كلية الحقوق

المواجهة الأمنية

للإرهاب الإلكتروني

الباحث

خالد جمعه سبيت احمد المخمرى

باحث دكتوراة

khaled-jumaa@hotmail.com

مقدمة:

من خلال اعتماد الإرهاب على الشبكة الدولية للمعلومات فقد أخذت قضية الإرهاب أبعاداً أكثر جدية وأثراً في العالم لما جعل الإرهاب يتخذ ألواناً جديدة وأساليب ما كانت لتكون لولا التقنية العالية والتقدم الكبير الذي حصلَ في التطور الإلكتروني.

حيثُ أصبحَ بالإمكان إرتكاب جرائم الإرهاب الإلكتروني من وإلى أقصى بقاع الأرض وسهولة التعاطي معها من أي مكان في العالم فرسالة واحدة يمكنها أن تعزز ارتكاب جريمة إرهابية عبر الشبكة الدولية للمعلومات من خلال تمريرها بواسطة الكثيرين من مقدمي الخدمات في أماكن مختلفة من العالم لها نظم قانونية مختلفة، وسرعة الإنتقال والإعداد والتنفيذ وسرعة زوال آثارها.

يتطلب هذا الأمر إتخاذ إجراءات سريعة لمنع ارتكاب جريمة في مرحلة التنفيذ مثل شن هجوم إلكتروني على بنية أساسية[١] وسوف نتناول فى هذا البحث التجارب العربية والدولية والتحديات الامنية فى مكافحة الارهاب الإلكتروني ومواجهتها، **وذلك من خلال المبحثين التاليين:**

المبحث الأول: التجارب العربية والدولية في مكافحة الإرهاب الإلكتروني.

المبحث الثاني: التحديات الأمنية في مكافحة الإرهاب الإلكتروني وكيفية مواجهتها.

---

(١) د. عبد الجليل اسماعيل حسن الشيخ زيني – الإرهاب الإلكتروني في القانون الدولي. طبعة أولى – منشورات الحلبي الحقوقية ٢٠٢٠ ص٢١٣.

المبحث الأول
التجارب العربية والدولية
في مكافحة الإرهاب الإلكتروني

تمهيد:

أثبتت التجارب ضرورة التعاون الأمني لمكافحة الإرهاب الإلكتروني لأن الدول لا تستطيع بجهودها المنفردة القضاء أو حتى الحد من جريمة الإرهاب الإلكتروني حيث ظهرت أشكال وأنماط جديدة من الجرائم الإلكترونية وأصبحت تشكل خطراً ليس على مستوى الدول التي تحدث فيها بل تتخطى هذه الدول.

وتعبر بأحداث ونتائج هذه الجرائم كل الدول وأصبحت تضرب في كل مكان فسرقت أموال بالمليارات من البنوك وحسابات الدول وتعرضت الكثير من المؤسسات التجارية لحملات التهديد والمطالبة بدفع مبالغ لقراصنة الكمبيوتر من أجل حماية أنظمتها المعلوماتية.

لذلك لا يمكن للدولة بمفردها القضاء على هذا النوع من الجرائم ولا يمكن ملاحقة وتعقب المجرمين إلا في حدود الدولة التابعة لها. فأصبح التعاون الأمني الدولي ضرورة ملحة وذلك للتعاون وتبادل المعلومات في الدول المختلفة للمساعدة في ملاحقة المجرمين بأقصى سرعة ممكنة.

وينقسم هذا المبحث إلى ثلاثة مطالب، يتناول الأول: الاتفاقيات العربية لمكافحة الإرهاب الإلكترونى، والثانى يتكلم عن أثر وسائل الاعلام فى محاربة الارهاب الإلكترونى، وفى المطلب الثالث: نتناول فيه: التجارب الأمنية الدولية في مكافحة الإرهاب الإلكتروني بما فيها منظمة حلف شمال الأطلسي ودور المنظمات العالمية المتخصصة في مواجهة الإرهاب الإلكتروني.

المطلب الأول
الاتفاقيات العربية لمكافحة الإرهاب الإلكتروني

هذا المطلب سيتناول الإتفاقيات العربية لمكافحة الإرهاب الإلكتروني ومنها القانون العربي الإسترشادي لمكافحة هذه الجرائم عام ٢٠٠٤ والإتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات ٢٠١٠ ودور الجامعة العربية في مواجهة الإرهاب الإلكتروني.

أولاً: القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام ٢٠٠٤: لقد أصدرت الدول العربية قانوناً عربياً نموذجياً موحداً لمكافحة جرائم تقنية المعلومات واعتمدت على جامعة الدول العربية من خلال الأمانة الفنية لمجلس وزراء العدل العرب ما يسمى بقانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها واعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار ٤٩٥- د ١٩ - ٢٠٠٣/١٠/٨ كما

تم إعتماده من مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم ٤١٧/د ٢١-٢٠٠٤.

ويتكون هذا القانون من ٢٧ مادة [١] ووفقاً للقانون المذكور يمكن تجريم القائمة التالية من جرائم الإرهاب الإلكتروني إذا مست مصالح محمية من القانون:

١. الدخول غير المشروع بهدف إلغاء أو حذف أو تدمير أو إتلاف أو إنشاء أو تغيير أو إعادة إنشاء بيانات أو معلومات شخصية.
٢. إعاقة أو تشويش أو تعطيل متعمد في برامج وأنظمة الكمبيوتر بأي وسيلة كانت أو أي تلاعب في البيانات والمعلومات.[٢]
٣. استخدام أسلوب التهديد والإبتزاز باستخدام الحاسب الآلي من خلال حمل او منع شخص ولو كان ذلك مشروعاً.
٤. استخدام الشبكة المعلوماتية أو أحد أجهزة الكمبيوتر وما في حكمها في التلاعب بالأرقام أو البيانات بدون وجه حق بقصد السيطرة على بيانات الغير أو أمواله.[٣]
٥. إنتاج أو إعداد أو إرسال أو تخزين بهدف المساس بالنظام العام في أجهزة الحاسب الآلي او الشبكة المعلوماتية. [٤]
٦. نشر أو إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسوب وما في حكمها بقصد الإتجار بالجنس البشري او تبسيط أمور التعامل معه.[٥]
٧. إفشاء أو نشر موقع على شبكة المعلوماتية أو أحد أجهزة الكمبيوتر أو ما في حكمها لجماعة إرهابية بمسميات مفبركة لتسهيل التواصل بين قياداتها أو اعضائها أو الترويج أو التمويل لها أو نشر تعليمات لتصنيع أجهزة أو أسلحة لإستخدامها في العمليات الإرهابية.[٦]
٨. مباشرة الدخول في مواقع أو أنظمة الكمبيوتر والشبكة للحصول على بيانات ومعلومات تمس الأمن الداخلي أو الخارجي لدولة ما وإقتصادها أو لإلغاء بياناتها ومعلوماتها وإتلافها وتدميرها أو الدعوة إلى ما ذكر.[٧]

---

(١) د. محمد طارق عبد الرؤوف الخن- جريمة الإحتيال عبر الإنترنت والأحكام الموضوعية والأحكام الإجرائية – منشورات الحلبي بيروت ٢٠١١ ص ١٢٦.

(٢) المادة ٧ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

(٣) المادة ١٠ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

(٤) المادة ١٣ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

(٥) المادة ١٧ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

(٦) المادة ٢١ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

(٧) المادة ٣٢ من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

ثانياً: الإتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات ٢٠١٠:

في عام ٢٠١٠ أثمرت جهود الجامعة العربية في توقيع إتفاقية عربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٠ من أجل تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الإرهابية الإلكترونية.

وتتكون الإتفاقية من ٤٣ مادة منها ٢١ مادة في باب التحريم و٨ مواد إجرامية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين وضبط المواد المستعملة ويتكون الفصل الرابع من ١٤ مادة تنظم التعاون بين الدول الأعضاء وتبادل المعلومات بهذا الخصوص.

وتضمنت الإتفاقية تجريم الأفعال المكونة لجرائم تقنية المعلومات كالإختراق والإعتداء والإعتراض على سلامة البيانات والملكية الفكرية وإساءة استخدام تقنية المعلومات والتزوير والإحتيال والإباحية الجنسية والإرهاب الإلكتروني وغسيل الأموال والمخدرات والمتاجرة بأعضاء البشر والأسلحة وإساءة إستخدام بطاقات الإئتمان والوثائق الإلكترونية. [١]

وتضمنت المادة ١١ من هذه الإتفاقية تجريم أفعال إنتاج وتوزيع وعرض وتشفير ونشر وشراء أو بيع أو إستيراد مواقع إباحية او مخلة بالحياء وتجريم المقامرة والدعارة والفجور وجرائم الآداب العامة والإعتداء على حرمة الحياة الخاصة أو الأسرية للأفراد أو التشهير والسب والقذف والإساءة إلى السمعة.

وتضمنت المادة رقم ١٠ على منع ما يلي وتجريمه:

١. نشر أفكار ومبادئ الجماعات الإرهابية او الدعوة لها.
٢. تمويل العلميات الإرهابية والتدريب عليها وتسهيل الإتصالات بين أعضائها وتنظيماتها.
٣. تقديم خدمات تصنيع المتفجرات التي تستخدم في العمليات الإرهابية.
٤. نشر الفتن والنعرات والإعتداء على الأديان والمعتقدات.[٢]

---

(١) د. رامي متولي القاضي- مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية – طبعة أولى- دار النهضة العربية- القاهرة – ٢٠١١- ص ٧٥.

(٢) المادة ٣٢ من القانون العربي الإسترشادي – مرجع سابق .

ثالثاً: دور الجامعة العربية في مواجهة الإرهاب الإلكتروني:

على الرغم من تأخر اهتمام جامعة الدول العربية على صعيد العمل الميداني حتى عام ١٩٨٣ بدأت الجهود العربية المشتركة لمكافحة الإرهاب في البحث عن إستراتيجية أمنية عربية بإشراف مجلس وزراء الداخلية العرب والتي أقروها بمجرد الوصول إلى تحقيقها والتي تنادي بضرورة الحفاظ على أمن الوطن العربي وحمايته من المحاولات العدوانية للإرهاب والتخريب الموجه من الداخل إلى الخارج وذلك في إطار خطة أمنية عربية.

وتم تكليف الأمانة العامة لمجلس وزراء الداخلية العرب بإعداد مشروع إستراتيجية عربية لمكافحة الإرهاب والتنسيق مع الأمانة العامة لجامعة الدول العربية وتم وضع صيغة نهائية لمشروع الإستراتيجية العربية لمكافحة الإرهاب وإقرارها في الدورة الرابعة عشر لمجلس وزراء الداخلية العرب بتاريخ ١٩٩٧/١/٥.

ونادت الأمانة العامة بوضع آليات لتنفيذ هذه الإستراتيجيات لمواجهة الإرهاب بكل أنواعه وذلك من خلال عدداً من المنطلقات والأهداف والمقومات والآليات التي تحدد الأسس التي تقوم عليها والسبل الكفيلة بتحقيق أقصى قدر من التعاون على الصعيد العربي والدولي.

ونادت أيضاً بتعزيز التعاون بين الدول الأعضاء وأكدت على أهمية تبادل الخبرات والتقنيات الحديثة والمعلومات في مجال التعاون الأمني مع الجماعات الإرهابية. [١]

واوصى المشاركون في المؤتمر العربي الثامن عشر لمجلس وزراء الداخلية العرب بتونس عام ٢٠١٥ بإتخاذ الوسائل اللازمة للحد من إنتشار التطرف والطائفية، ودعي إلى تبادل المعلومات بشأن المرتزقة الأجانب في بؤر التوتر في المنطقة العربية، وتقاسم التجارب بشأن التعامل مع المقاتلين العائدين.

المطلب الثاني

أثر وسائل الإعلام في محاربة الإرهاب الإلكتروني

إن دور وسائل الإعلام له أثر كبير في العمل على محاربة الإرهاب بصوره العامة والإرهاب الإلكتروني بشكل خاص، وبنفس الوقت تؤدي وسائل الإعلام دوراً مهماً في تحقيق أهداف وغايات الجماعات الإرهابية وتوزيع ونشر كل ما يتضمن أنشطتهم لتمكين الناس من الإنجذاب إليهم والإنضمام في مجموعاتهم.

---

(١) محمد حسين مصيلجي- الإرهاب وأشكاله وفقاً للإتفاقية العربية لمكافحة الإرهاب – المؤتمر العالمي لموقف الإسلام من الإرهاب في السعودية- الرياض- ٢٠٠٤ – ص ٤٧.

كما تستثمر الجماعة الإرهابية وسائل الإعلام لنشر جرائمهم المرتكبة، وقد قسمنا هذا المطلب إلى فرعين، نبين في الاول كيفية قيام الإرهابيين بإستغلال وسائل الإعلام والثاني عن تصدي ومكافحة الإرهاب الإلكتروني على النحو التالي:

الفرع الأول

كيفية إستغلال الإرهاب لوسائل الإعلام

تعتبر وسائل الإعلام هي أقوى أدوات التواصل العصرية التي تهم الجمهور المتلقي مصاحبة العصر ومحاولة التفاعل معه، حيثُ تؤدي الدور الرئيسي في إيضاح القضايا وعرضها على الرأي العام لتهيئته إعلامياً وخاصة فيما يمس الأمن الوطني، فضلاً عما يحدث على الصعيد العالمي..

كما يعتبر القرن الحادي والعشرين عصر الدعاية والإعلام بطابعها الدولي بجميع مكوناتها العسكرية والسياسية والإجتماعية والإقتصادية في ظل ثورة المعلومات والإتصالات.

حيثُ أن هذه الثورة لم تقم بالتوقف مع إستمرار عملية التغيير والإبتكار والتي أحدثت تطور ضخم وكبير في المجال التكنولوجي والمعلومات والإتصالات وقد جعلت الأقمار الصناعية نسيجاً في السماء أصبح كمسرحاً مفتوحاً لتصل رسالة الإعلام إلى العالم كله، ليكون العالم كقرية إلكترونية واحدة وشكل الإعلام والدعاية الدولية عنصراً مهماً في طبقة المجتمع.

وتجدر الإشارة بأن وسائل الإعلام تؤثر بشكل فعال في عملية الإصلاح السياسي في مختلف المجتمعات، إذا طبيعة العلاقة تعكس بين المجتمع والدولة من جهة والعلاقة بين الجماهير والنخبة من جهة ثانية.

وتسهم وسائل الإعلام في عملية الإصلاح الديمقراطي والسياسي على صورة وأعمال هذه الوسائل في المجتمع وحجم تلك الحريات وتعدد الإتجاهات والآراء في داخل هذه المؤسسات فضلاّ عن بعض العوامل المتأصلة في المجتمع الإجتماعية والسياسية والثقافية وتكون طبيعة وسائل الإعلام في دعم الديمقراطية وتعزيز قيم دعم المشاركة السياسية داخل البنيان الإجتماعي.[1]

وركزت وسائل الإعلام في بداية عام ٢٠١١ على ظاهرة التطرف والإرهاب وإنعكاسها على المستوى العربي والعالمي، من خلال ماهيتها التي ظهرت وتبلورت منذ عام ٢٠١٢ بالشمول والتطور، حيثُ أن المتبع لظاهرة التطرف والإرهاب تجد أنها تتمتع بإهتمام الحكومات والشعوب في العالم لما تتميز به من آثار خطرة على إستقرار أمن الدولة.

([1]) تحسين محمد أنيس شرادقة – دور وسائل الإعلام في مكافحة الإرهاب والتطرف– ورقة عمل مقدمة إلى المؤتمر الدولي في جامعة الزرقاء – الأردن– المنعقد للفترة ٣٠-٢٠١٦/٣/٣١.

بعد أن تبين بأن الإرهاب يشكل ظاهرة خطيرة وإجرامية منظمة تسعى إلى خلق حالة من الرعب والخوف والتهديد بإستعمال العنف ضد أفراد الشعب والممتلكات. مما يدل أن الإرهاب يهدف إلى اضطراب المجتمعات والتأثير في الاوضاع السياسية والإعتداء على إقتصادها الوطني.

وذلك من خلال خلق حالة من الفوضى وقتل الأبرياء، من أجل بروز وتضخيم أعمال الإرهاب وبيان نتائجها التدميرية في شريحة المجتمع علماً بأن الجماعات الإرهابية إستفادت من تطور وسائل الإعلام والتطور التكنولوجي في مجال الإتصالات للقيام بتنفيذ عملياتها ومخططاتها وأجندتها الإجرامية.

وبالإضافة إلى حضورها الفعال على الشبكة العنكبوتية والهدف من ذلك الترويج لأفكارها الإجرامية المتطرفة لجذب الشباب للإنضمام إلى صفوفها وهذا يبين بأن الوسائل الإعلامية تعتبر سلاحاً خطيراً في يد المجموعات الإرهابية، التي من خلال أفكارها المتطرفة توجه رسائل تؤثر سلبياً على الأفراد والمجتمع.

ومن الأدلة على ذلك ما قامت به الجماعات الإرهابية من أعمال في تفجير فنادق عمان عام ٢٠٠٦، كما قام التنظيم الإرهابي (داعش) ببث مناظر مرعبة من خلال مواقع التواصل الإجرامي (اليوتيوب) عن طريق عمل إجرامي منافي لمبادئ الشريعة الإسلامية ومبادئ الإنسانية وهي عملية إحراق الطيار معاذ الكساسبة الأردني الأصل.

بالإضافة إلى إرسال رسائل كثيرة عبر مواقع التواصل الإجتماعي عبارة عن مقاطع فيديو وصور تبين فيه جرائمهم البشعة والأفكار المنحرفة والقيام بتكفيرهم لفئات من المجتمعات العربية والغربية[١].

وتثار هنا عدة أسئلة ومنها على سبيل الحصر، هل تقوم التغطية الإعلامية بتغذية الأعمال الإرهابية عن طريق تشجيع الأشخاص الذين يقفون خلفها لإرتكاب الكثير من هذه الأعمال، وهل يساعد الإعلام في زيادة معدل العنف والإرهاب ونشر ثقافته ؟.

والجواب على هذه الأسئلة هو أن الأعمال الإرهابية محل إهتمام الحكومات والشعوب في أنحاء العالم، ويرجع ذلك إلى الآثر الخطير على إستقرار الدول وأمنها ويكون تهديد بخلق حالة من الرعب والخوف والقتل والتهديد بالإضافة عن خلق الفوضى ونشر الشائعات التي تسبب الخوف والقلق للرأي العام وبزرعها خلافاً للسلطات المحلية تبرير عدم إمكانيتها عن حماية أمنه.

---

(١) ورشة عمل حول دور الإعلام والأجهزة الأمنية في مكافحة الإرهاب – منشور في مجلة الدستور الإلكترونية– العدد ١٧٢٣٩– الشركة الأردنية للصحافة والنشر – عمان – الأردن– ٢٠١٥.

وذلك دفع الجماعات الإرهابية لإستغلال وسائل الإعلام المختلفة للترويج لأغراضهم وأهدافهم لتضليل أجهزة الدولة الأمنية.

وذلك بغرض السيطرة والتأثير على الرأي العام عن طريق نشر وتنفيذ العمليات الإرهابية التي يقومون بها وأن عمليات الجماعات الإرهابية التي يتم تغطيتها إعلامياً تكون عاملاً مساعداً في تحقيق أهدافهم التي تشكل من جانب رأيهم معياراً لمدى قياس نجاح العمليات الإرهابية.

كما يرى بعضهم أن الأعمال الإرهابية التي لا ترافقها جانب من التغطية الإعلامية تعد من الأعمال الفاشلة ومن ذلك يستغل الجماعات الإرهابية وسائل الإعلام للدعاية والترويج إلى ذكره الإرهاب لتحقيق أهدافه ووجوده وتقوم أحياناً وسائل الإعلام وبدون أي قصد بالدعاية والترويج لأهداف وغايات الجماعات الإرهابية وإعطاءها حجماً إعلامياً لا تستحقه.

وذلك في ظل الأهداف التي ترغب بتحقيقها من وراء هذا العمل الإرهابي أو الإعلامي من تأثير فكري وشهرة وسلطة ومال وقد يرى جانب من الباحثين في هذا الشأن من وجود بعض العلاقات المشتركة بين الإرهاب والإعلام.

فالإرهاب يحاول الحصول على الدعايات المجانية للترويج لأعمالهم الإرهابية فيستفيد أحياناً الإعلام مادياً عن طريق التقارير التي تنشر في هذا الشأن مما يزيد في عدد مشاهدي التلفاز وعدد قراء الجريدة، ومن ثم تزيد قيمة مبيعات الجرائد بسبب الدعاية المنشورة عليها بالإضافة إلى زيادة القيمة الترويجية التي تنشر من خلال التلفاز.[1]

الفرع الثاني

الإعلام والتصدي للإرهاب الإلكتروني

أضحى الإرهاب يشكل تحدي على المستوى الدولي والإقليمي بسبب عدم نجاح النهج الأمني والعسكري في محاصرته والقضاء عليه، أستهلَ المنطلق الإعلامي بالدور الذي يقدمه في التصدي للإرهاب بأساليبه وأشكاله المتنوعة، وذلك عبر قدرتها للوصول إلى البشر والتأثير في أفكارهم وعقولهم وقناعاتهم بالأساليب المختلفة.

لذا يعتبر من اولويات الإهتمام بوسائل الإعلام ومحاربة الإرهاب عن طريق صراع هذا الفكر المتطرف ومحاولة عدم تمكنه حول التأثير على الرأي العام وبالأخص فئة الشباب، وذلك عدم إشتراك الشباب في صفوف الإرهاب ومن ثم تطويقه والقضاء عليه لأن التصدي للإرهاب الإلكتروني لا تكون عبر الإجراءات الأمنية فقط ولكن من خلال الإستراتيجية لتعزيز و زرع ثقافة الحوار وترك ثقافة العنف.

([1]) هايل ودعان الدعجة – الإعلام والإرهاب– ورقة عمل مقدمة إلى مؤتمر جامعة الحسين بن طلال حول الإرهاب في العصر الرقمي المنعقد في الأردن للفترة من ١٠-٢٠٠٨/١٢/١٢ ص ٢-٣.

ويرى الباحث بأن ذلك الأمر يتطلب بذل مزيداً من الجهد لصياغة الخبر بصورة تضمن وصول الحقيقة وعدم تأثيرها في ذهن المواطنين. وقد خرجت الأصوات التي تنادي بالحاجة لإعادة الرؤية في محتوى العمل الإعلامي والصحفي وتعيدها بمحتوى جديد للنظر في معالجة ظاهرة الإرهاب والعنف، وأيضاً محاربة وسائل الإعلام للأدوار التحريضية التي تمارسها، حيثُ أنها مؤثرة في عقول الشباب وتمس وتهدد أمن المجتمعات والشعوب.[١]

وتتطلب أيضاً مقاومة الإرهاب التصدي للمعلومات المدمرة على الشبكة العنكبوتية لمعالجتها من خلال سن التشريعات المتكفلة بإغلاق هذه المواقع التي تقوم بترويج الأفكار المتطرفة وخصوصاً تلك المواقع التي تدعي نسبها وإنتمائها للدين الإسلامي الحنيف، ومع ذلك لابد من تجهيز نموذج شامل للإتصال لمجابهة الحرب النفسية التي تقوم بشنها المجموعات الإرهابية.[٢]

بدأت تحصيل مسألة الشدة والعنف والآثار الجماعية والفردية مع علو حجمه، إذا تكاثرت الصعوبات الإجتماعية حصيلة لزيادة حالات العنف، وعلى وجه الخصوص بعد الحرب العالمية الأولى، مما حثَ الدارسين والباحثين في هذا القدر، لتعلم أهمية وسائل الإعلام وعلاقته بأعمال العنف.

كما أثرت هذه الدراسة إلى الخروج بعدة نتائج ومنها النفوذ القوي أو المطلق (الرصاصة الإعلامية) ويتوهم أصحاب النظرية بأن لهذه النظرية تأثيراً شديداً وصريحاً لوسائل الإعلام لتقوم بدورها المؤثر في مكافحة الإرهاب التكنولوجي.

ومن الملموس أن مطلب إظهار العنف والجريمة عبر وسائل الإعلام يجعل المتابعين والمشاهدين يوافقون عليها بصورة أكثر من غيرها، إذا بينت معظم البحوث والدراسات وجود علاقة بين سلوك الناس العدواني والتعرض لهذه المصطلحات ومن أهم النتائج التي خلفها مشاهدة العنف ما يلي:

١. زيادة حدة الإثارة العاطفية والنفسية لدى الفرد، مما يدفع الفرد إلى إقتراف السلوك العنيف ضد الأخرين وينتهي ذلك على مدى الإحساس والشعور بالضيق والإحباط.
٢. تدعيم سلوك الأفراد القائم، وتؤدي مشاهدة مواقف العنف أو الإطلاع عليها إلى دعم وتعزيز سلوك الفرد، إذ يحس الشخص الحاد بأسباب العنف بداخله ويرى سلوكه بأنه على صواب.

([١])رأي الباحث من خلال ما استقاه من معرفته الاستقرائية وإدراكه المنطقي لقضية الإرهاب الإلكتروني وطرح ما يجب عمله فيما يراه من منظوره الخاص للتعاطي مع هذه المشكلة.

([٢])هايل ودعان الدعجة – الإعلام والإرهاب – ورقة عمل مقدمة إلى مؤتمر جامعة الحسين بن طلال حول الإرهاب في العصر الرقمي المنعقد في الأردن للفترة من ١٠-٢٠٠٨/١٢/١٢ ص ٦.

٣. التقليد والتعليم، فالمحاكاة والتقليد إحدى طرق التعليم ومنها تكمن خطورة المشاهد العنيفة حيثُ أن البعض يقوم بتقليدها. وفي الواقع أن المواضيع المعروضة للعنف في وسائل[١] الإعلام ونشرات الأخبار لم تتعرض إلى دراسة وافية.

ومع ذلك نجد وسائل الإعلام المرئية منها قد أصبحت جرائم إرهاب تشكل أداة إنتاج بالأساليب والأشكال المختلفة والبرامج التي تعرض على شاشات التلفاز جرائمها تتميز بالتطرف والعنف ومسببة للقلق في درجات الاوساط الإجتماعية في أنحاء العالم.

ومما يستحق الذكر ويتطلب على الدول أن تقدم المبادئ التوجيهية للإعلام أو أن تقوم بالتشجيع لوضع المبادئ الإختيارية التوجيهية لمحاربة إستعراض العنف الإرهابي بشكل مثير، كما تبرر وتنشر المعلومات التي تعتبر إستراتيجية للأهداف المحتملة.(٢)

وبالإضافة إلى نشر المعلومات التكتيكية للأعمال الإرهابية عند وقوعها وذلك يتسبب بتعريض حياة المواطنين للخطر، ويمنع إستخدام التدابير الفعالة لتطبق القانون بحظر الأعمال الإرهابية ومحاربتها والقيام بإلقاء القبض على المجرمين.[٣]

وقد برزت العولمة من خلال العقدين الأخيرين وعملت في ضمن تكنولوجيا الإتصالات والإعلام لتوحيد العالم لإظهار التجانس الثقافي حيثُ سعت معظم الشركات العالمية للإنتاج والإستهلاك وقد إستهلَ على المستوى الإجتماعي والسياسي أحلاف شعارات حقوق الإنسان والديمقراطية.

وقد دفعت هذه التطورات المجتمعات على إتساع دائرة العنف في العالم الثالث إذا تعاكست الثقافة المجتمعية للعالم الثالث مع تضمن القيم في النمط الإقتصادي الحديث، ولهيمنة هذا النمط ركزت الولايات المتحدة الأمريكية على إستعمال القوة كوسيلة لإقرار هذا النمط عالمياً.

حيثُ أنه من الطبيعي أن يستنفر ذلك الجماعات الإرهابية الجهادية وأن يتحول الإستنفار إلى تمهيد للعنف الذي يوجه للأنظمة السياسية لعجزها عن حمايتها.

ومن ناحية أخرى عدم نجاح مشاريع التنمية والتطوير الإقتصادي في البلدان العربية وتدهور الاوضاع الإقتصادية والإجتماعية في العالم الثالث وإنتشار عدة مظاهر سلبية إنطلاقاً من سوء معدلات التنمية وتدني مستوياتها وشيوع وبطش الأنظمة السياسية ورعايتها للفساد.

---

(١) أنتوني غيدنز– علم الإجتماع – ترجمة فايز الصباغ – بيروت– لبنان – مركز دراسات الوحدة العربية ٢٠٠٤ ص٥٠٨.

(٢) انتوني غيدنز – مرجع سابق ص ١٩٣

(٣) نزيه نعيم شلالا – الإرهاب الدولي والعدالة الجنائية – الطبعة الأولى – بيروت – لبنان – منشورات الحلبي الحقوقية ٢٠٠٢ ص ١١٦.

وهذه الظروف التي دفعت لبروز عدة قوى إجتماعية أدت إلى أعمال العنف، ويعتبر جيل الشباب هو القوى الرئيسية التي تؤيد العنف في محاربة الأنظمة السياسية لإعتبار أن هذه الشريحة تمثل غالبية السكان وتعتبر نفسها بأنها تملك الحق بالحاضر والمستقبل.

وكذلك على إعتبار أنها هي القادرة على تغيير وفهم الواقع ومحاربة ظاهرة الفساد ومع ذلك تسعى بالضرورة إلى إسقاط الأنظمة السياسية خصوصاً وأن البطالة تنتشر بينهم وتعوق نمو حياتهم مما ينشر التوتر والحرمان، الشيء الذي يجعل الشباب قوة[١] حاضرة ودائمة في أحداث العنف خصوصاً ذلك العنف الموجه لبنية النظام السياسي ورموزه [٢].

ولذلك قررت رابطة الجامعات الإسلامية عقد مؤتمر وعنوانه ((دور الإعلام في التصدي للإرهاب)) للنظر في دراسة الخلافات التي تتعرض لها الأمة الإسلامية، والعمل على إقتراح الحلول اللازمة وإستبانه دور الإعلام في محاربة الإرهاب بأساليبه وصوره المختلفة.

إذ اتفق المجتمعون على ضرورة محاربة الإرهاب وبعد المشاورات التي إستغرقت ثلاثة أيام خرج المؤتمر بالتوصيات الآتية:

١. يثني المؤتمر على الجهود التي بذلتها جمهورية مصر والدول العربية الأخرى التي كان لها دور في مكافحة الإرهاب، كما يثني المؤتمر كذلك على جهود رابطة العالم الإسلامي في ممارسة الإرهاب، من خلال إقامة المؤتمرات وإجراء الأبحاث والبرامج المختلفة في شتى أنحاء العالم.
٢. وأقر المؤتمر بأن على وسائل الإعلام مسؤولية ينبغي أن تشيد من خلالها بالقيم التربوية التي تستمد أصولها من الدين الإسلامي الحنيف بإعتبارها اولى الخطوات لبناء المسلم المتمكن على مواجهة الإرهاب والتطرف.
٣. يؤكد المؤتمر على حاجة دعم حرية الرأي والتعبير على أن تكون في نطاق الإسلام وأحكامه.
٤. الجزم على ميثاق الشرف الإعلامي التي يبين المعايير الأخلاقية والمهنية عند إذاعة ما يرتبط بالعمليات الإرهابية، والحد من بعض التجاوزات التي تمارسها وسائل الإعلام والتي تساعد في سرعة إنتشار ظاهرة الإرهاب متضمنة الغلو والتطرف والإقصاء.
٥. الإقرار على ضرورة تكاثف الجهود بين المؤسسات الثقافية والإعلامية والدينية والتربوية المتنوعة في العالم الإسلامي.

---

(١) علي ليلة – تقاطعات العنف والإرهاب في زمن العولمة – الطبعة الاولى – مرجع سابق.

(٢) علي ليلة– تقاطعات العنف والإرهاب في زمن العولمة، الطبعة الأولى، القاهرة، مصر، مكتبة الأنجلو المصرية ٢٠٠٧ ص ٧٩.

٦. أهمية التأكيد على وسائل الإعلام لإدراك الرأي العام المسلم لفعالية دور الأسرة في الحفاظ على الأجيال الصاعدة من الوقوع في شباك العنف والتطرف.

٧. أهمية قيام الوسائل الإعلامية بالمحادثة الدقيقة الواعية لأفكار الجماعات الإرهابية عن طريق المختصين وإزاحة الستار عن أخطارها وتطبيق أهدافها من خلال تعيين الأشكال والقوالب الإعلامية الجديدة.[١]

٨. أهمية الرسائل المرسلة للغرب للتفرقة بين الإبداع وحرية الرأي التي يتطلب تقديرها وإحترامها وحاميتها وبيان أهمية دور الإعلام الغربي في حاجة إحترام الأديان الأخرى والعقائد، وعدم الربط بين الإرهاب والإسلام.

٩. ويتوجب التأكيد بأن الإرهاب ليس له ديانة محددة ولا مكان محدد لوصم دين أو مكان معين بهذه الجريمة. وإقرار التوصيات التي انتهت إليها المؤتمرات الدولية بشأن عدم تناول الإعلام للرموز الدينية.

١٠. الجزم على ضرورة عدم السماح لوسائل الإعلام أمام مدعي العلم والدخلاء تشويه الصورة المشرقة والصحيحة للدين الإسلامي وكذلك عدم إثارة التعصب والفتنة والكراهية.

١١. تنشيط دور وسائل الإعلام وبذل الجهود في الدول الإسلامية لدعم الجاليات المقيمة في الخارج لإظهار حقائق وبراهين الإسلام وحمايته وشرح مبادئه الفضيلة.

١٢. الإهتمام بصورة فعالة بأقسام وكليات الإعلام في العالم الإسلامي وذلك من خلال تأهيل وتدريب الكوادر الإعلامية وحثهم على المنافسة، وإمدادهم بدروس ومناهج أخلاقيات الإعلام وتعلم آداب الحوار مع الآخرين تحت ظل تعاليم الإسلام.

١٣. التأكيد بأهمية التعاون والتنسيق بين مختلف المؤسسات والدوائر في دول العالم الإسلامي من خلال إتخاذ الإجراءات للحد من أشكال وظواهر الإرهاب الإلكتروني، لإعتبارها المحرك الرئيسي لنشر أفكار الجماعات الإرهابية.

وإذ تؤكد رابطة الجامعات الإسلامية بأنها ستعقد مؤتمر تدعو فيه علماء التكنولوجيا والإعلاميين للوصول إلى الطريقة الكفيلة بمتابعة وملاحقة الإرهابيين عبر شبكة الإنترنت ووسائل الإعلام الرقمية، وبالأخير يطلب المؤتمر إلى ضرورة وضع أسس إستراتيجية وإعلامية لمحاربة الإرهاب بصوره المتنوعة.[٢]

([١])البيان الختامي للمؤتمر الدولي لدور الإعلام في التصدي للإرهاب – المنعقد في جامعة أسيوط في مصر للفترة من ٣-٥ مارس ٢٠١٦ .

([٢]) البيان الختامي للمؤتمر الدولي – مرجع سابق .

المطلب الثالث

تجارب أمنية دولية لمواجهة الإرهاب الإلكتروني

تمهيد:

لابد أن يكون للجهود الدولية تجارب ملموسة في مجال طرق مكافحة الإرهاب الإلكتروني وهذا يتمثل في أهمية دور الشرطة الدولية الإنتربول وكذلك التنسيق المشترك بين المؤسسات الدولية في تحقيق هذا الهدف وفي المساعدة القضائية الدولية التي وضعت أطر قانونية يتم من خلالها حفظ حقوق الغير في أنظمته ومواقعه الإلكترونية وفي الكم الهائل من المعلومات التي تعتبر حقوق فكرية لأصحابها وسنتناول في هذا المطلب كل ما ذكر سالفاً على أساس تحقيق الأمن المعلوماتي على مستوى دول العالم.

منظمة حلف شمال الأطلسي(الناتو):

أنجزت منظمة حلف شمال الأطلسي السياسة الخاصة بها في مجال الدفاع السيبراني في ٢٠٠٨ من أجل توفير حماية لمواردها التكنولوجية وتلك الخاصة في بلدان الأعضاء[١] كما أنشأ الملف هيئة معينة للدفاع ضد هجمات الإرهاب الإلكتروني وفريقاً للاستجابة للحوادث الإلكترونية يتكفل بإرسال فرق الدعم التقني إلى دول الأعضاء ومركزاً متميزاً من أجل الدفاع عن جرائم الإرهاب الإلكتروني (السيبراني)[٢] ويشتمل هذا المركز الذي يقع مقره في أستونيا مجموعة من الخبراء يعملون بالبحث والتدريب في المجال الأمن السيبراني، كما تضم البلدان التي ترعى هذا المركز: لاتافيا وإستوانيا وألمانيا وليتوانيا وايطاليا واسبانيا والجمهورية السلوفاكية.[٣]

وعلاوةً على ذلك قدمت المنظمة تمارين في مجال الدفاع السيبراني حيثُ تجري فرق من دول الحلف بمحاولة الحماية عن الشبكات الإفتراضية من الإعتداء السيبراني والهدف من هذه التمارين زيادة الاهتمام بالبيئة السيبرانية الدولية وترسيخ التعاون الدولي لمعالجة الحوادث التقنية

---

(١) منظمة حلف شمال الأطلسي تمثل تحالفاً بين عدة دول من قارتي أوروبا وأمريكا الشمالية ويوفر كذلك إرتباطاً مميزاً من نوعه بين هاتين القارتين من أجل التعاون والتشاور في مجال الدفاع والأمن وتنفيذ عدة عمليات لجنسيات مختلفة لإدارة الأزمات، كما يلتزم الحلف بمبدأ يقوم على اعتبار أي اعتداء على أي دولة من دول الحلف يعتبر اعتداء على جميع دول الحلف، وهو مبدأ الدفاع والحماية الجماعي التي نصت عليها بالتفصيل في المادة رقم ٥ من معاهدة واشنطن وحتى الآن عملت بها مرة واحدة فقط وذلك رداً على هجمات الحادي عشر من سبتمبر التي تعرضت لها الولايات المتحدة الأمريكية، الموقع الرسمي لحلف الناتو www.nato.int .

(٢) الدفاع ضد الهجمات السيبرانية، الناتو www.nato.int ((Nato2020)), op.cit

(٣) مركز التميز للدفاع السبراني التعاوني www.ccdcoce.org

Defence exercise to boost skills for countering cyber attacks.

NATO-NEWS, 2010,op.cit

ووقعت كذلك الناتو مذكرة تفاهم فيما يتعلق بالأمن السيبراني مع الولايات المتحدة والمملكة المتحدة وأستونيا وتركيا وسلوفاكيا. [١]

دور المنظمات العالمية المتخصصة في مواجهة الإرهاب الإلكتروني:

وتضم هذه المنظمات العالمية المتخصصة أكثر من ١٩٢ عضواً وهي البلدان المشاركة فيها وما يزيد عن ٧٠٠ كيان من كيانات القطاع الخاص والمؤسسات الأكاديمية[٢] ومن هذه المنظمات الرئيسية الإتحاد الدولي للإتصالات والمنظمة العالمية للملكية الفكرية وسيتم تناولها عبر هذه الدراسة بالتفصيل ودور كل منها في مواجهة الإرهاب الإلكتروني.

١. الإتحاد الدولي للإتصالات[٣]:

ونشأ هذا الإتحاد قديماً منذ عام ١٨٠٥ بمقتضى إتفاقية باريس ثم تم تعديل الاسم إلى الإتحاد الدولي للإتصالات السلكية واللاسلكية في عام ١٩٤٧ حين إنضم الإتحاد إلى هيئة الأمم المتحدة ثم طرأ عليه الكثير من التطورات حتى وصل إلى ما هو عليه الآن.

ففي المادة رقم ٣٥ من ميثاق الإتحاد الدولي للإتصالات شجع الإتحاد بدعم التعاون بين الشركات الخاصة والقطاع العام من أجل تنسيق الجهود والعمل على تبني إستراتيجية عالمية للأمن اللإلكتروني وإنشاء بوابة إلكترونية للأمن الإلكتروني.

ومن أهم نتائج القمة العالمية هو تأمين الشبكات لمجتمع المعلومات وأصبح من دور الإتحاد بناء الثقة والأمن في إستعمال تكنولوجيا المعلومات والإتصالات.

ومن الجدير بالذكر أن بعض البلدان أحرزت تقدماً كبيراً في استراتيجياتها الوطنية في هذا المجال الأمني الإلكتروني وحماية بيئتها التحتية الحرجة للمعلومات وهذا شجع الآخرين فيما.

يجب إتخاذه من تدابير وإقامة تعاون على المستوى الملحي والإقليمي والدولي من خلال إستحداث قدرة إدارية على التحكم في الحوادث على كافة المستويات من أجل ردع الجريمة.

وهذا يتطلب تكاثف الجهود بين الحكومات والمؤسسات العام منها والخاص وذلك للنهوض بثقافة الأمن الإلكتروني وإعتبارها مسؤولية الجميع فلابد للدول المتطورة أن تساعد الدول النامية في إيجاد بنية تحتية قوية والقدرة على التقييم الذاتي وبناء القدرات وتوسيع نطاق المراقبة والإنذار

---

(١) أبرمت دول حلف شمال الأطلسي واستونيا اتفاقية بشأن الدفاع السيبراني، NATO- NEWS ٢٣ أبريل ٢٠١٠ على الموقع الإلكتروني www.nato.int

(٢) منشورة على الرابط التالي:

https//www.itu.int/dms_pub/itu-s/opb/gen/s-6EN-HLPW-2011.2018/6/25

(٣) الإتحاد الدولي للإتصالات هو وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والإتصالات والمسؤولة عن توزيع الطيف الراديوي والمدارات السائلية وعن معايير تكنولوجيا المعلومات والإتصالات وتنميتها في جميع أنحاء العالم.

وكذلك سرعة الإستجابة للحوادث كما يعمل الإتحاد الدولي للإتصالات على تشجيع تقاسم الخيرات بين البلدان المتقدمة والبلدان النامية[١].

ومن خلال التعاون الدولي والإقليمي والمحلي يمكن إعداد الكثير من البرامج الأمنية الإلكترونية ووضع إستراتيجيات وحلول تعزز الثقة والأمن في مجتمع المعلومات على المستوى الأممي وذلك بعمل مبادرات يشارك فيها الجميع لوقف مخاطر المجرمين والإرهابيين وغيرهم الذين يستغلون نقاط الضعف والثغرات في التشريعات المحلية والإقليمية ويجدون فرصتهم في ممارسة أعمالهم القذرة التي تسبب تدمير إقتصاد الدول وحتى تلك التي لديها قوانين صارمة.

ويرى الباحث بأن التعاون الدولي أصبح ضرورياً لملاحقة العابثين بمقدرات الشعوب شذاذ الآفاق يحتاجون من يقف لهم بالمرصاد ويضرب بيد من حديد على أيديهم ليكونوا عبرة لغيرهم.[٢]

والواقع يقول بأن التعاون الدولي في مجال الإتصالات يرتكز على بعض الأهداف الإستراتيجية وهي كما يلي:

- ❖ وضع استراتيجيات لإستحداث تشريعات نموذجية لمكافحة الجريمة الإلكترونية وترقى إلى ما تشهده هذه الجريمة من صور جديدة في الإرهاب الإلكتروني.[٣]
- ❖ وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة المناسبة على الصعيد الوطني والإقليمي فيما يتعلق بالجريمة الإلكترونية.
- ❖ وضع استراتيجية لصياغة معايير أمنية جديدة وخطط من أجل إعتماد أجهزة وبرمجيات وأنظمة تلقى القبول على المستوى الدولي.
- ❖ وضع استراتيجيات لإيجاد أطر عالمية من أجل الرصد والإنذار والإستجابة السريعة للحوادث وضمان التنسيق بين الدول عبر الحدود لسرعة القبض على المجرمين.
- ❖ وضع استراتيجيات عالمية لبناء القدرات البشرية والمؤسسية لتعزيز المهارات التقنية اللازمة.[٤]

ويقوم الإتحاد بالإشتراك مع الوكالة الاوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق الخاصة بمعايير الأمن في مجال تكنولوجيا المعلومات والإتصالات وكذلك في إنجاز

---

(١) صالح محمد النويجم – تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض –رسالة ماجستير في العلوم الإدارية – جامعة نايف للعلوم الأمنية ٢٠٠٥ ص ٩ .

(٢) رأي الباحث.

(٣) محمد محمد الألفي – الواجهة الأمنية والتشريعية لجرائم الإرهاب في الإنترنت – الطبعة الأولى – القاهرة – مصر المكتبة المصرية الحديثة ٢٠١١ ص ٢٨٣.

(٤) المرجع السابق ص ٢٨٣ –٢٨٤.

الإتفاقية الاوروبية حول الجريمة الإلكترونية ووضع إطار قانوني موحد لها وفي مؤتمر قطر ٢٠٠٨ دعي الإتحاد جميع الدول لوضع أطر وطنية ودولية لحفظ الأمن الإلكتروني وحماية البنية التحتية للمعلومات من أجل التصدي للتحديات المستحدثة التي تواجهها تكنولوجيا المعلومات والإتصال.[١]

وقد دعت القمة العالمية لمجتمع المعلومات التي عقدت في تونس ٢٠٠٥ إلى وضع آلية في مجال بناء الثقة والأمن فيما يتعلق بإستعمال تكنولوجيا الإتصال والمعلومات من خلال برنامج الأمن الإلكتروني العالمي وتم إختيار مجموعة من الخبراء لهذا الهدف والمهام الواقعة عليهم تتمثل في تقديم المشورة إلى الأمين العام للإتحاد عند وجود مسائل معقدة يتعرض لها الأمن الإلكتروني.[٢]

ويتألف فريق الخبراء رفيع المستوى من متخصصين مرموقين في مجال الأمن الإلكتروني ومن صناع السياسات في هذا المجال من أجل مساعدة الدول والمنظمات والجهات المرتبطة بهذا الإتحاد في تهيئة وتطوير بيئة ومجتمع المعلومات وتعزيز قدراتها في مجال أعمالها لمواجهة الأخطار التي تنتج عن إساءة إستغلال مثل هذه التقنيات من بعض الجهات الإرهابية التي تقبع في أكثر من مكان ولكن تنشر الإفساد والتخريب في كل مكان.

ويرى الباحث بأن للإتحاد دوراً مهماً يحتاج مشاركة ومساهمة الجميع فيه فالجميع في خطر ولابد من تفويت الفرصة على المجرمين والإرهابيين الذين لا يردعهم دين ولا مذهب ولا ثقافة ولا أدب ولا إنسانية مما يتطلب منا جميعاً وعلى مستوى العالم الوقوف كسد منيع في وجوههم والحد من جرائمهم التي لا تقف عند حدود معينة ولا دولة معينة بل تتخطى الجميع وقد يكون أقطابها موزعون في عدة دول ويعملون لهدف واحد.

٢. جهود منظمة التجارة العالمية في مكافحة الجريمة المنظمة:[٣]

تُبنى جهود منظمة التجارة العالمية بالأساس على مكافحة كافة صور النسخ والتقليد التي تتعرض لها البرامج، حيثُ اوصت الإتفاقية المعنية بحماية حق المؤلف بمجموعة من الأحكام

---

(١) المزيد من المعلومات على هذا الرابط

http://www.ituarabic.org/2008/clip/Doha. Delavation PDF . آخر زيارة ٢٠١٧/٦/٦

(٢) التقرير السنوي لإتحاد الإتصالات الدولي ٢٠٠٧ ص ٣٨.

(٣) تأسست منظمة التجارة العالمية في سنة ١٩٩٥ وهي واحدة من أصغر المنظمات العالمية عمراً، حيثُ أن منظمة التجارة العالمية هي خلفية الاتفاقية العامة للتعريفات والتجارة (أبحاث)، والتي تم إنشاؤها في أعقاب الحرب العالمية الثانية، بالإضافة بأن منظمة التجارة العالمية هي المنظمة العالمية الوحيدة المختصة بالقوانين الدولية المعنية بالتجارة ما بين الأمم وعملها الأساسي هو ضمان انسياب التجارة بأكبر قدر من السلاسة واليسر والحرية، الموقع الرسمي للمنظمة www.wtoarab.org

على الدول الأعضاء الأخذ بها لتطبيق مضمون هذه الحماية وخولت لمنتجي ومبدعي البرامج حقوق جوهرية دعت البلدان الأعضاء إلى احترامها ومن ضمنها حق المؤلف في تأجير برنامجه وكذلك تمنح الدول الأعضاء المؤلفين السماح أو حظر تأجير أعمالهم الأصلية المستخدمة بحقوق النسخ أو الطبع المنتجة عبر تأجير تجاري للجمهور[١]، وبذلك تعتبر منظمة التجارة العالمية قد عملت على حماية برامج الحاسب الآلي من اختراقات القراصنة التي تتعرض لها شأنها في ذلك شأن المنظمة العالمية للملكية الفكرية.

كما جاءت هذه الحماية ضمن نطاق النصوص والأحكام الخاصة بحق المؤلف على اعتبار أن البيانات والبرامج تتمتع بالحقوق المقررة للتأليف، إلا أنه كما أدرك البعض [٢]بأن هذه الحماية هي حماية ناقصة مع الأخذ بالاعتبار بأن الإتفاقية لم تعالج بصورة مباشرة مسألة التزام الدول بهذه النصوص، حيثُ أنها لم تأخذ بعين الاعتبار كذلك مسألة تعارض الإتفاقية مع أية دولة سابقة في حكم معين، وذلك من شأنه أن يؤدي إلى التفسيرات والتحويلات الخاطئة وهذا التقاعس أدى إلى خلق فراغ كبير أتاح من خلاله المجال للقراصنة للإنتفاع به والتهرب من العقاب.[٣]

كما يرى الباحث بأن هذه المنظمة لم تتخذ أي إجراء في مسألة الفيروسات بشكل صريح وهذا يعد أمر بغاية الخطورة وخصوصاً أن كثير من الإعتداءات التي تتعرض لها برامج الحاسب الآلي والمصنفات الفكرية تأتي عن طريق الفيروسات مما يتوجب معه الأمر النص بوضوح على حماية البيانات من هذا النوع من الاعتداء وتفصيل صوره وأنواعه عبر تنسيق الجهود لقصد وضع مناخ قانوني وتشريعي خصب كفيل بحماية هذه البرامج والأنظمة من مخاطر القرصنة[٤].

ورغم توجيه الانتقادات لهذه الاتفاقية فإنها تبقى مع ذلك بادرة محمودة وخصوصاً فإن الجهود التي نفذتها المنظمتين التجارة الدولية والعالمية للملكية الفكرية في سبيل توفير حماية

---

(١) د. فؤاد بن صغير – التجارة الدولية – مطبعة فضالة – المغرب – الطبعة الأولى ٢٠٠٠ – ص ٥٢.

(٢) د. أبو العلا النمر – الحماية الوطنية للملكية الفكرية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، ١٩٩٤، بحث مقدم إلى الندوة الدولية عن الترخيص في مجال الملكية الفكرية وتسوية المنازعات الناشئة عنها في الفترة من٩ إلى ١٠ مارس، مركز القاهرة الإقليمي للتحكيم التجاري الدولي، بالإشتراك مع مركز الويبو للتحكيم والوساطة. كذلك بحث: د. أبو العلا النمر – الحماية القانونية للتكنولوجيا في ظل اتفاقية أبحاث– بحث مقدم إلى مؤتمر القانون والتكنولوجيا بمناسبة اليوبيل الفضي لتأسيس كلية الحقوق جامعة أسيوط في الفترة من١٠ إلى١١ أبريل٢٠٠١ م.

(٣) مقال بعنوان: التعاون الأمني الدولي في مكافحة الجريمة المنظمة على الموقع الإلكتروني:

https //www-aim-council.org

(٤) رأي الباحث.

لبرامج الحاسب الآلي من القرصنة والأخطار بمظاهرها المختلفة او على نطاق الفيروسات التي تخترق النظم والبرامج وتنفذ أهدافها.[1]

([1]) د. شريف حسين محمد – القانون الواجب للتطبيق على الجريمة الإلكترونية – الطبعة الأولى – المصرية للنشر والتوزيع – ٢٠٢١ – ص ٦٩٠.

المبحث الثاني

التحديات الأمنية

في مكافحة الإرهاب الإلكتروني وكيفية مواجهتها:

تمهيد:

هناك الكثير من التحديات والصعوبات الأمنية التي تواجه كل سبل مكافحة الإرهاب الإلكتروني بما فيها التعاون القضائي الدولي والذي يعتبر الجبهة الدولية الاولى في محاربة ومكافحة الإرهاب الإلكتروني.

وفي هذا المبحث سيتم تقسيمه إلى ثلاثة مطالب: المطلب الأول لإبراز التحديات والصعوبات الأمنية التي تواجه التعاون الدولي والمطلب الثاني التدابير المقترحة لمواجهة الإرهاب الإلكتروني وكيفية القضاء على هذه الصعوبات، بينما يتناول المطلب الثالث: دور التدريب في مواجهة الإرهاب الإلكتروني.

المطلب الأول

التحديات والصعوبات الأمنية

في مكافحة الإرهاب الإلكتروني

هناك الكثير من العقبات التي تواجه التعاون الدولي في مجال مكافحة ومواجهة الجرائم الإلكترونية او ما يسمى الإرهاب الإلكتروني وهذا من الهموم التي تواجهها معظم الدول هذه الأيام وتتمثل هذه الصعوبات في مواقف متعددة تتعلق بطبيعة التعامل مع المشكلة او القوانين المحلية المتعلقة بها او بمدى وسرعة تطور هذه المشكلة او بطرق التعامل معها ونستعرضها بالتفصيل فيما يلي:

١. عدم وجود نموذج موحد للنشاط الإجرامي[١]:

من خلال تعاطي الأنظمة القانونية القائمة في كثير من الدول نجد أنها لا تملك إتفاقاً عاماً مشتركاً حول صور إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما هو مباح في أحد الأنظمة نجده إجراماً في غيرها والعكس بالعكس وهذا يرجع لعدة أسباب وعوامل منها على سبيل المثال لا الحصر: الظروف، العادات، التقاليد والثقافات التي تختلف من مجتمع لآخر وبذلك تختلف التشريعات وفقاً لذلك.[٢]

---

(١) د. عبد الفتاح بيومي حجازي- الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت - دار الكتب القانونية - القاهرة ٢٠٠٢ ص ١٠٢.

(٢) جميل عبد الباقي الصغير- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت-القاهرة- دار النهضة العربية ١٩٩٨ ص٧٥

٢. تنوع وإختلاف النظم القانونية الإجرائية:[١]

وهي تأتي نتيجة لعدم وجود نماذج موحدة وثابتة للنشاط الإجرامي. فطرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون بلا فائدة في دولة أخرى أو حتى قد لا يسمح بإجرائها. فطرق جمع الاستدلالات أو التحقيق قد لا تكون مشروعة في بعض الدول ومسموحة بأخرى.

فبعض الدول تجد أنها مكبلة بقوانينها المحلية في عملية إنقاذ القانون مما يعيق ما تطلبه منها الدولة الاخرى فيضيع عنصر التعاون بينهما فقد لا يسمح بإثبات الأدلة أو حتى تسليمها لدولة ما بحكم أن القانون المحلي لا يسمح بذلك حتى ولو كان في إختصاص قضائي وبشكل مشروع.

٣. عدم وجود قنوات إتصال:

إن الحصول على بيانات ومعلومات تتعلق بالمجرمين من خلال التعاون الدولي يجعل هذا الهدف ملزماً للجميع وذلك من خلال توفر قنوات إتصال بين جميع الأطراف وبدونها لا يمكن التواصل فتغيب الأدلة والمعلومات الكفيلة بمتابعة وملاحقة المجرمين وخاصة إذا كان في دول متعددة.

يرى الباحث أن غياب قنوات الإتصال وعدم توفر أنظمة ثابتة لجمع المعلومات والبيانات تعيق كل عمليات التصدي للمجرمين وهم يستغلون مثل هذه الثغرات لينفذوا إلى مواقع وأنظمة الدول والأشخاص ويعبثوا ويفسدوا بمقدراتها ويضيع هدف التعاون من أصله وفاقد الشيء لا يعطيه. فلابد من تحرير البلدان من هذه القيود المقيتة التي تفسد أي نوع من أنواع التعاون لمجابهة الإرهاب الإلكتروني.[٢]

مشكلة الإختصاص في الجرائم المتعلقة بالإنترنت:

من المعروف أن جرائم الإنترنت هي من أكبر الجرائم التي تثير مسألة الإختصاص على المستوى المحلي والدولي فقد يكون الإختصاص على المستوى الوطني او المحلي بصفة مستقلة حيثُ يتم الرجوع إلى المعايير المحددة قانوناً لذلك طبقاً لكل دولة وسيادة قوانينها على أرضها.[٣]

ولكن مسؤولية الإختصاص على المستوى الدولي تتمثل في إختلاف التشريعات والنظم القانونية التي تؤدي إلى التنازع في الإقتصاص بين الدول بالنسبة للجرائم الإلكترونية وتلك المتعلقة بالإنترنت والتي تتميز بكونها عابرة للحدود.

---

(١) د. شريف حسين محمد – القانون الواجب التطبيق على الجريمة الإلكترونية – رسالة دكتوراه – جامعة عين شمس – ٢٠٢١ ص ٤٥٩ .

(٢) رأي الباحث

(٣) وتعني هذه المعايير مكان القبض على المتهم، مكان وقوع الجريمة أو محل إقامة المتهم.

فقد نرتكب جريمة في إقليم دولة معينة من قبل أجنبي فالجريمة تكون خاضعة للإختصاص الجنائي بالدولة الأخرى إستناداً إلى مبدأ الإقليمية وتخضع لأختصاص الدولة التالية على أساس مبدأ الإختصاص الشخصي، والجريمة قد تهدد أمن وسلامة دولة أخرى وتدخل عند ذلك في إختصاصها إستناداً إلى مبدأ العينية.[1]

كما يمكن أن تثار فكرة تنازع الإختصاص القضائي في حالة تأسيس الإختصاص على مبدأ الإقليمية فلو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الإختصاص وفقاً لمبدأ الإقليمية في كل دولة من الدول التي طالتها الجريمة.

التجريم المزدوج:

مما يعوق تطبيق الإتفاقيات الدولية فيما يخص تسليم المجرمين أن النصوص القانونية في هذا الخصوص قد تختلف من دولة لأخرى في مدى تطبيقها. فالتجريم المزدوج من أهم الشروط الخاصة ونظام تسليم المجرمين وهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وهذا يشكل عقبة أمام التعاون الدولي في مجال تسليم المجرمين فيما يخص الجرائم المعلوماتية.

٤. الصعوبات الخاصة بالمساعدات المتبادلة بين الدول:

مع ضرورة تنفيذ وتحقيق المساعدات القضائية على المستوى الدولي كالإقامة القضائية مثلاً نجد أنها لا تتم إلا بالطرق الدبلوماسية مما يجعلها أكثر بطئاً وتعقيداً ويتعارض مع طبيعة المشكلة التي تتطلب عامل السرعة والحركة حيثُ أن الدولة متلقية الطلب غالباً ما تكون بطيئة في الرد بسبب نقص الموظفين المدربين او نتيجة صعوبة لغوية او فوارق في الإجراءات التي تزيد تعقيد الإستجابة السريعة فكم من القضايا قد شطب بسبب قد يكون بسيطاً لم تتم متابعته في الوقت المناسب.

([1]) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت مرجع سابق ص ٧٣.

٥. مشاكل التدريب الخاصة بالتعاون بين الدول:

عدم الرغبة في التدريب من بعض الدول وتخص بذلك بعض القيادات الإدارية بسبب عدم إدراكهم بأهميته ونظر البعض إليه بأنه مضيعة للوقت وكذلك الفوارق الفردية التي تظهر أثناء التدريب فتكشف نقاط الضعف في الإستيعاب وتتكشف قدرات ومهارات التعامل مع ما هو مطروح من شرح وتطبيقات عملية في المجال الإلكتروني الذي قد لا يجيده البعض فتصبح عملية التدريب ورطة للبعض يعمل جاهداً الخروج منها وتعتبر عند الآخرين عبء مما يفقد بيئة التدريب رونقها والهدف من وجودها ولا يمكن أن تبلغ حد التطابق مع المهام التي رصدت لها في بيئة العمل الطبيعية.[١]

المطلب الثاني

التدابير المقترحة

لمواجهة تحديات الإرهاب الإلكتروني

صعوبة عدم وجود نموذج للنشاط الإجرامي:

بما أن الدول غير قادرة على التصدي لتهديدات الجريمة الإلكترونية وما يلفها من إختلافات في النظم القانونية بين الدول جميعاً فهذا الأمر يقتضي توحيد هذه النظم بما يتوافق عليه الجميع من خلال تضييق الفوارق بين الأنظمة العقابية الداخلة وتحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام إتفاقيات خاصة تراعي هذا النوع من الجرائم.

وينصح الباحث أن يتم إرسال نشرة لكل دولة من أطراف إتفاقية التعاون الدولي تضم النظام الموحد لجميع الدول وعلى كل دولة أن تبين الفقرة التي لا تتوافق مع قوانينها وتبين السبب ويتم مناقشته ووضع الحل المناسب له بحيث تكون الصيغة النهائية مرضية لجميع الأطراف.[٢]

صعوبة تنوع وإختلاف النظم القانونية الإجرائية:

الصكوك الدولية التي تصدر عن الأمم المتحدة هي بطبيعتها تشجع الأطراف فيها على إستخدام بعض التقنيات الخاصة بالتحقيق لتخفيف مدى الإختلاف في النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال ممثلاً المادة ٢٠ من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة تشير إلى تسليم المراقبة الإلكترونية والعمليات المستترة وهي من أهم وسائل التصدي للجماعات الإجرامية المنظمة.[٣]

---

(١) د. حسين بن سعيد الجافري- بحث بعنوان الجهود الدولية في مواجهة جرائم الإنترنت - مرجع سابق ص ٥٤.

(٢) رأي الباحث

(٣) د. شريف حسين محمد - القانون الواجب التطبيق على الجريمة الإلكترونية،، طبعة أولى رسالة دكتوراه ٢٠١٦ جامعة عين شمس ٢٠٢١ ص ٤٦٣.

وهذا ما أكدت عليه أيضاً الإتفاقية الأوروبية للإجرام المعلوماتي حيثُ نصت المادة ٢٩ على سرية حفظ البيانات المعلوماتية المخزنة ولابدَ من طلب رسمي للحصول أو الكشف عن البيانات المتوفرة فيها.[١]

كما أكدت المادة ٣٠ من ذات الإتفاقية على سرعة الكشف عن البيانات المحفوظة والتي تقول في نصها " أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة بإتصال خاص تطبيقاً لما هو وارد في المادة ٢٩ فإن الطرف المساند إذا إكتشفَ أن الطرف الآخر طالب الخدمة قد شارك في نقل هذا الإتصال فإن عليه أن يكشف وبسرعة إلى الطرف طالب المساعدة ما يكفيه من بيانات متعلقة بالتجارة الغير المشروعة حتى يتم تحديد هوية مؤدي الخدمة والطريق الذي تم الإتصال من خلاله.[٢]

كما أكدت المادة ٣١ على السماح بالدخول إلى البيانات المحفوظة حيثُ أجازت لأي طرف أن يطلب من الآخر أن يقوم بالتفتيش او الدخول إلى البيانات المحفوظة في شبكة المعلومات داخل النطاق المكاني لذاك الطرف وفقاً للمادة آنفة الذكر رقم ٢٩ ولابد من الإستجابة لهذا الطلب بسرعة إذا كانت هناك أسباب تبين مخاطر الفقد والتعديل او أن التشريعات الواردة في الفقرة تستدعي التعاون السريع.

بينما نجد أن المادة ٣٢ من ذات الإتفاقية تسمح بالدخول للبيانات المخزنة خارج نطاق الحدود شرط وجود إتفاق او أن تكون بطبيعتها متاحة للجمهور.[٣]

فيما نصت المادة ٣٣ على ضرورة تعاون الدول الأطراف فيما بينها لجمع البيانات والمعلومات مع تنظيم الشروط والإجراءات المنصوص عليها في القانون الداخلي وكل طرف له حق الإستفادة من تلك المساعدة فيما يخص الجرائم المتوفر لها معلومات بشأنها وفي الوقت المتوفر لها على المستوى المحلي.

بينما المادة رقم ٣٤ من ذات الإتفاقية تنص على ضرورة التعاون في مجال الحصول على البيانات المتعلقة بمضمون الإتصالات النوعية التي تتم عن طريق شبكات المعلومات ومما تم عرضه مسبقاً يتضح أن الإتفاقية الاوروبية للإجرام المعلوماتي اوجدت بعض الحلول أو النفاذ إلى المعلومات عبر الشبكة المعلوماتية عند إختلاف النظم الإجرائية.

مشكلة عدم وجود قنوات إتصال بين جهات إنقاذ القانون:

---

(١) راجع في ذلك الأدلة التشريعية لتنفيذ إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة لها، منشورات الأمم المتحدة رقم المبيع (E.O.S.V2) الجزء الأول فقرة ٣٨٤.

(٢) د. شريف حسين محمد – القانون الواجب التطبيق على الجريمة الإلكترونية – مرجع سابق –ص ٤٦٥.

(٣) د. شريف حسين محمد – القانون الواجب التطبيق على الجريمة الإلكترونية – مرجع سابق –ص ٤٦٥.

بما أن الصكوك الدولية هدفها تشجيع التعاون بين الدول لإنشاء قنوات إتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بهدف تسهيل الحصول على هذه المعلومات وتبادلها كما نصت عليه المادة ٢٧ والمادة ٩ من إتفاقية ١٩٨٨[١] والمادة ٤٨ من إتفاقية الأمم المتحدة لمكافحة الفساد.[٢]

بينما البند الثاني من المادة ٢٧٠ من الإتفاقية الاوروبية بشأن الإجرام المعلوماتي والمادة ٣٥ من ذات الإتفاقية التي اوجبت على الاطراف تحديد نقطة إتصال تعمل على مدار الساعة وطوال أيام الأسبوع للمساعدة المباشرة في التحقيقات المتعلقة بجرائم البيانات والشبكات او إستقبال الأدلة الإلكترونية إن سمحت القوانين الداخلية بذلك مثل إسداء النصيحة وحفظ البيانات وفقاً للمواد٢٩، ٣٠ و جمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه بهم.[٣]

وحثت هذه المادة الدول الأطراف بضرورة التواصل عبر نقطة التواصل السريع وأن نتعهد الأطراف بتوفير الأفراد المدربين القادرين على تسهيل عمل الشبكة.

مشكلة الإختصاص في الجرائم المتعلقة بالإنترنت:

هناك حاجة ماسة إلى عقد إتفاقيات دولية ثنائية أو جماعية لتوحيد وجهات النظر فيما يتعلق بقواعد الإختصاص القضائي والتي تخص جرائم الإنترنت.[٤] إضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يناسب حركة التطور المتزايدة في عالم تكنولوجيا المعلومات والإتصالات.

([1]) United Nation Convention Against illicit traffic in Narcotic Drugs and Psychotropic Substances Article 9.

([2]) The same = Against Corruption, Article 48 law enforcement cooperation.

([3]) United Nation Convention Against Corruption Article 48, law enforcement cooperation

([4]) على سبيل المثال المادة رقم ٢٢ من الإتفاقية الأوروبية بشان الإجرام المعلوماتي.

مشكلة التجريم المزدوج:

والذي يعتبر من أهم الشروط الخاصة بتسليم المجرمين وركزت الإتجاهات والتطورات التشريعية على تحقيق الشرط فيما يخص تسليم المجرمين من خلال إدراج أحكام عامة في المعاهدات والإتفاقيات المعينة.

ويرى الباحث بأن هناك ما يجرم كجرائم او إعتبارها أفعال مخلة بمقتضى قوانين الدولتين معاً او السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة ويبقى التوافق بين الدول هو سيد الموقف في هذا الموضوع ويتم إجماع الأطراف على الحل الأمثل نظراً لحساسية موضوع التسليم.

التباطؤ في تقديم المساعدة المطلوبة:

باتت الحاجة ملحة لإيجاد وسيلة او طريقة سريعة يتم فيها تسليم طلبات الإنابة كتعيين سلطة مركزية او السماح المباشر بين الجهات المختصة لتعالج مشكلة البطء والتعقيد في تسليم طلبات الإنابة وهذا ما اوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي إنعقد في بانكوك في الفترة من ١٨-٢٠٠٥/٤/٢٥[١]، والذي أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية المشاركة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للإتصال فيما بينها لضمان تنفيذ الطلبات في الوقت المناسب[٢].

وفي المادة ٣٥ من نفس الإتفاقية الأوروبية اوجبت على الدول الأطراف تحديد نقطة الإتصال لتكون نشطة على مدار الساعة لتأمين المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشيكات وإستقبال الأدلة الإلكترونية من خلال الإتصال السريع بين الأطراف المعنية مع توافر الأفراد المدربين والذين هم على دراية بإدارة العمل كما يجب في تسهيل عمل الشبكة وكذلك سرعة الإستجابة لطلبات الإلتماس مع إستيفاء الشروط الكافية بكل ما يتعلق بمسألة الأمن والسلامة ويدخل ضمن ذلك الكتابة السرية.

صعوبة ما يواجهه التعاون بصفة عامة في مجال التدريب:

وهذه المشكلة تحتاج إلى حملات توعية لعرض مخاطر الجرائم المعلوماتية والأضرار التي قد يسببها وأهمية التدريب والتنسيق بين الأجهزة المعنية بتدريب رجال تنفيذ القانون وإيجاد برامج تدريب مشتركة تناسب جميع الفئات والقيام ببعض العمليات المشتركة التي يستفاد منها في صقل المهارات وكذلك تقريب وجهات النظر بشأنها.

([1]) The eleventh United Nations Congress on crime prevention and criminal justice " 11th congress" held by the Member States of the UN on 18-25 April 2005 in Bangkok , Thailand.

([٢]) تعزيز التعاون الدولي في إنقاذ القانون مرجع سابق ص ٢٦.

ومثال على ذلك ما أعلنته مؤسسة مايكروسوفت عن إفتتاح (مركز مايكروسوفت لمكافحة الجرائم الإلكترونية) وهو الذي يعمل على تطوير أساليب مواجهة الجرائم الإلكترونية وذلك في مقرها الرئيسي بريد موند – واشنطن ويضم المركز خبراء مايكروسوفت في المجالات القانونية والتقنية مع توفير أحدث الأدوات والتقنيات في هذا المجال وسيتم التعامل مع الجرائم المرتبطة بالبرمجيات الحديثة وسرقات حقوق الملكية الفكرية والجرائم الخاصة بالأطفال التي سهلتها التكنولوجيا ومن الطبيعي أن تستفيد دوائر القطاع العام من القطاع الخاص.

ولنا مثال في شركة مايكروسوفت ودورها في مكافحة الجريمة الإلكترونية والتي تمثل إضافة حقيقية لمكافحة التهديدات والإعتداءات على شبكة الإنترنت وأنظمة ومواقع الأفراد وبياناتهم ومعلوماتهم المخزنة وحقوقهم الفكرية وملكيتها وكذلك في الحد من جرائم الإرهاب الإلكترونية وملاحقة فاعليها ومرتكبي جرائمها وقد يستدعي ذلك الإستعانة بخبراء ومحققين أجانب سواء في الجرائم المعقدة أو في تدريب وإعداد كوادر على مهارة عالية وحديثة لحماية الدول من الجرائم الإرهابية بأنواعها المختلفة. ضعف دور الإعلام في تنشئة الاجيال وتنويرهم عن خطورة الإرهاب الإلكتروني ووضع برامج خاصة لمحاربته.

المطلب الثالث

دور التدريب في مواجهة الإرهاب الإلكتروني

أولاً: التقدم في تكنولوجيا الكمبيوتر:

إنه لمن واجب الجهات المسؤولة أن تقوم بتنفيذ القانون بخطوات متناسقة مع ما تشهده التكنولوجيا في عالم الكمبيوتر والإتصالات من أجل التصدي للأعمال الإرهابية التي تصاحب هذا التطور وهذا قد يتطلب إتباع إجراءات قد تتجاوز مفاهيم ومبادئ كان يعمل بها في السابق ومع حداثة الأسلوب في هذه الجرائم والقدرة المطلوبة على محو آثارها إذا ما أثبتت الوقائع وقوعها ومعرفة أبعادها.

حيثُ تم إرتكاب مثل هذه الجرائم أمام مرأى ومسمع رجال الشرطة حيثُ قام بعض رجال الشرطة بتقديم يد المساعدة لمجرمين سواء عن قصد أو جهل أو على سياق واجب المهنة الذي يلزمهم بها القانون وعند إتلاف الأدلة قد يحدث خطأ مشترك.[1]

وهناك شركة تعرضت للقرصنة في الولايات المتحدة الأمريكية فطلب منها أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكبي الجريمة ونتيجة لذلك تم إتلاف الملفات والبرامج التابعة لها بسبب ذلك.

([1]) امير فرج يوسف– جريمة مكافحة الإرهاب الإلكتروني – الجرائم المعلوماتية على شبكة الإنترنت – الإسكندرية، مصر – دار المطبوعات الجامعية – ٢٠١٢.

وقد يقع خطأ مشترك بين الخبراء وبين الجهة المجني عليها يؤدي لإتلاف الأدلة فهناك حصل وأن طلب بعض الأشخاص من إحدى الشركات التي زعم بأنه وضع قنبلة منطقية بنظام حاسبها الآلي، وعند الاستعانة بخبير لإزالة القنبلة تبين أنه تسبب بإتلاف كافة الأدلة الموجودة قبل الاستعانة بالشرطة.[١] وهذا الحدث وأمثاله يعيق سير العدالة الجنائية الممثلة في رجال الضبط القضائي أو رجال التحقيق أو المحاكم فمن متطلبات العدالة أن تتحمل الأجهزة الحكومية كامل المسؤولية تجاه إكتشاف الجرائم المعلوماتية والجناة القائمين بها لتحقيق العدالة ولابد للأجهزة أن تتسم بالكفاءة والقدرة على كشف غموض تلك الجرائم ومرتكبيها بسرعة ودقة[٢]

فعامل الزمن قد لا يكون في صالح القانون ومصلحته فتضيع الأدلة والإثباتات قبل حفظها أو الحصول عليها وهذا يحتاج إلى تطوير وسائل التدريب من أجل تحقيق أهدافها المنشودة[٣] ولهذا من الواجب أن يراعى في برامج التدريب المقدمة أن تكون على مستوى هذا التقدم الحاصل في تطور جرائم الإرهاب الإلكتروني.

ثانياً: أهمية التدريب في مكافحة الإرهاب الإلكتروني:

يلعب التدريب دوراً مهماً في عملية التنمية الإدارية وهو يعالج قضية الكفاءة والفعالية في إنجاز الأعمال ولذلك أصبح من أهم متطلبات النجاح في العمل وزيادة الإنتاجية في معظم مؤسسات الدولة العام منها والخاص فهو من أهم الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاءة الإنتاجية وتطوير الموظفين على مختلف درجاتهم ومسؤولياتهم وخاصة من جوانبها النظرية والعملية والفنية. فالخلفية القانونية أو أركان العمل الشرطي تعتبر من الجوانب الفنية في أي مجال عمل يختص بالقانون بالإضافة إلى القدرة على التعامل مع برامج وأجهزة الكمبيوتر المختلفة والتعرف على أنظمة العمل الشرطي والقانوني ليتسنى للعاملين فيه معرفة متطلبات مكافحة الإرهاب الإلكتروني.

ويرى الباحث بأن بدون التدريب في كل ما ذكر لا يمكن السيطرة والتحكم على عمليات مكافحة الإرهاب والتدريب يوفر الجهد والوقت والتكلفة وسرعة الوصول إلى الهدف فمن قال تعلمتُ في هذا المجال او ذاك فقط جهل لأن التطوير والتغيير مستمر باستمرار الحياة نفسها.

---

(١) أ.د. ذياب البداينة – دور الأجهزة الأمنية في مكافحة الإرهاب المعلوماتي – ورقة عمل مقدمة في الدورة التدريبية (مكافحة الجرائم الإرهابية المعلوماتية) – كلية التدريب – جامعة نايف العربية للعلوم الأمنية – القنيطرة – المغرب– ٩-١٣/٤/٢٠٠٦.

(٢) امير فرج يوسف– جريمة مكافحة الإرهاب الإلكتروني – مرجع سابق – ص ٢٣٧

(٣) يقوم التدريب بصقل المهارات والقدرات الواجب توافرها في شاغل الوظيفة ومن ثم زيادة أداء وقدرات الفرد، صالح محمد نويجم كفاءة العملية التدريبية، الرياض، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية، كلية الحقوق،٢٠٠٥ ص٩ .

والتدريب يخضع لفنون متنوعة منها ما يتم في مجموعات ومنها على مستوى فردي ويتم التركيز في المجموعات على مهارات مهمة ومحددة تخدم صاحبها في مجال العمل سواء على المستوى الفردي أو العمل الجماعي.

بينما يتناول التدريب الفردي مخصصات معينة قد تستهدف أفراد معينين لأغراض نادرة التخصص وذات حساسية خاصة كالوثائق السرية ومعلومات الملكية الفكرية وبرامج التحكم في أعمال القرصنة وأنواع الهجوم الإلكتروني وكيفية التصدي لها وكيفية حفظ وحماية المعلومات قبل وبعد الإجراءات القانونية الخاصة بها.

ويجب أن يخضع الجميع لتجارب عملية من أجل إكتساب الخبرة المطلوبة في كل مجال وقد يعهد التدريب لجهات متخصصة تقوم عليه لتأهيل الموظفين علمياً وفنياً وحتى بدنياً أحياناً من أجل تحقيق نتائج طبية في عمليات التدريب المقصودة.[١]

ولابد لنا القول هنا بأن إستقطاب المتخصصين والكفاءات في المجال المعلوماتي لابد أن يحظى بإهتمام كليات الشرطة وعلى كليات القانون أن تدرس التخصصات المعلوماتية التي تدخل في مكافحة الإرهاب الإلكتروني وذلك لأهمية دور العاملين فيه في هذا المجال فالثقافة القانونية تحتاج لزخم من المعلومات الإلكترونية والتكنولوجية والثقافة الحاسوبية لأن الكل أصبحَ مرتبط بعضه ببعض فالنظام الرقمي والإلكتروني بات هو المحرك لجميع الأعمال التعليمية والإقتصادية والإدارية والتجارية والشرطية وكل مؤسسات الدولة[٢].

فغرس الثقافة الحاسوبية وتطويرها وسط رجال القانون والشرطة وربطها بالثقافة الشرطية والقانونية أصبحت كفيلة بنجاح الأجهزة الأمنية وسلطات التحقيق فيها في مواجهة الإرهاب الإلكتروني.

---

(١) مدة الدورة تكون ٤ أسابيع، وتكون غالباً على تقنيات الجريمة المعلوماتية وأساليبها في كلية الشرطة بالولايات المتحدة وتشمل علم الكمبيوتر وبرامجه – أمن المعلومات والشبكات – القانون والإثبات والجريمة المعلوماتية.

(٢) الموقع الإلكتروني: .www.un.org

ثالثاً: مظاهر التعاون في مجال التدريب:

من حيث المبدأ لا يمكن أن توازي بين الجهوزية لمواجهة الجرائم المتعلقة بالشبكة الدولية للمعلومات وبين من يتعاملون معها كالدول النامية ليس لها قدرة الدول المتقدمة في هذا المجال فليس لها الموارد المادية الكافية ولا حتى الكوادر التي تستطيع أن تزاول تقنية العمل المطلوبة ولهذا يعتبر التدريب مصيرياً في هذا المجال وخاصة فيما يتعلق بالتعاون الدولي والمساعدات القضائية وتسليم المجرمين[١]، فتقدم الدولة ورقيها يحتم عليها الإهتمام ببرامج التدريب وتقاس عظمة الدول الآن بقدر ما يملكه شعبها من قوة في الخبرة والثقافة والمهارة المطلوبة لزيادة الإنتاجية وتحسين الأداء والجودة ومدى توفر روح الإبداع لدى كوادره وطواقم الأعمال وذلك بإشراف قيادة تستشرف المستقبل وتسعى للتميز فاليوم نسمع عن إلقاء القبض على كثير من المجرمين الذين استطاعوا النفاذ إلى أماكن حساسة وتلاعبوا في مقدرات وأموال الكثير من المؤسسات واصبحوا في يد العدالة ما كان هذا ليحصل لولا توفر هذه الكوادر التي تتابع وتتعقب مجرمي الإنترنت وأجهزة الهواتف المحمولة التي أصبحت تستخدم لعمليات تفوق الكمبيوتر الكترونياً مما عقدَ المسألة وجعلها تأخذ حيزاً جديداً في مجال الجرائم الإلكترونية.

وأصبحنا نسمع عن آلاف حالات النصب والإحتيال التي تتم عبر الهاتف المحمول فتجد من يقول أنه يتصل من البنك المركزي او البنك الذي نتعامل معه ويطلب منك بعض المعلومات لتجديد إشتراكك أو نقص في الوثائق أو خطأ في الرصيد أو أي سبب آخر يستطيع من خلال المعلومات التي يحصل عليها سحب كل الأرصدة الموجودة التي تخص الضحية.

ويرى الباحث بأن الناس العاديين يحتاجون إلى تدريب وتثقيف من خلال نشرات من هذه البنوك او برامج على التليفزيون لتوعية الناس وتحذيرهم من هؤلاء المجرمين.

فالتعاون مطلوب على المستوى المحلي والإقليمي والدولي ولابد للجميع أن يستفيد من التجارب التي تمت على مستوى العالم وقصص الغش والخداع وعلى الجميع أن ينظر إليها بمثابة دروس واقعية لكي لا تتكرر مع آخرين والتدريب الآن أصبح متوفر على شبكة الإنترنت من خلال بث برامج تدريبية منها ما هو مجاني ومنها ما هو مقابل رسوم فأصبح التدريب سهلاً سواء للأفراد أو المؤسسات وحتى المؤسسات الحكومية أصبح لها قاعات تدريب خاصة.[٢]

---

(١) د. عبد الجليل اسماعيل حسن الشيخ زيني –مرجع سابق ص ٢٢٩.

(٢) رأي الباحث

خاتمة البحث

بعد ان تناولنا فى هذا البحث موضوع المواجهة الأمنية للإرهاب الإلكتروني. وذلك من خلال المبحث الأول: التجارب العربية والدولية لمواجهة الإرهاب الإلكتروني وانقسم إلى ثلاثة مطالب تناول خلالها المطلب الأول التجارب الأمنية العربية في مواجهة الإرهاب الإلكتروني في حين أن المطلب ا٠٠٠٠٠٠٠٠لثاني تناولَ أثر وسائل الإعلام في محاربة الإرهاب الإلكتروني بينما ذكرَ المطلب الثالث التجارب الأمنية الدولية لمواجهة الإرهاب الإلكتروني.

بيد أن المبحث الثاني تم تقسيمه لثلاثة مطالب تناول التحديات والصعوبات الأمنية في مكافحة الإرهاب الإلكتروني في المطلب الأول بينما تناول المطلب الثاني التدابير المقترحة لمواجهة هذه التحديات والصعوبات وانتهى المطلب الثالث بدور التدريب في مواجهة الإرهاب الإلكتروني.

النتائج: ومن خلال عرضنا عبر الصفحات السابقة من موضوع الدراسة فقد وفق الله الباحث في الوصول إلى النتائج التالية:

- جريمة الإرهاب الإلكتروني جريمة متطورة وذلك يطور الطرق المستخدمة في هذا النطاق الإجرامي التقني الجديد فهي متصلة بالتطور الهائل المصاحب للثورة التكنولوجية المعلوماتية في العصر الحديث.
- يوجد قصور تشريعي في معظم القوانين على الصعيد الوطني او العربي او الأجنبي حيثُ أن القوانين الصادرة حالياً شبه عاجزة عن الحماية الجنائية للمعلومات المخزنة على الأجهزة الإلكترونية.
- لا تنحصر خطورة العمل الإرهابي على أهداف محددة فحسب بل تتجاوز إلى رعايا دول أخرى ويلحق الضرر بأموال وممتلكات لأناس أبرياء، وهذا السبب الذي جعل العالم اليوم يضع جل اهتمامه في التعاون الدولي لمكافحة جريمة الإرهاب الإلكتروني بكل أشكاله وأساليبه وبأعلى مستوياته.
- توجد صعوبات في تتبع جرائم الإرهاب الإلكتروني وإثباتها، حيثُ أنها من الجرائم التي لا تترك أثراً وكذلك منفذيها يمتلكون الخبرة التقنية والفنية التي يتعذر على المحقق التقليدي التعامل معها.
- يعتبر الإرهاب الإلكتروني الصورة الحديثة للإرهاب، حيثُ يعتبر إرهاب الحاضر والمستقبل الذي يستخدم التقنيات الحديثة والمعلومات للوصول إلى أهداف جديدة للعمليات الإرهابية ويشكل تهديد للسلم والأمن الدوليين حيثُ أن خطره يشمل جميع المناطق الجغرافية.
- تعزيز الرقابة المجتمعية والأسرية وترسيخ دور وسائل الإعلام للتصدي لجرائم الإرهاب الإلكتروني والتوعية اللازمة منها.

- تجريم الاتصالات بكل أشكالها وصورها بين الجماعات الإرهابية عبر الشبكة العنكبوتية بالإضافة لتجريم التدريب على هذه الأعمال عن طريق استعمال الإنترنت.
- الإرهاب الإلكتروني أضحى هاجساً يخيف ويرعب العالم الذي أصبح عرضة للهجمات الإرهابية عبر شبكة الإنترنت لتجاوز نشاطاتهم الإرهابية في كل مكان في العالم ولذلك بعض الدول تسعى إلى اتخاذ الإجراءات والتدابير الإحترازية لمكافحة الإرهاب الإلكتروني. حيثُ أن هذه الجهود تبقى قاصرة وتحتاج إلى مزيد من التصدي والمواجهة لهذا الخطر ولا سيما بأنه عابر للحدود.
- إن بعض جرائم الإرهاب الإلكتروني التي يتم إرتكابها عبر الشبكة العنكبوتية مثل جرائم التمييز العنصري وبعض جرائم الإرهاب الدولي حيثُ يمكن أن تؤدي إلى توتر بين أطراف المجتمع الدولي لنشوب حروب دولية او إقليمية جديدة.
- جرائم الإرهاب الإلكتروني ومنها الاقتصادية التي تسعى لتقويض الاقتصاد الوطني لبعض الدول، بالإضافة إلى الحرب الإلكترونية الجديدة قد توقف سبل الحياة في الدول لمقدرتها بتعطيل وتخريب شبكات المياه والمواصلات والكهرباء والمشافي وأغلب سبل الحياة فيها وأن الاعتماد على شبكات الإنترنت يزداد يوماً بعد يوم تطور وتقنية.
- أن يخصص برنامج يذاع يومياً تحت مسمى " مقاصد الإرهاب الإلكتروني" يتم فيه توعية الجمهور صغار وكبار عن مخاطر الإرهاب الإلكتروني وذكر بعض الأمثلة لأناس كانوا ضحايا لهذه الجريمة كأمثلة حية للجمهور لكي يعتبروا من أمثالها.

التوصيات:

- يوصي الباحث بالتدخل التشريعي لمواجهة اوجه القصور في القوانين والتشريعات الوطنية او يتم تحديثها بالنص صراحة على إدانة استعمال التقنيات الإلكترونية الحديثة بإلحاق الضرر في أمن الدولة من الداخل والخارج أسوة ببعض الدول كالإمارات ومصر والمملكة العربية السعودية.
- يقترح الباحث أن تفرض الحكومة رقابة على كل ما يبث في الشبكة المعلوماتية لحجب الدخول على المواقع التي تنشر الفكر الإرهابي عن طريق إنشاء برنامج وتكون مهمته منع المستخدمين من الحصول على معلومات غير صحيحة عن مواقع معادية وضارة وهذا ما أقدمت عليه الولايات المتحدة الأمريكية والصين.
- يوصي الباحث بالإستفادة من مرحلة التعليم والمعرفة بأن تقرر مادة علمية على الطلاب ضمن المقررات الدراسية يتضمن تعريف في البيئة الرقمية وجرائم الإرهاب الإلكتروني أبعادها وحجم الأضرار الناشئة عنها وصفات تجريمها وأساليب منع إرتكابها وتعقب مرتكبيها وذلك للحد من الآثار السلبية على شبكة الإنترنت وأيضاً يعتبر تشجيعاً للبحث عن هذه الظاهرة الإجرامية للوصول إلى حلول مبتكرة وجديدة.
- يقترح الباحث إنشاء استراتيجية إعلامية هادفة لنشر الوعي بين افراد المجتمع بمخاطر جريمة الإرهاب الإلكتروني وأساليبها عن طريق التنسيق بين الهيئات والوزارات ومؤسسات المجتمع المدني المتعلقة بذات الأمر.
- يقترح الباحث إنشاء منظمة عربية متخصصة في جرائم الإرهاب الإلكتروني مع تدريب كوادرها بصفة مستمرة وتكون على صورة أقسام، قسم للتدريب لوضع الخطط التدريبية والبرامج وقسم آخر يتولى تثقيف أفراد المجتمع، وقسم يتولى تطوير البحوث العلمية.

فهرس المراجع

- أمير فرج يوسف– جريمة مكافحة الإرهاب الإلكتروني – الجرائم المعلوماتية على شبكة الإنترنت – الإسكندرية، مصر– دار المطبوعات الجامعية – ٢٠١٢.
- أنتوني غيدنز– علم الإجتماع– ترجمة فايز الصباغ – بيروت– لبنان – مركز دراسات الوحدة العربية ٢٠٠٤.
- تحسين محمد أنيس شرادقة – دور وسائل الإعلام في مكافحة الإرهاب والتطرف– ورقة عمل مقدمة إلى المؤتمر الدولي في جامعة الزرقاء – الأردن– المنعقد للفترة ٣٠– ٢٠١٦/٣/٣١.
- جميل عبد الباقي الصغير– الجوانب الإجرائية للجرائم المتعلقة بالإنترنت–القاهرة– دار النهضة العربية ١٩٩٨
- رامي متولي القاضي– مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية – طبعة أولى– دار النهضة العربية– القاهرة – ٢٠١١.
- شريف حسين محمد – القانون الواجب التطبيق على الجريمة الإلكترونية – رسالة دكتوراه – جامعة عين شمس – ٢٠٢١.
- شريف حسين محمد – القانون الواجب التطبيق على الجريمة الإلكترونية،، طبعة أولى رسالة دكتوراه ٢٠١٦ جامعة عين شمس ٢٠٢١.
- صالح محمد النويجم – تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض –رسالة ماجستير في العلوم الإدارية – جامعة نايف للعلوم الأمنية ٢٠٠٥.
- عبد الجليل اسماعيل حسن الشيخ زيني – الإرهاب الإلكتروني في القانون الدولي. طبعة أولى – منشورات الحلبي الحقوقية ٢٠٢٠.
- عبد الفتاح بيومي حجازي– الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية – القاهرة ٢٠٠٢
- علي ليلة– تقاطعات العنف والإرهاب في زمن العولمة، الطبعة الأولى، القاهرة، مصر، مكتبة الأنجلو المصرية ٢٠٠٧
- فؤاد بن صغير – التجارة الدولية – مطبعة فضالة – المغرب – الطبعة الأولى ٢٠٠٠.
- محمد حسين مصيلجي– الإرهاب وأشكاله وفقاً للإتفاقية العربية لمكافحة الإرهاب – المؤتمر العالمي لموقف الإسلام من الإرهاب في السعودية– الرياض– ٢٠٠٤.
- محمد طارق عبد الرؤوف الخن– جريمة الإحتيال عبر الإنترنت والأحكام الموضوعية والأحكام الإجرائية – منشورات الحلبي بيروت ٢٠١١.

- محمد محمد الألفي – الواجهة الأمنية والتشريعية لجرائم الإرهاب في الإنترنت – الطبعة الأولى – القاهرة – مصر المكتبة المصرية الحديثة ٢٠١١
- نزيه نعيم شلالا – الإرهاب الدولي والعدالة الجنائية – الطبعة الأولى – بيروت – لبنان – منشورات الحلبي الحقوقية ٢٠٠٢.
- هايل ودعان الدعجة – الإعلام والإرهاب – ورقة عمل مقدمة إلى مؤتمر جامعة الحسين بن طلال حول الإرهاب في العصر الرقمي المنعقد في الأردن للفترة من ١٠-٢٠٠٨/١٢/١٢.