

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

Cybercrime - a contemporary concept of crime and a global challenge to penal protection

شويرب جيلالي

جامعة ثليجي عمار الأغواط

مخبر الحقوق والعلوم السياسية

dj.chouireb@lagh-univ.dz

ط د مراد فائزة *

جامعة الدكتور يحي فارس المدية كلية الحقوق

والعلوم السياسية /المخبر السيادة والعولمة

merad.faiza@univ-medea.dz

تاريخ نشر المقال: 2025/03/20

تاريخ قبول المقال: 2025/01/31

تاريخ إرسال المقال: 2024/10/21

الملخص:

تتميز الجريمة الإلكترونية بأنها جريمة يرتكبها مجرمون غير تقليديون وأنها عابرة للحدود مما يصعب من مكافحتها رغم ما تبذله الدول من تعاون قضائي أمني وما تقوم به الشرطة الجنائية الدولية ممثلة في الإنتربول وكذا ما يتم من مكافحة وفق آليات إجرائية أبرزها نظام تسليم المجرمين وتبادل الخبرات الفنية والتقنية وجهود التوعية الرقمية للحماية من هذه الأفعال رغم الصعوبات القانونية والميدانية التي تعيق هذا التعاون. الكلمات المفتاحية: الجريمة الإلكترونية، التعاون الدولي، آليات الحماية، الأمن المعلوماتي، الصعوبات

Abstract :

Cybercrime is characterized as a crime committed by non-traditional criminals and it is transnational, which makes it difficult to combat it despite the judicial and security cooperation of States and the criminal police represented by Interpol, as well as the fight against procedural mechanisms, most notably the extradition system, the exchange of technical and technological expertise and international awareness efforts to protect against these acts despite the legal and field difficulties that hinder this cooperation.

Keywords : cybercrime , international cooperation, protection mechanisms, information security, difficulties

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

مقدمة :

يشهد العصر الحديث ثورة تكنولوجية رقمية لا حدود لها، فهو عصر المعلومة بل التسابق نحو إكتسابها كقوة دفاعية للدول وللأفراد تحافظ من خلالها على الأمن القومي وتضع على أساسها استراتيجيتها الدفاعية والهجومية وقد أصبح الفضاء الإلكتروني مجالا لتبلور العلاقات الدولية سلبا أو إيجابا وفقا لتحكم كل دولة فيه من خلال إمتلاك المعلومة، كما أصبح مجالا للأفراد تستخدم فيه هذه المعلومة بأنماط مختلفة ومن هذه الإستخدامات نشأ نوع جديد من الإجرام جعل صورة

الجريمة الحديثة تختلف عن الصورة التقليدية من حيث طبيعتها ونطاقها ووسائلها وآثارها، إذ أخذ شكل إختراقات داخل أنظمة المعلومات مما أنتج سوء إستخدام للتكنولوجيا سيما شبكة الإنترنت. وتعد الجريمة الإلكترونية عدوانا على بيانات موجودة داخل أنظمة معلوماتية بغية نشرها أو تعطيلها أو إستخدامها إستخداما مضرا، هذه الأفعال فاجئت المجتمع الدولي وخلفت أضرارا مدمرة في ظرف وجيز، كما خلفت حروبا إلكترونية أوسبيرانية قائمة اليوم هي حرب المعلومة وواقع الحال يبرز ما لهذه الجرائم من تأثير وصل إلى شل حكومات وقطاعات بأكملها من خلال إختراق مواقع حكومية لدول كبرى وتعطيل عمل أنظمتها المعلوماتية، فضلا على تأثير هذا النوع من الإجرام على مجالات حياة الأفراد من خلال مساسه بحياتهم ومصالحهم المادية والمعنوية وخصوصيتهم وأمنهم وهو ما جعل الدول اليوم في تحد لأجل حماية الفضاء الإلكتروني وفق العمل على تأمين المعلومة أو الأمن السيبراني. وهو ما يضيف أهمية على دراسة الجريمة الإلكترونية وعلى دراسة الأمن المعلوماتي كسلاح إستراتيجي .

وعليه لابد من إستجلاء الإجراءات المتخذة دوليا لمكافحة الجريمة الإلكترونية على مستوى التشريع وفي ميدان العمل

ثم معرفة العراقيل التي تعيق تحقيق أهدافها، كما نبحت في بعض آفاق حماية الأفراد والدول باعتبار الضرر يمس كافة المستويات.

بناء على ما تقدم نطرح إشكالية الدراسة كالاتي

ما مدى التحديات القانونية والقضائية الدولية لتكريس الأمن المعلوماتي ومحاربة الجريمة الإلكترونية ؟

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

وللإجابة على الإشكال تناولنا الدراسة من خلال مبحثين خصصنا المبحث الأول للآليات أو الجهود الدولية لمكافحة هذا النوع من الإجرام من خلال التعاون القضائي و الأمني كأداة حماية في المطلب الأول ثم آلية تسليم المجرمين كأداة ردع في المطلب الثاني لنخصص المبحث الثاني للصعوبات التي تعترض العمل الدولي في المطلب الأول ثم آفاق وتطلعات العمل الدولي في مجال الحماية كمطلب ثان .

وقد إستخدمنا في دراستنا المنهج الوصفي في عرض المعلومات وتحليلها كما استخدمنا المنهج التاريخي عند تقديمنا لنظرة شاملة في بعض الأجزاء من الدراسة.

المبحث الأول: التحديات الدولية في تكريس أمن المعلومات

كما أسلفنا سابقا إن دولية الجريمة المعلوماتية وسرعتها وسهولة تنفيذها و إخفاءها صعب من تعريفها ومحاربتها ومن توفير الأمن المعلوماتي أو ما اصطلح عليه بالأمن السيبراني أي تأمين المعلومات من طرف جميع الدول متعاونة في ذلك بمقتضى الضرورة والحتمية في محاربة هذا النوع من الجرائم، و لأن الأسرار المعلوماتية هي السلاح الذي يستخدمه مجرمي المعلوماتية أو ما يطلق عليهم

hackers of informatics, hackers, fraudsters information, criminals of information

بات على الدول لزما التكاثر لتأمين حماية السر المعلوماتي، وعليه نتناول في المطلب الأول الآليات العملية أي الميدانية للتعاون الدولي في سبيل مكافحة هذا النوع من الجريمة

المطلب الأول: التعاون القضائي والأمني لمكافحة الجريمة المعلوماتية

فضلا على التشريعات والقوانين التي تتصلى هذا النوع من الإجرام والتي لا بد أن تتلائم مع ضرورة التعاون الدولي بين أنظمة مختلفة، نشير إلى دور الإجراءات القضائية الجنائية والأمنية ممثلة في القضاء و مؤسسات الشرطة والتي تلعب دورا هاما في تحقيق هذا التعاون والتي سنتناولها في مايلي

الفرع الأول : تطوير وسائل مكافحة الجريمة التقليدية لتلائم مع طبيعة هذه الجريمة

ونقصد بالوسائل آليات تنفيذ القواعد القانونية فرغم ما لتوحيد التشريعات الجنائية من أهمية في تجريم هذه الأفعال دوليا وهو أمر ضروري إلا أن وسائل التنفيذ تبقى هي المحرك للحماية المعلوماتية وعليه نتناول الإجراءات العملية التي كرسست من خلالها الدول هذه الآليات تباعا

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

1-التعاون القضائي: وهو التعاون بين سلطات الدول في ملاحقة المجرمين وعقابهم وهو ما لا تستطيع سلطة دولة واحدة القيام به فضلا على أنه من ناحية التحقيق في الجريمة وجمع الأدلة قد تصطدم سلطات دولة معينة بعقبة سيادة باقي الدول وعليه فالحل لا يكون إلا بالتعاون القضائي الذي يمكن سلطة الدولة من ملاحقة المجرم وإجراء عملها القضائي فوق أراضي دولة أخرى. وللتعاون القضائي صورتين

أ التعاون الأمني: إذ لابد من التعاون على المستوى الإجرائي الجنائي أين يسمح لأجهزة الشرطة في مختلف الدول بالإتصال المباشر وذلك بإنشاء مكاتب متخصصة لجمع المعلومات و الأدلة عن مرتكبي الجرائم المعلوماتية هذا كخطوة أولى تأتي بعدها مرحلة التحقيقات والملاحقة القضائية الأمر الذي يؤكد على أهمية التعاون الدولي من خلال أجهزة الشرطة في الدول المختلفة، ويتم التعاون بين هذه الأجهزة من خلال

أ-1 التعاون في مواجهة الأزمات والظروف الطارئة :

عند حدوث أزمات طارئة يستوجب على الدول التحرك لمواجهةها في أسرع وقت مما يتطلب إمكانيات وخبرات متطورة ولما كان التطور التقني والتكنولوجي يتفاوت من دولة إلى أخرى كما أن أجهزة العدالة الجزائية تختلف من ناحية مواجهتها للجريمة المعلوماتية إن كان على المستوى التشريعي أو التقني والإجرائي، فكان لابد من التعاون بين الدول .

أ-2 القيام بعمليات أمنية مشتركة:

إذ يتطلب تعقب مجرمي المعلوماتية والبحث عن الأدلة الرقمية وعمليات التفتيش العابرة للحدود للحواسيب والأنظمة المعلوماتية وشبكات الإتصال تعاوناً أمنياً وفنياً في مكافحة تلك الجرائم¹

كأهم منظمة للشرطة على المستوى الدولي²Interpolالفرع الثاني: جهود الإنتربول

¹رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017/2018، ص 304 وما بعدها

²منظمة دولية تأسست في 1923/9/7 من أجل تكريس التعاون بين الشرطة الدولية الجنائية، مركزها في ليون. فرنسا، تصدر إخطارات حمراء ووثائق تنبيه تضمن من خلالها التتبع العالمي للمجرمين المطلوبين في جميع أنحاء العالم وهي تسهل عمل الشرطة الوطنية من خلال تمكينها من التعرف على المطلوبين ومساعدتهم في تسليمهم. شعارها "ربط الشرطة من أجل عالم أكثر أماناً"

<https://fr.wikipedia.org/wiki/Interpol>

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

تضطلع الإنتربول كمنظمة دولية للشرطة الجنائية بمكافحة الجريمة المعلوماتية إذ تدخل مكافحة هذا النوع من الإجرام ضمن مجالات عملها كالجرام المالي والمرتبط بالتكنولوجيا الحديثة والمجرمون الفارون وتهديد الأمن العام والإرهاب وغيرها من المجالات التي يمسها هذا النوع من الجرائم وهي لأجل ذلك تقدم المساعدة لكافة البلدان الأعضاء³ لتمكين أجهزة الشرطة فنيا وميدانيا القيام بعملها دوليا. وعلى مستوى الدول تعمل المنظمة من خلال مكاتبها المركزية الوطنية في كل دولة عضو أين يعمل بها شرطيون مؤهلون أعلى تأهيل.

وتقوم الإنتربول بدور الوسيط بين أجهزة الشرطة المختلفة من خلال تبادل المعلومات والتعاون في ملاحقة المجرمين، كما تعد الإحصاءات حول معدلات الجريمة الدولية وتؤدي دورا مهما في مجال تسليم المجرمين.

وتعمل على التعاون بين الشركاء في القطاعات العامة والخاصة كما تلعب من خلال نطاقها العالمي دورا هاما في تكريس تعاون دولي شامل لعدة قطاعات وتطوير التعاون الشرطي الدولي، فهي تقوم بإنفاذ القانون وتوفير منصات آمنة لتبادل البيانات والتدريب على الحد من التهديدات السيبرانية من أجل عالم أكثر أمانا.

كما أن عملها يجمع بين المرونة و الأمن بغية تسهيل التواصل على مستوى عالمي بشأن الجريمة الإلكترونية ولها مساحة عمل تتعلق بتبادل المعارف المتعلقة بجرائم الحاسوب مستعملة المعلومات العامة الواردة من مصادر غير شرعية مفتوحة لجميع المستعملين المعنيين مثل هذه الأفعال. بالإضافة لمنصة خاصة بمكافحة الجريمة الإلكترونية⁴

و نشير إلى أن الجزائر إنضمت إلى منظمة الإنتربول في عام 1963 وقد ربط المشرع الجزائري إجراءاته بأعمال المنظمة من خلال نصه على إجراءات تسليم المجرمين وآثارها سواء تم ذلك بموجب إتفاقيات أو بطرق دبلوماسية وتعتبر الجزائر عضوا نشيطا في المنظمة وهي تشارك في جميع مؤتمراتها⁵

³ 195 دولة عضو بها تعمل وطينا من خلال مراكز شرطة وطنية تابعة للمنظمة.

<https://fr.wikipedia.org/wiki/Interpol>

⁴ Interpol, La cybercriminalité traverse les frontières et évolue rapidement, 2024

<https://www.interpol.int/fr/Infractions/Cybercriminalite>

⁵ رابحي عزيزة، المرجع السابق، ص 309

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

- بالنسبة لعملها المنتشر عبر القارات ضد الجريمة الإلكترونية نأخذ القارة الإفريقية على سبيل المثال

نظرا لأن الدول الإفريقية تعمل على دمج البنية التحتية الرقمية في جميع جوانب المجتمع بما في ذلك الحكومة، الشركات، البنوك وغيرها... كما أن إفريقيا شهدت طفرة في التكنولوجيا الحديثة إذ تعد من أسرع شبكات الإنترنت والهاتف نموًا في العالم سيما بسبب الاستخدام المتزايد للهواتف الذكية مما يجعل هدف المحتالين سرقة البيانات الشخصية ولذا وجب عليها تقوية إطار الأمن السيبراني بالتعاون مع الإنتربول والقطاعين العام والخاص وعليه فإن الإنتربول تتعاون مع⁶ AFRIPOI

من أجل منع التصيد الاحتيالي والابتزاز الإلكتروني من أمثلة القضايا التي تصدت لها الإنتربول في إفريقيا

- في ماي 2022 Delilah عملية -

أين تم إلقاء القبض على مواطن نيجيري في عملية دولية نفذت في أربع قارات أين قاد منظمة إجرامية إلكترونية عابرة للحدود الوطنية وقام بأفعال صنفت على أنها عمليات تصيد إحتيالي ضخمة وعمليات إحتيال في أوامر النقل المزيفة استهدفت الشركات والأفراد⁷.

كما تتعاون مع يوروبول والمكتب الأوروبي للشرطة EUROPOL وهو منظمة تابعة للاتحاد الأوروبي تتعامل مع

المخاطر الجنائية، هدفها تحسين فعالية وتعاون السلطات المختصة في الدول الأعضاء في الإتحاد المسؤولة عن منع ومكافحة الجريمة المنظمة الدولية الخطيرة والتي تعد الجريمة الإلكترونية وجهها الحديث. كما تساهم في تقديم جهود كبيرة في العمل القانوني للاتحاد الأوروبي ضد الجريمة المنظمة، مع التركيز على استهداف المنظمات الإجرامية والأهم من ذلك المساهمة في أمن الأفراد ودول الاتحاد. وتتعاون

⁶AFRIPOI est une institution technique de l'Union Africaine qui a pour mandat de renforcer la coopération entre les services de police des États membres de l'UA dans la prévention et la lutte contre la criminalité transnationale organisée, le terrorisme et la cybercriminalité. Son statut a été adopté par la Conférence de l'UA en janvier 2017 et est entré en vigueur immédiatement Afin de renforcer les capacités des policiers dans les pays africains et de contribuer à l'achat de dispositifs et d'équipements appropriés pour lutter contre la cybercriminalité, AFRIPOI a établi une coopération avec des organisations internationales, dont INTERPOL. <https://afripol.africa-union.org/fr/>

⁷Interpol, opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC), 2024 <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique-AFJOC>.

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

يوروبول مع الوكالات المتخصصة المحلية والدولية كما تمثل شراكة قوية مع الإنترنت في ما يخص مكافحة الجريمة عبر الحدود وتقوم بجهود مساعدة معتبرة في هذا المجال⁸

الفرع الثالث: المساعدة القضائية

وهي "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم " وتتخذ المساعدة القضائية الدولية في المجال الجنائي عدة صور

أولا - تبادل المعلومات:

أي تقديم المعلومات والبيانات والوثائق والأدلة التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما بالإضافة إلى الإتهامات والإجراءات المتخذة ضدها، كما يشمل التبادل السوابق القضائية للجناة وهو مانصت عليه المادة ستة وعشرون (26) من إتفاقية بودابست لمكافحة الجريمة المعلوماتية⁹

ثانيا: نقل الإجراءات

وهو ما يقتضي قيام دولة بمقتضى إتفاقية أو معاهدة باتخاذ إجراءات جنائية و هي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى و لمصلحة هذه الدولة متى توفرت مجموعة من الشروط أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها، بمعنى أن تكون مقررّة في قانون الدولة المطلوب إليها عن ذات الجريمة و أن تكون هذه الإجراءات ذات أهمية من شأنها أن تؤدي دورا مهما في الوصول إلى الحقيقة. ولقد أقرت العديد من الإتفاقيات الدولية و الإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية، منها معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في

⁸أمينة قفاف، البيوروبول ودوره في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر في القانون الجنائي والعلوم الجنائية، قسم الحقوق. كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي الأغواط، ص 12

⁹تنص المادة 26 "يجوز لدولة طرف، في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجزها في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررّة طبقا لهذه الاتفاقية أو أن ذلك قد يؤدي إلى تقديم طلب للتعاون من جانب تلك الدولة الطرف بموجب هذا الباب....".

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

المسائل الجنائية " وكذا إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية"¹⁰. مما يسهل عمل الشرطة الجنائية للدولة الطالبة.

ثالثا :الإنبابة القضائية الدولية

يقصد بها طلب إتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة هذا الأمر عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة وتعذر قيامها بهذا الإجراء بنفسها وهدف هذه الصورة تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع شهود أو إجراء تفتيش أو غيرها¹¹ وتجد الإنابة القضائية أساسها في القوانين الوطنية والإتفاقيات الدولية وفي مبدأ المعاملة بالمثل. ولأجل ذلك قد تشترط المعاهدات والإتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية وذلك بغرض التسريع في الإجراءات¹².

وقد نصت المادة الثامنة والعشرون (28) من إتفاقية بودابست على بعض أحكام الإنابة القضائية المتمثلة في

1-أن الدولة التي توجه الإنابة لا تتخلى بذلك عن سلطاتها للقاضي الأجنبي

2-كفالة أمن الشروط الموضوعية لحسن التنفيذ

وعليه فإن هذا الإجراء يعتبر من قبيل المساعدة القضائية للدولة الطالبة وليس نقلا للاختصاص .

رابعا-التنسيق القضائي والتقني :

¹⁰ نعمان عطاء الله الهيتي، قانون الحرب او القانون الدولي الانساني ، دار مؤسسة رسلان للطباعة والنشر والتوزيع، دمشق،

2008، ص 75

¹¹ نعمان عطاء الله الهيتي، نفس المرجع، ص 75

¹² صورية بوربابية، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 01، 2019، ص

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

أسلفنا أنه لابد من ملائمة القوانين الجزائية في ما يخص تجريم الفعل الذي يعتبر جريمة معلوماتية وهذا بأن يتم تجريمه في القوانين الوطنية للدولة الطالبة والمطلوب منها، فضلا على ملائمة التشريعات الوطنية الجزائية للاتفاقيات الدولية في هذا الشأن، إلا الأمر يبقى قاصرا عن محاربة متكاملة لهذا النوع من الإجرام لأنها وسيلة وقائية قاصرة لا تكتمل إلا بمساعدة تقنية ثنائية أو متعددة الأطراف.

كما لا يقتصر التعاون الدولي في مجال مواجهة الجريمة على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية و تبادل الخبرات بين الدول، ونجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها¹³، ذلك أن التقدم المتواصل في تكنولوجيات

المعلومات يفرض على الجهات القضائية والأمنية أن تواكب التطورات السريعة التي تشهدها هذه التقنيات والإلزام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى إن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم إتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذا النوع الجديد من الإجرام أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم وكذا رجال الضبطية القضائية، لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والقدرة في التعامل مع الجريمة والمجرم المعلوماتي. وعلى هذا الأساس كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للإستفادة من مهارات وتجارب الآخرين إذ لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية.

وهذه الأخيرة لا تتأتى دون تدريب متخصص يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب و بالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف و أماكن إختراقات الشبكة المعلومات و أجهزة الحاسبا لآلي وتحديد أنماط ونوعية الجرائم المعلوماتية وبياننا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية.

¹³ حيدر كاظم عبد علي، مبدأ التمييز بين المدنيين والمقاتلين، دراسة على ضوء القانون الدولي الانساني، مجلة الكلية الاسلامية

الجامعة، النجف، العدد 22، 2013، ص 422

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -**خامسا: الاعتراف بالأحكام الأجنبية**

أوجدت دولية الجريمة المعلوماتية هذه القاعدة كقاعدة عامة جرى العمل وفقها أن كل دولة لا تعترف إلا بأحكام قانونها الجنائي ولا تعتد إلا بالأحكام الجنائية الصادرة عن محاكمها الوطنية ولهذه القاعدة ما يبررها فهي من ناحية تعبير عن سيادة الدولة ومن ناحية أخرى فإن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، هذا ما يحول دون إمكانية تطبيق قانون أجنبي قد يتعارض مع نظام الدولة .

لكن مع استفحال ظاهرة الإجرام الدولي وضرورة تعاون الدول فيما بينها لمكافحة الجرائم العابرة للحدود وحتى لا يفلت الجناة من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة صار ممكنا الاعتراف بحجية الأحكام الأجنبية استنادا على معاهدات تبرم بين الدول.

إذن من المفاهيم التي يجب تجاوزها لدعم أواصر التعاون الدولي عدم قابلية الحكم الأجنبي للتنفيذ بحجة أنه مظهر لسيادة الدولة ولحقها في العقاب، حيث أنه لا ينبغي أن يقتصر الأمر على ما يرتبه الحكم الأجنبي من آثار سلبية تتعلق بعدم جواز محاكمة الشخص مرتين، حيث يدعوا الفقه الجنائي إلى ضرورة الإعتداد بالسوابق القضائية للحيلولة دون إفلات الجناة من العقاب¹⁴ وبذا يصبح للتعاون القضائي بين الدول آثار في تفعيل القواعد الجزائية .

المطلب الثاني: التعاون الدولي في مجال تسليم المجرمين

يعد نظام تسليم المجرمين الوجه الحقيقي للتعاون الدولي بالنسبة لمكافحة الجريمة العابرة للحدود سيما الجريمة المعلوماتية باعتباره آلية ردع للمجرمين تحد من خطرهم المنتشر خارج حدود الدولة الواحدة وتكاد تتحكم في خصوصية الفضاء الإلكتروني سيما التمويه وعدم وضوح الفعل والفاعل.

الفرع الأول: تعريف نظام تسليم المجرمين

هو آلية قانونية من آليات التعاون القضائي الدولي يهدف إلى قمع الجريمة بشتى أنواعها سواء كانت داخلية أو دولية يتم بين دولتين تسمى الأولى بالدولة الطالبة التي تسعى إلى إسترداد متهم لتحاكمه وتوقع الجزاء الجنائي عليه أو إسترداد محكوم عليه لتنفيذ عقوبة محكوم بها عليه.

¹⁴ رابحي عزيزة، المرجع السابق، ص 314

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

كما يعرف أنه مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى لكي يحاكم بها أو ينفذ فيها الحكم الصادر عليه من محاكمها أي قيام الدولة المطلوب منها التسليم بتسليم شخص موجود في إقليمها إلى الدولة طالبة التسليم بناء على طلب بغرض محاكمته عن جريمة نسب إليه ارتكابها أو تنفيذ حكم صادر ضده من محاكمها لمحاكمته أو تنفيذ العقاب عليه.

وقد عرفه النظام الأساسي للمحكمة الجنائية الدولية في المادة مائة واثنان (102) "يعني التسليم نقل دولة ما شخصا إلى دولة أخرى بموجب معاهدة أو إتفاقية أو تشريع وطني" ويظهر من هذا التعريف أن إستجابة الدولة المطلوب منها التسليم تكون متوافقة مع تشريع نافذ فيها أو إتفاقية تربط بين الدولتين¹⁵ كما قد ترفض الدولة لعدم وجود ذلك التشريع أو الإتفاقية

وهو ما يصعب مهمة تسليم المجرمين على أرض الواقع سيما المجرم الإلكتروني، فبالإضافة لخصوصية هذه الجريمة التي يصعب الوصول إلى مرتكبيها، هناك عقبة تسليم هؤلاء المجرمين التي قد تدوم لسنوات طويلة حتى يتم تسليمهم وقد لا يتم وإذا كان هذا الإجراء هو الوجه الحقيقي للتعاون الدولي كما أسلفنا فهو يعد من أصعب أوجه التعاون نظرا للعراقيل والصعوبات التي تعترضه.

الفرع الثاني : المصادر المرجعية لتسليم المجرمين

تنقسم مصادر تسليم المجرمين باختلاف الظروف التشريعية لكل دولة إلى

1-القوانين الداخلية التي تنظم تسليم المجرمين مثل المشرع الجزائري الذي أخذ بإجراء تسليم المجرمين كمظهر من مظاهر التعاون الدولي في قانون الإجراءات الجزائية في المواد 694 وما يليها

2-العرف الدولي الذي يطبق في حالة عدم وجود إتفاقيات أو قوانين داخلية

3-الإتفاقيات بين الدول سواء كانت ثنائية أو متعددة الأطراف، أو إتفاقيات دولية تتضمن أحكاما متصلة بتسليم المجرمين وتطبق في مثل هذه الحالات ولكنها ليست إتفاقيات تسليم¹⁶

¹⁵ رابحي عزيزة ،المرجع نفسه، ص 316

¹⁶ رابحي عزيزة ،المرجع نفسه، ص 317.318

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

كما أن تسهيل تسليم المجرمين عبر الحدود يعتبر جزءاً أساسياً من التعاون الدولي لمكافحة الجريمة الإلكترونية والذي يبنى على تبادل المعلومات والتعاون القضائي لتيسير تسليم المجرمين بين الدول كما يتطلب التدريب والمساعدة التقنية لتيسير عمليات التسليم والمساعدة القانونية المتبادلة بين الدول الأطراف

تركز هذه الآليات على:

تطوير نظم تبادل المعلومات لمحاربة الجريمة الإلكترونية على مستوى عالمي من خلال تحسين

وتطوير الأنظمة والمنصات الدولية لتبادل المعلومات لتعزيز القدرة على التصدي للتهديدات

المبحث الثاني: الصعوبات التي تواجه التعاون الدولي في نطاق حماية الأمن**المعلوماتية وتدابير الحماية**

إنه لأمر جلي أن التعاون الدولي بصورة عامة والتعاون القضائي والأمني في مجال مكافحة الجريمة المعلوماتية ليس بالأمر السهل وهذا لعدة أسباب تعيق العمل الميداني فضلا عن صعوبة ملائمة التشريعات سواء بسبب عقبة السيادة أو المصالح المتضاربة أو غيرها من الأسباب ونستعرض الصعوبات القانونية والإجرائية بشيء من التفصيل

المطلب الأول: الصعوبات القانونية والتقنية المعيقة للتعاون الدولي

رغم أن الاعتقاد دائما أن سبب فشل التعاون الدولي أو صعوبته في أي مجال يكمن في تطبيق القواعد القانونية من طرف الدول أو في قصر آليات هذا التعاون أو عدم الرغبة في تحقيقه، إلا أنه من الأسباب القوية لصعوبة مكافحة الجريمة الإلكترونية دوليا هو النص القانوني أو التشريع، فإختلاف التشريعات في تعاطيها مع الجريمة المعلوماتية سواء النصوص الإجرائية أو الموضوعية صعب من مهمة مكافحتها على النحو التالي

الفرع الأول: الصعوبات القانونية

أولا - عدم وجود نموذج موحد للنشاط الإجرامي :

يشكل عدم توحيد الشكل الإجرامي لسوء استخدام نظم المعلومات والحواسيب إحدى صعوبات مكافحة الجريمة المعلوماتية دوليا، فلم تتفق الأنظمة القانونية في بلدان العالم على صور محددة موحدة له، إذ هناك

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

تشريعات جرمت هذه الأفعال بصور مختلفة و أخرى لم تجرمها وهذا القصور في التشريع صعب من مهمة التعاون الدولي رغم ما يشهده الفضاء الرقمي من إختراقات وآثار تضر بالأفراد والجماعات والدول.

ثانيا-تنوع و إختلاف النظم القانونية الإجرائية:

ونقصد بالنظم الإجرائية طرق التحري والتحقيق والمحاكمة والتي قد تكون قانونية وفعالة في دولة وعلى العكس في دولة أخرى مما يمنع عمل سلطات إنفاذ القانون مثل نظام المراقبة الإلكترونية¹⁷

ثالثا - مشكلة الإختصاص:

يقصد بذلك الإختصاص الإقليمي للمحاكم الجزائية ويطرح مشكل الإختصاص من ناحية إمكانية خضوع الجرائم المعلوماتية التي ترتكب من خلال شبكة الإنترنت إلى القضاء الوطني بإعتبار القاعدة العامة تنص على إنعقاد الإختصاص

لمحكمة مكان إرتكاب الجريمة أو محكمة مكان إلقاء القبض على المجرم أو أحد شركائه أو محكمة موطن إقامة المجرم¹⁸ وهو ما لا يستساغ تطبيقه في جرائم عابرة للحدود تتم داخل فضاء معلوماتي أو سيبراني معقد من خلال شبكة غير مرئية

وغير تابعة لأي سلطة حكومية وعليه وجب تجاوز المعيار التقليدي الذي يحكم الإختصاص المكاني وهو ما يزيد من أهمية التعاون الدولي لتجاوز هذه العقبة مع توحيد التشريعات أو تقليص الفوارق بينها لحل إشكالية الإختصاص وهو تضيق لشغرة قانونية من بين الثغرات التي يستغلها مجرمو المعلوماتية وعليه لابد من توحيد وجهات النظر في ما يخص الإختصاص القضائي وملائمة القوانين الجنائية الموضوعية والإجرائية من خلال عقد إتفاقيات دولية ثنائية وجماعية. و مثاله ما نص عليه المشرع الجزائري في المادة 15 من القانون 04/09 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث نص عند تناوله الإختصاص القضائي على أنه "زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائية بالنظر في

¹⁷يتضمن هذا الأسلوب نظاماً إلكترونياً للمراقبة عن بعد، بموجبه يمكن التأكد من وجود أو غياب الشخص عن المكان المخصص لإقامته بموجب حكم قضائي؛ حيث يسمح للمحكوم عليه بالبقاء في منزله، لكن تحركاته محدودة ومراقبة بمساعدة جهاز مثبت في معصمه أو في أسفل قدمه -السوار الإلكتروني- وهو نظام يختلف من بلد إلى آخر بحيث لم تأخذ كافة الدول به.

¹⁸رابحي عزيزة، لمرجع السابق، ص 330

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني¹⁹ وعليه قد حسم المشرع الجزائري الأمر بنص داخلي وأرجع الاختصاص في الجرائم الإلكترونية التي تمس إقتصاد أو أمن الوطن إلى القاضي الوطني.

الفرع الثاني: الصعوبات العملية والتقنية

إذ تتفرد الجريمة المعلوماتية نظرا لخصوصيتها بتحديات تقنية أو فنية ترتبط بمجال تكنولوجيا المعلومات ما جعل مجال التحري عن المجرمين وجمع أدلة الجريمة أمرا دقيقا يحتاج إلى أهل الاختصاص وخلق إشكالات على أكثر من صعيد

أولا- الصعوبات المتعلقة بالمساعدات القضائية الدولية:

كما أسلفنا تتم المساعدة القضائية الدولية عن طريق إجراء الإنابة القضائية وهو ما يحصل من خلال الطرق الدبلوماسية أي عن طريق سفارة البلد، إلا أن هذا الأمر يتميز ببطء الإجراءات خصوصا بالنسبة للدولة المطلوب منها التسليم أو المساعدة والتي قد تدوم لعدة سنوات وهو ما يتعارض مع السرعة في التنفيذ والإخفاء الذي تتميز به الجرائم المعلوماتية .

ثانيا- الصعوبات المتعلقة بالتعاون الدولي في مجال التدريب :

بالنسبة لتدريب مختصين مؤهلين وكذا تبادل الخبرات الدولية فقد يصطدم الأمر بعدم رغبة بعض المسؤولين الإداريين بالقيام بها، فضلا على أن إمتلاك التكنولوجيا الحديثة بما تتميز به من تقنيات ليس بنفس المستوى لدى جميع الأفراد

فهناك من يحترفها وهناك من لا يفقه منها شيئا وهذا الأمر يعيق بطبيعة الحال عملية التدريب والتعاون الدولي في تبادل الخبرات.

¹⁹ المادة 15 من القانون رقم 09-04 المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 05/08/2009 الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 47

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

وعليه فإن آليات التدريب تهدف بشكل أساسي إلى تطوير نظم تبادل المعلومات لمحاربة هذا النوع من الإجرام على مستوى عالمي من خلال تحسين وتطوير الأنظمة والمنصات الدولية لتبادل المعلومات، لأجل التصدي للتهديدات بشكل وقائي و آخر علاجي.

المطلب الثاني : التدابير الإحترازية للحماية من الجريمة الإلكترونية

لابد للدول من القيام بمجموع تدابير للتوعية أولاً وللوقاية كأساليب لمكافحة جرائم المعلومات القائمة داخل إطار الإنترنت والتي تعتمد تكنولوجيا الإتصالات كأساس لعملها وتتمثل هذه التدابير في برامج تدريب لأفراد الأمن والقضاة، كما أنه من المهم توعية كافة أفراد المجتمع لوقايتهم من أن يقعوا ضحايا هذه الأفعال وعليه نتناول هذين النقطتين من خلال

الفرع الأول: توعية القضاة وأفراد الأمن الجنائي

يجب تقديم دورات تدريبية للقضاة لتعريفهم بالمفاهيم الأساسية للجريمة الإلكترونية وبرامج القرصنة والسرقة الإلكترونية سيما الخطيرة منها مثل برامج **التصيد**²⁰ أو **DDOS**²¹ **أوبوت نت** ونأخذ على سبيل المثال بوت نت أو شبكة البوتات **Botnet** وهي من أقوى برامج الإختراق الإلكتروني تتكون من مجموعة ضخمة من الأجهزة التي تم اختراقها عن طريق الإنترنت كل واحد منها يسمى بوت، تشغل عن طريق مكون البوتنت

²⁰التصيد الاحتيالي هو هجوم إلكتروني يستهدف إقناع الضحايا المحتملين بالكشف عن معلومات حساسة مثل كلمات المرور أو أرقام بطاقات الائتمان وبعده طرق فقد يقوم المجرم بانتحال هوية مزيفة أو التظاهر بالإستعجال وهو طريقة خطيرة وفعالة لعمليات الاختراق. كما يعمل عبر إرسال مجرمي الإنترنت لرسائل للأشخاص أو الشركات تتضمن رابطاً أو مرفقاً ضاراً ويكون الهدف من ذلك أن ينقر المستهدفون على الرابط وهو ما قد يقوم بتنزيل برنامج ضار أو يقودهم إلى موقع إلكتروني غير شرعي لسرقة معلوماتهم الشخصية. وتتحدد الطريقة استناداً إلى المهاجم والمعلومات التي يحاول الحصول عليها. ما هو التصيد الاحتيالي ؟

https://www.keepersecurity.com/ar_AE/threats/what-is-phishing.html

²¹ هجوم الحرمان من خدمة الموزع أو DDoS، هو نوع من الهجمات الإلكترونية ، يستهدف المهاجم موقع ويب أو خادم أو مورد شبكة بحركة مرور ضارة. ونتيجة لذلك، يتعطل الهدف أو يتوقف عن العمل، مما يؤدي إلى حرمان المستخدمين الشرعيين من الخدمة ومنع حركة المرور المشروعة من الوصول إلى وجهتها. Qu'est-ce qu'une attaque DDOS

<https://www.akamai.com/fr/glossary/what-is-ddos#:~:text=Dans%20le%20cadre%20d'une,r%C3%A9seil/2024>

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

أو ما يسمى بسيد البوت Bot Master يستخدم سيد البوت أوامر وتحكم لإدارة شبكته وتنفيذ هجماته وتسمية البوتنت هذه مشتقة من كلمة Robot Network أي

شبكات الروبوت حيث أن الأجهزة تخدم سيد البوت دون اختيارها، تمامًا مثل أجهزة الروبوت. إذ بمجرد أن ينضم الجهاز لشبكة الروبوت عن طريق إحدى طرق ضمه²² فإن سيد البوت يستطيع التجسس على صاحب الجهاز دون أن يشعر بذلك.

ومن المهم الإشارة إلى أنه من دون هذا الوعي الإلكتروني تكون القضايا الإلكترونية التي تم التحقيق فيها وملاحقتها بشكل جيد معرضة للخطر في المحاكم، نظرًا للطبيعة الشاملة للجريمة الإلكترونية التي قد تمس هذه القضايا ومهما كان تخصص القضاة والمدعين العامين سواء في قطاع المال والبنوك، أو في مجال الاتصالات، أو مكافحة الجريمة المنظمة والإرهاب أو استغلال الأطفال جنسيًا، فمن الضروري أن يكونوا مجهزين بفهم أساسي لظاهرة الجريمة الإلكترونية. ونفس الشيء بالنسبة للمحققين الجنائيين والمحليين الشرعيين، الذين يحتاجون إلى تحديثات مستمرة حول الاتجاهات الحديثة للإجرام والتحديات والتقنيات المتطورة²³

الفرع الثاني: توعية مستخدمي الإنترنت

إذ أصبح غالبية الأفراد في عصر الرقمية اليوم، إن لم نقل جميعهم يستخدمون الإنترنت ولذا وجب توعية جميع المستخدمين بالأفعال التي تمس بهم والتي تعد جرائم إلكترونية وهذا من أجل وقايتهم ألا يقعوا ضحايا لها وكذا إشراكهم في مكافحتها ويعتبر المسؤول الأكبر عن محو الأمية الرقمية هي الحكومات باعتمادها على الحملات الإعلامية في جميع وسائل التواصل والإعلام²⁴ سيما في ما يخص سرقة البيانات الشخصية للأفراد واستغلال الأطفال جنسيًا أو التحرش الجنسي الإلكتروني.

²² هناك عدة طرق لضم الأجهزة إلى شبكة الروبوت يمكن أن نقسمها إلى مباشرة وغير مباشرة 1- الطريقة المباشرة تكون بإرسال رسائل قصيرة لمعرفة إذا ما كان هناك ثغرة يمكن استغلالها للسيطرة على الجهاز وهو ما يعرف بـ Scanning ومن ثم تحميل برامج التحكم. 2- الطريقة الغير مباشرة تكون عن طريق استدراج الضحية لتحميل فايروس أو برامج خبيثة بالضغط على رابط وضعه سيد البوت، ورسائل البريد المزعجة Spam أشهر مثال على هذه الطريقة. شبكة البوتات، ويكيبيديا الموسوعة الحرة، 2024/01/12 سا
2024/10/01 17:55 الإطلاع
<https://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9>

²³ أمينة قفاف، مرجع سابق، ص 48.

²⁴ أمينة قفاف، المرجع نفسه، ص 45

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

وجدير بالذكر أنه حتى في الدول الصناعية والدول المتقدمة تكنولوجيا يعاني الأفراد من الأمية الرقمية رغم ما لتكنولوجيا الإتصالات من دور أساسي في حياتهم اليومية.

إذ أقرت الأجنحة الرقمية لأوروبا الصادرة عن الاتحاد الأوروبي في عام 2010 أنه

"تعاني أوروبا من نقص متزايد في مهارات تكنولوجيا المعلومات والإتصالات المهنية وعجز فيمحو الأمية الرقمية. هذه الفجوات تحرم العديد من المواطنين من المجتمع الرقمي والإقتصاد الرقمي وتعيق التأثير الكبير لتبني تكنولوجيا المعلومات والاتصالات على نمو الإنتاجية..."

وقد حثت الأجنحة الحكومات الوطنية على إطلاق حملات توعية لتمكين الأفراد من حماية أنفسهم من الجرائم الإلكترونية لأن التوعية خاصة بين الشباب تقلل بشكل كبير من هذه الأفعال، و يعتبر إجراء نشر المعلومات العامة الأفضل حول سلامة الكمبيوتر وسيلة لإنقاذ أعداد كبيرة من الناس من متاعب سرقة بياناتهم ومن أن يصبحوا ضحايا مباشرين للجريمة الإلكترونية.

وفي نتائج إحصائية وجد مقياس الأمن السيبراني الخاص لعام 2012 أن 74% من مواطني الاتحاد الأوروبي يعتقدون أن خطر أن يصبحوا ضحايا للجريمة الإلكترونية قد زاد في السنوات الأخيرة. كما أن الغالبية العظمى من مستخدمي الإنترنت يتجنبون الكشف عن المعلومات الشخصية عبر الإنترنت (89%)²⁵

الخاتمة:

نخلص إلى أن الجريمة المعلوماتية أو الإلكترونية تختلف إختلافا تاما عن الجريمة التقليدية، هذا الإختلاف النابع من الفضاء المعلوماتي الذي نشأت فيه، فأدواتها وأسبابها وخسائرها تتسم بالطابع المعلوماتي والذي يعتمد على معطيات وبيانات يتم إختراقها من طرف مجرمي المعلومات لإستعمالها في عمليات سرقة وتهديد ونشر وانتحال سواء على مستوى الأفراد أو لتعطيل قطاعات ومؤسسات بكاملها من خلال تشغيل شفرات الأنظمة المعلوماتية وهو ما يقوم به مجرمو المعلوماتية المحترفون أي الكراكرز .

هذا الأمر يتطلب ضرورة التعاون الدولي لتقويض الجريمة بإعتبار المصلحة المشتركة في مواجهتها، من خلال آليات ميدانية كالسلطات القضائية والأمنية التي عملت على مد يد العون وعلى إستعدادها

²⁵أمنية قفاف، المرجع نفسه، ص 46

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

المستمر ماديا وبشرياً للتدخل عند ملاحقة أو معاقبة المجرمين عبر مختلف الأقاليم، ورغم هذا إلا أن النسب الواقعية للجريمة المعلوماتية في تزايد مقلق على المستوى العالمي مما صعب السيطرة عليها أو إيقافها إذ وصلت في كثير من الأحيان إلى حد الهجوم السيبراني إن لم نقل الحرب السيبرانية، رغم ما يعترضها من صعوبات جعل عملها يتوقف أحيانا كما جعلتها تتطلع إلى تكريس تدابير موازية تحقق الحماية، يتشارك فيها الأفراد لحماية أمنهم وسلامتهم ولتحقيق حماية وقائية للمجتمع الدولي عن طريق التوعية الإلكترونية الحديثة. ورغم ذلك لابد من جهود وطنية أكبر و تعاون دولي أشمل من خلال وضع إستراتيجية أمنية على المستوى الوطني والدولي للقضاء على مشكلة أصبحت تهدد أمن المجتمع الدولي وذلك ب

-تدريب خبراء قانونيين تكون لهم الدراية والمهارة في مجال الحماية الأمنية أي الأمن المعلوماتي مهمتهم حماية الأنظمة المعلوماتية خصوصا داخل مؤسسات الدولة.

-وجود الإرادة السياسية الفعلية على المستوى الوطني و الإقليمي والدولي، لتفعيل التعاون الدولي على أرض الواقع لخلق تكامل إجرائي بين سلطات الدول ، فضلا على توحيد التشريعات لتجريم هذه الأفعال

-توعية الأفراد بأنماط الجريمة المعلوماتية من خلال الإعلام، فإذا كانت تكنولوجيا الإعلام والاتصال هي سلاح المجرمين فإنها سلاح ذو حدين وجب على الحكومات إستعمالها للتوعية الإعلامية لما لها من تأثيرو سرعة وسهولة في الوصول للأفراد

-تكوين القضاة وأعضاء الضبطية القضائية و أفراد الشرطة الجنائية وتدريبهم على إستعمال الوسائل والأدلة الرقمية الحديثة ومدهم بالخبرات الميدانية

-تكوين مستخدمي المؤسسات المالية خصوصا البنوك على المهارات التقنية والفنية التكنولوجية الحديثة في مجال الإتصالات لتمكينهم من الحماية الأمنية الإلكترونية لقطاع عملهم.

قائمة المصادر والمراجع

المصادر

1- إتفاقية بودابست لمكافحة الجريمة المعلوماتية 2001/11/23

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

2-القانون 04-09 المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال

ومكافحتها 2009/08/05

المراجع

الكتب

1-نعمان عطاء الله الهيتي، قانون الحرب أو القانون الدولي الانساني ، دار مؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، 2008

المذكرات والرسائل

1-رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية ، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2018/2017

2- أمينة قفاف، اليوروبول ودوره في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر في القانون الجنائي والعلوم الجنائية، قسم الحقوق. كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط. 2024/2023

المقالات

1-حيدر كاظم عبد علي، مبدأ التمييز بين المدنيين والمقاتلين، دراسة على ضوء القانون الدولي الانساني، مجلة الكلية الاسلامية الجامعة، النجف، العدد22، 2013

2-صورية بوربابة، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 01 2019

المواقع الإلكترونية

1- <https://www.interpol.int/fr/Infractions/Cybercriminalite>

2- <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique-AFJOC>

3- <https://afripol.africa-union.org/fr/>



ردمد إلكتروني: 2661-7404

المجلة الأكاديمية للبحوث القانونية والسياسية

ردمد ورقي: 2571-9971

ص.ص: 561 - 580

العدد: الأول

المجلد: التاسع

السنة: 2025

الجريمة الإلكترونية - مفهوم معاصر للإجرام وتحدي عالمي للحماية الجزائية -

4-https://www.keepersecurity.com/ar_AE/threats/what-is-phishing.html

5<https://www.akamai.com/fr/glossary/whatisddos#:~:text=Dans%20le%20cadre%20d'une,r%C3%A9se/2024>

6-<https://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9>