

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية United Nations Efforts in Fighting Cybercrime

بيدي أمال

جامعة الجلفة- الجزائر

a.biddi@univ-djelfa.dz

تاريخ النشر: 2022/06/03

تاريخ القبول: 2022/05/29

تاريخ الإرسال: 2022/01/30

الملخص:

لم تعد الجرائم اليوم بصورتها التقليدية تمثل خطرا بالمقابل لما أفرزته الثورة المعلوماتية من جرائم متطورة أو بما يعرف الجريمة السيبرانية، هذه الأخيرة التي أصبحت تهدد الفرد والمجتمع وأمن الدول، حيث تميزت بأنها جرائم عابرة الحدود عبر الوطنية، ذلك ما اقتضى تضافر الجهود الدولية والإقليمية والوطنية لمكافحتها. كما كان للأمم المتحدة دورا مهما ولافتا في هذا المجال، إذ حاولت من جهتها بعقد الكثير من المؤتمرات وإصدار العديد من القرارات التي من شأنها لفت الانتظار إلى أن الحلول التقنية وحدها لا تكفي لمكافحتها ولا لتوفير الحماية، بل لابد من وجود تشريعات جنائية ذات خصوصية تستوعب هذه الجرائم المعلوماتية.

الكلمات المفتاحية: الجريمة، السيبرانية، جهود، الأمم المتحدة، مكافحة.

Abstract:

Today's crimes in their traditional form are no longer a threat to the evolving crime of the information revolution or the so-called cybercrime, the latter of which threatens the individual, society and security of nations, whereby they were characterized as transnational crimes, which necessitated concerted international, regional and national efforts to fight them.

The United Nations also had an important and remarkable role in this field, where it tried per se to hold many conferences and issue many decisions that would draw attention to the fact that technical solutions alone are not sufficient to fight cybercrime or provide protection, but rather there must be specific criminal legislation that accom

modates these information crimes.

المؤلف المرسل

Keywords: Crime, cyber, efforts, United Nations, fighting.

مقدمة:

إن الانتشار الواسع و اللامتناهي للأنظمة المعلوماتية وشبكة الانترنت والتقنيات والبرمجيات أدى إلى ظهور نمط جديد من الجرائم والتي تعرف بالجرائم الالكترونية ، و تعد أحد أهم ما أفرزته الثورة المعلوماتية التي يشهدها العالم اليوم.

خاصة وأن استخدام أجهزة الحاسب الآلي أصبحت في متناول الجميع أفرادا ومؤسسات أي بمعنى أشخاص طبيعية أو معنوية وفي كل المجالات العامة والخاصة.

ولعل هذا ما أدى إلى انتشار هذا النوع من الجرائم ، حيث أن الجرائم السيبرانية أو الإلكترونية أصبحت من الجرائم العابرة للحدود ، وتعتبر شبكة الانترنت أداة الجريمة ، هذه الأخيرة التي تتميز بصعوبة اكتشافها وإثباتها ، إضافة إلى الطبيعة القانونية وخصوصيتها ، وأطرافها وأساليبها.

ونظرا لعدم قدرة وكفاية التشريعات سواء الوطنية أو الإقليمية على مكافحة هذا النوع من الجرائم لغياب الدليل المادي الذي يدين المجهني ، فإنها انتشرت بشكل واسع وأصبحت تهدد الأمن القومي للدول ، ولذلك كان من الضروري أن تبذل الأمم المتحدة جهودًا كبيرة في مجال مكافحتها.

حيث تقتضي أهمية الموضوع توضيح مفهوم الجريمة السيبرانية وأطرافها وخصوصية طبيعتها القانونية، والتأكيد على الفراغ التشريعي في مجال مكافحتها وصعوبة تحقيق التعاون الدولي بهذا الشأن.

وعليه حاولنا استعراض أهم الجهود التي بذلتها الأمم المتحدة في مجال مكافحة هذا النمط من الجرائم ، اعتقادا منها وإيمانًا بأن هذه الجرائم ذات خطورة بالغة ، تستوجب وتستدعي تعزيز تعاون كل الأطراف من أجل مكافحة هذه الجريمة والحد من انتشارها ، ومن أجل ذلك عقدت الكثير من المؤتمرات في إطار مؤتمراتها الخاصة بمنع الجريمة ومعاملة المجرمين والذي يعقد كل خمس سنوات منذ عام 1955م.

أما بالنسبة لأهداف الموضوع فهي تتمثل في التركيز على خطورة الجريمة وضرورة التعاون الأممي والدولي وعلى جُل المستويات من أجل المكافحة، أيضا من أهم أهداف الدراسة هو تقييم جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية والتأكيد على وجوب استيعاب هذا النوع من الجرائم وكل جوانبه سواء التشريعية أو طرق المكافحة وسبل الحماية والوقاية.

أما عن نطاق البحث : فتنحصر- دراستنا في البحث عن مفهوم الجريمة السيبرانية وكل ما يتعلق بها من خصائصها وأطرافها وطبيعتها القانونية التي تتميز بخصوصية سيتم التعرض لها أثناء دراسة موضوع البحث ، لنعرج في جزئية ثانية إلى جهود الأمم المتحدة في مجال مكافحة هذه الجريمة ، دون أن نتعرض إلى الجهود الإقليمية والوطنية حتى لا نخرج على نطاق موضوع البحث .

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

الإشكالية : تتمثل الإشكالية التي يثيرها موضوع البحث وتستوجب الإجابة عليها :

فما تتمثل جهود الأمم المتحدة لمكافحة الجريمة السيبرانية ؟ وهل وفقت في مكافحة هذه الجريمة واستيعاب خطورتها ؟

منهج البحث : يتم اختيار المنهج الواجب التوظيف في البحث من خلال طرح الإشكالية، وإشكالية موضوع هذا البحث تستوجب استخدام المنهج الوصف التحليلي ، وذلك بوصف الجريمة السيبرانية وتحليل مختلف الجهود التي بذلتها الأمم المتحدة في مجال مكافحتها ، مع توضيح أهم الصعوبات في هذا الشأن.

خطة البحث : للإحاطة بجميع جوانب موضوع البحث تعرضنا للكثير من النقاط : أهمها الإطار المفاهيمي للموضوع واستعراض مفصل للجهود الأيمية في مجال مكافحة هذه الجريمة وتقييم هذه الجهود، لنقف على أهم النتائج والتوصيات في الخاتمة.

1- الإطار المفاهيمي للجريمة السيبرانية

1.1- تعريف الجريمة السيبرانية :

يعرف هذا النوع من الجرائم بأنها : "كل عمل مخالف لأحكام قانون العقوبات والأخير يتضمن طبيعة العمل ومقدار العقوبة المنصوص عليها "

وهناك تعريف آخر هو : "كل عمل غير مشروع صادر عن إرادة آتمة يحدث لها عقوبة أو تدبير وقائي " أي بمعنى أنها الفعل أو الترك المعاقب عليه جنائياً¹ ، فالجريمة قانوناً هي الفعل أو الترك الذي نص عليه القانون بعقوبة مقدرة له.

أما كلمة السيبرانية فهي كلمة انجليزية مشتقة من كلمة (Cyber) وتعني الارتباط بالحاسوب ، أيضا يعني فضاء الانترنت ، أما معناها في اللغة اليونانية مشتق من كلمة (Kybemetes) وتعني الشخص الذي يدير دفة السفينة مجازاً للمتحكم².

ولم يتفق الفقه الجنائي على تسمية موحدة إذ يطلق عليها البعض الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية وآخرون يطلقون عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ، ويسميها البعض بجرائم الكمبيوتر والانترنت³.

¹ ألاء محمد رحيم حادي ، الجريمة السيبرانية ومخاطرها على الأطفال (الاشكاليات والحلول) (دراسة تحليلية في ضوء الاحصائيات البولوية والعربية والوطنية)، مجلة كلية التربية للبنات ، جامعة بغداد ، المجلد 28 ، العدد 4 ، 2017 ، ص: 1106.

² كركوري مباركة حنان ، خصوصية ارتكاب الجريمة السيبرانية في النظام المعلوماتي (دراسة تحليلية على ضوء القانون الجزائري) ، مجلة الدراسات الاستراتيجية والعسكرية ، المجلد 2 ، العدد 08 ، 2020 ، ص: 11.

³ مجمع البحوث والدراسات ، أكاديمية السلطان قابوس لعلوم الشرطة ، تروى - بسلطنة عمان ، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها ، البحث الفائز بالمركز الأول في مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015 ، 2016 ، ص: 20.

آمال بيدي

ولذلك فإن فقهاء القانون لم يستقروا على تعريف موحد جامع وشامل لمفهوم الجريمة المعلوماتية¹، ويرجع ذلك الاختلاف إلى تنوع الآراء والمفاهيم ، ولأن هذا النوع من الجرائم حديث ، وثقافة وقوانين الدول حول هذه الجرائم حديثة العهد ، زيادة على نخوف الدول من حصر هذه الجرائم في نطاق ضيق.²

ورغم الاختلاف حول تعريف هذه الجريمة، إلا أن خصائصها باتت شبه موحدة لدى الجميع ، ومن بين أهم الخصائص:

أ. الجانب التقني لهذه الجريمة: تستخدم في هذا النوع من الجرائم تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة ، كوسيلة من أجل تحقيق وتنفيذ الفعل الإجرامي المستهدف.³

ب. جريمة يصعب اكتشافها وإثباتها: تتسم هذه الجريمة بالسرعة والتطور في وسائل تنفيذها ، ولذلك يصعب اكتشافها وإثباتها، لأنها مستترة وسهلة في إتلاف الأدلة الخاصة بها، زيادة على نقص خبرة الجهات القائمة على مكافحتها ونقص القوانين الخاصة بهذا النوع من الجرائم.⁴

ج. الأسلوب المتميز في ارتكاب الجريمة: عادة تعتمد الجرائم التقليدية على أسلوب العنف من كسر وسرقة وقتل وخطف ... إلخ، أي بذل جهد عضلي لارتكابها، لكن الجرائم السيبرانية تحتاج إلى جهد عقلي وتقني والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.⁵

د. الجريمة المعلوماتية تتم عادة بتعاون: تتم الجريمة المعلوماتية بتعاون أكثر من شخص على ارتكابها ، فكل له جانبه من المشاركة ، فمنهم من يغطيها تقنياً أو فنياً ومنهم من يتولى أمر التلاعب وتحويل المكاسب.⁶

أما بالنسبة لأطراف الجريمة السيبرانية : هما طرفان المجرم السيبراني والمجني عليه.

1/المجرم السيبراني : يتمتع المجرم السيبراني بقدرة كبيرة من الذكاء ومهارة فائقة في اختراق الشبكات وكسر- الشفرات وكلمات المرور، موظفاً مهارته في تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات ، وعادة ما يكون هؤلاء الفئة من ذوي مكانة في المجتمع ، وقد أطلق عليهم مصطلح ذوي " الياقات البيضاء".⁷ ويصنف المجرم السيبراني إلى:⁸

أ. الهواة : ويكون إجرامهم بغرض التسلية دون الاضرار بالمجني عليه.

¹ خالد مدوح ابراهيم ، الجرائم المعلوماتية ، ط1 ، دار الفكر الجامعي ، الاسكندرية (مصر) ، 2009 ، ص:73.

² روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، المجلة الالكترونية الشاملة متعددة التخصصات ، الأردن ، العدد 24 ، 2020 ، ص:08.

³ شريف حسين محمد محمد حسن ، الجريمة الالكترونية في منظور القانون المجتمع ، حوليات آداب عين شمس ، عدد خاص ، المجلد 45 ، العدد

14 ، 2017 ، ص:22.

⁴ المرجع نفسه ، ص:23.

⁵ آلاء محمد رحيم حادي ، المرجع السابق ، ص:1109.

⁶ المرجع نفسه ، ص:1109.

⁷ روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، المجلة الالكترونية الشاملة متعددة التخصصات ، الأردن ، العدد 24 ، 2020 ، ص:14.

⁸ المرجع نفسه ، ص 15

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

- ب. **القرصنة**: ومنهم الهاكر وهم الذين يدخلون أنظمة الحاسبات وكسر الحواجز الامنية بهدف الفضول ، ومنهم الكراكر وهم المتسللون إلى أنظمة المعالجة للإطلاع على المعلومات المخزنة بهدف السرقة أو العبث بها.
- ت. **المهوس**: وهو المجرم الذي يكون في حالة الجنون و يهدف إلى تحطيم كل الأنظمة.
- ث. **الجريمة المنظمة**: أصبح جهاز الحاسوب أداة فعالة في أيدي المافيا.
- ج. **الحكومات الأجنبية**: وذلك باستعمال أجهزة الحاسوب في مجال الجوسسة.
- ح. **المتطرفون**: وهم الذين يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية ، والدينية المتطرفة.

ولتنفيذ المجرم السيبراني جريمته يستخدم تقنيات عالية الدقة والتطور من خلال التحايل والاختراق للأنظمة المعلوماتية ، عبر طريقتين إما عن طريق جهاز الضحية ويسمى بالخادم أو عن طريق جهاز مخترق ويسمى بالبرنامج المستفيد، ومن بين أهم البرامج التي يستخدمونها¹:

- أ. **حصان طراودة**: وهو برنامج صغير محتبئ ببرنامج أكبر ، يقوم بإطلاق فيروسات والدودة التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام ، وإرسال كلمات المرور السرية ومن أنواع هذا البرنامج القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطوره.
- ب. **فيروسات الكمبيوتر**: وهي برامج صغيرة تستخدم من أجل تعطيل شبكات الخدمات.
- ت. **الديدان**: تتكاثر عن طريق نسخ نفسها بواسطة الشبكات وهدفها الشبكات المالية مثل البورصات.
- ث. **الأبواب الخلفية**: وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه وقت الحاجة.
- ج. **الاختناق الموروي السيبراني**: وهو سد وخنق الاتصالات لدى المستهدف بحيث لا يمكنه تبادل المعلومات.

ح. **القصف السيبراني**: وهو الهجوم على شبكة المعلومات بحيث يسبب ضغط كبير على الموقع ، فيفقد الأخير قدرته على استقبال الرسائل من العملاء ، وبالتالي يوقف عن العمل تمامًا.

2/ **المجني عليه في الجريمة السيبرانية**: قد يكون المجني عليه شخصا طبيعيا عاديا ، وقد يكون شخصا طبيعيا ذا منصب سياسي رفيع أو رجل أعمال ، أو صاحب شهرة عالمية ، وقد يكون شخصا اعتباريا كالشركات والبنوك والمؤسسات والقطاعات الحكومية والمؤسسات المالية إذ تعتبر من أكثر الأماكن استهدافا نظرا لما لها من أموال.²

دون أن ننسى يمكن أن تكون الدولة مجني عليها في ظل الجريمة السيبرانية حيث قد تخترق سيادتها عن طريق الجوسسة وغيرها من صور الجريمة السيبرانية.

¹ المرجع نفسه، ص:15.

² روان بنت عطية الله الصحفي ، المرجع السابق، ص:16.

آمال بيدي

2.1- خصوصية الطبيعة القانونية للجريمة السيرانية:

إن الحديث عن الطبيعة القانونية للجريمة السيرانية يرتبط بالوضع القانوني للبرامج والمعلومات أو البيانات باعتبارها محل الاعتداء .

فهناك من يرى أن الأشياء المادية هي التي تكون قابلة للاستحواذ والحيازة ، وأن ما يمكن أن يكون موضوع سرقة لا بد أن يكون ماديا ملموسا أي قابل للاختلاس هذا الأخير المكون للركن المادي لجريمة السرقة¹ ، وبما أن المعلومة لها طبيعة معنوية لذلك لا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ ، إلا في ضوء حقوق الملكية الفكرية².

وعليه يرفض هذا الاتجاه ادراج المعلومات ضمن القيم المالية التي يمكن الاعتداء عليها ، إذ لا بد أن تكون قابلة للتملك ، والتي يترتب عليها الاستثناء بها وحدها و هي ضمن المعلومات التي لها طبيعة معنوية ولا يمكن أن تندرج في مجموعة القيم المحمية ، ما لم تكن تنتمي إلى المواد الأدبية أو الفنية أو الصناعية التي تحميها حقوق الملكية الأدبية أو الفنية أو الصناعية³.

أما الاتجاه الثاني يرى أن المعلومات تدخل في إطار الحقوق المالية مع استبعادها من طائفة القيم المالية، ومنه فإن المعلومات مال قابل للتملك أو الاستغلال نظرا لقيمتها الاقتصادية لا على أساسه المادي، ومنه استلزم الحماية القانونية ومعاملة المعلومة معاملة المال⁴.

و يرى أنصار هذا الاتجاه أن المعلومات لها علاقة مباشرة بفكرة المنفعة أو الخدمة ، فالإلمام بالمعلومة يؤدي إلى القيام بعمل بصورة أسهل وأسرع ، غير أن استبعاد المعلومات من نطاق القيم المالية ، لم يمنع الفقه والقضاء الفرنسي من محاولة فرض حماية قانونية لها في حالة الاستيلاء غير المشروع عليها⁵.

ولقد تنوع التأسيس بين تأسيس الخطأ على نظرية الإثراء بلا سبب أو تأسيسه على فكرة المسؤولية التقصيرية⁶.

وعليه يمكن القول أن الطبيعة القانونية للمعلومة هي طبيعة قانونية من نوع خاص تدخل ضمن قيم جديدة، إذ أن هناك من المال المعلوماتي المادي الذي يحتوي على مضمون معنوي و هو الذي يعطيه القيمة الحقيقية، وقد

¹ الزبير حمزة الزبير ، الجريمة الالكترونية مفهومها وطبيعتها القانونية على ضوء قواعد القانون الدولي العام -دراسة قانونية -، مجلة القلم للدراسات السياسية والقانونية ، مركز البحوث ودراسات دول حوض البحر الأحمر ، السودان ، العدد 01 ، 2020 ، ص:87.

² المرجع نفسه ، ص:87.

³ شيخة حسين الزهراني ، الطبيعة القانونية لهجوم السيراني وخصائصه ، مجلة جامعة الشارقة للعلوم القانونية المجلد 17 ، العدد 1 ، 2020 ، ص:793.

⁴ محمد علي العريان ، الجرائم المعلوماتية ، الاسكندرية ، دار الجامعة الجديدة للنشر ، 2004 ، ص:37.

⁵ شيخة حسين الزهراني ، المرجع السابق ، ص: 793.

⁶ المرجع نفسه ، ص:793.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

يمثل هذا المال المادي المعنوي في الشريط المغنط أو الاسطوانة المغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات، مثل ما يحدث في جرائم التجسس عن بعد.

وعليه يمكن القول أنه إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمتها المادية ، وهي ثمن الشريط أو ثمن الأسطوانة ، وإنما يسرق ما هو مسجل عليها من معلومات وبرامج.¹

وطالما أن موضوع الحياة (أي المعلومات) غير مادي ، فإن واقعة الحياة تكون من نفس الطبيعة غير مادية (ذهنية) وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر.²

ولتحديد الطبيعة القانونية للجريمة الالكترونية لابد من الإشارة إلى الصور الأكثر شيوعا لاختلاف كل منها في تكييفها عن الأخرى:³

1. الجرائم الالكترونية جرائم أموال : يظهر هذا النوع من الجرائم بصورتين:

أ. جرائم تستخدم فيها الحاسب الآلي من أجل تزيف العملة أو تزوير في محركات رسمية أو اختلاس ، أو الدخول غير المشروع للبيانات والمعلومات المخزنة على حاسب آلي آخر ، عن طريق شبكات الاتصال الدولية ، وكل هذا من أجل الحصول على منافع نقدية أو أخذ المعلومات والبيانات.

ب. جرائم واقعة على الحاسب الآلي بمشتملاته المادية أو المحتوى مثل : جرائم تعديل أو تحوير أو تقليد برامج الحاسب الآلي ، وجرائم تدمير المعلومات والبيانات الخاصة بالحاسب الآلي نفسه ، زيادة على الجرائم التقليدية التي تمس الشق المادي للحاسب الآلي مثل السرقة والإتلاف .

توصف الجرائم الالكترونية في هاتين الصورتين أنها جرائم أموال لأن موضوعها هو المال ، مع التسليم أن الجانب المعنوي للحاسب الآلي هو مال بالمعنى الفني والقانوني.⁴

2. الجرائم الالكترونية جرائم أشخاص: ينحصر أثر هذه الجرائم في مجموعة ضيقة من جرائم الأشخاص مثل جرائم : الدم ، القدح ، التحقير ، جريمة إفشاء الأسرار سواء التجارية أو الشخصية ، جرائم التهديد والتحرير ، وجرائم الاعتداء على الحياة الخاصة عبر الانترنت.⁵

كما يمكن أن يكون هذا النوع من الجرائم في شكل جرائم الابتزاز والاستدراج والمقامرة وترويج المخدرات بوسائل معلوماتية والجرائم الإباحية.⁶

¹ الزبير حمزة الزبير ، المرجع السابق ، ص:87.

² عبدالله دغش العصي ، المشكلات العلمية والقانونية للجرائم الالكترونية - دراسة مقارنة - ، مذكرة ماجستير في القانون العام ، جامعة الشرق الأوسط ، الأردن ، 2014 ، ص: 16.

³ المرجع نفسه ، ص:16.

⁴ المرجع نفسه ، ص: 17.

⁵ المرجع نفسه ، ص:18.

⁶ آلاء محمد رحيم حادي ، المرجع السابق ، ص: 1110.

آمال بيدي

3. الجرائم الإلكترونية جرائم أمن الدولة وجرائم مخلة بالثقة العامة و الآداب العامة: يمكن لهذا النوع من الجرائم ان يمس أمن الدولة سواء الداخلي أو الخارجي مثل : جرائم التجسس ، وجرائم الاتصال بالعدو ، جرائم إثارة الفتن ، الجرائم الماسة بالوحدة الوطنية.¹

أما الجرائم المخلة بالثقة والآداب العامة فهي أيضا قابلة للوقوع عبر الوسائل الإلكترونية وذلك مثل جرائم التزوير ، وتقليد الاختام ، وتزوير الأوراق البنكية، وانتحال الشخصية.²

ومن جهة ثانية تندرج الجريمة الإلكترونية ضمن الجرائم السياسية والاقتصادية ، ومثال عن ذلك الإرهاب الذي لم يعد بصورته التقليدية بل دخل العالم السيبراني في صفحات ومواقع عالمية على الانترنت، إذ أصبحت المجموعات الارهابية تستخدم تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية.³

2- الجهود الأمية في مجال مكافحة الجريمة السيبرانية وصعوبة تحقيقها :

1.2. أهم إسهامات الأمم المتحدة في مجال مكافحة الجريمة السيبرانية:

لاشك أن الأمم المتحدة قدمت جهودًا قيمة من أجل مواجهة ومجابهة الجريمة السيبرانية ، مؤكدة على وجوب تضافر جهود الدول والعمل المشترك الجماعي بهدف الحد من انتشار هذا النوع من الجرائم ، واعتقادا منها أن مكافحة هذه الجريمة يتطلب وعي دولي بخطورة هذه الجرائم وأبعادها الدولية.

ومن أهم المؤتمرات التي عقدتها الأمم المتحدة بهذا الشأن والتي سيتم التطرق عليها على سبيل الاستدلال والمثال لا الحصر.

أ. المؤتمر السابع لمنع الجريمة ومعاملة المجرمين والذي انعقد في مدينة ميلانو الإيطالية في الفترة الممتدة بين 26 أوت و 06 سبتمبر 1985م، وحينها كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتناء على الحاسب الآلي وإعداد تقرير قصد عرضه على المؤتمر الثامن.⁴

ب. المؤتمر الثامن للأمم المتحدة: عقد في هافانا الكوبية في الفترة الممتدة من 27 أوت إلى 07 سبتمبر 1990م ، والذي أقر المعاهدات النموذجية لتسليم المجرمين وتبادل المساعدة في المسائل الجنائية ، ونقل الإجراءات في المسائل الجنائية ونقل الإشراف على المجرمين المحكوم عليهم بأحكام مشروطة أو المفرج عنهم إفراجًا مشروطًا.⁵

¹ عبد الله دغش العجمي ، المرجع السابق ، ص: 18.

² المرجع نفسه ، ص: 18.

³ آلاء محمد رحيم حادي ، المرجع السابق ، ص: 1109.

⁴ سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة الحاج لخضر ، باتنة ، ، 2012-2013 ، ص: 83.

⁵ مكتب الأمم المتحدة المعني بالمخدرات والجريمة <https://www.unodc.org> تاريخ الإطلاع : 18 نوفمبر 2021 ، الساعة 20:23.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

أما في مجال الجرائم المتعلقة بالحاسوب ، فلقد أشار القرار في هذا المؤتمر إلى أن هناك إجراءات يستوجب على الدول اتخاذها والتي من بينها:¹

1. تحديث القوانين وأغراضها الجنائية من أجل تطبيق أفضل للقوانين الجنائية الراهنة وعلى نحو ملائم ، وإدخال تعديلات إن تطلب الأمر ذلك.
2. مصادرة العائد والأصول من الأنشطة غير المشروعة.
3. اتخاذ تدابير الأمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الانسان.
4. التأكيد على رفع الوعي لدى الجماهير والقضاة والأجهزة المعنية في هذا المجال بأهمية مكافحة هذا النوع من الجرائم ومحاكمة مرتكبيها، و ذلك بتدريب القضاة و المسؤولين على كيفية التحقيق والمحاكمة.
5. التعاون مع المنظمات المهتمة بهذا الموضوع ، ووضع وتدريب الآداب المتبعة في استخدام الحاسوب.
6. حماية مصالح وحقوق ضحايا جرائم الحاسوب.

كما قامت الجمعية الدولية بعقد المؤتمر الخامس عشر- لقانون العقوبات في ربي ودي جانيرو البرازيلية عام 1994م، ولقد أقر العديد من التوصيات بشأن جرائم الكمبيوتر منها:²

أ/ في الشق الموضوعي: لقد أوصى المؤتمر بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي:

1. الاحتيال أو الغش المرتبط بالكمبيوتر : ويشمل الادخال والإتلاف والمحو لمعطيات الكمبيوتر أو برامج ، أو القيام بأفعال تؤثر بمرجى المعالجة الآلية للبيانات وتؤدي الى الحاق الخسارة أو فقدان الحياة أو ضياع ملكية شخص ، وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
2. تزوير الكمبيوتر أو التزوير المعلوماتي : ويشمل ادخال أو اتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد - فيما لو ارتكبت بغير هذه الطرق - من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.
3. الإضرار بالبيانات والبرامج (الاتلاف) : وتشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.
4. تخريب وإتلاف الكمبيوتر : وتشمل الادخال أو المحو أو الاتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات).

¹ عوطف محمد عثمان عبد الحليم ، جرائم المعلوماتية : تعريفها ، صورها ، جهود مكافحتها دوليا ، إقليميا ، ووطنيا ، مجلة العدل ، السودان ، المجلد 10 ، العدد 24 ، 2008 ، ص: 70.

² تاريخ الإطلاع: 20 نوفمبر 2021، <https://alexalaw.ahlamontada.com>

آمال بيدي

5. الدخول غير المصرح به : وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق الاعتراض غير المصرح به ، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام الكمبيوتر أو عدة نظم أو شبكة اتصالات.

ب/ في الشق الإجرائي: أصدر المؤتمر في هذا الشق الكثير من الإجراءات من أهمها مايلي:

1. يتطلب التنقيب بالنسبة لجرائم الحاسب الآلي وضع تحت تصرف سلطات التحقيق والتحري ما يكفي لتحقيق حماية حقوق الإنسان وحرمة الحياة الخاصة له.
2. لتجنب تعسف السلطات الرسمية ، فإن القيود التي ترد على حقوق الإنسان، لا يمكن أن تكون مقبولة إلا إذا كانت بسند قانوني واضح ودقيق ومتماشية مع المعايير الدولية لحقوق الانسان.
3. على ضوء هذه المبادئ العامة يجب ان يحدد بوضوح ما يلي :
 - أ. السلطات التي تقوم بإجراء التنقيش والضبط في بيئة تكنولوجيا المعلومات ، وخاصة ضبط الأشياء وتفتيش شبكات الحاسب ، يجب تحديدها وضرورة وضع القواعد المتعلقة بالإثبات ومصادقة الأدلة.¹
 - ب. واجبات التعاون الفعال من جانب المجني عليهم ، والشهود ، وغيرهم من مستخدمي تكنولوجيا المعلومات ، وذلك حتى تكون الأخيرة متاحة ويمكن استخدامها للأغراض القضائية .
 - ج. السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب ذاته ، مع استخدام الأداة التي يتم الحصول عليها في الاجراءات أمام المحاكم.
 4. نظرا لتعدد وتنوع البيانات المدرجة في نظم معالجة البيانات ، يجب عند بدء التحريات أن يوضع في الاعتبار – بالإضافة الى القيم المالية التقليدية – كل القيم المرتبطة ببيئة تكنولوجيا المعلومات ، مثل: التجسس، انتهاك حرمة الحياة الخاصة ، مخاطر الخسارة الاقتصادية ، كلفة إعادة بناء تكامل البيانات كما كانت من قبل.

5. القواعد القائمة في مجال قبول ومصادقية الأدلة ، يمكن أن تثير مشاكل عند تطبيقها ، نظرا لتقييم تسجيلات الحاسبات في الاجراءات القضائية ،لذا ينبغي ادخال بعض التغييرات التشريعية في حالة الضرورة.

ج. المؤتمر التاسع للأمم المتحدة حول منع الجريمة ومعاملة المجرمين "الجريمة" المنعقد بالقاهرة المصرية في الفترة الممتدة بين 28 افريل و 5 ماي 1995م، أوصى هذا المؤتمر بوجود حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا، ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الاجراءات الضرورية والمناسبة.²

د. المؤتمر الثاني عشر للأمم المتحدة حول منع الجريمة والعدالة الجنائية المنعقد في سلفادور البرازيلية في الفترة الممتدة 12 و 19 أفريل 2010 ، حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات في مجال

¹ محمد طارق عبد الرؤوف الحن ، جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية والأحكام الاجرائية)، ط1، منشورات الحلبي الحقوقية ، 2011، ص: 188.

² سعيداني نعيم، المرجع السابق ، ص:84.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

مكافحة الجريمة ، لاسيما أن منظمة الأمم المتحدة تعد الإطار الأمثل لمكافحة الإجرام السيبراني، وقد وضعت مجموعة من القواعد الموضوعية والإجرائية لمواجهة هذا النوع من الجرائم.¹

وتأكيداً منها في هذا المؤتمر جاء البند 41 من تقريره، بحث الدول على بناء قدرات سلطاتها الوطنية من أجل التعامل مع الجرائم الإلكترونية، بما في ذلك المنع والكشف والتحقيق وملاحقة هذه الجريمة بكافة أشكالها وتعزيز الأمن في شبكات الكمبيوتر.

كما دعت لجنة منع الجريمة والعدالة الجنائية في البند 42 من تقرير هذا المؤتمر، النظر والدراسة الشاملة لمشكلة الجرائم الإلكترونية وردود فعل الدول الأعضاء عليها ، وطلب من المجتمع الدولي والقطاع الخاص بتبادل المعلومات بشأن التشريعات الوطنية، والمساعدة التقنية والتعاون الدولي يهدف دراسة الخيارات الوطنية ، والاستجابات القانونية الدولية أو غيرها من الاستجابات للجرائم الإلكترونية.²

هـ. المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة بقطر في الفترة الممتدة بين 12 و 19 أبريل 2015، ومن أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة السيبرانية ما يلي:

1. وجوب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة السيبرانية ومنعها، حيث أن هذا النوع من الجرائم يتطلب من الدول أن تنمي قدرتها في جانب تدابير المنع والتحري المضادة.
2. بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية والتحقق فيها، وعمليات الاستدلال الجنائي الرقمية ، وكيفية التعامل مع الأدلة الإلكترونية .
3. إمكانية استحداث أطر متعددة الأطراف، حيث أوصى اجتماع أفريقيا الإقليمي التحضيري للمؤتمر الثالث عشر بأن تنظر الدول في وضع اتفاقية بشأن الجريمة السيبرانية ضمن سياق المؤتمر.
4. الواضح أن الكثير من أجهزة إنفاذ القانون تواجه صعوبات في إمكانية الوصول إلى البيانات الموجودة خارج نطاق إقليمها أثناء التحري عن الجرائم السيبرانية، وفي المقابل لا بد من أن تكون ضمانات حقوق الإنسان وسيادة القانون و صون الحرمة الشخصية كافية لضمان أن يكون ذلك الوصول إلى البيانات من أجهزة إنفاذ القانون محددا وقابلا للتنبؤ ومتناسبا وخاضعا للرقابة .
5. التأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة السيبرانية .

¹ مراد مشوش ، الجهود الدولية لمكافحة الاجرام السيبراني ، مجلة الواحات للبحوث والدراسات ، جامعة غرداية، المجلد 12 ، العدد 2، 2019، ص:707.

² مكتب الأمم المعني بالمخدرات والجريمة ، المرجع السابق، تاريخ الاطلاع: 20 نوفمبر 2021، الساعة: 22:35.

آمال بيدي

6. يتعين على المحققين والجهات المختصة في مجال مكافحة لهذا النوع من الجرائم أن يعتمدوا استراتيجيات جديدة كأن يعملوا على تدعيم الشركات مع فرق بحث أكاديمية في مجالات متنوعة.¹

واستمررا لجهود الأمم المتحدة في هذا المجال فقد أصدرت دليلا عاما إرشاديا حول الجرائم المرتبطة بالكمبيوتر ويتم تعديله وتنقيحه كل فترة ، حيث تضمن هذا الدليل تحديد المشكلة وتعريفها بجرائم الكمبيوتر كما وضع تحديدا للحد الأدنى منها ، إضافة إلى العديد من المحتويات التي تتعلق بهذا النوع من الجرائم.²

2.2- المعوقات التي تحول الأمم المتحدة دون تحقيق مكافحة الجرائم السيبرانية :

هناك الكثير من المعوقات التي تحول الأمم المتحدة دون تحقيق مكافحة ناجعة حيال الجريمة السيبرانية، ويعود ذلك لعدة عوامل منها ما يتعلق بالجريمة المعلوماتية في حد ذاتها ، أو ما يتعلق بالجنى عليه ، أو ضعف التنسيق والتعاون الدولي في هذا المجال وهناك ما يتعلق بعملية التحقيق الجنائي.³

أ. المعوقات المتعلقة بالجريمة نفسها:

1. الشق الموضوعي: يتمثل في مدى إمكانية تطبيق النصوص التقليدية للقانون الجنائي على هذا النوع من الجرائم وضرورة احترام مبدأ الشرعية ، والتفسير الضيق للنصوص الجنائية.⁴

و نظرا لخصوصية وطبيعة الجريمة فإنها تتطلب نصوصا خاصة، فالأفعال غير المشروعة في البيئة الافتراضية لا يمكن توصيفها بجريمة إذ لم ينص عليها القانون صراحة ، وهذا القصور في النصوص القانونية الجنائية ، يترتب عليه من دون شك المساس بمبدأ شرعية الجرائم والعقوبات في حالة ما إذا توسع القضاة في تفسير النصوص العقابية التقليدية ، وهذا ما قد يؤدي بفلت الجناة من العقاب.⁵

أيضا هناك معوق آخر فيما يتعلق بقلّة المتخصصين الجنائيين في مجال الجرائم الالكترونية مقارنة بحجم المعلومات الرقمية وانتشار التقنية الرقمية ، والذي يستوجب تطور التحقيق الجنائي المستمر والمستحدث ، ذلك أن الحماية الأمنية للمعلومات الرقمية باتت ضعيفة مقارنة مع ضخامة واتساع المعلومات الرقمية ، وعدم المعرفة بمكونات الجريمة المعلوماتية من قبل الأطراف المعنية.⁶

¹ البند 5 من جدول الأعمال المؤقت ، حلقة العمل 3: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والإتجار بالمشكلات الثقافية بما في ذلك الدروس المستفادة والتعاون الدولي : A/conf.222/12 : <https://www.unodc.org> ، ص 14-18 تاريخ الإطلاع : 20 نوفمبر 2021 على الساعة : 23:30

² عواطف محمد عثمان عبد الحلیم ، المرجع السابق ، ص: 71.

³ عصام حسني الاطرش ، محمد محي الدين عساف ، معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية ، مجلة جامعة الشارقة للعلوم القانونية ، جامعة الشارقة ، المجلد 16 ، العدد 9 ، 2019 ، ص: 637.

⁴ عواطف محمد عثمان عبد الحلیم ، المرجع السابق ، ص: 65.

⁵ المرجع نفسه ، ص: 66.

⁶ عصام حسني الاطرش ، محمد محي الدين عساف ، المرجع السابق ، ص: 637.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

2. الشق الإجرائي : إن من أهم العقبات في هذا الشق تنفيذ الإجراءات التي تضمنتها القوانين الإجرائية كالفتيش والمعاينة والتحفيز والمصادرة لأن الأدلة غير مادية.¹

أيضا سهولة محو الأدلة وتدميرها وإخفاؤها في زمن وجيز ، زيادة على أن معظم الأدلة تحتاج إلى فهم وتحليل من متخصصين جراء اعتماد الحماية الفنية كاستخدام كلمة السر- أو التشفير ، للحيلولة دون الوصول إلى المعلومات والبيانات ، وهذا في حد ذاته يؤدي إلى إمكانية خروجها عن نطاق إقليم الدولة.²

كذلك قد يثور إشكال حول القانون الواجب التطبيق هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيها الآثار الضارة، ويعود ذلك إلى طبيعة الجريمة الالكترونية ، وقصور القوانين المتعلقة بها ، لذلك يستلزم ضرورة توحيد التشريعات فيما يتعلق بمكافحة هذا النوع من الجرائم إضافة إلى ضرورة إبرام الاتفاقيات والتعاون القضائي في هذا المجال.³

ب. ضعف التنسيق وعدم توحيد جهود التعاون الدولي بين أفراد المجتمع الدولي في مجال مكافحة الجريمة الالكترونية : إن التنسيق والتعاون الدولي في مجال مكافحة الجريمة الالكترونية لا يتلاءم مع حجم خطورتها على غرار بعض الجرائم مثل الجرائم الإرهابية ، وحيث أنه مع تفاقم اشكالية الاختصاص القضائي في ظل امتداد الملاحقة والتحري والضبط والفتيش خارج الحدود ، الأمر الذي يستوجب وجود تعاون دولي يكفل مكافحة الجريمة الالكترونية من جهة ، وعدم انتهاك مبدأ سيادة الدول على اقليمها من جهة أخرى.⁴

ورغم إدراك الأمم المتحدة وكل أفراد المجتمع الدولي بأهمية التعاون بين كل الأطراف من أجل مكافحة هذا النوع من الجرائم الذي بات يهدد الجميع ولم تعد الجريمة بصورتها التقليدية بل أصبحت لها تقنيات حديثة ومستحدثة ومتطورة في كل حين ، إلا أنها لم تحقق ما كانت تتطلع إليه من خلال كل مؤتمراتها وقراراتها ، ولعل من أهم الأسباب التي جعلت التعاون يصعب في هذا المجال هو:عدم وجود نموذج موحد متفق عليه فيما يتعلق بالنشاط الإجرامي ، ويرجع ذلك إلى عدم اتفاق الدول وأنظمتها على صور محددة يندرج ضمنها بما يعرف بإساءة استخدام نظم المعلومات الواجب اتباعها هذا من جهة ، ومن جهة أخرى عدم وجود تعريف محدد للنشاط المفروض أن يتفق على تجريمه.⁵

مع العلم أن العديد من الدول العربية لم تصدر قانونا يتعلق بالجريمة الالكترونية ، وما زال الجدل حول ما إذا أن تعديل تشريعاتها العقابية أفضل لي تستوعب هذا الجريمة ، أم انها تعدل قوانين حماية الملكية الفكرية كي

¹ عواطف محمد عثمان عبد الحليم، المرجع السابق ، ص: 67.

² عصام حسني الأطرش، محمد محي الدين عساف ، المرجع السابق ، ص: 37.

³ عواطف محمد عثمان عبد الحليم، المرجع السابق ، ص: 68.

⁴ يعينش تمام شوقي ، الجريمة المعلوماتية - دراسة تأصيلية مقارنة ، ط 1 ، مطبعة الرمال ، الوادي ، الجزائر ، 2019 ، ص 43.

⁵ ليندة شرايشة ، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية ، مجلة دراسات وأبحاث ، جامعة الجلفة ، المجلد 01، العدد 01، 2009، ص: 250.

آمال بيدي

تندرج هذه الجرائم في إطارها ويتم تجريمها ، أم أن أفضل الحلول اصدار تشريعات جديدة خاصة بهذا النوع من الجرائم¹.

ت. **المعوقات المتعلقة بالمجني عليه:** إن العديد من المعوقات التي تواجه مكافحة الجريمة الإلكترونية تتعلق بسلوك المجني عليه ، فالتقنية المستخدمة في نظم المعلومات تعد استثمارا تنسابق الشركات في تبسيط إجراءاتها وتسهيل استخدام البرامج والأجهزة وملحقاتها ، وارتكازها على جانب الخدمات دون الجانب الأمني².

والملاحظ في هذا النوع من الجرائم عدم الإبلاغ عنها ، وإحجام البعض عن إبلاغ السلطات المختصة في الجرائم التي ارتكبت بمقتهم ، خاصة الشركات التجارية والمؤسسات حتى في الدول المتقدمة من الناحية التقنية ويرجع ذلك إلى عدة أسباب منها³:

- عدم الإدراك بأن هذه الأفعال من قبيل الجرائم التي يعاقب عليها مرتكبها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دوليا.
- خوف المؤسسات الكبرى والشركات التجارية بسبب التحقيق والاحتجاز أو تعطيل الشبكات لمدة ، ففي بعض الأحيان تسبب إجراءات تحقيق خاطئة خسائر مادية أكثر مما تسببه الجريمة الإلكترونية في حد ذاتها.
- الإخفاء لأسلوب الجريمة حتى لا تنتشر مستقبلاً.
- أحيانا تتعلق الجرائم الإلكترونية بجرائم ابتزاز أو ترتبط بجرائم أخلاقية ، هذا ما يؤدي بالمجني عليه لعدم الإبلاغ تفاديا للفضيحة والعار.

وعليه لا بد من حث المواطنين و المؤسسات والشركات وكل الأطراف المتضررة بالإبلاغ، ناهيك على أن الأجهزة الأمنية يجب عليها نشر الوعي من خلال التعاون مع مؤسسات المجتمع الحكومية وغيرها بما فيها المجتمع المدني، ذلك أن الإبلاغ يعد خطوة مهمة في مجال مكافحة هذا النوع من الجرائم.

ج. **المعوقات المتعلقة بخصوصية الإثبات والتحقيق الجنائي في الجرائم الإلكترونية :** هناك الكثير من الإشكال في مجال الجرائم الإلكترونية خاصة قضية إثباتها لازال هذا النوع من الجرائم محل نقاش وتحليل من قبل رجال القضاء والقانون ، فإذا كان الدليل المادي في الجرائم التقليدية قد يصعب الوصول إليه أحيانا فإن الجرائم الإلكترونية يصعب حتى إثباتها⁴.

¹ مراد مشوش ، الجهود الدولية لمكافحة الإجرام السيبراني ، مجلة الواحات للبحوث والدراسات ، جامعة غرداية ، المجلد 12 ، العدد 2 ، 2019 ،

ص 707

² عصام حسني الأطرش ، محمد محي الدين عساف ، المرجع السابق ، ص:637.

³ المرجع نفسه ، ص: 630.

⁴ يعيش تمام شوقي ، المرجع السابق ، ص:50.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

ولذلك يرى بعض الباحثين ضرورة إعطاء الدليل الإلكتروني دلالة قانونية قاطعة ويدعوا إلى اعتماده من قبل المحكمة كدليل كاف لإثبات الإدانة أو البراءة ، وتبريرهم لذلك صعوبة استخلاص الأدلة في البيئة الرقمية ، كذلك نقص الكوادر المتخصصة وانخفاض كفاءتها، والقول بعكس ذلك يؤدي إلى إفلات الجناة من العقاب.¹

إضافة إلى ذلك فقد أعتبر عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الإلكترونية ، أحد أهم المعوقات في مكافحتها وهذا ما أدى إلى عدم وجود وحدة تحقيق أو قسم خاص متفرغ للتحقيق في هذه الجرائم، مع ارتفاع تكاليف جمع الأدلة نظير المبالغ الكبيرة التي يطالب بها المختصين الخبراء مقابل ضبطهم واستخلاصهم الأدلة الرقمية.²

فضلا على ذلك لا بد أن يكون المحقق الجنائي في هذا النوع من الجرائم ملما بالقوانين الجنائية التي تشكل أساسا في التحقيق الجنائي ، إضافة إلى أنه يستوجب عليه أن يتزود بالمعلومات العامة وجل العلوم القانونية المتعلقة بتكنولوجيا المعلومات والاتصالات وشبكة الانترنت ، فكل زيادة في المعلومة زاد مقابله اكتساب خبرة ودراسة في هذا المجال ، ومن أهم هذه القوانين : القانون الإلكتروني ، قانون المعاملات والعقود الإلكترونية ، قانون الإثبات باستخدام التوقيع الإلكتروني ، قانون مكافحة جرائم التنظيم المعلوماتية ، ومن العلوم علم النفس ، وعلم النفس الجنائي ، علم الاجتماع ، علم الإجرام ومنه فإن إلهم المحقق بهذه العلوم لا يقتضي- بالضرورة إلهام المتخصص فيها بل يكفي أن يكون ملما بأساسياتها.³

خاتمة:

سعت الأمم المتحدة جاهدة إلى مكافحة كل الجرائم التي من شأنها أن تهدد الإنسانية وأمنها ، لكن اليوم وفي ظل عصر التكنولوجيا والمعلومات والاتصالات التي أصبحت جزء أساسيا في حياة الجميع ، ساعدت بشكل أو بآخر في ظهور جرائم ذات طابع دولي جنائي خاص ، ذلك ما فرض على هيئة الامم المتحدة تجنيد الكثير من الجهود من أجل مكافحتها والحد من خطورتها ، فآثار هذه الجرائم تعد الحدود الدولية واستهداف كل الفئات سواء كانت أشخاصا طبيعية أو معنوية ، ولعل هيئة بحجم الأمم المتحدة لم تستطع استيعاب خطورة هذه الجريمة نظرا للتقنيات الفنية العالية التي تستخدم في ارتكابها وصعوبة كشفها وإثباتها حال دون تحقيق تعاون دولي ناجح ، مما يستوجب على الأمم المتحدة انتهاز استراتيجية دولية جنائية خاصة لهذا النمط الجديد من الجرائم.

¹ المرجع نفسه ، ص:53.

² عصام حسني الأطرش ، محمد محي الدين عساف ، المرجع السابق ، ص: 63.

³ يعيش تمام شوقي ، المرجع السابق ، ص:60.

النتائج :

1. لا يمكن أن نكر الجوانب الايجابية للثورة المعلوماتية والاتصالات ، لكن تعد الجريمة السيبرانية الجانب السلبي منها.
2. عدم وجود تعريف قانوني أو فقهي محدد لهذه الجرائم ، وعدم طرح الأمم المتحدة تعريفاً بشكل محدد ومضبوط ، واعتماد معايير معينة وبنائها في هذا النوع من الجرائم ، وهذا أيضاً ما يثير إشكالاً حول طبيعتها القانونية.
3. الفراغ التشريعي خاصة الجنائي منه وإشكالات القانون الواجب التطبيق ، لاسيما وأن الجريمة السيبرانية تعد من الجرائم العابرة للحدود.
4. عدم توصل الأمم المتحدة إلى إبرام اتفاقية دولية موحدة تركز استراتيجية محكمة في مجال المكافأة ، رغم إيمانها بخطورة الجريمة.
5. نقص الخبرات ومهمات التحقيق والتحري في إثبات الدليل وإدانة المجني ، ويرجع ذلك إلى الطبيعة الفنية المعقدة لهذه الجرائم.
6. ما زالت الأمم المتحدة غير قادرة على استيعاب هذا النوع من الجرائم في كل جوانبها ، هذا ما يقتضي- منها التحرك أكثر في بناء قدرات كل الأطراف والمساهمة في تعزيز التعاون الدولي لمكافحة الجريمة.

التوصيات :

1. ضرورة العمل على تطوير القوانين الجنائية من الناحية الموضوعية والإجرائية بحيث تشمل الجرائم السيبرانية وكل جوانبها وصورها وأساليبها خاصة بما يتلاءم مع طبيعتها الخاصة.
2. ضرورة نشر الثقافة والوعي بمخاطر الجرائم الالكترونية والتبليغ فيها ، حتى تتمكن الجهات المختصة والمعنية بإيجاد طرق وحلول لمكافحة هذه الجريمة ، بما فيها هيئة الأمم المتحدة التي تحتاج إلى تضافر جهود جميع أفراد المجتمع الدولي.
3. ضرورة قيام الأمم المتحدة ببناء قدرات الدول في مجال مكافحة هذه الجريمة ، وضرورة إنشاء أجهزة سواء كانت أمنية أو غيرها في هذا المجال.
4. ضرورة العمل على توحيد الجهود الدولية والأممية والإقليمية والوطنية في مجال مكافحة الجريمة السيبرانية ، وذلك من خلال تبادل المعلومات والبيانات في المجال المعلوماتي من أجل إيجاد الحلول المناسبة لكل جريمة حسب طبيعتها وصورتها.

جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

قائمة المراجع:

1/الكتب باللغة العربية :

1. مجمع البحوث والدراسات ، أكاديمية السلطان قابوس لعلوم الشرطة ، تروى - سلطنة عمان ، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها ، البحث الفائز بالمركز الأول في مسابقة ، 2016. جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015.
2. محمد طارق عبد الرؤوف الحن ، جريمة الاحتيال عبر الانترنت (الاحكام الموضوعية والأحكام الاجرائية)، ط 1 ، منشورات الحلبي الحقوقية ، 2011.
3. محمد علي العريان ، الجرائم المعلوماتية ، الاسكندرية ، دار الجامعة الجديدة للنشر ، 2004.
4. يعيش تمام شوقي ، الجريمة المعلوماتية - دراسة تأصيلية مقارنة ، ط 1 ، مطبعة الرمال ، الوادي ، الجزائر ، 2019.

2/المقالات العلمية المحكمة :

5. ألاء محمد رحيم حادي ، الجريمة السيبرانية ومخاطرها على الأطفال (الاشكاليات والحلول) (دراسة تحليلية في ضوء الاحصائيات الدولية والعربية والوطنية)، مجلة كلية التربية للبنات ، جامعة بغداد ، المجلد 28 ، العدد 4 ، 2017 .
6. الزبير حمزة الزبير ، الجريمة الالكترونية مفهومها وطبيعتها القانونية على ضوء قواعد القانون الدولي العام -دراسة قانونية -، مجلة القلم للدراسات السياسية والقانونية ، مركز البحوث ودراسات دول حوض البحر الأحمر ، السودان ، العدد 01 ، 2020.
7. كركوري مباركة حنان ، خصوصية ارتكاب الجريمة السيبرانية في النظام المعلوماتي (دراسة تحليلية على ضوء القانون الجزائري) ، مجلة الدراسات الاستراتيجية والعسكرية ، المجلد 2 ، العدد 08 ، 2020.
8. مراد مشوش ، الجهود الدولية لمكافحة الاجرام السيبراني ، مجلة الواحات للبحوث والدراسات ، جامعة غرداية، المجلد 12 ، العدد 2، 2019.
9. عوظف محمد عثمان عبد الحلیم ، جرائم المعلوماتية : تعريفها ، صورها ، جهود مكافحتها دوليا ، إقليميا ، ووطنيا ، مجلة العدل ، السودان ، المجلد 10 ، العدد 24 ، 2008.
10. عصام حسني الاطرش ، محمد محي الدين عساف ، معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الامنية ، مجلة جامعة الشارقة للعلوم القانونية ، جامعة الشارقة ، المجلد 16، العدد 9 ، 2019.
11. روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، المجلة الالكترونية الشاملة متعددة التخصصات ، الأردن ، العدد 24 ، 2020.
12. شيخة حسين الزهراني ، الطبيعة القانونية للهجوم السيبراني وخصائصه ، مجلة جامعة الشارقة للعلوم القانونية المجلد 17 ، العدد 1 ، 2020.

آمال بيدي

13. شريف حسين محمد محمد حسن ، الجريمة الالكترونية في منظور القانون المجمع ، حوليات آداب عين شمس ، عدد خاص ، المجلد 45 ، العدد 14 ، 2017.

3/الرسائل و الأطرحات العلمية :

14. سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، جامعة الحاج لخضر ، باتنة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، 2012-2013 .

15. عبدالله دغش العصبي ، المشكلات العلمية والقانونية للجرائم الالكترونية – دراسة مقارنة - ، مذكرة ماجستير في القانون العام ، جامعة الشرق الأوسط ، الأردن ، 2014.

4/تقارير الأمم المتحدة :

16. مكتب الأمم المتحدة المعني بالمخدرات والجريمة <https://www.unodc.org>

17. حلقة العمل 3: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والإتجار بالممتلكات الثقافية بما في ذلك الدروس المستفادة والتعاون الدولي : A/conf.222/12 : <https://www.unodc.org>