار قرار التسليم للدولة التي تطلبه وبالرغم من الإيجابيات التي

يوفرها هذا النهج حيث أن يمكن الشخص المطلوب تسليمه بأوجه دفاعاته كاملة أمام السلطات القضائية المختصة إلا أنه يعاب عليه بطء الإجراءات وهو ما ينعكس سلبا على ما تستوجبه سرعة ملاحقة مرتكبي جرائم الإنترنت لسهولة إندثار أدلة الإثبات عليها.

ثانيا: التسليم الإداري:

يوكل في مهمة تسليم المتهمين في هذا النظام إلى السلطة التنفيذية التي تملك الصلاحية المطلقة لقرار التسليم من عدمه وبالرغم مما يتمتع هذا النظام من تجنب الإجراءات المعقدة و البطيئة إلا أن ما يؤاخذ عليه إهداره لحقوق الأفراد الدفاعية من جهة ومن جهة أخرى خضوع قرار التسليم لإعتبارات سياسية أو لقواعد المجاملات الدولية فضلا عن أن نظام التسليم الإداري تتولاه السلطة التنفيذية التي قد تكون لا تمتلك الخلفية القانونية المقبولة للفصل في مثل هذه القضايا.

ثالثا: التسليم المختلط:

وهو الأسلوب الأكثر إنتشارا حيث أنه يمزج بين مزايا النظامين السابقين فهو يسهل الإجراءات و يسرعها كما يضمن للشخص المتهم حق الدفاع.

1.2.2.شروط تسليم المجرمين.

تجدر الإشارة إلى أن نظام تسليم المجرمين يخضع لجملة من الشروط ينبغي توافرها مثل صدور قرار التسليم و تكمن أهمية الشروط في توضيح حدود العلاقة بين الدول و الأطراف في عملية التسليم و يمكن إجمال هذه الشروط فيما يلي :

أولا : الشروط المتعلقة بالجريمة:

التجريم المزدوج: ويقصد به أن يكون الفعل مجرما في كلتا الدولتين ولاعبرة بالتكييف القانوني لهذه الجريمة وشرط التسليم المزدوج يجد أساسه في أن الدولة طالبة التسليم تهدف من خلال طلبها إلى محاكمة من نسب إليه إرتكاب السلوك الإجرامي أوتنفيذ العقوبة المحكوم بها عليه وهذا يفترض بداية أن

السلوك المجرم في تشريعاتها وإلا كان لا وجه لوجود متابعة جنائية أو تحريك دعوى عمومية ومن ناحية أخرى لا يتصور مطالبه دولة ما تسليم شخص لتوقيع عقوبته على سلوك غير مجرم أساسا في قوانينها العقابية وعلى هذا الأساس تتبع الدول في تحديد الجرائم نظام الحصر[8] وذلك بإعداد قائمة تدرج فيما على سبيل الحصر الجرائم المعنية بالتسليم.

درجة جسامة الجريمة:

حيث نجد أن بعض الدول تشترط درجة معينة من جسامة الجريمة أو إشتراط حد أدنى من العقوبة الموافقة لهذه الجريمة وفق تشريعاتها الداخلية حتى يقع التسليم وهذا الشرط بالذات ورد في بعض الإتفاقيات الدولية كما هو عليه الحال في المادة 2 من المعاهدة النموذجية بشأن تسليم المجرمين و المادة 24 من الإتفاقية الأوربية للإجرام المعلوماتي[9].

ثانيا: الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

عدم جواز تسليم الرعايا:

لقد إستقر الفقه الدولي و معظم التشريعات الوطنية على مبدأ عدم جواز تسليم الرعايا الوطنيين إلى دول أجنبية أيا كان نوع الجريمة المتابعين بها في هذه الحالة تكون الدولة التي ينتمي إليها المتهم بإرتكاب الجريمة أولى بمحاكمته و توقيع العقوبة المناسبة وفقا لمبدأ شخصية القوانين.

عدم جواز تسليم اللاجئين السياسيين:

ويعتبر هذا المبدأ عرفا دوليا درجت الممارسة الدولية على إتباعه كما أقرته الإتفاقيات الدولية و التشريعات الوطنية وإعتبرته استثناء على واجب الإلتزام بتسليم المجرمين ولعل الأساس الذي يقوم عليه هذا المبدأ هو تحقيق العدالة وحماية حقوق الإنسان خشية أن تكون التهمة ملفقة من قبل سلطات الدولة طالبه التسليم.

عدم جواز تسليم المحاكمين على ذات الجريمة:

وذلك اقرار لمبدأ عدم تكرار العقوبة على ذات المجرم الذي أقرته القوانين الوطنية وأكدته الإتفاقيات الدولية فمتى كان الشخص المطلوب تسليمه قد حوكم من قبل عن الجريمة المطلوب تسليمه لأجلها بمقتضيات العدالة تقتضي أنه إذا كان برأ أو قضى عقوبته فإنه لا يجوز تسليمه حتى لا يتعرض هذا الشخص لعقوبة مزدوجة.

يجب التنبيه أن تسليم المجرمين يخضع للشروط المنصوص عليها بواسطة القانون الداخلي للطرف المطلوب منه التسليم أو لإتفاقيات تسليم المجرمين المطبقة بما في ذلك الأسباب التي من أجلها يمكن أن يرفض المطلوب منه هذا التسليم[10].

1.3. التعاون الدولي في مجال التدريب لمكافحة جريمة الإنترنت.

لقد أثبت الواقع العملي أن النصوص القانونية الحالية تقف عاجزة أمام التقدم الهائل والتطور المستمر لتكنولوجيا المعلومات و الإتصالات و بالتالي فإن النصوص القانونية العقابية تكشف عن قصور في مكافحة جريمة الإنترنت لذا توجب على الدول أن تسن تدريبات وتتخذ إجراءات تواكب هذا التسارع نظرا لما تتسم به جرائم المعلوماتية من تنوع وتجدد في الأساليب الإجرامية و كذا سرعة تنفيذها و إمتداد آثارها وحتى القدرة على إخفائها ومحو آثارها .

وبالتالي فإن هذا النمط من الجرائم أصبح يشكل عبئا ثقيلا على عاتق جميع الأجهزة الأمنية الحكومية وكذا مختلف مستويات أجهزة العدالة .

ولهذه الأسباب كان لزاما على تلك الأجهزة أن تكون على قدر كبير من المسؤولية والكفاءة للكشف عن هاته الجرائم وملاحقة مرتكبيها فكفاءة رجال العدالة تعد عاملا حاسما في مواجهة هذه الظواهر المستحدثة والتصدي لها وهذا الأمر لا يتحقق دون المرور على عمليات تدريب وتكوين ترفع من قدرات العاملين بهاته الأجهزة وتؤهلهم لتحقيق أهدافهم بفعالية.

1.3.1. أهمية التدريب في مكافحة جرائم الإنترنت.

يعد التدريب عنصرا حيويا لبناء الخبرات والمهارات وقطاع العدالة ولأجهزة لأمنية ليست في منأى منه فيجب أن تتوفر لدى رجال العدالة الأرضية القانونية والخبرة الفنية اللازمة في مجال الجريمة المعلوماتية وهذه الخبرة الفنية لاتتأتي دون تدريب متخصص يشمل كل ما يتعلق بتكنولوجيا المعلومات كالبرمجة أوتصميم لأنظمة أو إدارة الشبكات المعلماتية كما يتضمن التعرف على المخاطر والتهديدات التي تنتج عن مثل هذه الجرائم وكذ مواقع وأساليب إختراق شبكة المعلومات كالبرمجة أو تصميم الأنظمة أو إدارة الشبكات المعلوماتية كما يتضمن التعرف على المخاطر والتحديدات التي تنتج عن مثل هذه الجرائم وكذا مواقع وأساليب إختراق شبكة المعلومات وأجهزة الإعلام الآلي كما أن عملية التدريب قد تمس الجوانب الإجرائية بإجراءات التحقيق كتجميع المعلومات وتحليلها ومراجعة النظم الفنية للبيانات بسرعة و دقة متناهيتين أو إجراءات التفتيش والضبط وكيفية إستعمال جهاز الإعلام الآلي كآدة لإسترجاع البيانات واستنباط أدلة الإتهام وهذا الأمر يتطلب أن يعهد بالتدريب إلى جهات متخصصة مما توفر فيهم الخبرة العلمية والقدرة الفنية و يجب أن يراعي عملية التدريب أن تكون مستمرة لا سيما و أن جرائم الإنترنت تتميز بتطورها المستمر والمتسارع[11]، وإنه من المعلوم أن الكثير من الدول إن لم يكن أغلبها يتوفر على الإمكانيات المادية والإطارات البشرية الكفيلة بمواجهة جرائم الإنترنت وعليه يتوجب نقل التجارب والخبرات من الدول التي قطعت باعا كبيرا في هذا الميدان إلى الدول التي مازالت تعاني قصورا واضحا في مواجهة جرائم المعلوماتية وهذا لا يتأتى إلا بخلق أروقة تعاون بين الدول تسهم بشكل فعال في الحد من هذه الظاهرة الإجرامية المستحدثة.

واقتناعا بأهمية التدريب أوصى مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء الذي عقد بهافانا بشأن الجرائم ذات الصلة بالكمبيوتر بضرورة اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن الجرائم ذات الصلة بأجهزة الحاسوب والقائمين بمهام التحقيق والتفتيش فيها[12].

1.3.2. صور التعاون الدولي في مجالات التدريب.

لعله من البديهي القول أن الكثير من الدول النامية لا تملك الجاهزية المطلوبة تؤمنها لمواجهة الجرائم المتعلقة ومثيلاتها من الجرائم المستحدثة إن هذا العجز يمكن رده إلى عدة عوامل أهمها الإفتقار إلى الموارد الكافية مادية كانت أو بشرية وإن المنظومة القانونية التقليدية لهذه الدول تعوزها النصوص التي تتصدى وعلى نحو فعال لهذا النوع من الجرائم، وعليه يستحيل على الدولة بمفردها مواجهة هذه الأنماط المستحدثة من الجرائم دون تعاون أو تنسيق مع غيرها من الدول، وبتفحص الاتفاقيات الدولية والإقليمية نجد أنها تؤكد على ضرورة التعاون بين الدول في مجال التدريب ونقل الخبرات والدليل على ذلك ما ورد في المادة 29 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 والمادة 9 من مشروع الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

التعاون الدولي قد يأخذ أشكالا عدة لا يمكن حصرها فقد يتحقق من خلال عقد مؤتمرات أو ندوات أو ورشات عمل متخصصة مواجهة لكل الجرائم الصعيدين الدولي ولإقليمي حيث تقدم هذه الفعاليات العلمية عصارة أبحاثها ودراساتها ومختلف المستجدات المتعلقة بالجرائم الإلكترونية، وقد يتحقق التعاون عن طريق تنظيم تربصا ت دورية أو إقامة دورات تدريبية للعاملين في أجهزة العدالة والأجهزة الأمنية ويعد هذا الأسلوب الأسلوب الأمثل والأنجع لكونه يمكن رجال العدالة والأجهزة الأمنية من تبادل الخبرات والاستفادة من المساعدة التقنية الضرورية والتعرف على أحدث التقنيات والمستجدات في مجال الجريمة المعلوماتية وأساليب مكافحتها[13]، الأمر الذي ينعكس إيجابا على قدرة القائمين على مكافحة جريمة المعلوماتية .

2. معوقات التعاون الدولي في مجال مكافحة جرائم الإنترنت .

إنه بالرغم من وجود قنوات للتعاون الدولي لمكافحة جرائم المعلوماتية، الأمر الذي يوفر بصورة أو أخرى آليات للحد من هذه الجريمة إلا ان طبيعة جرائم الأنترنت وعدم وجود مفهوم دولي مشترك لتعريف الجريمة الإلكترونية فضلا

عن قصور الآليات الإجرائية دوليا كلها، شكلت عوامل أسهمت في الحد من فعالية التعاون الدولي في مواجهة ظاهرة الإجرام المعلوماتي.

2.1. عوائق تتعلق بطبيعة جرائم الإنترنت.

تتسم جرائم المعلوماتية بطبيعة خاصة، حيث أنها تتخذ وتوظف الوسائل التكنولوجية كأرضية لارتكاب جرائم أخرى لا يتسع المجال لحصرها، وكلها تتضمن نسبة عالية من درجة الخطورة فضلا عن كونها لا تعترف بالحدود الإقليمية مع صعوبة التوصل الى الأدلة الرقمية والتحفظ عليها.

2.1.1. **سهولة إخفاء الجريمة.**

الجريمة المعلوماتية في أغلب الأحيان تكون مستترة و خفية فالجاني في مثل هذه الجرائم يحاول إخفاء هويته مما يضعف إلى حد كبير فرصة المجني عليه في إثبات الإعتداء فالأفعال من قبيل إختراق قواعد البيانات و تغيير محتوياتها أو التخريب المنظم للأنظمة بإستعمال الفيروسات يمكن إرتكابها من بعد و دون تحديد مصدرها (الشخص المسؤول).

فجرائم المعلوماتية تتميز بكونها جرائم فنية لا تترك أثرا كالآثار التي قد تتواجد في جرائم السرقة أو العنف لأنها تتعامل مع بيانات ومعلومات مخزنة إلكترونيا تأخذ شكل الأرقام والرموز[14].

2.1.2.صعوبة إثبات الجريمة.

إن الطبيعة الخاصة لمثل هذه الجرائم تجعل من عنصر الإثبات أمرا صعب المنال وسهولة محو آثارها. فغالبا ما يقف رجال الشرطة وجهات الإدعاء والقضاء عاجزين للوصول إلى دليل قطعي وكاف للإثبات كما أن أدلة الإثبات قد تقتصر على جوانب ذات طبيعة معنوية مما يحول دون إثبات الضرر.

والدليل العملي على كون جرائم الحاسب الآلي تتميز بصعوبات جمة تعترض طريق اكتشافها هو أن هذه الجرائم لم يكتشف منها إلا 1 % فقط من الجرائم المرتكبة، أما التي تم الإبلاغ عنها فلم تتعدى 5 % بل وحتى القضايا التي طرحت على القضاء للفصل فيها لم تكن الأدلة كافية للإدانة إلا في حدود الخمس[15].

2.1.3.إحجام الحجات المتضررة عن الإبلاغ عن الجرائم المعلوماتية.

إن هذا التردد في الإبلاغ يبدو منطقيا بالنظر إلى أن الجهات المتضررة لا سيما المالية منها كالمصارف والبنوك والمؤسسات الإقتصادية تفضل كتمان هذه

الجرائم تفاديا للآثار السلبية التي قد تنجم حين الكشف عنها فقد يؤدي ذلك إلى ركود أسهمها في الأسواق المالية واهتزاز الثقة مع المتعاملين لديها.
وقد لا تقف هذه الجهات إلى حد الامتناع عن الإبلاغ عن الجرائم بل تتعداه إلى الامتناع عن تقديم الأدلة أو تقديم مساعدة للجهات التحقيقية[16].

2.1.4.الطبيعة الدولية للجرائم المعلوماتية.

الجرائم المعلوماتية في أغلب الأحيان ترتكب من قبل أشخاص من خارج الحدود كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارجية يتيح لها فضاء إلكتروني يتسم بالتغيير والديناميكية والإنتشار الجغرافي العابر للحدود.

2.2. عوائق تتعلق بالأنظمة القانونية الداخلية.

غني عن البيان أن الإمكانيات التقنية العالية التي توظف في الاجرام المعلوماتي تؤدي الى ممارسة الأنشطة الاجرامية في دولة ما لتكون آثاره في دولة أخرى، وقد يكون الضحية من دولة ثالثة، فالجريمة المعلوماتية لا تقف عند الحدود الإقليمية ولا تعترف بالجغرافيا، الأمر الذي يحيلنا مباشرة إلى مسألة تنازع القوانين سواء تعلق الأمر بالقواعد الموضوعية أو بالقواعد الإجرائية فتضاربالقوانين الوطنية يبقى على رأس معوقات التعاون الدولي، وإن كان الفقه الدولي الحديث اتجه إلى معالجة جرائم المعلوماتية وفق الاختصاص القضائي العالمي، وذلك بتطبيق المبادئ المعمول بها في الجرائم التقليدية.

2.2.1. عدم وجود توصيف موحد لجريمة *الإنترنت*.

بتفحص الأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت يتبين أنه لا يوجد تصور موحد فما يكون سلوكا مشروعا في نظام قانوني معين قد يعد سلوكا إجراميا في نظام قانوني آخر ويمكن أن يعزى السبب في ذلك لإختلاف الأنظمة التشريعية من مجتمع لآخر والتي اتكزت بالأساس على التنوع الثقافي و الديني من مجتمع لآخر .

2.2.2.تعدد النظم القانونية الإجرائية.

إن القوانين الإجرائية للدول لا تتخذ نموذجا موحدا في كل الدول فطرق التحقيق أو التفتيش أو المحاكمة التي تسري في بلد ما ليست بالضرورة ناجعة أو حتى مسموح بها في بلد آخر فالمراقبة الإلكترونية و طرق جمع الإستدلالات بالتجسس المأذون به من السلطات المختصة قد يكون أمرا متاحا و قانونيا في

بلد ما في حين يعتبر في بلد ثاني من قبيل التعدي على الحقوق و الحريات العامة و بالتالي يعد إجراءا غير مشروع .

2.2.3. إشكالية التجريم المزدوج.

قد يقف شرط التجريم المزدوج عقبة أمام التعاون الدولي في مجال تسليم المجرمين إذا كان قانون الدولة المطلوب منها التسليم لا يجرم مثل هذه الأفعال خاصة وأن جرائم المعلوماتية من الجرائم المستحدثة التي لم تستمر بعد في الأنظمة القانونية العقابية لمعظم الدول بل يتم التعامل معها وفق النصوص التقليدية.

2.2.4.إشكالية الاختصاص.

تعد جرائم الإنترنت نموذجا عمليا لمشكلة الإختصاص فبما أن مثل هذه الجرائم تعد عابرة للحدود فإن تكون محلا لتنازع الإختصاص فقد يحدث أن ترتكب الجريمة في إقليم دولة ما من قبل أجنبي وعليه فقد تخضع الجريمة للإختصاص الجزائي لهاته الدولة تطبيقا لمبدأ الإقليمية وقد تخضع الجريمة لدولة الجاني إعمالا لمبدأ الإختصاص الشخص قد تتدخل دولة ثالثة هددت مصالحها على أساس مبدأ العينية[17]. إن هذا الإشكال من شأنه أن يطرح امتداد مسألة قواعد الإختصاص والقانون واجب التطبيق حتى يمكن معالجة أنشطة الملاحقة والتحري والتفتيش خارج الحدود الوطنية[18].

2.3. سبل التغلب على الصعوبات التي تواجه التعاون الدولي.

إنه من الضروري أن تواكب التشريعات الوطنية التطور الملحوظ في جرائم المعلوماتية، فقد أسفر الواقع المعاش على تخلف النصوص التشريعية في معظم البلدان لاسيما النصوص الجنائية خاصة في الدول العربية، الأمر الذي يستوجب تفعيل التعاون الدولي لمواجهة جرائم المعلوماتية، وذلك بإقرار القواعد الاتفاقية أولا، ثم تعزيزها بالآليات الإجرائية التي تكفل ولو نسبيا التصدي لهذه الظاهرة الإجرامية.

2.3.1.فيما يتعلق باختلاف المنظومة القانونية.

لقد سعى المهتمون بمكافحة جرائم المعلوماتية إلى تذليل الصعوبات التي تحول دون تكامل التعاون الدولي ففي ما يتعلق بإختلاف النظم القانونية سواء العقابية منها أو الإجرائية تسعى الدول إلى تحديث التشريعات المحلية لتواكب الجرائم المستحدثة كما تعمل على إبرام إتفاقيات خاصة تعني بهذا النوع من الجرائم هذا من جهة، ومن جهة أخرى فإن ترسانة الصكوك الدولية الصادرة عن لأمم المتحدة تشجع الدول الأطراف على السماح باستخدام بعض تقنيات التحقيق الخاصة الأمر الذي قد يخفف من تطرف وإختلاف النظم القانونية للدول ويفتح المجال أمام تعاون دولي فعال فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير إلى المراقبة الالكترونية وغيرها من أشكال المراقبة التي تعتبر من أهم التقنيات المستخدمة للتصدي للجماعات الإجرامية المنظمة[19]، وهذا ما أكدت عليه أيضا الاتفاقية الأوروبية للإجرام المعلوماتي حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الالكترونية، كما أكدت المادة 30 من ذات الاتفاقية على وجوب الكشف السريع عن البيانات المحفوظة، ونصت المادة 33 منها على ضرورة تعاون الدول الأطراف فيما بينها بجمع البيانات، وفيما يتعلق بإشكالية التجريم المزدوج ركزت الاتجاهات التشريعية الحديثة على تخفيف التطبيق الصارم بهذا الشرط، أما بالنسبة لمشكلة الاختصاص فإن الضرورة أصبحت ملحة لإبرام اتفاقيات دولية ثنائية أو جماعية يتم فيها وضع تصور موحد لقواعد الاختصاص القضائي حين يتعلق الأمر بجرائم الإنترنت، وهذا المسعى لا يمكن تحقيقه دون الوصول إلى تضامن دولي شامل يقوم على الموازنة بين متطلبات مكافحة جرائم المعلوماتية ووجوب حماية السيادة الوطنية وحقوق الأفراد وحماية خصوصياتهم[20].

2.3.2. فيما يتعلق بالصعوبات التي ترجع لطبيعة جرائم المعلوماتية.

إن أنشطة مكافحة جرائم المعلوماتية أظهرت تحديات ومشاكل كثيرة تختلف في جوانب عدة عن التحديات والمشاكل المرتبطة بالجرائم التقليدية الأخرى، وعليه فإن القضاء أو الحد من هذه الظاهرة الإجرامية يستوجب وجود خبرة فنية دقيقة وعالية ومتخصصة، إذ أنه يصعب وربما يستحيل على رجال العدالة العاديين التحقيق أو التعامل معها لكون مرتكبيها يستعملون خدعات تضليلية، إن القصور

في توفير الوسائل والإمكانيات من شأنه أن يؤدي إلى صعوبة في اكتشاف هذه الجرائم، وهذا يرجع إلى قلة خبرة السلطات التي تتولى التحقيق بل في الغالب انعدام تلك الخبرة، لذلك توجبت الاستعانة بالنخبة المتخصصة في الحاسب الآلي لضبط هذه الجرائم واكتشافها[21]، ومنه وأمام خطورة هذه الجرائم وصعوبة متابعتها والكشف عنها والتعرف على مرتكبيها فإن أول خطوة في مكافحة هذه الجرائم تبدأ من تحديد هذه الجرائم ثم تحديد الجهة التي يجب التعامل معها ، ثم تكوين وتدريب الإطارات تكوينا فنيا ومتخصصا يتناسب مع طبيعة هذه الجرائم، ثم وضع آليات وإجراءات لمكافحتها والتعامل معها وكل هذا لايتأتى دون ودود تعاون دولي فعال .

2.3.3. فيما يتعلق بالجوانب الإجرائية للتعاون الدولي .

إن البعد الإجرائي أو الفني لجرائم الإنترنت ينطوي على تحديات ومشكلات جمة ومن هذا المنطلق تبرز أهمية التعاون الدولي لردم الهوة الواسعة بين الدول التي قطعت شوطا كبيرا في مكافحة الجريمة المعلوماتية وتلك الدول التي لاتزال تدرج خطواتها الأولى في هذا المجال ، وعليه يتوجب الحد من مشكلة عدم وجود قنوات إتصال بين الجهات المسؤولة عن مكافحة مثل هذه الجرائم وذلك بإنشاء قنوات إتصال بين السلطات المختصة والدوائر المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها، كما أنه من المعلوم أن هناك حالات حرجة وحالات أخرى يكون عنصر السرعة فيها حاسما ولذلك فإن وجود إدارات أو أشخاص مخولة لإتخاذ القرار بسرعة يساعد في تحقيق وتعقب مثل هذه الجرائم[22]، وهذا ماأكدت عليه الصكوك الدولية مثل إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 27 منها والمادة 48 من إتفاقية الأمم المتحدة لمكافحة الفساد والمادة 27 من الإتفاقية الأوربية لمكافحة الإجرام المعلوماتي والمادة 35 من ذات الإتفاقية التي نصت على ضرورة وجود نقطة إتصال دائمة بين الدول لتؤمن المساعدة فيما يتعلق بجرائم البيانات وشبكات المعلوماتية ، أما فيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية فقد أوصى مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي أنعقد في بانكوك في الفترة 18 – 25 أفريل 2005 بضرورة تعزيز فعالية السلطات المركزية المعنية للإرتقاء بالمساعدة القانونية للمستوى المطلوب بغية تنفيذ الطلبات القضائية في الوقت المناسب ، ونفس

الأمر أكد عليه المادة 25 من الإتفاقية الأوربية للإجرام المعلوماتي، أما في ما يتعلق بالصعوبات التي تواجه التعاون الدولي في مجال التدريب لا يمكن التغلب عليها إلا بمزيد من التنسيق بين الأجهزة المعنية بتدريب رجال تنفيذ القانون وإيجاد برامج تدريبية مشتركة تناسب جميع المستهدفين ، بالإضافة إلى القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها[23].

2.3.4.العوائق التي تتعلق بالجوانب الإجرائية.

أ- عدم وجود قنوات إتصال:

إن أهم غايات التعاون الدولي في مكافحة جرائم المعلوماتية هو الحصول على المعلومات و البيانات المتعلقة بالجريمة و المجرمين و لتحقيق هذا الهدف كان لزاما أن يكون هناك نظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أجنبية لجمع الأدلة و المعلومات فعدم وجود مثل هذا النظام يعني عدم القدرة على التصدي لهذه الجرائم و بالتالي تنعدم الفائدة من هذا التعاون[24].

كما أن إنشاء شبكة طوارئ لتفعيل المساعدة المتبادلة على غرار ما نصت عليه المادة 25 من اتفاقية بودابست للإجرام المعلوماتي والتي يطلق عليها الشبكة 7/24 أي تلك الشبكة التي تعمل على توفير المساعدة الفورية على مدى 24 ساعة وبمعدل 7 أيام، ذلك أن هذه الشبكة تهدف لتسهيل الممارسة السريعة وتعد وسيلة فعالة في مواجهة مشكلات الإجرام المعلوماتي وأداة ناجعة للتغلب على التحديات الكبيرة التي يفرضها عصر المعلوماتية[25].

ب- الصعوبات الخاصة بمد المساعدة القضائية :

إن المعمول به دوليا أن طلبات الإنابة و المساعدة القضائية تتم عبر القنوات الدبلوماسية لكن هذا الأسلوب يتميز بالبطء. الأمر الذي يتعارض مع طبيعة الإنترنت وما تتسم به من سرعة كذلك أن الرد عن هذه الطلبات يمر بمراحل و إجراءات معقدة الأمر الذي ينعكس سلبا على القدرة على مكافحة جرائم الإنترنت.

جـ-العوائق في مجال التدريب :

إن الفوارق الفردية بين المتدربين و تأثيرها على عملية الإكتساب للمهارات المستهدفة لا سيما في مجال تكنولوجيا المعلومات و شبكات الإتصال حيث يوجد من لا يفقه في هذا المجال شيئا و على النظير من ذلك يوجد أناس على درجة

كبيرة من المعارف العلمية الدقيقة به كذلك أن الواقع العملي مختلف بين الدول فالملامح العامة للعملية التدريبية و ما يتعلق بها من وقائع و ملابسات لا يبلغ حد التطابق مع بيئة العمل الطبيعية للمتدربين المستهدفين.

الخاتمة :

إن جرائم المعلوماتية تعد ظاهرة إجرامية مستجدة نسبيا ولقد تنبهت حكومات الدول إلى حجم المخاطر والخسائر الناتجة عنها بإعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة يرتكبها الأشخاص على قدر كبير من الذكاء يمتلكون أدوات المعرفة التقنية التي يستخدمونها في الإعتداء على الحق في خصوصية المعلومات وعلى المعطيات المخزنة أو المنقولة عبر نظم وشبكات الإنترنت.

إن خطورة مثل هذه الجرائم تكمن في أنها تطال الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية. وإن إدراك الدول للآثار السلبية لهذه الجرائم يفرض على الدول إعطاء أهمية إستثنائية للتعامل مع هذه الظاهرة والحد من نطاق مخاطرها الإقتصادية والأمنية والإجتماعية والثقافية ولا يتأتى هذا إلا بتعاون دولي فعال لكونه يمثل الأسلوب الأمثل لموجهة هذا النوع من الجرائم نظرا لأنها غالبا ما تتم من أماكن مختلفة من العالم إن هذا التعاون لا يمثل خيارا فقط بل أضحى حتمية حيث انه يشكل الآلية الأكثر فعالية للوقاية من خطورة تلك الجرائم ولمنع مرتكبي هذه الجرائم من الإفلات من العقاب ولذلك يتوجب التوصل إلى قدر من الإتفاق بشأن معايير هذا التعاون وآليات تفعيل وكيفية مواجهة هذه الجرائم.

وفي الأخير يمكن أن تشفع هذه الورقة بمجموعة من التوصيات المتواضعة التي إستقيناها من هنا وهناك:

1/ التوسع في إجراء الدراسات الميدانية للوقوف على الأسباب الحقيقية الكامنة وراء تطور ونمو هذه الظاهرة الإجرامية .

2/ تنظيم المزيد من المؤتمرات والملتقيات العلمية حول جرائم المعلومات بحيث تتاح الفرصة لتبادل الخبرات بين كافة المعنيين بما في ذلك رجال الأمن ورجال القضاء والقانون والإعلام وخبراء تقنيات المعلومات .

3/ التأكيد على ضرورة عقد إتفاقيات دولية تعنى بظاهرة الإجرام المعلوماتي وحث الدول على الإنضمام إليها .
4/ إرساء قواعد التعاون الدولي في مجال حماية التكنولوجيا ومكافحة جرائم المعلومات وتفعيل الموجود منها
5/ رفع مستويات التنسيق والتعاون بين المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية سواء على مستوى الوقاية أو على صعيد ملاحقة الجناة ومحاكمتهم وإنزال العقاب بهم .
6/ دعم قدرات الأنظمة الجنائية الوطنية على مكافحة هذه الجرائم وذلك بتقديم المساعدة لسد الفراغ الحاصل في أنظمتها التشريعية وتعزيز تدابير وآليات مكافحة هذه الجرائم .

التهميش و الإحالات :

[1]- غالبا ما يتم انشاء هذه المكاتب بموجب اتفاقيات ثنائية بين دولتين أو إقليمية خاصة لما يتعلق الأمر بالدول المتجاورة جغرافيا.

[2] - تدابير مكافحة الجرائم المتصلة بالحواسيب مؤتمر الأمم المتحدة لمنع الجريمة وللعدالة الجنائية: المنعقد في بانكوك في18-2005/04/25 وثيقة رقم 1/conf 203/14 على الموقع الالكتروني: htt://www.un.org/arabic/events/conferences/crime-html (اخر زيارة (2019/12/22

[3] - حسين الغفاري ،**الجهود الدولية في مواجهة جرائم الانترنت**، بحث منشور على الموقع الالكتروني:www.cip.org.sa/vb/sharthread.php3697 ، ص 08 (أخر زيارة (2019/03/22.

[4] - هلالي عبد اللاه أحمد ،**إتفاقية بوداست لمكافحة جرائم المعلوماتية**، دار النهضة العربية، القاهرة، مصر،طبعة2007، 1 ،ص327.

[5] - صدرت هذه المعاهدة في الجلسة العامة68 للجمعية العامة للأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة ضمن اختصاص السلطة القضائية في الدولة طالبة المساعدة.

[6] - اعتمدت هذه المعاهدة بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14 .

[7] - هلالي عبد اللاه أحمد، مرجع سابق،ص332.

[8] - على سبيل المثال من بين الجرائم التي حصرتها الاتفاقية الأوربية للإجرام المعلوماتي المادة 1 الدخول غير المشروع ،المادة 2 الاعتراض غير المشروع،المادة 4. التدخل في البيانات ،المادة 5 التدخل غير المشروع في المنظومة ، المادة 6 إساءة استخدام الأجهزة، المادة 7 جريمة التزوير المتعلقة بالكمبيوتر ،المادة 8 جريمة التدليس المتعلقة بالكمبيوتر، المادة9 الجرائم المتعلقة بالأعمال

الإباحية و صور الأطفال الفاضحة ،المادة 10 الجرائم الخاصة بالانتهاكات الخاصة بحقوق الطبع و النشر و الحقوق المتعلقة بها.

[9] - تنص المادة 24 من الاتفاقية الأوربية للإجرام المعلوماتي " **تطبق هذه المادة على عملية تسليم المجرمين فيما بين الدول الأطراف للجرائم المنصوص عليها وفقا للمواد 2،11 بهذه الإتفاقية بشرط أن يعاقب عليها القانون بموجب القوانين بالدولتين المعنيتين طرفي الإتفاقية بالحرمان من الحرية لفترة لا تزيد عن سنة واحدة على الأقل أو بعقوبة أشد.** " أنظر هلالي عبد اللاه أحمد ، مرجع سابق، ص 300 .

[10] - هلالي عبد اللاه أحمد، مرجع سابق، ص 307.

[11] - حسين الغفاري، مرجع سابق، ص12.

[12] - محمد حمادة مرهج العيتي، **جرائم الحاسوب**، دار المناهج للنشر والتوزيع،عمان ، الأردن، 2005، ص167.

[13] - في الوقت الحاضر تقدم وزارة العدل الأمريكية مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا و آسيا و أوربا الشرقية و أمريكا اللاتينية بالإضافة إلى ما توفره من تدريب و تكوين لأجهزة تنفيذ القانون بهاته البلدان .

[14] - عبد الفتاح بيومي حجازي ، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت**، دار الكتب القانونية، القاهرة ، مصر ، 2002، ص 36.

[15] - محمد حمادة مرهج العيتي، مرجع سابق، ص210.

[16] - المرجع نفسه، ص،218.

[17] - جميل عبد الباقي الصغير ،**الجوانب الإجرائية للجرائم المتعلقة بالانترنت** ، دار النهضة العربية، القاهرة، 1998،ص73.

[18] - بورازم أحمد ،جرائم المعلوماتية،ص 5. بحث منشور على الموقع الالكتروني: www.cour de Batna.mjustici.dz ' اخر زيارة2019/06/15)

[19] - د/ حسين الغفاري، مرجع سابق، ص13.

[20] - بورازم أحمد ، مرجع سابق، ص4.

[21] - عبد الفتاح بيومي حجازي ، مرجع سابق ص،37.

[22] - ورقة عمل مقدمة من قبل خالد صالح المكاوي بعنوان " **تعزيز قدرات الموارد البشرية في عمليات التحقيق والإدعاء والمحاكمة في الجرائم المتصلة بالكومبيوتر**" بمناسبة الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر –الدار البيضاء- المملكة المغربية 3-9/جوان2007 على الموقع الالكتروني: www.arab.naiba.org/publications/crime/casablanca/Mawri3a.pdf

[23] - حسين الغفاري، مرجع سابق، ص14.

[24] - نفس المرجع ، نفس الصفحة.

[25] - هلالي عبد اللاه أحمد، مرجع سابق،ص388.

المراجع:

1-الكتب:

- جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998 .
- محمد حمادة مرهج العيتي ،جرائم الحاسوب،دار المناهج للنشر والتوزيع، الأردن، 2005 .
- عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت، دار الكتب القانونية، القاهرة ، مصر 2002 .
- هلالي عبد اللاه أحمد ، اتفاقية بوداست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر،طبعة2007،1.

2-المواقع الالكترونية:

- بورازم أحمد ، جرائم المعلوماتية،بحث منشور على الموقع الالكتروني: www.cour de Batna.mjustici.dz
- حسين الغفاري،الجهود الدولية في مواجهة جرائم الانترنت،بحث منشور على الموقع الالكتروني: www.cip.org.sa/vb/sharthread.php3697
- مؤتمر الأمم المتحدة لمنع الجريمة وللعدالة الجنائية: المنعقد في بانكوك في18-2005/04/25 وثيقة رقم conf/1 203/14 على الموقع الالكتروني: htt://www.un.org/arabic/events/conferences/crime-html
- ورقة عمل مقدمة من قبل خالد صالح المواري بعنوان " تعزيز قدرات الموارد البشرية في عمليات التحقيق والإدعاء والمحاكمة في الجرائم المتصلة بالكومبيوتر" بمناسبة الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر –الدار البيضاء- المملكة المغربية 3-9/جوان2007 على الموقع الالكتروني: www.arab.naiba.org/publications/crime/casablanca/Mawri3a.pdf