مجلة التراث

J-ALT

2018/ Vol:8 N°01

Available online at http://www.asjp.cerist.dz

الإرهاب الإلكتروني و انعكاساته على الأمن الإجتماعي

- دراسة تحليلية-

الأستاذة صباح كزيز جامعة محمد خيضر بسكرة

والأستاذة أمال كزيز جامعة قاصدي مرباح ورقلة

ملخص:

يعالج هذا الموضوع ظاهرة الإرهاب الإلكتروني، إذ تعد هذه الظاهرة المتزايدة في العالم إحدى القضايا الرئيسية للمجتمع الدولي، حيث أثبت الواقع العملي أن الدولة لا تستطيع بجهودها المنفردة القضاء على هذه الجرائم المستحدثة مع هذا التطور المذهل في كافة ميادين في الاتصالات وتكنولوجيا المعلومات، خاصة وأن الجرائم السيبرانية تتميز بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي.

الكلمات المفتاحية: الإرهاب الإلكتروني، الجهود الدولية، الجهود الإقليمية، الأمن المعلوماتي، استراتيجية مواجهة الإرهاب الإلكتروني.

Abstract:

This topic deals with the phenomenon of cyber terrorism, as this growing in the world phenomenon is one of the key issues for the international community, where the practice has proved that the state can not single elimination efforts on these novel crimes with this stunning development in all fields in the telecommunications and information technology, especially since the crimes cyber characterized by being universal, cross-border, the control can not be achieved only if there is international cooperation.

مقدمة:

بالنظر للإنتشار الواسع و المتسارع للتقنية العالية المتمثلة في الأنظمة المعلوماتية، و التطور الهائل في علم البرمجيات و تزايد الإعتماد على الحاسبات الآلية و شبكة الإنترنت إلى ظهور جملة من الجرائم تعددت صورها و أشكالها أطلق عليها "الجرائم السيبرانية"، التي تعتبر من أخطر التحديات التي تواجه المعاملات الإلكترونية التي ألغت جميع الفواصل بين الدول، لتكون وسيلة مثالية لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية لتتغير الجريمة من صورتها التقليدية المادية إلى أخرى معنوية عابرة للدول و القارات. أصبحت الجرائم الإلكترونية تشكل خطرا كبيرا دول العالم، وذلك بعد أن استطاع "الإنترنت" اختراق جميع الحواجز والقيود التي تُسيطر على المجتمعات ، ومن منطلق هذه المخاطر الإلكترونية التي يأتي في مُقدمتها ما يُعرف بـ الإرهاب الإلكتروني – **CyberTerrorism**، ما تطلب تضافر الجهود الدولية بغرض التصدي ومواجهة هذه الظاهرة العابرة للحدود التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية، وخاصة أن الإجرام المعاصر يثير الكثير من الإشكاليات والتحديات من نواحي عديدة أهمها صعوبة اكتشاف هذه الجرائم وإثباتها.

تكمن أهمية هذه الدراسة في تناولها لظاهرة مستحدثة وهى ظاهرة جرائم التطور التكنولوجي وخاصة السيبرانية منها، فالتطور التكنولوجي على الرغم من آثاره الإيجابية إلا أن له العديد من السلبيات التي تهدد أمن واستقرار المجتمعات ،حيث ترتكز هذه الدراسة أساسا على تحليل ظاهرة الإرهاب الإلكتروني، هذه ظاهرة المتزايدة في العالم إحدى القضايا الرئيسية للمجتمع الدولي، حيث أثبت الواقع العملي أن الدولة – أي دولة – لا تستطيع بجهودها المنفردة القضاء على هذه الجرائم المستحدثة مع هذا التطور الملموس والمذهل في كافة ميادين في الاتصالات وتكنولوجيا المعلومات، خاصة وأن الإرهاب الإلكتروني والجرائم السيبرانية كلل تتميز بالعالمية لكونها عابرة للحدود فإن التصدي لها ومواجهتها لا تتحقق إلا بتظافر الجهود الدولية .

وتهدف هذه المداخلة إلى التعرف على ظاهرة الإرهاب الإلكتروني وكيفية معالجته بتفعيل الجهود الدولية وأهميتها في مجال مكافحة الجرائم المتعلقة بالإنترنت مع بيان للصعوبات التي قد تواجه هذا التعاون وذلك لما تشكله هذه الظاهرة من إشكالات أمنية وقانونية واقتصادية و اجتماعية معقدة، على هذا الأساس تتحدد إشكالية المداخلة في:

كيف يمكن تفعيل الجهود الدولية في مجال مكافحة الإرهاب الإلكتروني ؟

وتنطلق الدراسة من فرضية أساسية:

يتحدد نجاح مكافحة الإرهاب الإلكتروني بحجم تفعيل آليات التعاون الدولي في المجال القانوني والأمني.

تم تناول الدراسة وفق ثلاث محاور أساسية:

المحور الأول/ الإرهاب الإلكتروني (مفهومه ومخاطره)

المحور الثاني/ جهود المنظمات الدولية في مكافحة الإرهاب الإلكتروني

المحور الثاني/ الجهود الإقليمية في التصدي للإرهاب الالكتروني

المحور الثالث/ الصعوبات العملية في مواجهة الإرهاب الإلكتروني و وفرص التغلب عليه

المحور الأول : الإرهاب الإلكتروني (مفهومه و مخاطره)

أولا– مفهوم الإرهاب الإلكتروني:

كلمة إرهاب في اللغة مصدر للفعل أرهب يرهب، بمعني:[1]

أخاف وأفزع وكذلك يستعمل الفعل تَرَهَّبَ بمعنى توعد إذا كان متعديا فيقال تَرَهَّبَ فلانا : أي توعده. وكذلك تستعمل اللغة العربية صيغة استفعل من نفس المادة فنقول استرهب فلاناً أي رَهَّبَهُ. واسترهبه :أي استدعى رهبته حتى رهبه الناس وقال ابن الأثير: هي الحالة التي تُرهِب أي تُفزِع وتُخوِف. وبذلك كلمة الرهبة في اللغة العربية تعني الخوف[2]، والإرهاب هو الإزعاج والإخافة . والإرهاب يعني في اللغات الأجنبية القديمة مثل اليونانية: حركة من الجسد تفزع الآخرين.[3]

ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب، ولا يختلف الإرهاب الإلكتروني عن الإرهاب العام إلا في نوعية الأداة المستخدمة لتحقيق الغرض الإرهابي. وقد عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م الإرهاب بأنه:" الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة".

أما **الإرهاب الإلكتروني**: يعتمد الإرهاب الإلكتروني على استخدام إمكانيات أو مقدرات الحاسب الآلي في ترويع أو إكراه الآخرين، وعلى سبيل المثال الدخول بصورة غير مشروعة إلى نظام الكمبيوتر في أحد المستشفيات بغرض تغيير مقادير ومكونات وصفة طبية لمريض ما لتكون جرعة قاتلة تؤدي إلى وفاة المريض على سبيل الانتقام. وهذا الدخول غير الشرعي يمثل حالة مستحدثة للإرهاب الإلكتروني والتي أصبحت تهدد النظام العلمي المعاصر في القرن الحادي والعشرين. ويُعد الإرهاب الإلكتروني نمطاً جديداً من الحروب التي لا تعتمد على استخدام الأسلحة والمتفجرات وينطوي على استخدام أو استغلال المجرمين لعدم حماية أو قابلية الأنظمة المدنية والعسكرية للمخاطر على النحو الذي يؤدي إلى التأثير على الأمن الوطني والعالمي، لذلك فيشهد مستقبل الإرهاب في القرن الحالي أسوء أنواع الإرهاب الإلكتروني[4].

وبالتالي يمكن تعريف للإرهاب الالكتروني بأنه العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد .

والإرهاب الإلكتروني هو أحد الاستخدامات غير سلمية للفضاء الإلكتروني، وهو نتيجة لتفاعل العالم المادي مع العالم الافتراضي، وكانت بداية استخدام كلمة "**cyber terrorism**" في دراسة ل(بارى كولن) و الذى توصل فيها إلى أنه من الصعب الوصول إلى تعريف محدد لظاهرة الإرهاب الإلكتروني، وهذا المفهوم يشير إلى استخدام الفضاء الإلكتروني كأداة لإلحاق الضرر بالبنية التحتية سواء كانت" طاقة– مواصلات– خدمات حكومية" أي يشير إلى الهجمات التي يستخدم فيها الكمبيوتر ضد الاقتصاد والحكومات. أهداف الإرهاب الإلكتروني تكون غالباً أهداف سياسية وقد يأتي الإرهاب الإلكتروني في صورة: تدمير نظم المعلومات لدى الخصم و افقاده القدرة على الحصول على المعلومات، شل قدرته على التواصل مع

---

[1] عبدالله بن مطلق بن عبدالله المطلق، **الإرهاب وأحكامه في الفقه الإسلامي**، دار ابن الجوزي، الرياض، 1431هـ، ص ص 115- 117

[2] –أحمد هلال الدين، **الإرهاب والعنف السياسي**، دار الحرية،القاهرة، 1989، ص 22. [2] –

[3] –عبد الرحيم صدق، **الإرهاب السياسي والقانون الجنائي**، دار النهضة العربية، 1985القاهرة،، ص81.

[4] – أحمد فلاح العموش، **مستقبل الإرهاب في هذا القرن**، جامعة نايف العربية للعلوم الأمنية،الرياض، 2006،ص 89

أعضائه عن طريق تدمير مواقعه الإلكترونية، إختراق شبكات المعلومات الرسمية للوزارات والحكومات بغرض تدميرها أو الحصول على معلومات سرية .

ثانيا– مخاطر الإرهاب الإلكتروني:

ظهر الارتباط بين الانترنت و الارهاب بشكل واضح بعد أحداث 11 سبتمبر، وانتقلت المواجهة مع الإرهابيين من المواجهة المادية المباشرة إلى المواجهة الإلكترونية وأصبحنا نعيش الحرب الرقمية (الالكترونية) هناك حرب تكنولوجية بين المجرمين وصناعة الأمن، فالمجرمون يسعون بشكل دائم نحو التغلب على التقدم التكنولوجي في وسائل مكافحة الجريمة [1]، كما أن تأثير الوسائل التكنولوجية التي تستخدم لحماية البنوك والمساكن وغيرها لمواجهة المنظمات الإجرامية قد يحد من نشاط تلك المنظمات، إلا أن هذا التأثير يكون لفترة قد تطول أو تقصر، ويتوقف البعد الزمني لفاعليتها على مدى قدرة المنظمات الإجرامية على استخدام الوسائل التكنولوجية المضادة[2]. كما أن التطور في مجال تكنولوجيا الأسلحة أدى إلى استخدام الأسلحة الكاتمة للصوت في جرائم القتل، واستخدام الأسلحة سريعة الطلقات في جرائم مقاومة السلطات وجرائم الحرب عن بعد. كما أن السيارات أصبحت محلا لبعض الجرائم، حيث تقع على السيارات جريمة السرقة إما بقصد الحصول على المال بواسطة عصابات سرقة السيارات وإما بقصد الرغبة في الظهور بواسطة عصابات الأحداث، وإما بقصد تفجيرها في عمليات إرهابية بواسطة الجماعات الإرهابية[3]، وتكمن خطورة الإرهاب الإلكتروني بشكل كبير في الدول المتقدمة والتي تعتمد على الحواسب الآلية والشبكات المعلوماتية في إدارة بنيتها التحتية، وبالتالي قدرة الجماعات الإرهابية على تدمير البنى المعلوماتية وأحداث أضرار فائقة.

وتتمثل هذه الأضرار على سبيل المثال في: شل أنظمة القيادة والسيطرة والاتصالات، قطع شبكة الاتصال بين الوحدات والقيادات المركزية، تعطيل أنظمة الدفاع الجوي، التحكم في خطوط الملاحة الجوية والبحرية والخطوط البرية، اختراق النظام المصرفي وإلحاق الأضرار بأعمال البنوك وأسواق المال العالمية، ويتم استخدام تقنية المعلومات لإصابة المرافق الحيوية ومن ثم فان الأهداف التي تتعرض للتهديد: تخزين المعلومات، عمليات ادخال المعلومات، إرسال وإستقبال الرسائل، استهداف البنية التحتية للمعلومات وخاصة في قطاعات الكهرباء والاتصالات والكمبيوتر والتي تعد وبحق ركائز الأمن القومي الجديد .

وقد أدى الفضاء الإلكتروني إلى تحول الإرهاب الى تهديد عالمي، وأصبح الإرهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتصاعد نشاط الجماعات الإرهابية عبر الفضاء الإلكتروني وتعزيز بعدها العالمي وتم استخدام المنجزات التكنولوجية في ممارسة الإرهاب، والتي استطاع الإرهابيون من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض[4].

استغلت الجماعات الإرهابية بكافة أشكالها وأنماطها الفكرية المزايا الإلكترونية كعنصر حيوي لدعم وتحقيق أهدافها، وتحولت بعد أن كانت مجموعات قلائل من الأفراد موزعة جغرافياً إلى مجتمع افتراضي غير محدد الأبعاد الكمية وكان ذلك له

[1]Mann, David & Sutton, Mike, **Net crime**, Brit. J. criminal, Vol., 38, No. 2, Spring 1998, p. 220.

[2]– السيد عوض، **الجريمة في مجتمع متغير**، المكتبة المصرية، 2004الاسكندرية، ص ص 201– 202

[3]ربيع حسن؛ سيد رفاعي، **مبادئ علمي الإجرام والعقاب**، المؤسسة الفنية للطباعة والنشر،القاهرة، 2001، ص ص191–

[4]– ربيع حسن؛ سيد رفاعي، **مبادئ علمي الإجرام والعقاب**، المؤسسة الفنية للطباعة والنشر، 2001القاهرة، ص ص191– 194

دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات، و الارهاب هو سلاح الضعيف غير القادر على شن حرب ضد الدولة، ومن ثم يلجأ إلى الإرهاب في محاولة منه إلى إلحاق الأذى بالقوة العظمى وهزيمتها، ويمثل الإرهاب وسيلة لتأكيد الهوية وجذب الانتباه.

يمثل الإرهاب ظاهرة دائمة التغير، وبالتالي وسائل الإرهاب في تغير مستمر لتتواكب مع التطورات التكنولوجية وتصبح قادرة على تحقيق أهدافها، لقد ظهر التزاوج بين الإرهاب والانترنت بشكل أكثر وضوحاً بعد أحداث 11 سبتمبر، ولكنه منذ عام 1999 كانت كل الجماعات الإرهابية حاضرة على الانترنت بشكل كبير وبعد عام 2001 كان هناك أكثر من 5 ألاف موقع إلكتروني وغرف محادثة الكترونية تابعة للجماعات الإرهابية وتستخدمها للتأثير على الرأي العام من خلال معركتها الفكرية، أو استخدامها للقيام بأعمال إرهابية مادية عن طريق جمع المعلومات والتنسيق والتنظيم. وللإرهاب الإلكتروني عدد من الأهداف منها:[1]

زعزعة الأمن ونشر الخوف والرعب وإخلال نظام الدول العام.

تهديد وابتزاز الأشخاص والسلطات العامة والمنظمات الدولية.

السطو وجمع الأموال .

جذب الانتباه، والدعاية والإعلان

المحور الثاني/ جهود المنظمات الدولية في مكافحة الجريمة الإلكترونية

أدركت الدول والمنظمات الدولية أهمية التعاون الدولي وأحست بأنه أمر محتّمٌ لتجاوز تحديات الجرائم الإلكترونية، فعمدت الكثير منها إلى عقد اتفاقيات لتسهيل مهمة التحقيق في هذه جرائم الكمبيوتر والأرهاب الإلكتروني[2]

أولا– جهود منظمة الأمم المتحدة:

في إطار الجهد المبذول فإن هناك العديد من الهيئات الدولية التي تلعب دورا ملحوظا في هذا المجال على رأسها منظمة الأمم المتحدة التي بذلت جهودا لا يستهان بها، مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشار الجريمة المعلوماتية والإرهاب الإلتكروني، و هذا من خلال مؤتمراتها لمنع الجريمة و معاملة المجرمين بدءا بالمؤتمر السابع عام 1985 إلى غاية المؤتمر الثاني عشر عام 2010. إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات و ذلك تحت إشراف الأمم المتحدة عام 1994، الذي نتج عنه عدة توصيات و قرارات ذات صلة بالجرائم المعلوماتية، و قد تضمنت شقين اثنين واحد موضوعي يتناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، و ثاني إجرائي يتضمن الإجراءات الواجب إتباعها لتطبيق القواعد الموضوعية.

وفيما يخص مؤتمرات الأمم المتحدة في هذا المجال نجد المؤتمر السابع المنعقد **بميلانو عام1985** الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلي وإعداد تقرير يعرضه على المؤتمر الثامن،

[1]– خلف إدريس الحبابسه، الإرهاب الإلكتروني،2016/10/10، متوفر على الرابط الإلكتروني:
http://www.lawjo.net/vb/showthread.php?38805

[2]محمد الأمين البشري، "**التحقيق في جرائم الحاسب الآلي**"، ورقة بحثية ضمن ملتقى علمي حول: القانون والكمبيوتر والإنترنت بكلية *الشريعة والقانون*،الإمارات ، أيام 1 – 3 مايو 2000، ص1078.

وقد عقد هذا الأخير في **هافانا عام 1990** وقد خرج بالعديد من التوصيات أهمها التأكيد على ضرورة الاستفادة من التطورات العلمية والتكنولوجية في مواجهة الجريمة الالكترونية.

أشار إلى مسألة الخصوصية واختراقها بالإطلاع على البيانات الشخصية المخزنة داخل النظام المعلوماتي.

كما أكد على ضرورة تحديث القوانين التي تتناول هذه الجرائم وتحسين تدابير الأمن والوقاية المتعلقة بها

تدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة فيها، وكذا التعاون مع المنظمات المهتمة بهذا الموضوع.

كما عقد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في القاهرة **عام 1995** والذي أوصى بوجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة، كما أوصى كذلك المؤتمر العاشر المنعقد في بودابست عام 2000 بوجوب العمل الجاد من أجل الحد من جرائم تقنية المعلومات المتزايدة والتي اعتبرت نمطا من الجرائم المستحدثة والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة.

بالإضافة إلى مؤتمرات الأمم المتحدة نذكر في هذا المجال المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي **عقد في ريو دي جانيرو عام 1994** وقد خرج بالعديد من التوصيات منها:

وضع قائمة بالحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل الجرائم المعلوماتية

وجوب تحديد الجهات التي تقوم بإجراء التفتيش والضبط، وضرورة وضع القواعد المتعلقة بالإثبات الإلكتروني ومصداقية الأدلة

ثانيا– جهود المنظمة العالمية للملكية الفكرية:

تلعب الوكالات والمنظمات العالمية العاملة تحت لواء الأمم المتحدة دورا في هذا المجال ومن ذلك **المنظمة العالمية للملكية الفكرية (WIPO)** هذه الأخيرة شكلت مجموعة عمل تضم عددا كبيرا من الخبراء بهدف دراسة الأساليب المناسبة لحماية برامج الحاسب الآلي من خلال إخضاعها لقوانين حماية حق المؤلف.[1] ويظهر الدور البارز للمنظمة العالمية للملكية الفكرية في هذا المجال أيضا، من خلال خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الآلي و هذا من خلال المادة 04 و 05 من إتفاقية تريبس.

ثالثا– الإتحاد الدولي للاتصالات:

هناك جهد كبير مبذول من قبل **الاتحاد الدولي للاتصالات** في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبل الأمين العام للإتحاد عام 2007، و الذي يرمي إلى تحقيق عدة أهداف أبرزها استحداث تشريع نموذجي لمكافحة الجريمة المعلوماتية يمكن تطبيقه عالميا ويكون قابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني و الإقليمي.

رابعا– جهود منظمة الشرطة الجنائية الدولية (الانتربول):

يبرز دور الانتربول – المنظمة الشرطية – في العالم دوراً كبيراً في مكافحة الجرائم الالكترونية بما فيها الإرهاب الإلكتروني والتي يعتبرها أحد مجالات الإجرام الأسرع نموا نظراً للتسهيلات والسرعة التي تقدمها التقنيات الحديثة وخصائصها مميزات

[1]– نعيم سعداني المرجع السابق، ص125.

الطابع العالمي للإنترنت في إخفاء الهوية الأمر لمرتكبيها الذي يساعد على تزايد الأنشطة الإجرامية . ولقد مرت جهود المنظمة في هذا المجال بمراحل عديدة ، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، بيونس أيرس لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك. وفي هذا السياق أكد الأمين العام لمنظمة الشرطة الجنائية الدولية (الانتربول) رونالد نوبل أن الجهود المبذولة عالمياً لمكافحة الجرائم الالكترونية، وتعزيز الأمن الالكتروني بحاجة إلى تطبيق قانوني وإلى العمل المباشر مع شركات القطاع الخاص التي تعمل في مجال أمن الإنترنيت، بالإضافة إلى تنسيق القوانين والأحكام حول هذا الشأن في مختلف البلدان العالم.[1]

على مستوى الجهود الدولية أيضا صدر في عام2000 مسودة اتفاق عالمي حول الجريمة والإرهاب الإلكتروني من جامعة "ستاندفورد " فيما عرف بخطة ستاندفورد وشملت تلك الخطة العديد من النقاط حول هدف الوصول إلى تعاون دولي أوسع في مقاومة هجمات الفضاء الإلكتروني، وذلك على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين، وخاصة مع التطور المستمر في التكنولوجيا وجمود الأطر القانونية الحالية في مواجهة الأخطار والهجمات، وفي المادة 12 من تلك الخطة اقتراح بإقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات.[2]

وبعد أحداث 11 سبتمبر2001 طلب من مكتب الأمم المتحدة للمخدرات والجريمة في فيينا وضع ارشادات للدول عند تشريع وتطبيق وسائل محاربة الإرهاب .وتنفيذاً لذلك وضع المكتب سنة 2006 قائمة بالإرشادات تضمنت أربعة أقسام :الأول في الأعمال المجرمة، والثاني في الوسائل التي تضمن التجريم الفعال، والثالث في القانون الإجرائي، والرابع في وسائل التعاون الدولي في المسائل الجنائية، ووضع المكتب في نهاية الإرشادات مشروع قانون ضد الإرهاب

المحور الثالث: الجهود الاقليمية في التصدي للإرهاب الإلكتروني

أولا– جهود الاتحاد الأوربي

لعب المجلس الأوروبي دورا مهما في محاولة الحد من الجرائم الالكترونية والإرهاب الإلكتروني، من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الإستخدام وحماية تدفق المعلومات، وفي 28/ 1981/01 تم توقيع اتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية. وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية .وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد اتفاقية في هذا الإطار.[3]

وقد أثمرت جهود الإتحاد عن ميلاد أولى المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية والإرهاب الإلكتروني بالعاصمة المجرية بودابست عام 2001، و قد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم

---

[1]-Malcom Anderson , Policing the world: Interpol the Politics of International Police Co – Operation , Clarendon press, Oxford, 1989, p. 168-185.

[2] رائد العدوان،" المعالجة الدولية لقضايا الإرهاب الإلكتروني"، 2016/12/12، متوفر على الرابط الإلكتروني:
http://repository.nauss.edu.sa/bitstream/hand

[3] – سعيداني نعيم، مرجع سابق، ص85.

المعلوماتية في جميع أنحاء العالم من خلال تنسيق و انسجام التشريعات الوطنية ببعضها البعض، و تعزيز قدرات القضاء و كذا تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات الجرائم المعلوماتية في إطار القوانين المحلية. ما قام به المجلس في هذا المجال هو إشرافه على اتفاقية بودابست الموقعة ورغم أن هذه الاتفاقية هي في الأصل أوروبية الميلاد إلا أنها دولية الطابع تظهره من بعد حقيقي عن الإهتمام الدولي بهذه النوعية من الجرائم، حيث أعدّ مجلس أوروبا هذه الاتفاقية بالتعاون مع كندا واليابان وجمهورية جنوب إفريقيا والولايات المتحدة الأميركية وعرضت للتوقيع في بودابست في 2001/11/23 ودخلت حيّز التنفيذ في 2004/07/01 ، تهدف الاتفاقية إلى إرساء نظام سريع وفعّال للتعاون الدولي. و بالتالي فهي تتضمّن الاتفاقية أحكاماً تهدف إلى استحداث هكذا إطار في سبيل تعاون دولي سريع وموثوق وتطلب من الدول الأطراف مدّ بعضها البعض بمختلف أشكال التعاون.[1]

وقد بينت المذكرة التفسيرية لهذه الاتفاقية أن تحديد الجرائم الالكترونية فيها هدفه تحسين وإصلاح وسائل منع وقمع الجريمة المعلوماتي، من خلال تحديد معيار بالحد الأدنى المشترك ، الذي يسمح باعتبار بعض التصرفات من قبيل الجرائم المعلوماتية ، وأنه بالإمكان أن يتم استكمال هذه القائمة في القوانين الداخلية ، كما أنه يأخذ في الاعتبار الممارسات غير المشروعة الأكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد، وقد حددت الاتفاقية (اتفاقية بودابست) الجرائم الالكترونية وصنفتها في خمسة عناوين في القسم الأول من الاتفاقية.

العنوان الأول: ويضم جوهر جرائم الحاسب أو الجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات والنظم.

العنوان الثاني: ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، و تضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.

العنوان الثالث: ويشمل الانتهاكات والجرائم المرتبطة بالمحتوي، وهي التي تخص الإنتاج والنشر غير المشروع ، في المادة التاسعة من الاتفاقية.

العنوان الرابع: ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة العاشرة من الاتفاقية.

العنوان الخامس: وهو يشتمل على أحكام إضافية بخصوص الشروع والاشتراك وأيضا الجزاءات والإجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوي.[2]

كما أنشأ الإتحاد الأوروبي أجهزة تساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوروبول و المركز الأوروبي لمكافحة الجريمة المعلوماتية والإرهاب الإلكتروني و الذي أفتتح في جانفي 2013.

[1] – كريستينا سكولمان،" **الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية**"، ورقة بحثية مقدمة ضمن الندوة الإقليمية: الجرائم المتصلة بالكمبيوتر، المغرب، 2007، ص ص 119. 120.

[2] نورة طرشي، "**مكافحة الجريمة المعلوماتية**"، مذكرة ماجستير في القانون الجنائي، (كلية الحقوق، جامعة الجزائر، 2012)، ص 67.

وفي إشارة لجهود الدول الغربية نذكر:

تعتبر **السويد** أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها.

تبعت **الولايات المتحدة الأمريكية** السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانونا تشريعاً يحمل الرقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت[1] المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي، كما صدر في 8 فبراير 1996 قانونٌ بشأن الاتصالات يستهدف تقييد حرية القصر في الإطلاع على الصور والمواد المخلة بالآداب أو التي يكون الأولاد القصر طرفا فيها ويمكن الاطلاع عليها من خلال التعامل مع الانترنت، ورغم أن هذا القانون لم يقم إلا بمد نطاق العقوبات الجنائية السارية بشأن الأعمال الفاضحة التي تتمِ باستخدام اتصال هاتفي ليشمل أي اتصال يتم بأية وسيلة من وسائل الاتصالات، وجعل من سوء النية ركنا في تلك الجرائم واستحقاق العقاب عنها حينما قرر المشرع عدم مسؤولية المستعمل أو من يقوم بتوفير خدمات الإنترنت إذا وقع منه بحسن نية، إلا أن بعض الجماعات المدافعة عن الحقوق المدنية اعتبرت أحكام هذا القانون تخالف التعديل الأول للدستور الأمريكي الذي يكفل حرية التعبير عن الرأي وطالبت هذه الجماعات من القضاء وقف العمل بهذا القانون لحين الفصل في عدم دستوريته، وفي 12 يونيو 1996،[2] وبناء على دعوى أخرى بوقف العمل بذلك القانون، صدر حكم من محكمة فيلادلفيا الاتحادية ليؤكد أن جماعات الحقوق المدنية أثبتت أن النصوص الخاصة بقانون آداب الاتصال تخالف التعديل الأول للدستور الأمريكي وبتاريخ 26 يونيو 1997 أصدرت المحكمة العليا الأمريكية حكمها القاضي بعدم دستورية بعض نصوص قانون آداب الاتصالات، وعولت هذه المحكمة في حيثيات حكمها على أنه لا يجوز ترتيب المسؤولية الجنائية على توجيهات أو قرارات عامة لم توضح الأسباب التي تقوم عليها، أو عبارات نصوص عامة غير محددة الألفاظ من شأنها أن تقيد حرية التعبير عن الرأي التي يكفلها الدستور.

في فرنسا، صدور قانون 6 يناير 1978 خاص بالمعالجة الإلكترونية للبيانات الأسمية، وبينما كان مطروحا للنظر أمام مجلس الشيوخ مشروع قانون أعد لتعديل قانون حرية الاتصالات الصادر 1986 ليتفق مع التوجيهات الأوروبية الجديدة، تقدمت الحكومة الفرنسية بتعديل لهذا المشروع يتعلق بإضافة مواد جديدة للقانون المذكور بشأن الإذاعة والتليفزيون مستهدفة الحكومة من هذا التعديل تعريف القائم على تقديم خدمة الإنترنت، وشروط التقدم لممارسة هذه الخدمة التي منها ضرورة الحصول على موافقة مسبقة كغيره ممن يقومون بتوفير خدمات الاتصالات السمعية والبصرية من المجلس الأعلى للإذاعة

[1] – عبد العال الديربي، "الجريمة الالكترونية بين التشريع والقضاء في الدول الغربية"، المركز العربي لأبحاث الفضاء الإلكتروني،2017/01/12، على الرابط الإلكتروني: www.accronline.com/print_article.aspx?id=9679

[2] مدحت رمضان، **جرائم الاعتداء على الأشخاص والإنترنت**، دار النهضة العربية،القاهرة، 2000، ص17 – 19 .

والتليفزيون، وقد اعتبر جانب من الفقه أن المشروع عندما قام بتعريف الاتصالات السمعية والبصرية قد وسّع في التعريف بحيث شمل خدمات الإنترنت من بين وسائل الاتصال، وعندما عرض المشروع على المجلس الدستوري قرر عدم دستورية الفقرتين 2 و3 من المادة 43 من المشروع استنادا إلى أن نص هاتين الفقرتين يخل ويقيد حرية الاتصال وتبادل الأفكار والآراء التي تعدّ من أسمى حقوق الإنسان الذي من حقه أن يتكلم ويكتب ويطبع بحرية طالما لم يسئ استخدام هذه الحرية التي حددها القانون، وكانت مآخذ المجلس الدستوري على المشروع أنه لم يضع ضوابط يتم بمقتضاها إصدار الموجهات العامة والقرارات التي تصدر بناء عليها وخصوصا أنه قد يترتب عليها قيام المسؤولية الجنائية.

وعقب فشل المشرع الفرنسي تنظيم استعمال الإنترنت في عام 1996 صدر القانون رقم 19 لسنة 1988 المتعلق ببعض الجرائم المعلوماتية مع التعديل الذي أدخل في سنة 1992، ثم صدر قانون رقم 230 لسنة 2000 في شأن الإثبات والمتعلق بالتوقيع الإلكتروني .

وعلى الرغم من فشل محاولة المشرع الفرنسي والمشرع الأمريكي وضع ضوابط وتنظيم استعمال الإنترنت، إلا أن النصوص القائمة كانت في أغلبها منطبقة على الجرائم التي تقع عن طريق الإنترنت، كتلك النصوص الخاصة بحماية حرية الحياة الخاصة، والنصوص المتعلقة بتجريم القذف والسب، والنصوص التي تحمي الصغار من الاستغلال الجنسي.

في **المملكة المتحدة (بريطانيا)** جرت تحقيقات أولية على يد لجنة القانون الاسكتلندي ضمنتها مذكرة استشارية مسببة نشرت عام 1982 ، وفى عام 1987 تم نشاط مماثل فيما أعدت فيه ورقة قامت بوضعها لجنة القانون في عام 1988، ووضعت تقريرها النهائي في عام 1989 ، وقد أسفر عن هذه الأنشطة توصيات وضع على أساسها قانون أطلق عليه إساءة استخدام الحاسب الآلي الذي تمت الموافقة عليه في يونيو 1990 ودخل حيز التنفيذ في أغسطس من السنة ذاتها.

ويبدو أن هذه الجهود والمبادرات الغربية لموجهة الجرائم الإلكترونية والإرهاب الإلكتروني كانت متأخرة بمنظور الزمن، وذلك على خلفية أن أول جريمة إليكترونية وقعت في الولايات المتحدة الأمريكية كانت عام 1956، وأن أول جريمة وقعت في البلاد الاسكندينافية كانت في فلندا عام 1968 متعلقة بتقليد برامج الحاسب الآلي، في حين أن المبادرة الأولى بإصدار تشريع يتعلق بمعلومات الحاسب الآلي كانت من السويد التي أصدرت قانونا بشأن حماية المعلومات الشخصية الخاصة المخزَّنة في الحاسب الآلي والانترنت عام 1973، وعدلت تشريعاتها في سنة 1982، وتلتها الولايات المتحدة الأمريكية التي أصدرت في عام 1976 قانونا خاصا بحماية الحاسب الآلي، وفي عام 1984 تبنى الكونجرس قانونا متعلقا بالتحليل المعلوماتي ، عدل بالقانون رقم 1213 / 1986 لمواجهة جرائم الحاسب الآلي، ومنذ عام 1993 وجميع ولايات الولايات المتحدة الأمريكية لها تشريعات خاصة بجرائم الحاسب الآلي، وأخيرا صدر في 14 فبراير 2002 قانونٌ للمعاملات التجارية الرقمية.[1]

وفي 11 ماي 2004 أصدرت دول الثمانية بيانا مشتركا صدر بعنوان مواصلة تعزيز القوانين المحلية، الذي وصى جميع الدول أن تواصل تحسين القوانين التي تجرم اساءة استخدام الشبكات الالكترونية والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالأنترنت. و في 17 نوفمبر 2004 انعقد الاجتماع الوزاري لمنظمة الأبيك في شيلي، وصدر بيان مشترك من زعماء

[1]- مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحديات"، ورقة بحثية مقدمة ضمن الملتقى الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، أيام 23-25 / 9 / 2012، ص8- 9.

الابيك لتعزيز اقتصاديات الدول الأعضاء للقدرة على مكافحة الجريمة الالكترونية والإرهاب الإلكتروني من خلال سن تشريعات محلية بما يتفق مع أحكام الصكوك القانونية الدولية بما في ذلك اتفاقية الجرائم الالكترونية.[1]

ثانيا– الجهود العربية في مواجهة الجريمة الإلكترونية:

أسفرت الجهود العربية هي أيضا عن ميلاد إتفاقية عربية لمكافحة جرائم تقنية المعلومات، و هذا كنتيجة للاجتماع المشترك لمجلسا وزراء الداخلية و العدل العرب والمنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة و ذلك في ديسمبر 2010 و هذا بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات. على مستوى الدول العربية، من خلال ما سمي بالقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، أين تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر ويعد هذا القانون أبرز الجهود العربية المبذولة في مجال الحماية من الجرائم المعلوماتية من الناحية التشريعية، وقد تضمن هذا القانون 27 مادة موزعة على أربعة أبواب يعالج الباب الأول الجرائم المعلوماتية. والتي تم النص عليها في المواد من 3 إلى 22 ومن أهمها[2]:

جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان بغرض

إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية.

جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعماله.

جريمة الإدخال الذي من شأنه إيقاف الشبكة المعلوماتية عن العمل، أو إتلاف البرامج أو البيانات فيها.

جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية.

الجرائم المخلة بالآداب العامة عبر الشبكة المعلوماتية.

وتناول الباب الثاني التجارة والمعاملات الإلكترونية، أما الباب الثالث فقد تناول حماية حقوق المؤلف عبر الوسائط الإلكترونية في حين عالج الباب الرابع الإجراءات المتعلقة بالجريمة المعلوماتية. وإن كان القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها جاء موفقا إلى حد ما في أحكامه الموضوعية حيث شملت بيانا لأهم الجرائم التي يمكن أن ترتكب في مجال الأنظمة المعلوماتية، إلا أنه يؤخذ عليه خلوه من الأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، فلم يتعرض لمسألة الإختصاص القضائي بشكل واضح ولم يشر إلى إخضاع البيانات والمعلومات لإجراءات التفتيش والضبط، ولم يتعرض كذلك لمفهوم الدليل التقني وشروطه وحجيته.

أما على المستوى الوطني فقد استدرك المشرع الجزائري الفراغ التشريعي من خلال القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل و المتمم لقانون العقوبات الذي ينص على الحماية الجزائية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات. إضافة إلى إصداره للقانون رقم 09-04 المؤرخ في 2009/08/05 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها. محاولا بذلك وضع إطار قانوني يتلاءم مع خصوصية الجريمة الافتراضية ،و وضع الإطار القانوني الذي يتلاءم مع خصوصية الجريمة

[1] محمد سيد سلطان، في أمن المعلومات وحماية البيئة الالكترونية، 2016/11/22، متوفر على الرابط الإلكتروني:
http://www.nashiri.ne

[2] – نعيم سعيداني، مرجع سابق، ص86.

الافتراضية، ويجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها.

المحور الرابع/ الصعوبات العملية في مواجهة الإرهاب الإلكتروني وفرص التغلب عليه

أولا/ الصعوبات والتحديات:

خلفت ثورة تقنية المعلومات انعكاسات واضحة على إثبات الجريمة المعلوماتية عبر الوطنية بخلاف الجرائم التقليدية، بالنظر إلى طبيعة هذا النوع من الجرائم وما تتسم به من خصائص وسمات، الأمر الذي بات يثير كثيرا من التحديات أمام القائمين بمكافحتها، هناك العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر عند ارتكاب أحد جرائم الإنترنت، وتجعل هذا التعاون ليس بالأمر اليسير وذلك كما يلي:[1]

1/**عدم وجود نموذج موحد للنشاط الإجرامي**: إذ لم تتفق الأنظمة القانونية في بلدان العالم على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة الإلكترونية و الإرهاب الإلكتروني، فما يكون مجرما في بعض الأنظمة قد لا يكون كذلك في أخرى. ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صور موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على ارتكاب جرائمهم دون تقيد بالحدود الجغرافية.

2/ **اختلاف النظم القانونية الإجرائية**: إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما اعتبرت أن طريقة ما من طرق جمع الإستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة.

3/ التجريم المزدوج : يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين، وقد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة الالكترونية، سيما وأن معظم الدول ما زالت نصوصها العقابية خالية من هذا النمط الإجرامي.

وفي الحقيقة فإن المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب على هذه الصعوبات وإيجاد تعاون دولي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتخفيف من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية.

4/عدم وجود قنوات اتصال: أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم ، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة ، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين . وبالتالي تنعدم الفائدة من هذا التعاون.[2]

---

[1]- سعيداني نعيم ، مرجع نفسه، ص ص 95.96

[2]- حسين بن سعيد بن سيف الغافري، "**الجهود الدولية في مواجهة جرائم الإنترنت**"، ورقة بحثية مقدمة ضمن الملتقى العلمي: سبل مكافحة الجرائم الالكترونية،

5/ مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت :الجرائم المتعلقة بالإنترنت من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلى أو الدولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلى حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية.

ثانيا/ المتطلبات العملية:

إن صياغة خطة محكمة لتجاوز واحتواء التأثيرات المحتملة للإرهاب الإلكتروني هي ليست بالمهمة السهلة ولكن يبدو أكثر قبولا هو إمكانية التقليل من المخاطر المحتملة التي قد تنتج عن التهديدات المعلوماتية إلى حدود الدنيا ومنه تفاقم المخاطر إلى دائرة واسعة .

ويمكن تقسيم المنهج الأمثل للتقليل من مخاطر الإرهاب الإلكتروني إلى عدة مستويات:

المستوى الاول : حماية البني التحتية الوطنية :

وتعالج من خلال هذا المستوى مسألة حماية نظم البني التحتية الوطنية من عمليات الاختراق المعلوماتي أو الهجمات المعلوماتية التي قد ينشأ منها تدمير أو إتلاف لأجزاء كبيرة من هذه المنظومات ويمكن تقسيم هذا المستوى إلى عدة خطوات :

الخطوة الأولى/ معالجة مسألة قابلية الاختراق عبر ما يأتي :

صياغة سياسات أمنية وطنية واضحة المعالم ومحكمة للتقليل من إمكانية اختراق النظم المعلوماتية .

إجراء تقييم مستمر لقابلية الاختراق من محاولة متخصصين بمحاولة اختراق شبكات المعلومات الوطنية وتحديد الثغرات الموجودة فيها والسعي لمعالجتها .

تدريب الكوادر المعلوماتية والارتقاء بمستوى مهاراتها بميدان الأمن المعلوماتي وتعميق الوعي بمسألة الأمن والتنبه إلى مخاطرها الكبيرة .

إعادة تصميم نظم الشبكات المعلوماتية في ضوء التقدم الحاصل بتقنيات الأمن المعلوماتي التي تضمن زيادة مستوى كف الهجمات المحتملة .

الارتقاء بقدرات الرد وكف الهجمات المعلوماتية لدى كوادر النظم المعلوماتية من خلال مضاهاة أداء الشبكات المعلوماتية بتطبيق أسلوب المحاكاة (Simulation) وتحديد مواقع الثغرات الموجودة على الشبكة ومعالجتها.

الرياض،4/5/ 2004، ص 52.

الخطوة الثانية/ الارتقاء بالأمن المعلوماتي للنظم المعلوماتية من خلال تبني ما يأتي :

عزل الموارد المعلوماتية بالغة الأهمية عن نظم الشبكات المحلية وشبكة الانترنيت لضمان حمايتها من عمليات الاختراق .

استخدام تقنيات متقدمة لتشفير المعلومات ومعالجتها بحيث لا يمكن الوصول إليها .

توظيف تقنيات متقدمة لحماية النظم المعلوماتية مثل الجدران النارية وبرمجيات مكافحة الفيروسات والديدان المعلوماتية .

صياغة سياسات أمنية محكمة لضمان أمن نظم المعلومات، قادر على التكيف مع السياسات المعتمدة على مستوى البنى التحتية الوطنية وتتكامل معها .[1]

المستوى الثاني: الحماية الفيزيائية للأدوات المعلوماتية

تتألف منها نظم المعلومات من خلال :[2]

إدارة حسابات مستخدمي الشبكة وكلمات العبور التي يصلون بواسطتها الى قواعد بياناته .

تحديد أطر الدخول عن بعد وصياغة حدود واضحة للتخويل بالدخول .

توفير برمجيات حماية النظام من التأثيرات الضارة بالفايروسات والديدان.

تهيئة نسخ احتياطية للموارد المعلوماتية وحفظها في اماكن آمنة.

إختيار التطبيقات البرمجية المناسبة لحالات الاستخدام المختلفة .

توفي خطط جاهزة لتجاوز الازمات التي قد تعصف بالنظام المعلوماتي.

المستوى الثالث: الحماية القانونية والتشريعية[3]

– سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملا للقواعد الموضوعية والإجرائية، وعلى وجه الخصوص النص صراحة على تجريم الدخول غير المصرح به إلى الحاسب الآلي وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة، أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات .

– تكريس التطور الحاصل في نطاق تطبيق القانون الجنائي من حيث الزمان والمكان، وتطوير نظام تقادم الجريمة الإلكترونية .

– منح سلطات الضبط والتحقيق الحق في إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها، على أن تمتد هذه الإجراءات إلى أية نظم حاسب آلي آخر له صلة بمحل الجريمة .

– تفعيل التعاون الدولي على مستوى المنظمات الدولية ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة .

---

[1]– كريمة شافي جبر، الارهاب المعلوماتي، مجلة كلية الآداب، العدد 96، ص 652، متوفر على الرابط الالكتروني:
http://aladabj.net/wp-content/upload

[2]– حسن مظفر الرزو، **الفضاء المعلوماتي**، مركز دراسات الوحدة العربية،بيروت، 2007، ص 225.

[3]مفتاح بوبكر المطردي، مرجع سابق، ص54.

– العمل على تطور مجال الأمن الالكتروني من خلال إعداد أنظمة ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية.

خاتمة:

بعد معالجتنا للموضوع، خلصت الدراسة إلى أهمية تعزيز الجهود الدولية في مكافحة الجرائم المستحدثة الإرهاب الإلكتروني، إذ يمكن القول إن الطبيعة الدولية للجريمة المعلوماتية استوجبت تعاون دولي من أجل مكافحة فعالة، حيث لم تعد الحدود القائمة بين الدول حاجزا أمام مرتكبي الجرائم السيبرانية والإرهاب الإلكتروني، و بما أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القانونية كان لابد من إيجاد آلية معينة للتعاون مع الدول باعتبارها عضو في المجتمع الدولي مما يفرض عليها الإيفاء بالالتزامات المترتبة على هذه العضوية و من بينها الارتباط بعلاقات دولية و ثنائية تتعلق باستلام و تسليم المجرمين إضافة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال العدالة الجزائية، أما أهم النتائج التي تم التوصل اليها فتمثلت في الآتي:

إن تنامي ظاهرة الجرائم المعلوماتية عبر الوطنية بما فيها الإرهاب الإلكتروني، وتخطي آثارها حدود الدول ، أفرز جملة من التحديات على الصعيد الدولي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموسا، كما هو الحال في الجرائم التقليدية .

بالرغم من الجهود التي بُذِلت ولا تزال تُبذل على المستوى الدولي، فإن هذه التحديات تبقى عصيّة على الحل في كثير من الأحيان في غياب إستراتيجية واضحة للتعامل مع هذه الصنف من الجرائم ومرتكبيها لاسيما في الدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تناسب مع متطلبات هذا العصر .

تتطلب المحاربة الفعلية للإرهاب الإلكتروني تعاونا دوليا متزايدا وسريعا وفعّالا في المسائل الجنائية، فلا بد للبلدان كافة من تجريم استعمال أجهزة الحاسوب لغايات غير مشروعة في تشريعاتها المحلية، كما يجب دعم الجهود المحلية بنوع جديد من التعاون الدولي بما أن الشبكات العالمية تسهّل ارتكاب الجرائم العابرة للحدود، تتطلّب المحاربة الفعلية للجرائم المرتكبة بواسطة جهاز الحاسوب والجمع الفعلي للأدلة بالشكل الإلكتروني ردا يكون في منتهى السرعة.

إن الإرهاب الإلكتروني هي جريمة عابرة للحدود وبالتالي تستدعي المحاربة الفعالة لهذه الظاهرة تعاونا دوليا في المسائل الجرمية، فبما أن التعاون الدولي هو وقف على الأنظمة القانونية السائدة في كلّ بلد، تحول مسائل مثل غياب التشريعات وعدم التعريف بوضوح بالجرائم الإلكترونية في القوانين المحلية أو عدم استحداث الآليات الضرورية للتحقيق في الجرائم الإلكترونية، واستحالة حجز الأصول غير المادية وعدم كفاية الأحكام المتعلقة بالترحيل وبالمساعدة القانونية المتبادلة دون استجابة البلد المعني بالشكل المناسب لطلب تعاون دولي.

العمل على إرساء قواعد التعاون الإقليمي والدولي في مجال حماية التكنولوجيا ومكافحة الجرائم التي تتم باستخدام الكمبيوتر أو عبر شبكة الانترنت، والسعي نحو إيجاد إطار قانوني للتعاون بين النيابات العامة العربية والأجنبية، أو الاجهزة المساعدة لها للعمل على الحد من نمو وتطور هذه الجرائم.

التأكيد على أهمية الإجراءات الوقائية والتعاون الدولي لمحاربة الجرائم المتصلة بالكمبيوتر.

قائمة المراجع :

1. أحمد هلال الدين، الإرهاب والعنف السياسي، دار الحرية، القاهرة،1989.
2. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.
3. السيد عوض، الجريمة في مجتمع متغير، المكتبة المصرية، الاسكندرية،2004.
4. ربيع حسن؛ سيد رفاعي، مبادئ علمي الإجرام والعقاب، المؤسسة الفنية للطباعة والنشر، القاهرة، 2001
5. عبد الرحيم صدق، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية، القاهرة، 1985.
6. عبدالله بن مطلق بن عبدالله المطلق، الإرهاب وأحكامه في الفقه الإسلامي، دار ابن الجوزي، الرياض، 1431هـ.
7. محمد الأمين البشري، "التحقيق في جرائم الحاسب الآلي"، ورقة بحثية ضمن ملتقى علمي حول: القانون والكمبيوتر والإنترنت بكلية *الشريعة والقانون*،الإمارات ، أيام 1 – 3 مايو 2000.
8. نعيم سعيداني، "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري"، مذكرة ماجستير في العلوم القانونية، (كلية الحقوق، جامعة الحاج لخضر باتنة، 2013).
9. كريستينا سكولمان،" الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، ورقة بحثية مقدمة ضمن الندوة الإقليمية: الجرائم المتصلة بالكمبيوتر، المغرب، 2007.
10. نورة طرشي، "مكافحة الجريمة المعلوماتية"، مذكرة ماجستير في القانون الجنائي، (كلية الحقوق، جامعة الجزائر، 2012.
11. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.
12. مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحديات"، ورقة بحثية مقدمة ضمن الملتقى الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، أيام 23-25 / 9 / 2012.
13. حسين بن سعيد بن سيف الغافري، "الجهود الدولية في مواجهة جرائم الإنترنت"، ورقة بحثية مقدمة ضمن الملتقى العلمي: سبل مكافحة الجرائم الالكترونية، الرياض، 4/5/ 2004.
14. حسن مظفر الرزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، بيروت، 2007.

– المراجع الالكترونية:

1. عبد العال الديربي، "الجريمة الالكترونية بين التشريع والقضاء في الدول الغربية"، المركز العربي لأبحاث الفضاء الإلكتروني،2017/01/12، على الرابط الإلكتروني:
   www.accronline.com/print_article.aspx?id=9679
2. كريمة شافي جبر، الارهاب المعلوماتي، مجلة كلية الآداب، العدد 96، ص 652، متوفر على الرابط الالكتروني:
   http://aladabj.net/wp-content/upload
3. محمد سيد سلطان، في أمن المعلومات وحماية البيئة الالكترونية، 2016/11/22، متوفر على الرابط الإلكتروني:
   http://www.nashiri.ne
4. رائد العدوان،" المعالجة الدولية لقضايا الإرهاب الإلكتروني"، 2016/12/12، متوفر على الرابط الإلكتروني:

http://repository.nauss.edu.sa/bitstream/hand

5. خلف إدريس الحبابسه، الإرهاب الإلكتروني،2016/10/10، متوفر على الرابط الإلكتروني:
http://www.lawjo.net/vb/showthread.php?38805

المراجع الأجنبية:

1. Malcom Anderson , Policing the world: Interpol the Politics of International Police Co – Operation , Clarendon press, Oxford, 1989.
2. Mann, David & Sutton, Mike, Net crime, Brit. J. criminal, Vol., 38, No 2,Spring 1998, p. 220.