المجلة الجزائرية للعلوم السياسية والعلاقات الدولية المجلد 13العدد 18
جوان 2022

أساليب التعاون الدولي في القضاء على الجرائم الالكترونية

International Cooperation Methods in Eliminating Electronic Crimes

ط. د: عبد القدوس بوعزة(*)، ط. د: أيوب مخرمش(**)

تاريخ الاستلام: 2020/04/25 تاريخ القبول: اليوم 2022/4/13 تاريخ النشر: 2022/06/30

ملخص:

إن التطور السريع في تكنولوجيا الإعلام والاتصال، وظهور ما يعرف بشبكة الانترنت بكل ما حملته من تقدم وخدمات وما قدمته للبشرية من خدمات جليلة، ساهمت في تطورها ورقيّها في جميع المجالات وخصوصا في مجال المعاملات الالكترونية بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهر إلى الوجود نوع جديد من الجرائم يعرف بالجرائم الالكترونية أو الجرائم المعلوماتية.

وتأسيسا على ما تقدم سوف نحاول من

Abstract

The rapid development in information and communication technology, and the emergence of what is known as the internet network with all its progress and services and the great facilities it provided to mankind, contributed to the development of all fields, especially the domain of electronic transactions, whilst, it had a negative impact on the lives of people and the interests of states. All of these implications were manifested in the transformation of the internet and electronic spheres into a venue of malfeasance and misconduct, and thus a new type of crime emerged, known as electronic crime or information crime.

(*)- مخبر علم النفس وجودة الحياة، جامعة ورقلة، bouazza.abdelkouddous@univ-ouargla.dz

(**)- مخبر علم النفس وجودة الحياة، جامعة ورقلة، mekhermeche.ayoub @univ-ouargla.dz

خلال هذه الدراسة، معالجة هذا الموضوع وذلك من خلال الحديث عن مفهوم الجرائم الالكترونية أو ما يسمى بالجرائم المعلوماتية، حيث سنتعرض بالشرح والتفصيل إلى تعريف هذا النوع من الجرائم، وأنواعها والخصائص التي تميزها عن باقي الجرائم التقليدية، كما سنتطرق إلى مظاهر الجهود الدولية من أجل محاربتها والقضاء عليها ومعاقبة مرتكبيها.

كلمات مفتاحية: الجرائم الالكترونية؛ الجرائم المعلوماتية؛ جرائم الكمبيوتر؛ جرائم الانترنيت؛ محاربة الجرائم الالكترونية.

Based on the foregoing, the article seeks through this study, to address this issue by discussing the concept of electronic crime or what is called information crime and explaining its definition, types and exploring its characteristics that distinguish it from the rest of the traditional crimes, as well as addressing the international efforts carried out to combating and eliminating this new crime trend and the taken measures to punish the actors involved in these matters.

Keywords : Cybercrime, Information Crime, Computer Crime, Internet Crime, Combating Cyber Crime.

مقدمة:

لقد أدى التطور التكنولوجي الذي شهده العالم نهاية القرن العشرين وبداية القرن الواحد والعشرين وخاصة في مجال الاتصالات واختراع ما يسمى بالحاسوب الذي صار يستعمل في العديد من المجالات العلمية والترفيهية في الحياة، حيث أصبح وسيلة لا يستغنى عنها في كل مجالات العمل كالأعمال العسكرية والبنكية، ومع ظهور ما يسمى بشبكة المعلوماتية الدولية " الانترنيت " التي امتدت عبر كامل أنحاء المعمورة وربطت بين شعوبها، حيث تحول العالم إلى ما يعرف "بقرية كبيرة ".

أدى كل ذلك الى ظهور طائفة جديدة من الجرائم العابرة للحدود، مختلفة عن باقي الجرائم التقليدية سميت بالجرائم المعلوماتية أو الالكترونية أو جرائم الانترنيت التي تعد هذه الأخيرة أداة لارتكابها ومحلا لها.

ويعتبر هذا النوع المستحدث من الجرائم على درجة بالغة من الخطورة، كما أن الأشخاص المجرمين الذين يقومون بهذا النوع من الجرائم على قدر عالٍ من الذكاء والحنكة.

ومع تفاقم هذا النوع من الجرائم وجدت الدول نفسها عاجزة عن محاربة هذا النوع من الجرائم بمفردها، الأمر الذي أدى إلى تكاتف الجهود الدولية وتعزيز سبل التعاون بينها واتخاذ التدابير الفعالة من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة بذاتها، ولا توجه الى مجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات، مستغلة في ذلك التطور المذهل لوسائل الاتصال، وأملهم في كل ذلك القضاء عليها ومعاقبة مرتكبيها.

ولكن ورغم التطور التشريعي الهام الذي عرفته السياسات الجنائية إن على المستوى الوطني او الدولي وما صاحب ذلك من تغيير للمفاهيم القانونية في سبيل محاربة الجريمة المعلوماتية التي لا تعترف بالإقليم فلا زالت هناك مجموعة من الإشكالات والصعوبات التي تعرقل وتقلص المجهودات الرامية إلى وضع حد لهذه الجرائم. لذلك تبرز العديد من المشكلات والتي تقف عائقا أمام مكافحة الجريمة المعلوماتية، منها ما يتعلق بالكشف عن الجريمة والوصول إلى الجناة، وبعضها متعلق بإثبات الجريمة المعلوماتية، كما قد يبرز للوجود صعوبات متعلقة بالتعاون القضائي الدولي وتحديد قواعد الاختصاص.

إشكالية الدراسة: كيف تستطيع الدول في إطار تعاون دولي (جماعي او ثنائي) مكافحة الجرائم السيبرانية؟ وما هي مختلف الإشكالات القانونية التي تعترض هذا التعاون؟

- أولا: مفهوم الجريمة الالكترونية:

قبل التطرق الى الموضوع وجب علينا تعريف الجريمة الالكترونية ومعرفة أنواعها، كذا معرفة الأسباب التي دفعت الى هذا النوع من الجرائم.

1. تعريف الجريمة الالكترونية (cybercrime):

تتكون الجريمة الإلكترونية أو الافتراضية **(cybercrimes)** من مقطعين هما الجريمة **(crime)**والإلكترونية **(cyber)** ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات.[1]

---

[1]- دياب موسى البداينة، **الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**، ملتقى علمي بالمملكة الأردنية الهاشمية.بتاريخ 04-09-2014م، ص 3.

لقد تعددت التعاريف التي حاولت أن تضع مفهوما دقيقا لما يعرف بالجريمة الالكترونية، ورغم ذلك لا يوجد إجماع على تعريف هذا النوع من الجرائم، من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية؟ وكما يقول فان دير هلست ونيف" هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة ...وفي اغلب الأحيان تستخدم الافتراضية والحاسوب والالكترونية والرقمية وكلها تعكس فجوات مهمة في العريف". وتعرف الجرائم الالكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.[1]

فجاء بعضها تعريفا تقنيا فنيا و بعضها الأخر تعريفا قانونيا ، و من ذلك منهم من يسميها بجرائم الحاسوب أو الانترنيت، أو جرائم التقنية العالية أو جرائم الياقات البيضاء ، و منهم من عرّفها بأنها كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية أو باستخدام تقنية اجهزة الحاسوب وشبكة المعلومات أو وسائل التواصل الاجتماعي , وينتج عنها حصول المجرم على فوائد مادية أو معنويه مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة او اتلاف المعلومات وتتعدى ذلك الى سمعة وشرف الشخص المعتدى عليه أو المعتدى عليها في هذه الجرائم , وتعتبر هذه الجرائم جناية أو جنحة ترتكب ضد فرد أو جماعة بدافع جرمي ونية الإساءة لسمعة الضحية أو جسده أو فكره أو ماله أو حياته ، سواءً كان ذلك بطريقة مباشرة أو بطريقة غير مباشرة باستخدام وسائل الاتصالات الحديثة والانترنيت.[2]

وقد عرّفها أحمد صياني بأنها تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها.[3]

وعرّفها البعض بأنها "الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب بالأذى الجسدي أو النفسي للضحية بشكل

---

[1]- المرجع السابق، ص 3.

[2] عمر احمد الشمري، أدوات الجرائم الإلكترونية ومخاطرها، مقال منشور على موقع يومية الزمان الدولية، على الرابط:**https://bit.ly/3cJMOt4** ، تاريخ الاطلاع: 2020/03/01.الساعة:17،45د

[3] إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط **http://democraticac.de/?p=35426:** تاريخ الاطلاع: 2020/02/29، على الساعة :18،22.

مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (غرف الدردشة، البريد الإلكتروني..)، والهواتف الجوالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت".[4]

وزارة العدل الأمريكية تقسم جرائم الإنترنت من أجل وضع تعريف دقيق لها إلى ثلاث فئات:

- ✓ الجرائم التي يكون فيها جهاز الحوسبة هو الهدف - على سبيل المثال، للوصول إلى الشبكة. الجرائم التي يستخدم فيها الكمبيوتر كسلاح - على سبيل المثال، لشن هجوم رفض الخدمة.
- ✓ الجرائم التي يتم فيها استخدام الكمبيوتر كملحق لجريمة - على سبيل المثال، استخدام الكمبيوتر لتخزين البيانات التي تم الحصول عليها بطريقة غير مشروعة.[5]

وتعرف اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية، الجريمة الإلكترونية بأنها مجموعة واسعة من الأنشطة الضارة، بما في ذلك الاعتراض غير القانوني للبيانات، وتدخلات النظام التي تعرض سلامة الشبكة وتوافرها، وانتهاكات حقوق الطبع والنشر.[6]

ومن تلك التعاريف نستخلص بأن الجرائم الالكترونية هي أي نشاط إجرامي ينطوي على جهاز كمبيوتر أو جهاز متصل بالشبكة أو شبكة. فبينما يتم تنفيذ معظم جرائم الإنترنت من أجل تحقيق ربح للمجرمين الإلكترونيين، يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة مباشرة لتدميرها أو تعطيلها، بينما يستخدم آخرون أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات غير القانونية أو الصور أو مواد أخرى. تقوم بعض الجرائم الإلكترونية على حد سواء - أي استهداف أجهزة الكمبيوتر لإصابتها بفيروس الكمبيوتر، والذي ينتشر بعد ذلك إلى أجهزة أخرى، وأحيانًا إلى شبكات كاملة فيعمل على تعطيلها أو تدميرها.

---

[4] –رماح الدلقموني، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، مقال منشور على موقع الجزيرة الإخبارية الالكتروني، قسم علوم وتكنولوجيا، بتاريخ 2015/04/06 على الرابط : ***https://bit.ly/2VQFDYX***. تاريخ الاطلاع 2020/02/29، الساعة: 14،22 د

[5] Margaret Rouse, cybercrime, [Available online] : **https://searchsecurity.techtarget.com/definition/cybercrime,** Date of perusal: 06/03/2020.à 15h35m.

[6] نفس المرجع.

2. أنواع الجرائم الالكترونية:

لقد تعددت الآراء واختلفت في وضع تصنيف للجرائم الالكترونية، فهناك من صنفها بحسب موضوعها وآخر قسمها بحسب طريقة ارتكابها.

فمعهد العدالة القومي بالولايات المتحدة الأمريكية صنّفها عام 1985 بحسب علاقتها بالجرائم التقليدية، فاعتبر أن:[7]

- **الصنف الأول**: يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة.
- **الصنف الثاني**: يتضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال، المخدرات، الاتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات.
- **الصنف الثالث**: يشمل كل ما يتعلق بالدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب.
- **الصنف الرابع**: يتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الانترنت.
- **الصنف الخامس**: الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية.

بينما يذهب الاتجاه العالمي الجديد خاصة ما ورد بالاتفاقية الأوروبية لعام 2001 لجرائم الكمبيوتر والانترنت فقد قسمت هذه الجرائم إلى:[8]

---

[7] **التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات**، "مركز هردو لدعم التعبير الرقمي"، القاهرة 2018.ص،8.

- ✓ الجرائم التي تستهدف عناصر المعطيات والنظم.
- ✓ الجرائم المرتبطة بالكمبيوتر "التزوير والاحتيال.
- ✓ الجرائم المرتبطة بالمحتوى " الأفعال الإباحية والأخلاقية.
- ✓ الجرائم المرتبطة بحقوق المؤلف والحقوق المجاورة.

ومع الانتشار الواسع للهواتف الذكية ووسائل التواصل الاجتماعي التي تُبلغ عن كل خطوة نقوم بها، فليس من المستغرب أن الجرائم الإلكترونية في ارتفاع .من السرقة إلى الاحتيال إلى الاستدراج، وفيما يلي تسعة جرائم إنترنت شائعة:[9]

- **التصيد**: يحدث التصيد الاحتيالي عندما يرسل المجرمون رسائل بريد إلكتروني احتيالية يتظاهرون فيها بأنهم من شركات مشروعة، في محاولة لجمع معلومات شخصية حساسة .في كثير من الأحيان، ستتم إعادة توجيه أي روابط في البريد الإلكتروني إلى موقع ويب مملوك من قبل المحتال، لذلك يجب الحذر بشأن المعلومات التي تقدمها على الإنترنت.

- **التحرش**: يستخدم المتسللون عبر الإنترنت الاتصالات الإلكترونية، مثل البريد الإلكتروني أو وسائل التواصل الاجتماعي أو مواقع الويب لمطاردة الأشخاص ومضايقتهم .تشمل أشكال المضايقات عبر الإنترنت القذف أو الاتهامات الكاذبة أو التهديدات أو أي سلوك آخر يحط من قدر شخص ما أو يحرجه .يمكن أن تتضمن أحكام المطاردة عبر الإنترنت عقوبة السجن وغرامات باهظة.

- **انتزاع الفدية**: يمكن لمجرمي الإنترنت تثبيت برامج ضارة على نظامك والتي ستحتجز معلوماتك المهمة كرهينة حتى تلبي مطالبهم .سيؤدي هجوم برامج الفدية الشائعة إلى إغلاق كمبيوتر الضحية أو تشفير ملفاتهم، والموافقة على إطلاق

---

[8] ITU, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February2009.available at https://bit.ly/2VOoNtO,

[9] Criminal defense,**9 Most Common Computer and Internet Cyber Crimes**, Elliott Kanter , Retrieved from: **https://bit.ly/3mek56w, 18/12/2021.**

سراحهم فقط إذا دفعت الضحية فدية .في كثير من الأحيان، ومع ذلك، لا يتم استرداد الملفات مطلقًا.

- **الدعارة**: سيقوم العديد من المرافقين بالإعلان عن خدماتهم في الإعلانات المبوبة عبر الإنترنت أو منتديات الوسائط الاجتماعية أو مواقع الويب الشخصية الخاصة بهم، مما يسهل على الأشخاص العثور عليها.

- **استغلال الأطفال في المواد الإباحية والاستغراب**: سيستخدم الجناة الإنترنت للوصول إلى الصور الجنسية الصريحة للأطفال، وأحيانًا الترتيب لعقد اجتماع وجهًا لوجه.

- **سرقة الملكية الفكرية**: يُعرف الإنترنت أكثر بالقرصنة، وهو يزخر بالكتب والموسيقى والأفلام وغير ذلك الكثير التي تم الحصول عليها بشكل غير قانوني وإتاحتها للتنزيل المجاني .على الرغم مما يقوله بعض الناس، فإن القرصنة ليست جريمة بلا ضحايا .لا يخسر الفنانون والمبدعون فحسب، ولكن العديد من التنزيلات غير القانونية تحتوي أيضًا على برامج ضارة مخفية يمكنها تدمير جهاز الكمبيوتر الخاص بك[10].

- **قرصنة الحساب**: نعلم جميعًا مدى أهمية حماية كلمات المرور الخاصة بنا - فكر في الضرر الذي يمكن أن يحدثه شخص ما إذا تمكن من الوصول إلى حساب بريدك الإلكتروني الذي يحتوي على جميع معلوماتك الشخصية.

- **الاتجار بالمخدرات**: مع صعود العملة المشفرة، زادت تجارة المخدرات عبر الإنترنت بشكل كبير خلال السنوات القليلة الماضية .المخدرات غير القانونية مثل الماريجوانا والكوكايين والميث والإكستاسي والهيروين كلها على بعد نقرات قليلة.

---

[10] What is intellectual property Theft? Criminal defense attorneys, retrieved from: **https://bit.ly/30CtVaO,** Retrieved, 18/12/2021.

- **تزوير بطاقة الائتمان**: يبدأ نصف جميع عمليات الاحتيال المتعلقة ببطاقات الائتمان ببرامج التجسس والبرامج الضارة المثبتة دون قصد على كمبيوتر الضحية أو الجهاز المحمول باليد .تعمل برامج التجسس في الخلفية، وتجمع بياناتك وترسلها مرة أخرى إلى المجرم، الذي يستخدم بطاقتك بعد ذلك لإجراء عمليات شراء احتيالية.

3. أسباب الجريمة الالكترونية

يمكن تلخيص الأسباب التي تؤدي إلى ظهور وانتشار الجريمة الالكترونية فيما يلي:

- **الانبهار بالتقنية المعلوماتية:** حيث أن انتشار التقنية المعلوماتية في المجتمعات الحديثة أدى إلى انبهار المجرمين بها، لذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة.
- **الرغبة في تحقيق الثراء السريع**: إن الحصول على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، قد تحقق ربحا سريعا وثراء فاحشا، وهذا يعد من أكثر الأسباب التي تدفع إلى انتشار الإجرام الالكتروني، بحيث تظهر الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات...).[11]
- **الأسباب الشخصية**: قد يكون الدافع إلى ارتكاب الجريمة الالكترونية نفسيا، حيث تتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الحقد أو الانتقام. فقد تبدأ الرغبة لدى الشباب نحو العبث بالأنظمة المعلوماتية من أجل ممارسة هواية اللعب، أو تعود إلى وجود ميل زائد لدى البعض بأن الاعتقاد بأن كل شيء يرجع إليهم، إذن تلك تمثل آفة نفسية تصيبهم ويتفاخرون بما قاموا به من جرائم، ليظهروا تفوقهم على الأنظمة المعلوماتية، وقد يكون الدافع نحو ارتكاب الجريمة المعلوماتية هو عامل الانتقام من عدو أو غيره.

---

[11] محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والانترنت**، منشأة المعارف بالإسكندرية 2006 – ص 106.

4. خصائص الجرائم الالكترونية

للجرائم الالكترونية خصائص تميزها عن باقي الجرائم الالكترونية يمكن أن نلخصها فيما يلي: [12]

- صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل أمنيّة ذات تقنية عالية، قد لا تكون متاحة لدى كل الدول.
- صعوبة قياس الضّرر المُترتّب عليها، كونه ضرراً يمسّ الكيانات المعنوية ذات القيم المعنوية أو القيم الماديّة أو كلاهما.
- سهولة الوقوع فيها، بسبب غياب الرّقابة الأمنية عند الكثير من الدول.
- سهولة إخفاء وطمس معالمها وآثارها والدّلائل التي تُدلّ على مرتكبها.
- قد لا تسبب عنفا جسديّاً مثل الجرائم التّقليدية.
- عابرة لحدود الزمان والمكان، بمعنى جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين.[13]

- ثانيا: التعاون الدولي في مجال محاربة الجريمة الالكترونية.

أمام تصاعد ظاهرة الجريمة الالكترونية، وجدت الدول نفسها عاجزة بمفردها على محاربة هذه الظاهرة لذا كان واجب عليها التكاتف والتعاون من أجل مواجهة الجريمة الالكترونية

1. مفهوم التعاون الدولي:

يمكن تعريف التعاون الدولي على أنه مجموع الجهود المبذولة بين دول العالم من أجل تحقيق مصلحة الدول المتعاونة وفي سبيل تحقيق الأمن والسلم الدوليين ومواجهة

---

[12] اسراء جبريل رشاد مرعي، الجرائم الإلكترونية" الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية، على الرابط: ***https://democraticac.de/?p=35426*** تاريخ الاطلاع: 2020/03/08.الساعة: 22،14د

[13] عبد الله حسين على محمود: "**سرقة المعلومات المخزنة في الحاسب الآلي**"، دار النهضة العربية، القاهرة، 2002، ص 351.

التحديات السياسية والاجتماعية والاقتصادية والأمنية. وهناك من عرفه " بأنه مد العون المتبادل، أي تبادل المساعدة والعون لتحقيق هدف معين".

أما مصطلح التعاون الدولي لمكافحة الجرائم الالكترونية، فيعد من المفاهيم التي يصعب تحديد تعريف جامع مانع لهاو ويرجع ذلك لعدة أسباب من بينها اتساع المجال والصور والأشكال التي يتخذها هذا التعاون وعدم إمكان حصرها أو حصر الوسائل الجديدة والمتجددة التي تجعل من هذا التعاون ظاهرة متغيرة ومتطورة بشكل مستمر، كذلك طبيعة واختلاف الصور الإجرامية لهذا النوع من الجرائم.[14]

2. أساليب التعاون الدولي في محاربة الجرائم الالكترونية:

لقد أثبت الواقع أن الدولة لا تستطيع بمفردها القضاء على الجرائم الالكترونية، وهذا لما تتميز به هذا النوع من الجرائم عن غيرها من الجرائم التقليدية من جهة، والتطور المذهل لوسائل الاتصال من جهة أخرى، فاذا كان من الضروري أن تمتلك الدول الامكانات التشريعية والقضائية والفنية لمكافحة الجرائم الالكترونية، فإن الأهم من ذلك أن تكون تلك القوانين متلائمة ومتجانسة بين مختلف الدول لأنها تحمي مصلحة مشتركة.

والتعاون الدولي في مجال مكافحة الجرائم الالكترونية قد أخذ عدة أوجه منها ما تعلق بضرورة التعاون في تفعيل القوانين لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجرائم الالكترونية، ويتمثل ذلك في التعاون القضائي وتسليم المجرمين المدانين بارتكاب الجرائم، والتعاون الشرطي، وابرام الاتفاقيات، ومنها ما تعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية والفنية التي من شأنها أن تمنع ارتكاب الجرائم الالكترونية.

ويمكن توضيح أساليب التعاون الدولي في محاربة الجرائم الالكترونية فيما يلي:

---

[14] ترجمان نسيمة، التعاون الدولي في مجال مكافحة جرائم التوقيع الالكتروني، مجلة صوت القانون، مج7، عدد1، 2020، ص، 56.

1.2التعاون القضائي الدولي في مواجهة الجرائم الالكترونية:

يعد هذا النوع من التعاون الآلية الرئيسة للكفاح ضد الجرائم العابرة للدول بأبعادها المختلفة.[15]

ويتخذ هذا النوع من التعاون عدة صور منها:

- ✓ تبادل المعلومات: وهـو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والاجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة.
- ✓ نقل الاجراءات: وتعني قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ اجراءات جنائية وهي بصدد جريمة ارتكبت في اقليم دولة أخرى ولمصلحة هذه الدولة متى ما توفرت شروط معينة، من أهمها التجريم المزدوج، وأن تكون الاجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تودي دورا مهما في الوصول إلى الحقيقة.[16]

وقد أقرت العديد من الاتفاقيات الدولية والاقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الاجراءات في المسائل الجنائية.[17]

إن التعاون القضائي الدولي يوفق بين الدول واستقلال كل دولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب وبدون هذا التعاون لا يمكن للدولة من الناحية العملية إقرار حقها في العقاب، ومن هنا فإن التعاون الدولي تحتمه الضرورة العملية لسببين:

---

[15] أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم، ورقة مقدمة في المؤتمر المغاربي الأول **حول المعلوماتية والقانون** المنعقد في: 28-2009/10/29 بطرابلس- ليبيا، ص3

[16] سالم محمد سليمان الأوجي: **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية**، رسالة دكتوراه (غير منشورة)، كلية الحقوق بجامعة عين شمس، 1997، ص425.

[17] اعتمدت بموجب **قرار الجمعية العامة للأمم المتحدة45/118** بتاريخ 1990/12/14.

الأول: تقييد سلطات الدولة بحدود إقليمها، فقانون العقوبات يمكنه التصدي في نطاق تطبيعه ما يتجاوز حدود إقليم الدولة، إلا أنه لا يمكنه مباشرة الإجراءات خارج حدود الدولة للإقليم الوطني لها وفقاً لمبدأ سيادة الدولة الأجنبية الأخرى.

الثاني: لا يمكن تطبيق قانون العقوبات بدون قانون إجراءات جنائية.[18]

- ✓ الانابة القضائية الدولية: هي طلب رسمي من محكمة لمحكمة أجنبية للحصول على بعض أنواع المساعدات القضائية، وتهدف هذه الصورة إلى تسهيل الاجراءات الجنائية بين الدول بما يكفل اجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود أو اجراء التفتيش وغيرها. و في هذا الصدد ابرمت العديد من الاتفاقيات التي ساهمت في اختصار الاجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على امكانية تبادل المعلومات شفويا في حالة الاستعجال.[19] و نفس الشيء نجده في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الاسلامي لمكافحة الارهاب الدولي 1999، و المادة 15 من اتفاقية الرياض العربية للتعاون القضائي 1983، و المادة 53 من اتفاقية شنغن 1990 الخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأعضاء ، و الفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمحاربة الفساد .

2.2 التعاون الشرطي:

ويعد التعاون الشرطي الدولي من أهم صور التعاون الدولي في مجال الجرائم العابرة للحدود ومنها جرائم الإنترنت ، لذلك سعت العديد من الدول إلى بناء اتفاقيات دولية ، حيث يستهدف ذلك تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وذلك بتجميع بيانات ومعلومات متعلقة بالمجرم المعلوماتي والجريمة من

---

[18] هلال عبد الله احمد، **الجوانب الموضوعية والاجرائية للجرائم المعلوماتية**، ط1، دار النهضة العربية، 2007، ص 521.

[19] الصغير جمال عبد الباقي، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية، 2002، ص 86.

خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة، وتبادل المعلومات والبيانات فيما بينها، والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة الوطنية في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها. أي أن عضو الإنتربول لا يقوم بنفسه بإجراء القبض على المتهم، بل أن هذا العمل منوط بجهاز الشرطة الوطنية في الدولة التي يتواجد المجرم في إقليمها، الأمر الذي يؤكد على احترام مبدأ السيادة الوطنية.[20]

3.2 تسليم المجرمين:

هذا النوع من التعاون الدولي هو نتيجة طبيعية للتحولات التي حدثت في كافة المجالات ومنها مجال الاتصالات وتقنية المعلومات، بحيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، فالمجرم المعلوماتي أصبح مجرما دوليا، لأن نشاطه الاجرامي لم يعد قاصرا على دولة معينة أو أقاليم، لأن المجرم قد يخطط لجريمته في دولة وينفذها في دولة أخرى ويهرب إلى دولة أخرى للابتعاد عن أيدي العدالة.

ولما أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية علة المجرمين الفارين من العدالة، كان لابد من ايجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الاجراءات القضائية فوق اقليمها، تتمثل في تسليم المجرمين الفارين لها. وهذا الاجراء يحقق مصلحة لكلا الدولتين، الأولى يضمن لها معاقبة المجرم الذي أخلّ بقوانينها وفي ذات الوقت يحقق مصلحة للدولة الأخرى المطلوب إليها التسليم كونه يساعدها على تطهير اقليمها من الأفراد الخارجين عن القانون. ولذلك حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين، ومنها الجزائر التي اتخذت من هذا الاجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الاجراءات الجزائية في المواد 469 وما يليها.

---

[20] مصطفى محمد موسى، **أساليب اجرامية وبالتقنية الرقمية ومكافحتها**، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003، ص 531.

4.2 الاتفاقيات والمعاهدات الدولية في مجال مكافحة جرائم الإنترنت:

مكافحة الجرائم المعلوماتية لن يكون له تأثير يذكر إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق والتعاون، وعليه يمكن القول بأي أي مجهود أو إجراءات لا أياً من الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم.[21]

إن الاتفاقيات الدولية هي وحدها الأداة التي يمكن أن تتبع عنها الالتزامات بين الدول، من ثم فإنه بدون الاتفاقية الدولية وخارج الشروط التي تنص عليها لا يمكن للدولة أن تعتمد على مساعدة الدولة المطلوب منها، على أن كل ما ملزماً يظل مع ذلك ممكناً وفقاً لما ينص عليه القانون الداخلي في كلاً من الدولتين.

كما أن عقد المعاهدات الدولية هي الأساس الذي ترتكز عليه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية وقد تم عقد العديد من المعاهدات الدولية التي تعمل على التعاون في مجال مكافحة الجرائم المعلوماتية.

ومن هذه المعاهدات نذكر:

- ✓ معاهدة بودابست لمكافحة جرائم الإنترنت: "the BuDAPEst convention on Cybcrimes"

في 2001/11/23م، شهدت العاصمة المجرية بودابست ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت "internet crimes" وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات، وبعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم عبر شبكة الإنترنت واستخدامها استخداما سيئا.[22]

وقد وقعت على هذه المعاهدة 26 دولة أوروبية بالإضافة إلى كندا وجنوب أفريقيا والولايات المتحدة الأمريكية. وللمعاهدة أهمية قصوى في توفير أسس الأمن العام، وتتضمن تلك المعاهدة 48 مادة وبعد التوقيع على تلك المعاهدة دولياً والتي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت " **internet crimes** " والتي انتقلت من مرحلة ابتدائية

---

[21] سليمان احمد محمد فضل، **المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، د.د.ن، القاهرة ،2007، ص512

[22] كوثر مازوني، **الشبكة الرقمية وعلاقتها بالملكية الفكرية**، دار الجامعة الجديدة، 2008، ص 640.

كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها الهواة في الأغلب الأعم من الحالات ودون أي فرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الإنترنت للخطر.[23]

- ✓ توصيات المجلس الأوروبي" بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات"**Europe council"** :

فنظراً للتطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشهود الدولة الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال. فقد أصدر المجلس الأوروبي التوصية رقم 13195 في سبتمبر 1995م في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات لحث الدول الأعضاء بمراجعة القوانين الجنائية الوطنية لتلاءم التطور في هذا المجال .[24]

ومن أهم ما ورد في توصية المجلس الأوروبي:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها المعلومات أثناء انتقالها.
- أن تسمح الإجراءات الجنائية لجهة التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بالتفتيش العادي.
- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل[25].

---

[23] محمد عبيد الكعبى، **الجرائم الناشئة عن الاستخدام غير مشروع لشبكة الانترنت**، ط2، دار النهضة العربية، 2009، ص 612.

[24] حسين بن سعيد الغافرى، **السياسة الجنائية في مواجهة جرائم الانترنت**، دار النهضة العربية، ص711.

[25] مصطفى محمد موسى، مرجع سابق ص520-521.

- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات (برامج – بيانات) تتعلق بأجهزة الكمبيوتر وتسليمها.
- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة. يتعين عندئذ أن تسمح السلطة الأخيرة بإجراء التفتيش والضبط[26].

إن التعاون الدولي في مجال محاربة الجرائم الالكترونية لا يقتصر على الجانب القضائي والأمني فحسب، وإنما يشمل كذلك المساعدات التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة لأخرى بحسب تقدم الدولة ورقيها.

و من ذلك نجد العديد من الاتفاقيات الدولية و الاقليمية ذات الصلة بمكافحة الجرائم الالكترونية ، قد دعت إلى ضرورة وجود تعاون دولي في مجال التدريب و نقل الخبرات بينها، ذلك أن التقدم المتواصل في مجال تكنولوجيات المعلومات يفرض على الجهات القضائية و الأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات و الالمام بها حتى يمكن التصدي للأفعال الاجرامية التي صاحبت هذه التكنولوجيا ، و من ناحية أخرى فإن تطبيق القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ اجراءات قد تتجاوز المفاهيم و المبادئ الموجودة في المذكرة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب و سرعة في التنفيذ و محو الآثار ،الأمر الذي يجعل الأجهزة القضائية -من قضاة تحقيق و قضاة حكم - أمام عاجزين على التعامل مع هذا النوع من الجرائم ، و من ذلك كان لابد أن تكون تلك الأجهزة على اختلاف أنواعها على درجة كبيرة من الكفاءة و المعرفة و القدرة في التعامل مع الجريمة المعلوماتية و المجرم المعلوماتي .

وعلى ذلك كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية من قبل أشخاص أكفاء ومؤهلين وخبراء في مجال تقنية المعلومات، لإكسابهم خبرة فنية في مجال الجرائم المعلوماتية. هذا التدريب راعى فيه العناصر الشخصية

[26] هلال عبد الله احمد، مرجع سابق ص630.

للمتدرب من حيث توافر الصلاحيات العلمية والقدرات الذهنية والنفسية لتلقي التدريب، وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان المخاطر والتهديدات ونقاط الضعف[27]وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية.[28]

أما فيما يتعلق بمنهج التدريب على التحقيق في الجريمة المعلوماتية فإنه يشتمل على اجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات وأساليب المعمل الجنائي، بالإضافة إلى ما يتعلق بالتفتيش، والضبط وكيفية استخدام الحاسوب كأداة للمراجعة والحصول على الأدلة.[29]

3.3 الإشكالات القانونية ومعوقات مكافحة الجرائم المعلوماتية.

رغم التطور التشريعي الهام الذي عرفته السياسات الجنائية الدولية وما صاحب ذلك من تغيير للمفاهيم القانونية في سبيل محاربة الجريمة المعلوماتية التي لا تعترف بالإقليم، وعلى الرغم من أن مواجهة هذه الطائفة من الجرائم تتم بعدة اتجاهات، سواء بسن الدول لتشريعات جديدة أو تعديل تشريعاتها القائمة، إلا أن محاولات التصدي لها اصطدمت بعدة صعوبات، نظرا لخصوصية الجريمة المعلوماتية، والتي ترتكب في عالم افتراضي لا يستغرق زمن ارتكابها سوى زمن بسيط، كما أن محو آثارها وإتلاف أدلتها عملية سهلة، وكشف هوية مرتكبها ليس بالأمر الهين، ولما كانت هذه الجرائم من طبيعة خاصة، فإن خطرها أو آثارها لم

---

[27] هشام محمد فريد رستم، **الجرائم المعلوماتية: أصول التحقيق الجنائي الفني**، بحث مقدم لمؤتمر القانون و الكمبيوتر والانترنيت، ط2، كلية الشريعة والقانون بجامعة الامارات العربية المتحدة، في الفترة 2005/03/01، ص496.

[28] الغافري حسين بن سعيد، ***الجهود الدولية في مواجهة جرائم الانترنيت***، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي خلال اجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجريمة الالكترونية الأول، الرياض يومي 05-06أفريل2004، ص20.

[29] نفس المرجع، ص 21.

تعد محصورة في النطاق الإقليمي لدولة معينة، الأمر الذي بات يثير بعض التحديات أمام السلطات القضائية الدولية. وسنحاول من خلال العناصر الآتية عرض مجموعة من الإشكالات والصعوبات التي تعرقل وتقلص المجهودات الدولية الرامية إلى وضع حد لهذه الجرائم:

- عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها.[30]

وربما يتجلى سبب غياب هذا النموذج في كثرة التعاريف والمفاهيم القانونية التي تؤطر هذا الجانب فكل دولة تضع تعريفات ومصطلحات حسب أنظمتها القانونية الجنائية بالخصوص هذه الكثرة الناتجة أساسا عن التطور الذي يعرفه المجال المعلوماتي وبالتالي تطور تقنيات وسائل ارتكاب الجرائم المعلوماتية او جرائم الانترنيت.

- مسألة الطبيعية القانونية للمال المعلوماتي ومدى اعتباره مالا ماديا او معنويا ومنقولا باعتبارها هذا الأخير محلا لمعظم جرائم الأموال.[31]
- عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بخصوص الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق [32]فجرائم الحاسب الآلي آثار خارجية ظاهرة ، وإنما تنصب على البيانات والمعلومات والمستندات المخزنة في نظم المعلومات والبرامج وبالتالي عدم الحصول على آثار مادية تشكل دليلا لإثبات الجريمة المعلوماتية الواقعة وفي غياب أعمال العنف والاقتحام والتكسير على خلاف الجرائم العادية يصعب إثبات الجريمة. بالإضافة إلى ارتكاب الجريمة المعلوماتية في الخفاء وتعمد الجاني عدم ترك أي دليل إدانة بعد ارتكابه للجريمة.

---

[30] حجازي عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت**، دار الفكر الجامعي، ط1، 2006 ص 142، 143.

[31] لحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، **مجلة الواحة القانونية**، العدد 2 السنة الرابعة، ص 376.

[32] نفس المرجع.

- عدم وجود معاهدات ثنائية أو جماعية بين الدول نحو يسمح بالتعاون المثمر في هذا المجال وحتى في حال وجودها فإنها لا تستطيع مواكبة التطور السريع لنظم وبرامج الحاسب وشبكة الانترنت[33].

وتبرز أهمية وضرورة وجود مثل هذه المعاهدات عندما نستحضر الطابع العابر للحدود والقارات الذي تتميز به الجريمة المعلوماتية بحيث تتباعد المسافة بين الجاني ونتيجة فعله مما يؤثر سلبيا على أعمال البحث والتحري والتحقيق ونتيجة الطابع العابر للحدود لهذه الجريمة تظهر مشكلة الاختصاص على المستوى الوطني والدولي والقانون الواجب تطبيقه[(35)].

- ضخامة كم البيانات المعلوماتية التي تقف عائقا أمام إجراءات التحقيق الجنائي والبحث عن دليل الإدانة والأكثر من ذلك تتجلى الصعوبة عندما يقوم الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الابقاء على أي دليل إثبات إضافة إلى أن طباعة كل ما هو موجود على الدعامة الممغنطة لحاسب متوسط العمر، يتطلب مئات ألاف الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدا للتحقيق.

خاتمة:

لقد ساعد التطور المتزايد لتكنولوجيا المعلومات في انتشار النشاط الإجرامي والجريمة الإلكترونية، لذلك بات من الضروري بدل المزيد من الاهتمام من المجتمع الدولي لمحاربة هذا النوع من الجرائم، وبما أن الدول لا تستطيع مكافحة هذا النوع من الجرائم لوحدها، كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية، حيث تتميز بصعوبة اكتشافها

[33] حجازي عبد الفتاح بيومي، مرجع سابق، ص، 145.

[(35)]- نفس المرجع، ص ،144.

وإثباتها، ويرجع ذلك إلى خصائص تقنية المعلومات ذاتها، وخاصة السرعة العالية التي ترتكب بها، وهو ما يسهل ارتكابها ويسهل طمس معالمها ومحو آثارها قبل اكتشافها.

الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة، أو خلال ملاحقة الجناة وكشف جرائمهم عبر الحدود. وهو ما استوجب تحسين التعاون الدولي من خلال بناء سياسة جنائية مشتركة من أجل مكافحتها في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية ببعضها البعض، وتعزيز قدرات القضاء، إضافة إلى تحديد عقوبات الجرائم المعلوماتية في إطار القوانين المحلية، كلّه يندرج في مكافحة طبيعة هذه الجرائم والتي تتميز بطابع خاص تقني بالدرجة الأولى وتمس أمن واقتصاديات مختلف دول العالم.

لكن غياب سياسة واضحة للتعاون الدولي والتنسيق بين الدول في مقاومة هذا النوع من الجرائم، قابله في ذات الوقت تعاون واضح بين محترفي الاجرام المعلوماتي، ففضلا عن البرامج التي يستعين بها القراصنة في أنشطتهم الاجرامية، فإنهم يتعاونون فيما بينهم ويتبادلون النصائح والخبرات.

كما أن العديد من المعوقات والإشكالات القانونية تقف أمام مكافحة هذا النوع من الجرائم، منها ما يتعلق بالكشف عن الجريمة والوصول إلى الجناة، وبعضها متعلق بإثبات الجريمة الالكترونية، إضافة إلى وجود صعوبات متعلقة بالتعاون القضائي الدولي وتحديد قواعد الاختصاص، أضف إلى ذلك كله:

- عدم وجود نموذج موحد للنشاط الاجرامي، حيث أن الأنظمة القانونية القائمة لمواجهة الجرائم الالكترونية في كثير من دول العالم، لا يوجد بينها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنيت الواجب تجريمها.
- اختلاف النظم القانونية الإجرائية، حيث نجد أن طرق التحري والتحقيق والمحاكمة التي ثبت فائدتها وفاعليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى.

- عدم وجود معاهدات ثنائية وجماعية بين الدول، وحتى في حال وجودها فهي قاصرة على عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسوب والانترنيت.

لذلك بات من الضروري على جميع الدول أن تسعى إلى تعديل قوانينها الداخلية وجعلها تواكب التطور العلمي والتكنولوجي، والعمل على إبرام اتفاقيات دولية ثنائية ومتعددة الأطراف لاحتواء هذه الجرائم والتخفيف منها.

قائمة المراجع:

-دياب موسى البداينة، **الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**، ملتقى علمي بالمملكة الأردنية الهاشمية. بتاريخ 04-09-2014م، ص 3.

-حجازي عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت**، دار الفكر الجامعي، ط1، 2006 ص 142، 143.

-عمر احمد الشمري، أدوات الجرائم الإلكترونية ومخاطرها، مقال منشور على موقع يومية الزمان الدولية، على الرابط: ***https://bit.ly/3cJMOt4***، تاريخ الاطلاع: 2020/03/01.الساعة:17،45د

-إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط ***http://democraticac.de/?p=35426*** :تاريخ الاطلاع: 2020/02/29، على الساعة :22،18.

–رماح الدلقموني، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، مقال منشور على موقع الجزيرة الإخبارية الالكتروني، قسم علوم وتكنولوجيا، بتاريخ 2015/04/06 على الرابط : *https://bit.ly/2VQFDYX*، تاريخ الاطلاع 2020/02/29، الساعة: 14،22 د

-Margaret Rouse, cybercrime, [Available online] :

https://searchsecurity.techtarget.com/definition/cybercrime, Date of perusal: 06/03/2020.à 15h35m.

- **التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات**، "مركز هردو لدعم التعبير الرقمي"، القاهرة 2018.ص،8.

محمد عبد الله أبو بكر سلامة، **جرائم الكمبيوتر والانترنت**، منشأة المعارف بالإسكندرية 2006 – ص 106.

-اسراء جبريل رشاد مرعي، الجرائم الإلكترونية" الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية، على الرابط: ***https://democraticac.de/?p=35426*** تاريخ الاطلاع: 2020/03/08.الساعة: 14،22د

-عبد الله حسين على محمود: **"سرقة المعلومات المخزنة في الحاسب الألي"**، دار النهضة العربية، القاهرة، 2002، ص 351.

-ترجمان نسيمة، التعاون الدولي في مجال مكافحة جرائم التوقيع الالكتروني، **مجلة صوت القانون**، مجلد 7، عدد1، 2020، ص، 56.

-أبو المعالي محمد عيسى، **الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم**، ورقة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في: 28-2009/10/29 بطرابلس- ليبيا، ص3

- سالم محمد سليمان الأوجي: **أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية**، رسالة دكتوراه (غير منشورة)، كلية الحقوق بجامعة عين شمس ،1997، ص425.

- **قرار الجمعية العامة للأمم المتحدة45/118** بتاريخ 1990/12/14.

-هلال عبد الله احمد، **الجوانب الموضوعية والاجرائية للجرائم المعلوماتية**، ط1، دار النهضة العربية، 2007، ص 521.

-الصغير جمال عبد الباقي، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية, 2002، ص 86.

-مصطفى محمد موسى، **أساليب اجرامية وبالتقنية الرقمية ومكافحتها**، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003، ص 531.

- سليمان احمد محمد فضل، **المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية**، د.د.ن، القاهرة ،2007، ص512

-كوثر مازونى، **الشبكة الرقمية وعلاقتها بالملكية الفكرية**، دار الجامعة الجديدة، 2008، ص 640.

-محمد عبيد الكعبى، **الجرائم الناشئة عن الاستخدام غير مشروع لشبكة الانترنت**، ط2، دار النهضة العربية، 2009، ص 612.

-حسين بن سعيد الغافرى، **السياسة الجنائية في مواجهة جرائم الانترنت**، دار النهضة العربية، ص711.

-هشام محمد فريد رستم، **الجرائم المعلوماتية: أصول التحقيق الجنائي الفني**، بحث مقدم لمؤتمر القانون و الكمبيوتر والانترنيت، ط2، كلية الشريعة والقانون بجامعة الامارات العربية المتحدة، في الفترة 2005/03/01، ص496.

-الغافري حسين بن سعيد، **الجهود الدولية في مواجهة جرائم الانترنيت**، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي خلال اجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجريمة الالكترونية الأول، الرياض يومي 05-06أفريل2004، ص20.

-لحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، **مجلة الواحة القانونية**، العدد 2 السنة الرابعة، ص 376.

-ITU, **ICT Applications and Cybersecurity** Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February2009.available at https://bit.ly/2VOoNtO,

-Criminal defense,9 Most Common Computer and Internet Cyber Crimes, Elliott Kanter , Retrieved from: **https://bit.ly/3mek56w**, 18/12/2021.

-What is intellectual property Theft? Criminal defense attorneys, Retrieved from: **https://bit.ly/30CtVaO**, Retrieved, 18/12/2021.