جهود منظمة الأمم المتحدة في سبيل مواجهة الجريمة الإلكترونية

United Nations efforts to combat cybercrime

أحمد رجدال [*1]،

[1] جامعة امحمد بوقرة بومرداس كلية الحقوق، (الجزائر)

REJDAL AHMED[1*]

University of Mohamed Bouguerra Boumerdes, Faculty of Law, ALGERIA [1]

تاريخ الاستلام: 2024/02/11 تاريخ القبول للنشر: 2024/06/21 تاريخ النشر: 2024/06/30.

ملخص: تهدف هذه الدراسة القانونية الى التعرف حول ما يشهده العالم من تأثير المتغيرات الدولية الناتجة عن ظهور العولمة والتطور التكنولوجي في مجال الثورة المعلوماتية، بشكل أدخل المجتمع الدولي في مرحلة جديدة نقلت معظم مجالات الحياة الى فضاء رقمي، هذا التطور صاحبه في نفس الوقت ظهور مشكلات وتصرفات جديدة لم تكن موجودة من قبل، بل استحضرتها الممارسة السلبية لتكنولوجيا المعلومات عبر المواقع الإلكترونية، إلى أن حملت في طياتها العديد من السلوكات الإجرامية نحو الفضاء الالكتروني، مخلفة ضحايا من مستخدمي الإنترنت، هذه الأنماط المستحدثة تختلف كثيرا عن الجرائم الكلاسيكية من حيث طبيعتها وتأثيرها، إضافة الى خصائص متميزة بأشكال غير مألوفة ومعقدة، تتجاوز حدود الدول في مدة زمنية قياسية، مع عدم توفر الوسائل الكافية والمناسبة للرقابة، خاصة في ظل صعوبة تطبيق النصوص التقليدية عليها.

لذا كان من المناسب خلال هذه الدراسة ضرورة البحث عن جهود منظمة الأمم المتحدة في تحديد الصور الناجمة عن الاستعمال الإجرامي للتكنولوجيا الحديثة بشكل تعكس فيه الدقة الواجبة للتجريم علي المستوى القانوني والنظر في جوانب التعاون الدولي بخصوص أبعاد هذه التقنيات.

الكلمات المفتاحية: الجريمة الالكترونية، الفضاء الإلكتروني، التطرف بوسائل الكترونية .

Abstract : This legal study aims to identify what the world is witnessing in terms of the impact of international changes resulting from the emergence of globalization and technological development in the field of information revolution, in a way that has brought the international community to a new stage that transformed all areas of life. to take the digital character that takes place in cyberspace, this evolution has been accompanied at the same time by the emergence of new problems and behaviors that did not exist before.

* أحمد رجـدال: ahmed.rejdal3@gmail.com

Rather, it was caused by the negative practice of information technologies through websites, until they transferred many criminal behaviors to cyberspace, causing victims among internet users,

These new crimes differ greatly from traditional crimes in terms of nature and impact, in addition to having distinct characteristics in unusual and complex forms, crossing national borders in a record time, with the absence of adequate means of control and appropriate, given the difficulty of applying traditional texts to them. it was therefore timely, during this study whether the United Nations has succeeded in identifying these images resulting from the criminal use of modern technology in a way that reflects the accuracy required for criminalization at the legal level and to consider aspects of international cooperation regarding the dimensions of these technologies.

Keywords Cybercrime, Cybercrime, cyberspace, extremism by electronic means.

* أحمد رجـدال: ahmed.rejdal3@gmail.com

مقدّمة:

لقد ظلت المجتمعات على مر العصور في حركية دائمة، من أجل السعي إلى التطور بمستوى الحياة إلى الأحسن، و تمكنت بفضل ما قدمته ظاهرة العولمة والتكنولوجيا، التي تم استعمالها في مختلف المجالات العلمية والتقنية، من مسايرة الأحداث وتخطي الصعوبات .

وبقيت الأبحاث متواصلة على مستويات عالية من التحليل إلى أن لحق بالعالم تقنيات جديدة، بظهور الإنترنت وربطها بوسائل الإتصال والإعلام وذلك عن طريق اجهزة متنوعة تمتلك قدرات هائلة للقيام بالعديد من المهام في ظرف قياسي.

هذه المتغيرات والأدوات الجديدة ساهمت في نقل كافة مجالات الحياة لتأخذ طابعاً رقمياً يدور في فلك الفضاء الإلكتروني الذي يستخدم بشكل إيجابي في تحقيق نوع من التواصل الإنساني بين العديد من التجمعات البشرية والأفراد من كافة أنحاء الدول.

ومع أنه لا يمكن إنكار ما لهذه الوسائل الإلكترونية الحديثة من فوائد يصعب حصرها، فإن الوجه الآخر والمتمثل في الإستخدامات السيئة والضارة لهذه التقنيات الحديثة خاصة التي تستعمل في الكثير من الأحيان أساليب العنف والتطرف وصناعة الكراهية، أين اتخذت بعدا خطيرا ساعد في ميلاد أنواع جديدة من الجرائم. فالعالم اليوم أصبح يواجه جرائم مستحدثة بصور مختلفة، تقترف بأحدث الأساليب التقنية، بشكل متغير عن تلك الجرائم التقليدية، وقد تعددت تسمياتها حيث أطلق عليها عدة تعابير"الجريمة المعلوماتية" أو الجريمة الإلكترونية" أو "الجريمة السيبيرانية".

نود التأكيد أنه وإذا كانت المجموعة الدولية قد إهتمت بحماية مجتمعاتها من الجريمة بشكل عام، غير أن اليوم ما نشهده في ظل الجريمة المستحدثة هو بعض التأخر في إدراك خطورة الجريمة الواقعة في الفضاء الإلكتروني، خاصة عندما أفرزت معها تحديات جديدة على الدول.

في ظل هذه الظروف أصبح المجتمع الدولي يواجه عدد كبير من التهديدات الإجرامية التي تتسم بتغيرها وتطورها المستمر، وإتساع نطاق تأثيرها[1]، وصار تجريم السلوك الإجرامي وملاحقة الجناة في الجرائم المرتكبة في الفضاء الإلكتروني مسألة صعبة المنال، خاصة في ظل القوانين الجزائية التي تبدو غير كافية للتصدي لهذه الجرائم من حيث المواكبة في التجريم القانوني للأفعال المستحدثة والمرتبطة بالتطور التكنولوجي على المستوى الوطني والدولي.

[1] - **نوران شفيق**، اثر التهديدات الالكترونية على العلاقات الدولية" دراسة في أبعاد الأمن الإلكتروني"، المكتب العربي للمعارف، الطبعة الأولى، مصر، 2016، ص 19

على هذا الأساس نهدف من خلال هذه الدراسة بالإطلاع على التحول الحاصل في وسيلة إرتكاب الجريمة التي إنتقلت الى الفضاء الإلكتروني وتوظيفه كأداة لارتكاب الجرائم بعدما كان وسيلة عالمية لتبادل المنافع والمعلومات والمشاركة في إنتاجها عالميًا.

كما تتمحور الورقة البحثية حول إبراز الاستجابة الدولية لمنع ومكافحة الجرائم المستحدثة خاصة في ظل عدم وجود اتفاقية دولية تتناول خصيصاً قضايا الجريمة الإلكترونية، فنجد أن الدول تمارس تحقيقها القضائي في هذه المسائل بإستنادها إلى ما هو قائم من تدابير دولية أو إقليمية الى جانب توصيات مؤتمرات الأمم المتحدة لتعزيز اليات التعاون الدولي ذات الصلة.

وعلى خلفية ما سبق ذكره نطرح إشكالية الدراسة فيما يلي: **إلى أي مدى ساهمت جهود منظمة الأمم المتحدة في التصدي للجريمة الالكترونية ؟**

للإجابة عن الإشكالية المطروحة تستدعي منا التطرق الى مفهوم الجريمة الإلكترونية إلى جانب التعرض لأهم صورها بنوع يحيط بالأساليب الإجرامية الجديدة في الفضاء الرقمي في (المبحث الأول)، ثم ننتقل إلى الإستجابة الدولية لمنع ومكافحة الجرائم المستحدثة في إطار منظمة الأمم المتحدة (المبحث الثاني).

المبحث الأول

الأنماط الجديدة للجريمة في الفضاء الرقمي الدولي

على مدار التاريخ لعبت التقدم التكنولوجي دورًا أساسيًا في نقل أساليب حياة المجتمعات إلى الأفضل غير أن الواقع اليوم كشف لنا أن هذا التطور صاحبه نمو تطرف عبر الفضاء الالكتروني، الذي كان أمده بعد إنتشار إستعمال شبكة الإنترنت وربطها بالحواسيب والهواتف الذكية وهو ماعرف بـ "الجريمة الإلكترونية" .

ينبغي القول أن هناك عدة تقسيمات لأنماط وصور الجرائم الإلكترونية، كالجرائم الموجهة ضد أجهزة الحاسب الألي وأنظمة تقنية المعلومات والإتصالات بقصد تدميرها أو تعطيلها.

غير أن التقسيم الذي سنعمد على إتباعه هو الذي يكون فيها الحاسب الألي أو أي ألة تقنية مرتبطة بالإنترنت كوسيلة لإرتكاب مختلف الجرائم، والتي تكون غالبا هذه الإعتداءات الإلكترونية واقعة ضد سرية البيانات الشخصية وسلامة الأموال حيث سيتم التطرق إليها في (المطلب الأول) إضافة إلى الجريمة الإلكترونية التي تمس أمن وسلامة الدول كونها تتحدى الحدود الجغرافية في(المطلب الثاني).

المطلب الأول: الجرائم الإلكترونية ضد سرية البيانات الشخصية وسلامة الأموال.

منذ الأزل والجريمة جزءا من سلوك الإنسان في المجتمع، حيث توارثت بين الأجيال في مختلف الشعوب وعلى الرغم من الجهود الدولية التي تبذلها كل دولة لمقاومة الظاهرة الإجرامية، إلا أن الإحصائيات تشير دوما إلى زيادة نسبة الإجرام في غالبية دول العالم، وخصوصا في القرن الأخير الذي شهد ثورة معلوماتية من نمط متميز، وما أفرزته تلك الأخيرة من جرائم مستحدثه، مغايرة عن التقليدية بحداثتها من حيث الأساليب والأدوات المستعملة في تنفيذها[1]

ولابد الإعتراف أنه مع التوسع الكبير في إستخدام شبكات المعلومات إزدادت المخاطر التي تعترضها وظهرت سلوكيات جديدة خارجة عن القانون تمارس ضد الأفراد أو مجموعة منهم بغرض إيذائهم وإساءة سمعة الضحايا، أين تخلف ضرر مادي أو نفسي بصفة مباشرة أو غير مباشرة مثل ما يحدث جراء غرف الدردشة و البريد أين ستمس الدراسة أهم الصور في هذه الجزئية في (الفرع الأول).

غير أنه غالبا ما يكون الباعث الرئيسي للإعتداء والغرض من معرفة أو إفشاء هذه المعلومات هو الحصول على المال مما يعد من الإعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات، والتي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم، وهو ما سنتوقف بإبراز هذه الصور في (الفرع الثاني).

الفرع الأول: الجريمة الإلكترونية المرتكبة ضد سلامة وسرية البيانات الشخصية

إن الفعل الإجرامي الذي إنتقل مع الطفرة النوعية الرقمية بشكل بات يعرفها الإنترنت[2]، قد ألحق في العديد من المرات أضرار بالضحايا ومؤسسات الدولة، إضافة الى وجود الركن المعنوي من خلال وجود نية مسبقة للإجرام، تتبين من خلال تصفح مجرمي الإنترنت[3]، وإرتكاب العديد من الجرائم التي مست عدة فئات من الأفراد.

---

[1] ـ **هروال هبة نبيلة**، جرائم الانترنت(دراسة مقارنة)، أطروحة دكتوراه، جامعة أبو بكر بلقايد تلمسان، الجزائر، كلية الحقوق والعلوم والسياسية، 2013، ص 13/ كذلك راجع في فكرة تطور الظاهرة الاجرامية عبر المراحل التاريخية: ـ **ساحي فوزية، بوكابوس عبد القادر**، ظاهرة الجريمة المفهوم الأسباب والأشكال، مجلة أبحاث، المجلد07، العدد01، 2022،ص ص 82- 96، ص83 وما يليها

[2] – **عبد الإله النوايسية**، جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، دار وائل للطباعة والنشر والتوزيع، الطبعة الأولى، الاردن، 2017، ص 29

[3] – **خالد ممدوح إبراهيم**، أمن الجريمة الالكترونية ،الدار الجامعية، الإسكندرية، د ط، مصر، 2010، ص 6

ولا بد لنا من الإشارة إلى الإعتداءات التي تمس البيانات الشخصية والمعلومات السرية المتصلة بالحياة الخاصة بطرق غير مشروعة من أجل الإمتثال إلى أوامرهم و تحقيق أغراض عديدة[1]، وفي مجال هذه الافعال والتصرفات نذكر أهمها :

أولا ـ جرائم إنتحال الشخصية عبر المواقع الالكترونية : إن مسالة إنتحال الشخصية ليس بموضوع جديد في تاريخ البشرية، فقد كان القانون صارم اتجاه هذه الجريمة، لما تشكل من ضرر للضحايا، غير أن الجديد في هذا الفعل هو إنتقاله الى الطابع الإلكتروني معتمدا على الحاسوب وشبكة الإنترنت كأداة للجريمة.

ويعرف إنتحال الشخصية عموما على أنه : "الظهور أمام الأخرين بمظهر الفرد الذي تم إنتحال شخصيته"، بحيث الناظر إليه والمتعامل معه يعتقد أنه يتعامل مع الشخص الذي إنتحل شخصيته [2].

ويكون إما بالظهور على روابط يقوم بانشاؤها وعرضها أمام الفئات الأخرين وإيهامهم أنه الشخصية الأصلية تكون عادة معروفة أو مشهورة ، كما قد يكون بواسطة انتحاله لوظيفة أو إنتمائه لهيئة أو مؤسسة معروفة .

ويتسنى ذلك عن طريق تحميل هوية وبيانات تختلف عن هويته غرضها الخداع ، النصب أو الاحتيال أو الحصول على مزايا التي يتمتع هؤلاء الاشخاص. وفي كلتا الحالتين فقد يستدرج المجرم ضحيته ليأخذ المعلومات بأسلوب غير مباشر، من أجل توظيفها ليتحصل على مكاسب مادية أو محاولة التشهير بسمعة أشخاص بعينهم، أو إفساد علاقاتهم الإجتماعية أو المهنية .

ويزيد من إحتمالات الخداع حالة التخفي التي يتيحها مواقع التواصل الإلكتروني على بناء وتكوين صورة ذهنية معينة عن الطرف المنتحل الذي يخفي تماما لحقيقته، وقد ينبني على هذه الصورة الذهنية مشاعر معينة كالحب مثلا أو الصداقة، غير أن في الواقع يختلف تماما حيث تظهر عملية الخداع والتضليل التي تكون صدمة لأحد الطرفين[3].

---

[1] – **ذياب موسى البداينية**، الجرائم الالكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقى العلمي" الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية"،المنعقد خلال الفترة من 02الى 04 سبتمبر 2014، تحت إشراف كلية العلوم الإستراتيجية ، عمان، الاردن، 2014، تم الإطلاع عليه بتاريخ 2024/05/19 ، متاح عبر الرابط الإلكتروني:
https://www.researchgate.net/profile/Diab-Al Badayneh/publication

[2] – هذا التعريف متاح عبر الرابط الالكتروني الويكيبيديا :
الموسوعة الحرة https://ar.wikipedia.org/wiki/

[3] ـ **بوفاتح محمد بلقاسم**، الجريمة الإلكترونية، دراسة سوسيو قانونية، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، العدد 03، 2009، ص ص 52ـ 66، ص 53

ثانيا - إختراق البريد الإلكتروني: يقصد بالبريد الإلكتروني نقل الرسائل أو الملفات في نظام بين الحواسيب أو أي جهاز تقني، وفي الغالب ما يتم هذا باستخدام مخزن وطريقة نقل معينة أو طريقة إرسال النصوص إلكترونيا من حاسوب مركزي أو نهاية طرفية إلى نهاية أخرى" [1].

أما من الناحية الإجرائية فهو" كل رسالة أو ملف أيا كان نوعه نصي أو صوتي بصور أو أصوات يتم بعثها عبر شبكة عامة للإتصالات ويتم تخزينها على أحد خوادم هذه الشبكة أو في حواسيب خاصة بالمرسل إليه حتى يتمكن هذا الأخير من استعادتها" [2].

ويكون الإختراق من خلال محاولة الدخول إلى أنظمة أو شبكات التواصل أو المنشأة بمساعدة بعض البرامج المختصة في السرقة وفك كلمات السر عن طريق المهارات والفنيات المكتسبة، واستغلالها في أعمال تضر بمالكه[3].

ولعل من أكثر هذه الانتهاكات إنتشارا هو محاولة إغراق البريد الإلكتروني بالرسائل الالكترونية إلى الحد الذي لا يصبح قادرا على إستقبال أية رسائل حقيقية موجهة له، وقد تتم هذه العملية شكل هجوم متعدد الأطراف من قبل عدة حاسبات مرتبطة بالانترنت .

في نفس السياق يمكن أن يتم الاختراق عن طريق ما يعرف بإسم الهندسة الاجتماعية وهي طريقة يتم استخدمها لإيقاع مستخدم الحسابات في الفخ وفتح الملفات الخبيثة الملحقة بالرسائل[4].

كما يتم تهديد الأشخاص من خلال إرسال الصور أو الكتابات إلى الشخص المراد تهديده أو ابتزازه، بغية حمله على القيام بفعل معين أو منعه من القيام به، و يتم إرسال هذه الكتابات إلى البريد الالكتروني لشخص في حال التعرف عليه .

ثالثا ـ القرصنة المعلوماتية : يقصد بها عموما سرقة المعلومات من برامج وبيانات بصورة غير شرعية، وهي مخزنة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية، وتتم هذه العملية إما بالحصول على كلمة السر أو بواسطة إلتقاط الموجات الكهرومغناطيسية بحاسبة خاصة، ويمكن وضعها في عجلة صغيرة أو في مكان قريب من مركز إرسال هذه الموجات[1].

---

[1] – خالد ممدوح إبراهيم، المرجع السابق ، ص 90

[2] – عدي جابر هادي، الحماية الجزائية للبريد الالكتروني (دراسة مقارنة)، مجلة رسالة الحقوق، العدد الثالث، 2010، ص ص 154-179، ص 156

[3] – أنظر : بوفاتح محمد بلقاسم، المرجع السابق، ص 52

[4] – هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة ، دار النهضة العربية ، القاهرة ، 2015، ص 209

[1]– يحياوي محمد، مخاطر القرصنة المعلوماتية على الحكومة الالكترونية، Revue de Recherches et Etudes Scientifiques، المجلد 05، العدد 01، 2011، ص ص 257-285، ص 265

وقد يحاول من خلال عملية القرصنة التّوصل إلى المعلومات السّرية والشّخصية، وإختراق (Hackers) الحاسب الآلي من أجل التوصل إلى الخصوصية وسرّية المعلومات بسهولة، وذلك راجع إلى أنّ التّطور المذهل في عالم الحاسب الآلي والشّبكات المعلوماتية يصاحبه تقدّم أعظم في الجرائم المعلوماتية وسبل ارتكابها، ولاسيّما وأنّ مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي[1].

علاوة على ذلك تتيح التكنولوجيا عدة وسائل مبتكرة كالتهديد، الابتزاز، والتهديد بالوثائق المزورة التي يتم تزويرها إلكترونيا لدرجة لا يمكن ملاحظة الفرق بين الصورة الأصلية أو المزورة، بغض النظر عن نشر المواد الاباحية.

الفرع الثاني: الجرائم المتصلة بالكومبيوتر والأنظمة التقنية للأموال .

إذا كانت الجرائم المعلوماتية بأنها الجرائم التي تتم بإستعمال جهاز الكمبيوتر أو وسيلة متصلة بشبكة المعلومات لغرض تعطيل الأجهزة أو إلحاق الضرر بها، وقد ساهم إستخدام الإنترنت بتوسيعها، كما يجهز هذا النوع من الجرائم من لدن أفراد أو مجموعات مبتدئة أو محترفة، غير أن الدافع الأساسي للجرائم المعلوماتية هو المال، ويُمكن أن تُنَفَّذ عبر العديد من الوسائل التقنية، ومن بين الجرائم التي يمكن التطرق في هذه الجزئية نذكر ما يلي :

أولا ـ جرائم غسيل الأموال عبر الإنترنت : تعد جرائم غسل الأموال عبر الإنترنيت من الجرائم الاقتصادية الحديثة، وقد تطورت صور هذه الجريمة في هذا العصر الذي أصبحت فيه تقنية المعلومات من أساسيات الحياة، بإعتبار أن بعض الأطراف الفاعلة تستغل هذه التقنيات الحديثة وتوظفها في مآرب غير مشروعة[2] .

وقد شهد إستغلال عدة وسائل إلكترونية في عملية غسيل الأموال أهمها الحاسب الآلي بشكل عام الى جانب شبكة الإنترنيت، وإحترفت هذه الجماعات تحويل الأموال عن طريق : الحسابات الإلكترونية والبطاقات التي تحمل أرقاما سرية ، وكذلك اختراق المواقع الإلكترونية [1].

ثانيا – الاعتداء على الأموال إلكترونيا: وهي الأموال المتداولة إلكترونيًّا سواء أكان ذلك في إطار التجارة الإلكترونية أو غيرها، مثل عمليات سحب وإيداع الأموال التي تقوم بواسطة أجهزة الصراف الآلي أو الهاتف المصرفي أو الخدمات المصرفية بواسطة الإنترنيت وربطها بأنظمة البنوك، أين تصبح بإمكانية تعرّض هذه

[1] – انظر / لينا محمد ألأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دار الحامد للنشر و التوزيع، الأردن، الطبعة الأولى ، 2015، ص 45

[2] – **JEAN-François Thony ,** Money laundering and terrorism financing: an overview, pp 01-20, p 03, consulté le /05/ 202020, available sur le site web https://www.imf org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf

الودائع للسرقة، ويكون ذلك عموما بواسطة بطاقات إئتمان غير مطابقة وتم إنشائها بالتزوير أو إنتهت صلاحية هذه البطاقات أو سرقت من مالكها الأصلي، أو إختراق المواقع الإلكترونية، أو الأجهزة التقنية للبنوك [1].

ثالثا ـ الإحتيال الإلكتروني : تتكون هذه الجرائم أساسا من التلاعب بالمدخلات، حيث يتم إدخال بيانات غير صحيحة في الكمبيوتر، أو عن طريق التلاعب بالبرنامج وتدخلات أخرى في مسار معالجة البيانات.

فالاحتيال هو" الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تؤدي إلى تسليم ذلك المال، فهي وسيلة من وسائل التدليس التي ينص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكا لغيره نتيجة الوقوع في الغلط "[2].

فهي جريمة ناشئة عن الإستخدام الغير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي، وهذا ما أدى إلى إطلاق مصطلح الجريمة الالكترونية على هذا النوع من الجرائم.

ويمكن القول أنه في ظل وجود الإنترنت لعرض المنتجات التجارية فإنه أصبح بإمكان المحتالين والنصابين عرض منتجات وهمية على الروابط والمواقع والمطالبة بالدفع عبر حسابات تفتح لاستقبال الأموال بصفة مؤقتة وتغلق بعد الحصول عليها ، حيث ميزت هذه الجريمة سهولة إختفاء المجرمين.

المطلب الثاني : الجرائم الإلكترونية الماسة بأمن و إستقرار الدول

تتمثل عموما في الاشخاص والجهات المتطرفة التي تتصدرها الجماعات الارهابية والإجرامية كونها أصبحت تباشر في عملية الاستخدام الغير السلمي للتقنيات الحديثة في تنفيذ مخططاتها الإجرامية لغرض ضرب إستقرار وسلم الدول، أين أفرزت لنا عدة تهديدات حديثة، حيث نذكر في هذا الخصوص : الإرهاب الإلكتروني والتهديدات الإلكترونية ضد المؤسسات الحيوية للدول.

الفرع الأول : تحديات الإرهاب والجريمة المنظمة في البيئة الالكترونية

لقد تبين من خلال إنتقال الجريمة والعنف الى البيئة الإلكترونية أنه شكل تحديا خطيرا على المجتمع الدولي بالنظر لتطور جرائم الارهاب والجريمة المنظمة العابرة للحدود الاقليمية بين الدول ، مع وجود أجهزة الحاسوب المرتبطة بالإنترنت من غير أن تخضع للزمان والمكان، ويكون من المناسب تناول الإرهاب الإلكتروني والجريمة المنظمة المرتبطة بالانترنت .

---

[1] – **أحمد رجدال، أمال يوسفي**، التصدي للتقنيات الحديثة في تمويل الارهاب الدولي، الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 13، العدد02، 2021 ، ص 264 –279 ، ص 270

[2] – **شهيرة بولحية، دنيا راد سويح**، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية ، المجلد 02 ، العدد 02، ص ص37ـ46، ص 38

أولا ـ الإرهاب الإلكتروني : بقصد بجريمة الإرهاب الإلكتروني النشاط غير القانوني، الذي يقوم به شخص أو أشخاص سواء كانوا طبيعيين أو اعتباريين بواسطة التقنية الإلكترونية الرقمية عبر شبكاتها لتحقيق غرض محدد " فالإرهاب الإلكتروني"هو نشاط إجرامي مخطط ومنظم مخالف للقانون يقوم به التنظيم الإرهابي بواسطة التقنية الإلكترونية الرقمية لتحقيق غرض معين"[1] .

وإلى جانب مظاهر جرائم الإرهاب الإلكتروني الممتثلة في التجنيد والتمويل الإلكتروني،[2] هناك ما يتعلق بإنشاء المواقع وتدميرها من طرف التنظيمات الإجرامية والإرهابية.

أين يتم إنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشأت مواقع لتعليم صناعة المتفجرات، وكيفية إختراق وتدمير المواقع، وطرق الإعتداء على البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة وأساليب نشر الفيروسات وغير ذلك[3].

و إذا كانت تسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الانترنت في شهر أكتوبر من سنة 2000إلى أكثر من 22مليون موقع[4] .

كما يتم تدمير المواقع عن طريق الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بشبكة الإنترنت من خلال نظام ألي[5]، وذلك بهدف تخريبها من خلال الثغرات المتعددة في التطبيقات، وتستخدمها التنظيمات الإرهابية غالبا لتخريب الأنظمة الأمنية أو أجهزة الإتصالات، وذلك من أجل إفشال عمليات المراقبة والتتبع التي تفرضها الأجهزة الحكومية لكشف مخططاتهم، وتتبع إتصالاتهم ومشاريعهم أو أماكن تحركهم وغيرها[6].

ثانيا – الجريمة المنظمة المرتبطة بالإنترنت: من الملاحظ أن الجماعات والتنظيمات التي تنطوي ضمن ممارسة مختلف أشكال للجريمة المنظمة العابرة للوطنية لم تكن بمعزل عن فرض تواجدها من خلال إستغلال الشبكة الإلكترونية للقيام بمخططاتها الإجرامية، حيث إعتمدت بشكل كبير على الإنترنت كنظام سهل عليها

---

[1] – مصطفى محمد موسى ، الإرهاب الإلكتروني ، دراسة قانونية أمنية نفسية اجتماعية ، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، دار الكتب و الوثائق القومية المصرية، الطبعة الأولى، 2009، ص 173

[2] – أكثر التفاصيل حول هذه المظاهر راجع : أحمد رجدال ، القانون الدولي في مواجهة تطورات جرائم الإرهاب الدولي (من الطابع التقليدي إلى الفضاء الالكتروني)، رسالة دكتوراه، جامعة أمحمد بوقرة بومرداس، كلية الحقوق، 2023، ص 83 وما يليها

[3] – شعنبي صابرة، الإرهاب الإلكتروني الأشكال والدوافع، مجلة العلوم الإجتماعية والإنسانية، جامعة المسيلة، العدد العاشر،2017، ص ص 435 ـ 448، ص444

[4] – محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع ، الطبعة الأولى ، الأردن ، 2017، ص 186

[5] – هلالي عبد اللاه أحمد، المرجع السابق ص 193

[6] – نصير لعرباوي، فاتح النور رحماني، الجريمة الإرهابية الالكترونية، مجلة المعيار، العدد43،2018 ،ص 382

الدخول الى عالم أوسع من الشكل التقليدي وبوقت وجيز، لا يتطلب إلا على الإستعانة ببعض المواقع والروابط حسب كل مجال، بشكل يتنافى مع كل المبادئ ولا ينجر فقط عن إلحاق الذعر والخوف للأشخاص فقط بل يتعدى ذلك بتهديد أمن الدول بأكملها.

وفي هذا المقام يمكن أن نعتمد على عدة أمثلة كالتجارة الإلكترونية للمخدرات التي تعد من أولى النشاطات غير المشروعة التي مارستها هذه المجموعات الاجرامية[1] ، الى جانب المتاجرة الالكترونية بالبشر[2]، حيث يعد الإنسان سلعة يتداول على بيعها أو شرائها والمقايضة بعد خطفه أو إغوائه بقصد استدراجه أو استقطابه. كما قد تقتل هذه الفئات لغرض المتاجرة بأعضاء البشر من طرف مجموعة إحترفت هذا النشاط الغير مشروع وإنتهكت الحق في الحرية والكرامة.

والأمثلة على نشاطات المجموعات الاجرامية العابرة للدول التي تستعين بالإنترنت كثيرة كالإستغلال الجنسي للأطفال و نشر الإباحية والهجرة غير الشرعية، الاتجار بالأسلحة.....الخ[3].

الفرع الثاني: التهديدات الإلكترونية ضد المؤسسات الحيوية للدول

يعد من أخطر مصادر التهديد الالكتروني للمؤسسات من خلال اختراق شبكات اتصالاتها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة، وفي ظل المنافسة التي تشهدها معظم الأسواق الحالية، أصبح التجسس على مختلف الشركات من قبل منافسيها، مصدر قلق حقيقي[4].

كما يمكن ضرب إستقرار المصالح الحيوية للدول والدخول إلى شبكات التحكم في المرافق الحيوية ، مما يتسبب في شلل للبنية التحتية الأساسية، بل وإحتمال تدميرها كليا، فالدول أصبحت معرضة لما يسمى بالدمار الشامل باستخدام الأسلحة المعلوماتية المتمثلة في الفيروسات التي تخترق حدود الدول وتحطم البنية التحتية

---

[1] – أنظر لهذه الأمثلة: أخام بن عودة زواوي مليكة، تحديات ظاهرة الجريمة المنظمة العابرة للأوطان والثورة المعلوماتية، ورقة عمل مقدمة في المؤتمر المغاربي الأول حول المعلوماتية والقانون، تحت إشراف: أكاديمية الدراسات العليا، طرابلس، ليبيا ، 27-30 أكتوبر 2009، منشورة عبر الرابط :
https://www.researchgate.net/publication/328064682_aljraym_alalktrwnyt_almfhwm_walasbab

[2] – للإطلاع على أكثر التفاصيل راجع/ كردي نبيلة ، الإتجار بالبشر عبر الإنترنيت، مجلة أبحاث، المجلد 07 ، العدد 02، 2022 ، ص ص 521 ـ 523

[3] – أكثر التفاصيل راجع: ـ سليم سولاف، علاقة الجريمة المنظمة بشبكة الإنترنت، مجلة البحوث والدراسات القانونية والسياسية، المجلد 08، العدد01 ، 2019، ص ص 186 ـ204

[4] – راجع حول هذه التهديدات الالكترونية : – سعيد عبيدي ،الإرهاب الإلكتروني ، مجلة العلوم الإنسانية، الجزائر، العدد 02، 2017، ص ص 32 43

لشبكة المعلومات، مثل الدخول لبرامج الدول المتعلقة بالموانئ والمطارات والمرافق الحساسة، دون أن تستطيع تحديد هوية مرتكب الجريمة، إلا عن طريق أجهزة معينة تملكها بعض المؤسسات الأمنية، لبعض البلدان[1].

ومهما يكن فقد تكون البرامج الإلكترونية تارة محلا للجريمة الالكترونية، وقد تكون وسيلة لارتكابها تارة أخرى، وهي تختلف عن الجرائم التقليدية كونها مازالت في طور النشأة ومحاولة استيعابها وشمولها في الحماية القانونية[2].

وعلى خلفية ما تم التطرق إليه نجد أن الفراغ التنظيمي والقانوني لدى بعض الدول حول الجرائم المعلوماتية يعتبر من الأسباب الرئيسية في إنتشارها وتعددها، وأمام هذه التحديات نادت العديد من الأصوات وخصوصا المهتمين بالشأن الحقوقي بضرورة وضع إطار قانوني دولي، لذا سيتم البحث ضمن الترتيبات والتدابير المندرجة في الاجهزة الرئيسية والفرعية للأمم المتحدة في الجزء الثاني من هذه الدراسة.

المبحث الثاني

الاستجابة الدولية لمكافحة الجرائم المستحدثة في إطار منظمة الامم المتحدة

لا يمكن إنكار أن الوسائل التقنية ساعدت في تنفيذ الجرائم الالكترونية بشكل تجاوز الحدود الوطنية، الأمر الذي يجعل الدولة المعتدى عليها عاجزة عن التصدي بمفردها لمثل هذه الجرائم، وبالتالي ضرورة البحث عن جهود الأمم المتحدة من خلال الجمعية العامة والإتفاقيات الدولية والإقليمية (المطلب الأول)، إضافة الى ترتيبات مؤتمرات الأمم المتحدة بشأن التصدي للجرائم الإلكترونية (المطلب الثاني).

المطلب الأول: التدابير القانونية لتامين الفضاء الالكتروني ومعاقبة مرتكبي الجرائم المحيطة به

لقد بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة الإجرام الإلكتروني، و ذلك لما تسببه من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيماناً منها بأن منع هذه الجرائم ومكافحتها يتطلب إستجابة دولية تتطلب تأمين الإستخدام السلمي للفضاء الالكتروني من التهديدات الإجرامية، وذلك ما إهتمت به أجهزة منظمة الأمم المتحدة خاصة الجمعية العامة **(الفرع الاول)**،كما نحاول البحث عن الأطر القانونية للتجريم و

[1] – محمد علي محمد، كوارث الإرهاب الالكتروني بين الفلسفة القانونية و تطور الأمن التقني، دار النهضة العربية، مصر، الطبعة الأولى، 2018، ص 39

[2] – أكثر التفاصيل راجع : وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد7، العدد 2 ، 2019، ص 64، ص ص 62-73

توقيع العقاب من خلال الاتفاقيات التي وُضعت لتيسر التعاون الدولي بشان التحقيق حول الجرائم السيبيرانية **(الفرع الثاني)**.

الفرع الأول: إعلانات الجمعية العامة بشان الحدِّ من إساءة استخدام الفضاء الإلكتروني

يبدو أن الأمم المتحدة أصدرت عبر الجمعية العامة عددًا من الاعلانات التي تبين مدى تصاعد الإهتمام العالمي بإستخدام تكنولوجيا الإتصال والمعلومات إستخدامًا غير سلمي، وجاء ذلك عبر سلسلة منها: الدورة 70/53 في 4 ديسمبر 1998 وفي الدورة 49/54 في ديسمبر 1999، والدورة 28/55 في 20 من ديسمبر 2000، والدورة 19/56 في 29 نوفمبر 2001، بشأن إرساء الإطار القانوني لمكافحة إستعمال تكنولوجيا الإتصال والمعلومات في أعمال إجرامية، والدورة 53/57 في 22 نوفمبر 2002 بشأن التطورات الحادثة والمتوقعة في ميدان المعلومات والاتصالات السلكية واللاسلكية لتحقيق الأمن الدولي[1].

ركزت هذه الإعلانات في مجملها على ضرورة مواكبة التكنولوجيا لتحقيق الأمن والسلم الدوليين، وأن هذه التطورات يمكن أن تكون لها عدة تطبيقات مدنية وعسكرية على السواء، وأنه لابد علينا من مواصلة وتشجيع التقدم المحرَّز في تسخير العلم والتكنولوجيا لأغراض التطبيقات المدنية.

ومما لا شك فيه أنه دعت الدول لضرورة النظر في الأخطار القائمة والمحتملة في مجال أمن المعلومات وكذلك فيما يمكن اتخاذه من تدابير للحدِّ من المخاطر التي تبرز في هذا الميدان، بما يتماشى مع المحافظة على التدفق الحر للمعلومات،والتدابير التعاونية التي يمكن اتخاذها للتصدي لها، والعمل على تشكيل فريق من الخبراء الحكوميين.

---

[1] – أكثر التفاصيل في هذا الشأن أنظر :

ـ إعلان الجمعية العامة في الدورة 70/53 في 4 ديسمبر 1998، متاح على الرابط التالي:
https://www.insdip.com/ar/53o-periodo-de-sesiones-1998-1999-agnu/

ـ إعلان الجمعية العامة في الدورة 49/54 في ديسمبر 1999 ، رقم الوثيقة A / RES /54 / 49

ـ إعلان الجمعية العامة في الدورة 28/55 في20 ديسمبر 2000، بعنوان "التطور في مجال المعلومات والاتصالات"، الوثيقة رقم A/RES/55/28

تم الاطلاع على اعلانات الدورة 54و55 عبر الرابط الالكتروني التالي:
https://www.insdip.com/ar/54o-periodo-de-sesiones-1999-2000-agnu/

ـ اعلان الجمعية العامة في الدورة 19/56 في ديسمبر 2001، الوثيقة رقم A/RES/56/19، تم الاطلاع عليه عبر الرابط
https://documents-dds ny.un.org/doc/undoc/gen/n01/476/26/pdf/n0147626.pdf?openelement

بالإضافة إلى كل من إعلان الجمعية العامة في الدورة 239/57 في 31 جانفي 2003 بشأن إرساء ثقافة عالمية لأمن الفضاء الإلكتروني، وإعلان الجمعية العامة في الدورة 199/58 في 23 من ديسمبر 2003 [1].

من جهتها ساهمت الجمعية العامة في تشكيل "مجموعة الخبراء الحكوميين GGE" في عام 2001 أين وافق معظم أعضاء الأمم المتحدة على إنشائها وعملها في عام 2004 بهدف النظر في الأخطار القائمة والمحتملة في ميدان أمن المعلومات الدولية ومناقشتها ، والإجراءات الممكنة لرسم الأسس الدولية التي تهدف إلى تقوية أمن نظام الإتصالات والمعلومات، وكانت المرة الأولى التي يتخذ فيها قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى مراحل عملية [2]، وتم تشكيل هذه المجموعة من أربعة فرق للخبراء الحكوميين، لمعالجة الأخطار القائمة والمحتملة في الفضاء الإلكتروني وتدابير التعاون الممكنة للتصدي لها.

وفي سياق سبل ووسائل الحفاظ على إستعمال الفضاء الخارجي لأغراض سلمية تم الإتفاق في تقرير لجنة استخدام الفضاء الخارجي في الأغراض السلمية في دورتها الثانية والستون للجمعية العامة 2019، على أنَّ لها دوراً أساسيًّا عليها أن تلعبه في تعزيز الشفافية وبناء الثقة بين الدول وكذلك في ضمان الحفاظ على استخدام الفضاء الخارجي في الأغراض السلمية، وذلك من خلال أعمالها في المجالات العلمية والتقنية والقانونية ومن خلال سعيها إلى تشجيع الحوار وتبادل المعلومات على الصعيد الدولي بشأن مختلف المواضيع المتعلقة باستكشاف الفضاء الخارجي واستخدامه [3].

---

[1] – إعلان الجمعية العامة في الدورة 239/57 في 20 من ديسمبر 2002 بشأن " إنشاء ثقافة عالمية للأمن السيبراني" متاح في الرابط : https://digitallibrary.un.org/record/482184?ln=zh_CN

[2] ـ **عادل عبد الصادق**، مقال بعنوان : الأمم المتحدة ودعم الاستخدام السلمي الفضاء الالكتروني،دوريات قضايا استراتيجية، منشور بتاريخ،6 اوت 2015، الاطلاع بتاريخ 2024/05/15 على الساعة 12سا00 ، متاح على الرابط http://accronline.com/article_detail.aspx?id=22762

[3] – الجمعية العامة للأمم المتحدة الصادر عن لجنة استخدام الفضاء الخارجي في الأغراض السلمية في دورتها الثانية والستون ، بتاريخ 21 جوان 2019، الوثيقة رقم A/74/20، متاح عبر الرابط:
https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420_0_html/V1906075.pdf

الفرع الثاني: ملاحقة ومعاقبة مرتكبي الجرائم الالكترونية من خلال الإتفاقيات الدولية والإقليمية

نجد أن آليات التعاون الدولي في الصكوك العالمية لمكافحة الجريمة الالكترونية، لم تخصص أساساً قانونياً للتعاون في العديد من القضايا التي ترتكب فيها أعمال عبر الإنترنت التي يقوم بها أشخاص ضالعون في إرتكاب تصرفات غير قانونية، لذا يجب النظر في الاتفاقيات الإقليمية ذات الصلة ومن أهمها يمكن ذكر:

أولا ـ معاهدة بودابست لمكافحة جرائم الإنترنت في **2001**: تعد أولى المعاهدات المتعلقة بالجرائم التقنية والتي تمت في العاصمة المجرية بودابست في 23 نوفمبر 2001 ،والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الالكترونية ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والإستخدام السيء لها، كما خضعت مواد الإتفاقية المقترحة لغرض المناقشة وتبادل الآراء والتي أثمرت لاحقا ما يعرف باتفاقية الجرائم الالكترونية ـ سيبر كرايم[1].

ينبغي الإشارة أن هذه التدابير التشريعية والتنظيمية سعت لضمان معاقبة مرتكبي هذه الجرائم ومحاولة كشفها وتوفير قواعد ملائمة من أجل التحري والتحقيق وتوحيد اجراءات الضبط، التفتيش والمحاكمة، مع التركيز على أهمية التعاون على المستوى المحلي والإقليمي والدولي مع ضرورة اقامة التوازن بين متطلبات تنفيذ القانون وبين الزامية احترام الحقوق الاساسية والسيادة[2].

وهكذا يتبين أن الإتفاقية جاءت نتيجة جهود دولية وإقليمية فقد أكدت في مقدمتها أيضا على أهمية ما أنجز من جهود في مجال الإجرام السيبراني من طرف الأمم المتحدة ، إضافة الى منظمة التعاون الاقتصادي والتنمية الى جانب الاتحاد الأوربي ومجموعة الدول الصناعية، كما نجد أن الاتفاقية قد ركزت على ثلاثة عناصر أساسية، إنطلاقا من التدابير التشريعية التي تضمنت (نصوص التجريم) في الفصل الأول،إضافة الى

[1] في الفترة الممتدة ما بين أفريل 1997 وديسمبر 2000، عقدت اللجنة الأوروبية المعنية بمشاكل الإجرام 10 إجتماعات في جلسات عامة و15 إجتماع لفريق الصياغة المفتوح لعضوية الدول، وعقب انتهاء مدة بنودها المرجعية الموسعة، عقد الخبراء تحت رعاية اللجنة، ثلاثة اجتماعات أخرى لوضع اللمسات النهائية على مشروع المذكرة التوضيحية ومراجعة مسودة الاتفاقية في ضوء الجمعية البرلمانية، التي طلبت منها لجنة الوزراء في أكتوبر 2000 إبداء رأيها بشأن مسودة الإتفاقية الذي إعتمدته في الجزء الثاني من دورتها العامة في أفريل 2001

نقلا عن: – التقرير التفسيري لاتفاقية الجريمة الالكترونية 2001 ، المجلس الاوروبي، سلسلة المعاهدات الاوروبية 185، النسخة المترجمة بالعربية ، تم الاطلاع عليه بتاريخ 2024/05/22 على الرابط :

https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174

[2] – راجع ديباجة معاهدة بودابست لمكافحة جرائم الإنترنت 2001

الفصل الثاني الذي تناول التدابير التشريعية الاجرائية التي تتخذ لإجراء تحقيقات أكثر فعالية خاصة فيما يتعلق بجرائم الكمبيوتر.

ويلاحظ أن هذه التدابير يمكن اللجوء اليها عند استعمال الكومبيوتر كوسيلة لارتكاب الجرائم، وصولا الى الفصل الثالث الذي يبين أهمية التعاون الدولي والإقليمي في مجال مكافحة الجرائم السيبرانية[1].

نود التأكيد أن اتفاقية جرائم الإنترنت هي المعاهدة الدولية السباقة التي تسعى لمعالجة ومواجهة الجرائم الإلكترونية من خلال انسجام القوانين الوطنية وقوانين الدول الأخرى ومن أهم أهداف الاتفاقية :

– توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

– توفير الإجراءات القانونية اللازمة للبحث والتحري عن الجرائم المرتكبة إلكترونيا .

– جمع المعلومات عن البيانات وعن إمكان وجود الاختراق أو التدخل في محتواها[2].

كما تضمنت المبادئ العامة المتعلقة بالتعاون الدولي في تسليم المجرمين، والمساعدة الدولية، وتبادل المعلومات بصورة آلية، وتفعيل الولاية القضائية على أي جريمة[3].

ثانيا ـ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010: على إثر إزدياد مخاطر الجرائم المرتكبة بواسطة تقنية المعلومات، بشكل أصبح يشكل هاجس كبيرا للدول عامة والعربية خاصة، لذلك أدركت هذه الدول ضرورة التعاون فيما بينها فسارعت إلى إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أبرمت بالقاهرة سنة 2010 [4].

---

[1] – راجع مواد معاهدة بودابست لمكافحة جرائم الإنترنت 2001

[2] – أكثر التفاصيل راجع : مراد مشوش، الجهود الدولية لمكافحة الاجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد2، 2019، ص 711 و ما يليها

[3]- voir : - PAUL De Hert, GLORIA González Fuster, BERT-Jaap Koops, Fighting cybercrime in the two Europes, The added value of the EU framework decision and the council of Europe convention, Revue International de Droit Pénal, RIDP, 2006, vol. 77, pp 503 à 524

–كما أبقت الاتفاقية المجال مفتوح في تيسير المشاورات واتخاذ التدابير اللازمة لمساعدة الأطراف في جهودها الرامية إلى إستكمال الاتفاقية أو تعديلها حسب الإحتياجات قائمة في مجال الوقاية والمتابعة الفعالة للجرائم الإلكترونية وقضايا الخصوصية المرتبطة بها. راجع : ـ فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، جامعة محمد خيدر ببسكرة، العدد 02، 2015 ، ص ص 07 ـ 21

[4] – الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في ديسمبر 2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، المنشور في الجريدة الرسمية للجمهورية الجزائرية العدد 57 بتاريخ 4 ذو الحجة عام 1435هـ الموافق لـ 28 سبتمبر 2014.

ومن أهدافها حسب ما ورد في المادة الأولى من هذه الإتفاقية فإن من اولوياتها تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة الجرائم التقنية للمعلومات ، الذي يمكن من تدارك الأخطار الناجمة عن هذه الجرائم ، إضافة إلى الحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[1].

لتنص الاتفاقية في الفصل الثاني بعنوان التجريم على جملة الأفعال التي تعتبر جرائم تقنية المعلومات، حيث خصت في المادة 16 منها على الأفعال الخاصة بالجرائم المنظمة التي ترتكب بواسطة الانترنت مثل جريمة الإتجار بالأشخاص، كنوع من جرائم تقنية المعلومات، بينما خصصت الاتفاقية الفصل الثالث لتناول الأحكام الإجرائية[2].

ولو أمعنا النظر في بنود هذه الإتفاقيات بغية تنفيذ الإلتزامات الواردة فيها فإن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين ، لذا كان لابد من البحث عن التدابير التي تطلع إليها منظمة الأمم المتحدة لتفعيل التعاون بين الدول حول الإجراءات القانونية المناسبة داخل إقليمها، وذلك ما تسعى إليه تطلعات المؤتمرات الدولية ذات الصلة .

المطلب الثاني: تعزيز آليات التعاون من خلال مؤتمرات الأمم المتحدة

يبدو أن مؤتمرات الأمم المتحدة تعمل على مسايرة تطور الجريمة الإلكترونية، حيث أكدت على ضرورة تضافر الجهود الدولية والعمل على تحسين إجراءات مكافحة الجريمة في الفضاء الإلكتروني عن طريق تبادل الخبرات التقنية والتجارب والمعلومات بأفق تمكنها من وضع إستراتيجيات دولية.

في هذا المقام يمكن التطرق إلى المؤتمرات المنعقدة من طرف لجنة منع الجريمة والعدالة الجنائية،[3] التي تعد الهيئة التحضيرية لمؤتمرات الأمم المتحدة لمكافحة الجريمة كما تُحيل الإعلانات المعتمدة إلى الجمعية العامة للمصادقة عليها. وقد كان لهذه المؤتمرات أثرا هاما في رسم السياسة الجنائية وتعزيز التعاون الدولي، إضافة الى التصدِّي للمخاطر والتهديدات الإجرامية العابرة للحدود الوطنية بما فيها المرتكبة عبر الفضاء الرقمي .

---

[1] – راجع : المادة 01 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010

[2] – وردة شرف الدين، الأحكام الاجرائية لمكافحة جريمة الإتجار بالبشر المرتكبة بواسطة تقنية المعلومات ـ دراسة ضمن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010 ـ ، مجلة الإجتهاد القضائي،جامعة محمد خيدر بسكرة، الجزائر، العدد السادس عشر، مارس 2018، ص ص 93 ـ 118، ص 94

[3] – أُنشأت لجنة منع الجريمة والعدالة الجنائية كإحدى اللجان المتخصصة المنبثقة عن مجلس الأمم المتحدة الإقتصادي والإجتماعي بموجب إعلان الجمعية العامة رقم 152/46 بتاريخ 18 ديسمبر 1991 بشأن وضع برنامج فعال للأمم المتحدة في مجال منع الجريمة والعدالة الجنائية.

وسعيا من الأمم المتحدة من أجل مواجهة الجرائم الإلكترونية عقدت مؤتمراً دولياً خاصا بمنع إجرام تقنية المعلومات في سبتمبر 1990 بهافانا، الذي أصدر توصيات تحث على ضرورة مراجعة قوانين والإجراءات الجنائية الوطنية للدول لتتلائم مع التطور العلمي في جرائم شبكة الإنترنت[1] .

كما سعى المؤتمر الى حث المؤسسة المالية أن تقيم وتوثق مخاطر غسل الأموال وتمويل الجماعات الإجرامية وغيرها من الأنشطة غير المشروعة التي تشكلها الآليات والمعاملات المصرفية الإلكترونية، والمعاملات الإلكترونية الأخرى التي يتم من خلالها بدء علاقة العمل ومزاولتها والإستمرار فيها[2].

في نفس الإطار ومن أجل توطيد هذا التعاون فقد حث مؤتمر الأمم المتحدة **الثامن** لمنع الجريمة ومعاملة المجرمين في قراره المتعلق بالجرائم ذات الصلة بالحاسوب وبالدول الأعضاء أن تكثف جهودها لمكافحة الجرائم المعلوماتية باتخاذ عدد من الإجراءات منها مضاعفة الأنشطة التي تبذلها الدول على الصعيد الدولي ، بما في ذلك دخول الدول الأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بالجرائم المعلوماتية [3].

من جهتها توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجراء الدولي لمواجهة جرائم الإنترنت يتطلب من الدول الأعضاء إتخاذ عدة ترتيبات لمكافحتها[4].

في نفس السياق وتأكيدا على الإستعمال غير السلمي لشبكة الإنترنت عقدت الأمم المتحدة **المؤتمر العاشر** لمنع الجريمة ومحاكمة المجرمين في فيينا في أفريل سنة 2000، خصصت خلاله حلقة لدراسة جرائم الإنترنيت وإستخداماته السلبية باعتباره يمثل أحد التهديدات الأمنية في القرن الحادي والعشرين [1].

---

[1] – مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، الذي جاء بعنوان"منع الجريمة والعدالة الجنائية على الصعيد الدولي في القرن الـ21"، المنعقد خلال الفترة ما بين 27 اوت الى 07 سبتمبر ، 1990 هافانا بكوبا ، تم الاطلاع عليه بتاريخ 2024/05/25، الساعة 13:00 على الرابط :
https://www.unodc.org/congress/ar/previous-congresses.html#:~:text=

[2] – أحمد رجدال، أمال يوسفي، المرجع السابق، ص 271

[3] – يمكن الاطلاع على تفاصيل هذا المؤتمر من خلال الرابط المتاح عبر الرابط التالي:
– مؤتمرات الأمم المتحدة لمنع الجريمة و العدالة الجنائية (1955-2020) ،65 عاما من الانجازات ، الرابط الالكتروني
https://unis.unvienna.org/pdf/2020/CrimeCongress/65-years-brochure_ar.pdf

[4] – أمال بيدي، جهود الامم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08 ، العدد01، 2022، ص ص 299 ـ 316، ص306

لتواصل منظمة الأمم المتحدة جهودها بعقد المؤتمر **الثاني عشر** بالبرازيل أيام 12 إلى19 أفريل 2010 لمنع الجريمة والعدالة الجنائية، حيث ناقش فيه الدول الأعضاء مختلف التطورات الأخيرة في إستخدام التكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية وإحتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[2].

كما دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد إجتماع لفريق من خبراء دوليين مفتوح العضوية من أجل دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها، ركز فيه فريق الخبراء دراسته لهذا الموضوع على ظاهرة الجريمة السيبرانية بالتطرق إلى عدة توصيات[3].

وفي المؤتمر **الثالث عشر** المنعقد بالدوحة دولة قطر 2015 قررت الجمعية العامة للأمم المتحدة أن يعد الموضوع الرئيسي للمؤتمر، الذي قد شارك فيه حوالي 5000 شخص ممثلين لـ 142 دولة، إدماج منع الجريمة والعدالة الجنائية ضمن برنامج جدول أعمال الأمم المتحدة بشكل واسع لغرض التصدِّي للتحدِّيات الإجتماعية والإقتصادية إضافة الى تفعيل سيادة القانون على المستوى الوطني والدولي [4].

وقد كان لهذه المؤتمرات أثرها في دعم أسس العدالة الجنائية، إلى جانب تفعيل التعاون الدولي لمواجهة المخاطر التي تهدِّد المجتمع الدولي بما فيها الجريمة المنظَّمة .

---

[1] – ـ المؤتمر العاشر بشان الجريمة و العدالة الصادر عن الامم المتحدة لمنع الجريمة و معاملة المجرمين، المنعقد في فيينا من 10 الى 17 افريل ، بعنوان " مواجهة تحديات القرن الحادي و العشرين 2000"، تم الاطلاع عليه بتاريخ 2024/05/25 ، الرابط:

https://www.unodc.org/congress/en/previous/previous-10.html

[2] – المؤتمر الثاني عشر الصادر عن الأمم المتحدة لمنع الجريمة والعدالة الجنائية، بعنوان " الاستراتيجيات الشاملة لمواجهة التحديات العالمية، " نُظم العدالة الجنائية ومنع الجريمة وتطورها في عالم متغير"بالبرازيل أيام 12 إلى19 أفريل 2010 ، تم الاطلاع عليه بتاريخ 2024/05/25 ، متاح على الرابط:

https://www.unodc.org/congress/en/previous/previous-12.html

Voir aussi ; BRIGITTE Pereira , La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité , Revue Internationale de Droit Economique , R.I.D.E , 2016/3 (t. XXX), pages 387 à 409

[3] – تقرير الخبراء الحكومي الدولي المفتوح العضوية بشأن اجراء دراسة شاملة لمشكلة الجريمة السيبرانية 2011، تم الاطلاع على الموقع الالكتروني بتاريخ 2024/05/26 عبر الرابط:

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/V1701247_A.pdf

[4] – مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية خلال الفترة من (12 ـ 19) أفريل 2015، مركز قطر الوطني للمؤتمرات، الدوحة ، قطر، تم الاطلاع بتاريخ 2024/05/25، الساعة 21سا ،رابط الاطلاع على مخرجات المؤتمر :

https://www.unodc.org/congress/en/previous/previous-13.html

خاتمة:

ختاما لهذه الدراسة نستخلص أن الجرائم الالكترونية قد تجاوزت العادة المعروفة في الأوساط الإجرامية السابقة، وتفاقمت أثارها المدمرة والمختلفة حسب الأهداف التي تعمل الجهات الإجرامية للوصول إليها إتجاه الدول المستهدفة من هذه الجرائم باعتبارها عابرة للحدود، وكان لإقتران هذا النوع من الجرائم لأحدث التقنيات التكنولوجية المعاصرة أمرا بالغا في الخطورة على الدول والعلاقات الدولية.

ورغم المقدار الذي بلغه الإهتمام الدولي والاقليمي بمواجهة جرائم الفضاء الالكتروني والذي تجسد في شكل معاهدات عالمية وإقليميه حاولت وضع الأسس والأطر التشريعية الدولية بالتجريم ومواجهة الجرائم الإلكترونية، وإصدار إعلانات الجمعية العامة لغرض إرساء قواعد عالمية للحد من مخاطر إساءة استعمال التكنولوجيا، إضافة الى تدابير المؤتمرات الدولية تحت مظلة الامم المتحدة عبر لجنة منع الجريمة والعدالة الجنائية.

غير أن الواقع العملي أثبت عجز الأجهزة الدولية في التصدي بشكل فعال للجرائم الالكترونية بالنظر للصعوبات القانونية في مجال التعاون الدولي، والذي نتج عن عدم وضع حتى اليوم مفهوم قانوني واضح لإحتواء هذه الظاهرة في صك قانوني دولي على شكل معاهدة دولية شارعة موحدة ، بينما بقي العمل في إطار التعاون الدولي القضائي والأمني وفق ما تمليه بنود إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التي قد لا تتناسب مع التطورات الحاصلة في الجريمة الإلكترونية.

ينبغي التنويه أن هذه التصرفات والسلوكات الإجرامية الغير مشروعة في ظل هذه الظروف تجعل منفذيها غالبا ما يفلتون من العقاب في ظل غياب الدليل المادي للجريمة، إضافة إلى نقص المنظومة التشريعية على المستوى الوطني في تحديد الفعل وتكييفه حسب العقوبة المناسبة له، الأمر الذي انعكس سلبا على المستوى الدولي.

وعلى خلفية ما تم إدراجه من نتائج نقترح بعض الإقتراحات التي تتمحور حول عدة نقاط أهمها :

- ضرورة عقد إتفاقية دولية موحدة تحت مظلة الأمم المتحدة تختص بمكافحة الجريمة الالكترونية ، وتستجيب باحتواء جميع التهديدات والمخاطر الناجمة عن إرتكابها ، ووضع إستراتيجية لمكافحتها ومنع حدوثها .
- عقد مؤتمر دولي لتحديد الأعمال والتصرفات التي تعد ضمن أنماط وصور الجرائم الإلكترونية خاصة في ظل التطورات التي يشهدها العالم في مجال التقنيات الجديدة.

– الحث على تعزيز مبدأ التعاون الدولي كضرورة حتمية تفرضها الخطورة الإجرامية في ظل الوسائل التقنية المتطورة، كما تفرضه العلاقات الدولية المتطورة التي تقوم على إعتبار التعاون الدولي في إقرار السلم والأمن الدوليين.

– تفعيل الأليات القضائية والأمنية المتاحة بين الدول والبحث عن أرضية عالمية مشتركة بشأن تبادل الخبرات والمعلومات حول تحرك مرتكبي الجرائم الالكترونية على المستوى العالمي و الإقليمي، مثل ألية الأنتربول والأفريبول

– ضرورة التأكيد على محاربة الجريمة الإلكترونية من خلال الإتفاقيات والمعاهدات الدولية مع تكييف التشريعات والقوانين الداخلية لتتماشى وروح هذه الاتفاقيات، خاصة في مجال القانون الدولي الجنائي حتى يتسنى تعميم القانون على الجرائم الالكترونية بِغض النظر عن مكان وقوعها وجنسية الجاني .

ـ امكانية أن يشمل القوانين الجنائية أساليب التكنولوجيا الجديدة في الفضاء السيبراني ذات القصد الإجرامي وهو ما قد تضمنته قوانين مقارنة إحتوت هذه التصرفات الغير مشروعة .

قائمة المراجع والمصادر:

أولا ــ اللغة العربية:

أ-الكتب:

1.خالد ممدوح إبراهيم، امن الجريمة الالكترونية ،الدار الجامعية، الإسكندرية، دون طبعة ، مصر، 2010

2.عبد الإله النوايسية، جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية في قانون الجرائم الالكترونية، دار وائل للطباعة والنشر والتوزيع ، الأردن،2017

-محمد علي محمد، كوارث الإرهاب الالكتروني بين الفلسفة القانونية و تطور الأمن التقني، دار النهضة العربية، مصر، الطبعة الأولى، 2018

3.محمود أحمد القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، الأردن، 2017

4.مصطفى محمد موسى، الإرهاب الإلكتروني ، دراسة قانونية أمنية نفسية إجتماعية ، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، دار الكتب و الوثائق القومية المصرية، 2009

5.لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دار الحامد للنشر و التوزيع، الأردن، 2015

6.نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية "دراسة في أبعاد الأمن الإلكتروني"، المكتب العربي للمعارف، مصر، 2016

7.هلالي عبد اللاه أحمد، جرائم الحاسب والانترنت بين التجريم الجنائي وآليات المواجهة ، دار النهضة العربية، القاهرة ، 2015

2 ــ الرسائل الجامعية :

- **أحمد رجدال** ، القانون الدولي في مواجهة تطورات جرائم الإرهاب الدولي (من الطابع التقليدي إلى الفضاء الالكتروني)، رسالة دكتوراه ، جامعة أمحمد بوقرة بومرداس، كلية الحقوق، 2023

- **هروال هبة نبيلة**، جرائم الإنترنت(دراسة مقارنة)، أطروحة دكتوراه، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم والسياسية، 2013

3- المقالات:

-أحمد رجدال، أمال يوسفي، التصدي للتقنيات الحديثة في تمويل الارهاب الدولي، الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 13، العدد02، 2021، ص ص 264-279

- أمال بيدي، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية ، مجلة البحوث في الحقوق والعلوم السياسية، المجلد08، العدد01، 2022، ص ص 299 ـ 316

ـ بوفاتح محمد بلقاسم، الجريمة الإلكترونية، دراسة سوسيو قانونية، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، العدد 03، 2009، ص ص 52ـ 66

ـ ساحي فوزية، بوكابوس عبد القادر، ظاهرة الجريمة المفهوم الأسباب والأشكال، مجلة أبحاث، المجلد07، العدد01، 2022،ص ص 82- 96

ـ سعيد عبيدي ،الإرهاب الإلكتروني ، مجلة العلوم الإنسانية، الجزائر، العدد 02، ص ص 32 43، 2017

ـ سليم سولاف، علاقة الجريمة المنظمة بشبكة الإنترنت، مجلة البحوث والدراسات القانونية والسياسية، المجلد 08، العدد01 ، 2019، ص ص 186 ـ204

ـ شعنبي صابرة، الإرهاب الإلكتروني الأشكال والدوافع، مجلة العلوم الاجتماعية والإنسانية ، جامعة المسيلة ، العدد العاشر،2017، ص ص 435 ـ 448

– شهيرة بولحية، دنيا راد سويح، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية ، المجلد 02 ، العدد 02، ص ص37ـ46

– عدي جابر هادي، الحماية الجزائية للبريد الالكتروني (دراسة مقارنة)، مجلة رسالة الحقوق، العدد الثالث، 2010، ص ص 154-179

– فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، جامعة محمد خيدر ببسكرة، العدد 02، 2015 ، ص ص 07 ـ 21

– كردي نبيلة ، الإتجار بالبشر عبر الإنترنت، مجلة أبحاث، المجلد 07 ، العدد 02، 2022 ، ص ص 521 ـ 523

– مراد مشوش، الجهود الدولية لمكافحة الاجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، العدد2، 2019، ص ص 703ـ726

ـ نصير لعرباوي، فاتح النور رحماني، الجريمة الإرهابية الإلكترونية ، مجلة المعيار، العدد43، 2018، ص ص 376ـ386

– وردة شرف الدين، الأحكام الاجرائية لمكافحة جريمة الإتجار بالبشر المرتكبة بواسطة تقنية المعلومات ـ دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010 ـ ، مجلة الاجتهاد القضائي،جامعة محمد خيدر بسكرة، الجزائر، العدد السادس عشر، مارس 2018، ص ص 93 ـ 118

– وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي، جامعة مستغانم، الجزائر، المجلد7، العدد 02،2019

– يحياوي محمد، مخاطر القرصنة المعلوماتية على الحكومة الالكترونية، Revue de Recherches et Etudes Scientifiques، المجلد 05، العدد 01، 2011، ص ص 257-285، ص 265

4 ـ المداخلات وأوراق العمل العلمية المقدمة في المؤتمرات :

– أخام بن عودة زواوي مليكة، تحديات ظاهرة الجريمة المنظمة العابرة للأوطان والثورة المعلوماتية، ورقة عمل مقدمة في المؤتمر المغاربي الأول حول المعلوماتية والقانون، تحت إشراف: أكاديمية الدراسات العليا، طرابلس، ليبيا ، 27-30 أكتوبر 2009، منشورة عبر الرابط :

https://www.researchgate.net/publication/328064682_aljraym_alalktrwnyt_almfhwm_walasbab

– ذياب موسى البداينية، الجرائم الالكترونية: المفهوم والاسباب، ورقة مقدمة في الملتقى العلمي" الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية و الدولية"،المنعقد خلال الفترة من 02الى 04 سبتمبر 2014، تحت اشراف كلية العلوم الاستراتيجية ، عمان، الاردن، 2014، تم الاطلاع عليه بتاريخ 2024/05/19 عبر الرابط الالكتروني المتاح :

https://www.researchgate.net/profile/Diab-Al Badayneh/publication/328064682_aljraym

5 ـ وثائق الجمعية العامة للأمم المتحدة:

– إعلان الجمعية العامة في الدورة 70/53 في 4 ديسمبر 1998، متاح على الرابط التالي:
https://www.insdip.com/ar/53o-periodo-de-sesiones-1998-1999-agnu/

– إعلان الجمعية العامة في الدورة 49/54 في ديسمبر 1999 ،رقم الوثيقة A / RES /54 / 49

– إعلان الجمعية العامة في الدورة 28/55 في20 ديسمبر 2000، بعنوان "التطور في مجال المعلومات والاتصالات"، الوثيقة رقم A/RES/55/28

تم الاطلاع على اعلانات الدورة 54و55 عبر الرابط الالكتروني التالي:
https://www.insdip.com/ar/54o-periodo-de-sesiones-1999-2000-agnu/

– إعلان الجمعية العامة في الدورة 19/56 في ديسمبر2001، متاح في الرابط الالكتروني :

https://documents-dds ny.un.org/doc/undoc/gen/n01/476/26/pdf/n0147626.pdf?openelement

– إعلان الجمعية العامة في الدورة 239/57 في 20 من ديسمبر 2002 بشأن " إنشاء ثقافة عالمية للأمن السيبراني" متاح في الرابط :

https://digitallibrary.un.org/record/482184?ln=zh_CN

– إعلان الجمعية العامة في الدورة 199/58 في 23 من ديسمبر 2003، الرابط:

https://www.insdip.com/ar/58o-periodo-de-sesiones-2003-2004-agnu/

– تقرير الجمعية العامة للأمم المتحدة الصادر عن لجنة إستخدام الفضاء الخارجي في الأغراض السلمية في دورتها الثانية والستون ، بتاريخ 21 جوان 2019، الوثيقة رقم A/74/20، متاح عبر الرابط:

https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420_0_html/V1906075.pdf

6 ـ مؤتمرات الامم المتحدة:

– مؤتمر الأمم المتحدة **الثامن** لمنع الجريمة ومعاملة المجرمين، الذي جاء بعنوان"منع الجريمة والعدالة الجنائية على الصعيد الدولي في القرن الـ21"، المنعقد خلال الفترة ما بين 27 اوت الى 07 سبتمبر ، 1990 هافانا بكوبا ، تم الاطلاع عليه بتاريخ 2024/05/25، الساعة 13:00 على الرابط :
https://www.unodc.org/congress/ar/previous-congresses.html#:~:text=

– المؤتمر العاشر بشان الجريمة والعدالة الصادر عن الامم المتحدة لمنع الجريمة و معاملة المجرمين، المنعقد في فيينا من 10 الى 17 افريل ، بعنوان " مواجهة تحديات القرن الحادي و العشرين 2000"، تم الاطلاع عليه بتاريخ 2024/05/25 ، متاح على الرابط:
https://www.unodc.org/congress/en/previous/previous-10.html

– التقرير التفسيري لاتفاقية الجريمة الالكترونية 2001 ، المجلس الاوروبي، سلسلة المعاهدات الاوروبية 185، النسخة المترجمة بالعربية ، تم الاطلاع عليه بتاريخ 2024/05/22 على الرابط :
https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174

– المؤتمر الثاني عشر الصادر عن الأمم المتحدة لمنع الجريمة والعدالة الجنائية، بعنوان " الاستراتيجيات الشاملة لمواجهة التحديات العالمية، " نُظم العدالة الجنائية ومنع الجريمة وتطورها في عالم متغير"بالبرازيل أيام 12إلى19 أفريل 2010 ، تم الاطلاع عليه بتاريخ 2024/05/25 ، متاح على الرابط:
https://www.unodc.org/congress/en/previous/previous-12.html

-. مؤتمر الأمم **المتحدة الثالث عشر** لمنع الجريمة والعدالة الجنائية خلال الفترة من (12 ـ 19) أفريل 2015، مركز قطر الوطني للمؤتمرات، الدوحة، قطر، تم الاطلاع بتاريخ 2024/05/25، الساعة 21سا ،رابط الاطلاع على مخرجات المؤتمر :
https://www.unodc.org/congress/en/previous/previous-13.html

– تقرير الخبراء الحكومي الدولي المفتوح العضوية بشأن اجراء دراسة شاملة لمشكلة الجريمة السيبرانية 2011، تم الاطلاع على الموقع الالكتروني بتاريخ 2024/05/26 عبر الرابط:
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/V1701247_A.pdf

7 – المعاهدات والاتفاقيات :

– معاهدة بودابست لمكافحة جرائم الإنترنت 2001

– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في ديسمبر 2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، الجريدة الرسمية للجمهورية الجزائرية العدد 57 بتاريخ 4 ذو الحجة عام 1435هـ الموافق لـ 28 سبتمبر 2014

ثانيا ــ مراجع اللغة الاجنبية:

- BRIGITTE Pereira , La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité , Revue Internationale de Droit Economique, R.I.D.E, 2016/3, pages 387 à 409
- PAUL De Hert, GLORIA González Fuster, BERT-Jaap Koops, Fighting cybercrime in the two Europes, The added value of the EU framework decision and the council of Europe Convention, Revue International de Droit Pénal , RIDP, 2006, vol. 77, pp 503 à 524
-JEAN-François Thony , Money laundering and terrorism financing: an overview, pp 01-20, p 03, consulté le /05/ 202020, available sur le site web https://www.imf org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf

1

1